

# JOURNAL OF ENGINEERING RESEARCH & SCIENCES

# JENRS



[www.jenrs.com](http://www.jenrs.com)  
ISSN: 2831-4085

**Volume 3 Issue 9**  
**September 2024**



## EDITORIAL BOARD

### Editor-in-Chief

**Prof. Paul Andrew**  
Universidade De São Paulo, Brazil

### Editorial Board Members

**Dr. Jianhang Shi**

Department of Chemical and Biomolecular  
Engineering, The Ohio State University, USA

**Prof. Kamran Iqbal**

Department of Systems Engineering, University  
of Arkansas Little Rock, USA

**Dr. Lixin Wang**

Department of Computer Science, Columbus  
State University, USA

**Dr. Unnati Sunilkumar Shah**

Department of Computer Science, Utica  
University, USA

**Dr. Qichun Zhang**

Department of Computer Science, University of  
Bradford, UK

**Dr. Prabhash Dadhich**

Biomedical Research, CellfBio, USA

**Dr. Qiong Chen**

Navigation College, Jimei University, China

**Ms. Madhuri Inupakutika**

Department of Biological Science, University of  
North Texas, USA

**Dr. Jianhui Li**

Molecular Biophysics and Biochemistry,  
Yale University, USA

**Dr. Sonal Agrawal**

Rush Alzheimer's Disease Center, Rush  
University Medical Center, USA

**Dr. Ramcharan Singh Angom**

Biochemistry and Molecular Biology,  
Mayo Clinic, USA

**Dr. Anna Formica**

National Research Council, Istituto di  
Analisi dei Sistemi ed Informatica, Italy

**Prof. Anle Mu**

School of Mechanical and Precision  
Instrument Engineering, Xi'an University  
of Technology, China

**Dr. Mingsen Pan**

University of Texas at Arlington, USA

**Dr. Żywiłek Justyna**

Faculty of Management, Czestochowa  
University of Technology, Poland

**Dr. Diego Cristallini**

Department of Signal Processing &  
Imaging Radar, Fraunhofer FHR, Germany

**Dr. Haiping Xu**

Computer and Information Science Department, University of Massachusetts Dartmouth, USA

## Editorial

The research contributions featured in this volume reflect the diverse and critical challenges faced by our society from energy sustainability and artificial intelligence in medicine to biometric security and environmental conservation. These studies not only highlight the current technological advancements but also underscore the need for multidisciplinary approaches to solve complex problems. The intersection of engineering, healthcare, data science, and environmental monitoring is increasingly becoming the driving force behind innovation and progress. Each of the following studies provides a distinct yet equally significant addition to the broader scientific discourse.

Addressing the pressing issue of energy reliability in Pakistan, the study examines the technical and economic feasibility of implementing distributed solar generation in rural areas. By investigating high-loss, agriculture-based feeders connected to the Zafarwal Grid Station, the researchers propose the integration of 1 MW of solar power through optimized placement along the distribution lines. Using advanced tools such as ArcGIS, GPS-based field data collection, and Synergee Electric Software, the analysis reveals a 3.5% improvement in voltage regulation and a substantial 35.21% reduction in line losses. These outcomes emphasize the potential of decentralized solar energy systems to not only improve energy efficiency and reduce losses but also enhance power quality in underserved regions. The study advocates for the development of regulatory standards, particularly for inverter harmonics, to ensure safe and effective integration of distributed generation into existing grids [1].

Artificial intelligence stands poised to revolutionize clinical research, as evidenced by the critical evaluation of its integration into clinical trials. This paper explores the dual nature of AI its ability to streamline and refine processes such as patient recruitment, data analysis, and predictive modeling, while also confronting significant ethical and regulatory challenges. The authors urge the creation of robust ethical and legal frameworks to manage concerns around data privacy, algorithmic bias, and equitable access. By emphasizing transparency and ethical rigor, the study envisions a future where AI catalyzes innovation in clinical research without compromising on trust, safety, or fairness. Such a balanced approach could significantly improve patient outcomes and broaden the horizons of medical discovery [2].

Biometric security systems continue to evolve, with fingerprint authentication remaining at the forefront of identity verification technologies. This comprehensive review delves into the technical enhancements addressing challenges like image distortion, spoofing threats, and processing speed. With a focus on deep learning techniques and minutiae-based matching algorithms, the paper presents a state-of-the-art overview of advancements in fingerprint indexing and retrieval. It also explores novel applications across age demographics, including neonatal identification and healthcare record management. Beyond security, fingerprint systems are contributing to forensic science and medical diagnostics, demonstrating their growing relevance across disciplines. The study presents a holistic view of the field, combining technical analysis with a vision for future development in secure, efficient, and reliable biometric systems [3].

In the realm of environmental monitoring and agricultural sustainability, the development of HivePool emerges as a significant tool for advancing our understanding of honey bee health. The study introduces an interactive platform that combines time series data visualization with predictive analytics to monitor and interpret hive behavior in relation to environmental changes. HivePool supports both data-driven exploration and example-based forecasting, enabling beekeepers and researchers to detect and respond to patterns indicative of health threats or environmental stress. By equipping users with actionable insights, this tool represents a step

forward in ecological data science, fostering proactive management strategies for maintaining healthy bee populations, which are critical for biodiversity and agriculture alike [4].

Together, these contributions reflect a shared commitment to scientific excellence, social relevance, and technological innovation. Whether through optimizing energy systems, ensuring ethical AI deployment, advancing biometric security, or supporting ecological health, each study exemplifies the power of targeted research in addressing contemporary global challenges. This collection stands as a testament to the transformative potential of interdisciplinary inquiry and its role in shaping a sustainable and equitable future.

## References:

- [1] U. Asghar, S.Z. Hassan, M. Ahmed, A. Masood, M. Naqi Raza, T. Kamal, "Improving Distribution Power System Efficiency using Power Loss Reduction by Installing the Distributed Generations," *Journal of Engineering Research and Sciences*, vol. 3, no. 9, pp. 1–15, 2024, doi:10.55708/js0309001.
- [2] M. Yaqub, L. He, "The Dual Impact of AI in Clinical Trials: Perspective," *Journal of Engineering Research and Sciences*, vol. 3, no. 9, pp. 16–25, 2024, doi:10.55708/js0309002.
- [3] D. Maiti, M. Basak, D. Das, "Fingerprint Bio-metric: Confronting Challenges, Embracing Evolution, and Extending Utility - A Review," *Journal of Engineering Research and Sciences*, vol. 3, no. 9, pp. 26–60, 2024, doi:10.55708/js0309003.
- [4] T. Feng, S. Columbia, C. Campell, R. Tashakkori, "HivePool: An Exploratory Visualization System for Honey Beehive Data," *Journal of Engineering Research and Sciences*, vol. 3, no. 9, pp. 61–74, 2024, doi:10.55708/js0309004.

**Editor-in-chief**

**Prof. Paul Andrew**



## CONTENTS

|                                                                                                                            |    |
|----------------------------------------------------------------------------------------------------------------------------|----|
| <i>Improving Distribution Power System Efficiency using Power Loss Reduction by Installing the Distributed Generations</i> | 01 |
| Usman Asghar, Syed Zulqadar Hassan, Muhammad Ahmed, Arsalan Masood, Muhammad Naqi Raza and Tariq Kamal                     |    |
| <i>The Dual Impact of AI in Clinical Trials: Perspective</i>                                                               | 16 |
| Muhammad Yaquub and Lan He                                                                                                 |    |
| <i>Fingerprint Bio-metric: Confronting Challenges, Embracing Evolution, and Extending Utility - A Review</i>               | 26 |
| Diptadip Maiti, Madhuchhanda Basak and Debashis Das                                                                        |    |
| <i>HivePool: An Exploratory Visualization System for Honey Beehive Data</i>                                                | 61 |
| Tinghao Feng, Sophie Columbia, Christopher Campell and Rahman Tashakkori                                                   |    |

# Improving Distribution Power System Efficiency using Power Loss Reduction by Installing the Distributed Generations

Usman Asghar<sup>1</sup>, Syed Zulqadar Hassan<sup>1</sup>, Muhammad Ahmed<sup>2</sup>, Arsalan Masood<sup>1</sup>, Muhammad Naqi Raza<sup>1</sup>, Tariq Kamal<sup>3</sup>

<sup>1</sup>Department of Electrical Engineering, University of Sialkot, 51310 Sialkot, Pakistan

<sup>2</sup>Interdisciplinary Research Center (IRC) for Sustainable Energy System (SES), King Fahad University of Petroleum and Minerals, Daharan, Saudi Arabia

<sup>3</sup>School of Technology and Innovations, Electrical Engineering, University of Vaasa, 65200 Vaasa, Finland

Emails: baryar\_usman@yahoo.com; zulqadar.hassan@uskt.edu.pk; muhammad.ahmad@kfupm.edu.sa; arsalan.masood@uskt.edu.pk; naqi.raza@uskt.edu.pk, tariq.kamal@uwasa.fi

\* Corresponding author: Usman Asghar, University of Sialkot; email: [baryar\\_usman@yahoo.com](mailto:baryar_usman@yahoo.com)

**ABSTRACT:** The current scenario of Pakistan's power sector stipulates the financial and technical viability of the utility companies to meet the escalating demands for electricity. Financial resources are required for the generation of electricity; which Pakistan cannot afford in the present situation. Pakistan have a huge potential for renewable energy resources; different areas across the country have a good irradiation value of solar energy. Through distributed generation arrangement, electricity can be generated near the consumer, e.g., a solar panel array or a small wind turbine, so that line losses of the distribution system decrease and voltage drop can be improved, and customers can also benefit through investing in DGs. This research aims at a comprehensive investigation of 07 High loss and tube well-dominated rural distribution feeders emanating from 132 KV Zafarwal Grid Station in Zafarwal, so that 1 MW Solar Distributed Generation study can be implemented for its impact on the high voltage Grid Station and optimization using the latest software tools like Arc GIS for geo database and GPS device for collection of real-time data from the field and Synergee Electric Software for load flow studies for PV and further optimization in the distribution network. The results of this research show that the optimal placement of solar PV on distribution lines introduces a power source near the load center, resulting in a reduction of voltage drop up to 3.5% and 35.21 % reduction in line losses. This decrease in voltage drop will lead to an improvement in power quality for users. It is recommended that before going to increase the level of distributed generation in the system a standard procedure should be developed, and it must be ensured that the inverter used by various consumers should not be allowed beyond a certain level of Harmonic contribution.

**KEYWORDS:** Solar Distributed Generation, Rural Distribution Network, Voltage Drop Reduction, Line Loss Minimization, Harmonic Distortion Control

## 1. Introduction

The global energy demand is expected to evolve as countries try to lower-carbon energy sources to reduce greenhouse gas emissions and combat climate change [1–3]. In particular, the adoption of renewable energy sources is expected to increase in the coming decades as technology improves and costs continue to decline. According to the International Energy Agency, the top

three sources of global electricity generation in 2020 were coal (27%). Natural gas (24%) and renewables (25%) include hydropower, wind, solar, and other sources. The remaining 24% of global electricity was generated from nuclear power, oil, and other sources [4].

Energy is the lifeblood that drives households, companies, and industries in Pakistan, making it a vital component of the nation's economy. This industry uses a

wide variety of energy sources, such as nuclear power [5], hydroelectricity [6], renewable energy, and fossil fuels [7]. The capacity of production of electricity in Pakistan is shown in Figure 1. Historically, an extensive reliance on petroleum-based products such as oil and natural gas has resulted in issues such as shortages of energy and price instability. Still, the country is aggressively pursuing a more sustainable and equitable energy mix. Plans include the construction of hydroelectric plants to tap through the country's tremendous potential, encouraging the use of renewable energy sources such as solar and wind energy, and the enforcement of laws that will encourage private investment.

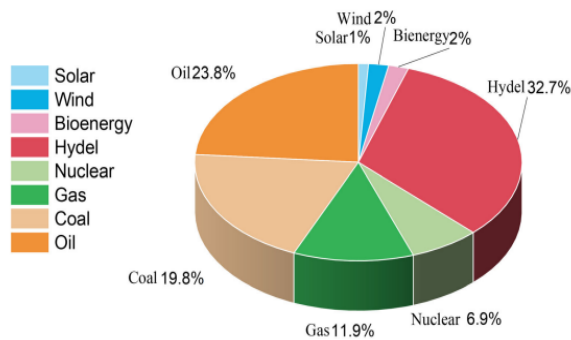


Figure 1: Production Capacity of Electricity in Pakistan [8]

An effective and robust energy sector is ensured by continuous efforts in policy formation, infrastructure development, and diversification, even in the face of obstacles such as circular debt and inefficient infrastructure. A strong energy industry has a profound socioeconomic impact that cannot be exaggerated, since it directly affects Pakistan's population growth, economic well-being, and overall development trajectory [9]. Maintaining economic development requires a sustainable, diversified, and stable energy supply, which is why it is so important to prioritize it as the nation navigates its energy environment. The energy sector in Pakistan is diverse, with a mix of traditional fossil fuel sources such as coal, natural gas, and oil, as well as renewable energy sources such as hydropower, solar, and wind. Pakistan's energy mix has historically relied heavily on fossil fuels, particularly natural gas and oil. However, the government has been working to increase the share of renewable energy in the energy mix, to generate 30% of the country's electricity from renewable sources by 2030. In recent years, Pakistan has made significant progress in expanding its hydropower capacity and has also made significant investments in solar and wind energy [10], [11].

The country's electricity sector is primarily managed and regulated by the National Electric Power Regulatory Authority (NEPRA). Pakistan has faced significant challenges in meeting the growing electricity demand, and the country has historically suffered from chronic power shortages and frequent power outages [12], [13]. In recent years, Pakistan's government has implemented several

initiatives to improve the reliability and sustainability of the power system, including investing in new power generation capacity, upgrading and expanding the transmission and distribution networks, and promoting the adoption of renewable energy sources. Despite these efforts, many people in Pakistan still lack access to reliable electricity, particularly in rural areas [14].

A power system is a network made up of essential parts that cooperate to generate, transmission, and redistribute electrical energy. Power plants use a variety of energy sources, including nuclear, renewable, and fossil fuels, to generate electricity. Energy losses are reduced by high-voltage lines and substations, which enable the efficient flow of electrical power across the system. The distribution component guarantees that power is delivered to end users, such as homeowners, businesses, and industrial consumers, by using transformer and lower-voltage wires. Protection mechanisms preserve the electrical network against faults, while control centers keep an eye on and oversee system operations, balancing supply and demand. The load is represented by consumers, who use electricity for a variety of purposes. Energy storage facilities and technologies for smart grids improve system efficiency, and grid interconnections increase reliability [15]. The distribution network is the part of the power system that delivers electricity from the transmission system to the end user. It is made up of lower-voltage lines and equipment that distribute electricity to customers over a smaller geographic area, typically a city or region [16].

The distribution network is typically owned and operated by a utility company, which is responsible for maintaining the network and ensuring that electricity is delivered to customers reliably and safely. GEPCO is responsible for operating and maintaining the distribution network in its service area, including the transmission and distribution lines, substations, and other electrical equipment that are used to deliver electricity to customers. GEPCO is also responsible for billing customers for the electricity that they consume and for providing customer service and support [17]. An overview of the main components and sections of power systems is shown in Figure 2 [18].

## 2. Methodology

### 2.1. Contributions

Net Metering is a significant shift towards renewable energy adoption in the Pakistan, but effective management still presents challenges. The research focuses on enhancing the performance of distribution network power systems by reducing power loss through Distributed Generation (DG). This approach optimizes energy distribution and contributes to sustainability by minimizing wastage.



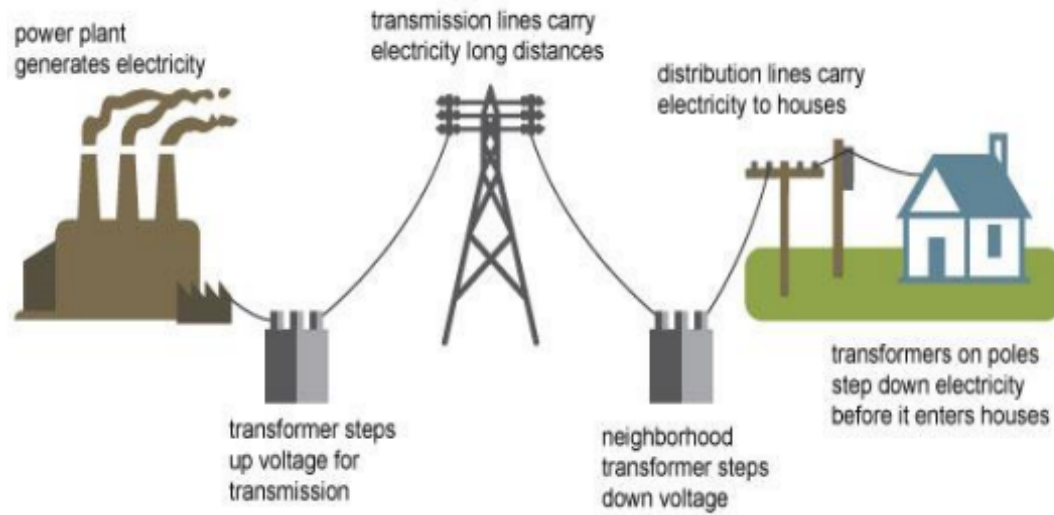


Figure 2: Overview of Power System [1]

Drawing from a case study of GEPCO, the study evaluated the feasibility and impact of DG installation on reducing power losses. The insights can be applied to all Distribution Companies (DISCOS) in the country, allowing for broader implementation and advancing energy sustainability goals.

## 2.2. Problem Statement

Our country is suffering from a lack of electricity. Approximately more than 60% of electricity is produced through thermal energy. Thermal power is not only expensive, but it also pollutes the environment. Most of the countries have shifted towards renewable resources. China had a total installed solar PV capacity of 131.1 GW, India 18.3 GW, UK 12.7 GW, France 8 GW, Australia 7.2 GW and Spain 5.6 GW, whereas Pakistan had an installed solar capacity of only 730 MW and Pakistan has a potential of 2.334 million MW of electricity per year through the photovoltaic and solar thermal system [6]. The other problem is that our installed systems are old and power losses in our transmission and distribution system result in decreased available electricity and an increase in voltage drop. According to the power division Ministry of Energy Report 2021-22, all the discos in Pakistan have 16.85% line losses [7].

The following research focuses on enhancing the efficiency of the GEPCO distribution system, which bears a significant amount of daily electric power loss without cause and a huge economic loss. Therefore, improving the electrical system's efficiency through power loss reduction is necessary. Therefore, for a more efficient distribution system, it is required to upgrade the structure of the distribution transformer in such a way that it would offer minimum power losses, high reliability, and be environmentally friendly, having excellent performance in full load conditions.

## 2.3. Criteria for Selection of 11KV feeder for DG Placement

For the technical feasibility of 11 kV feeder lines, different criteria are considered for the selection of feeders for Solar PV initiative sizing of Solar PV and optimum location of Solar PV placement on selected feeders. Details of the criteria considered for this study are discussed below:

### 2.3.1. Distribution Line Losses

Lengthy and high line loss feeders are selected so that after the placement of DG, the distribution line losses will decrease. It is an important criterion for selection of feeders for 11 kV solarization.

### 2.3.2. Reduction in Voltage Drop

11kV distribution feeders having higher voltage drop are expected to be reduced from optimal placement of solar PV on 11kV feeders. This criterion is used for the selection of a feeder and optimal site for 11 kV solarization.

## 2.4. Feeder Categories

### 2.4.1. Residential Feeder

Residential feeders are in the load centres alongside the populated areas. These feeders are usually not very long but have higher loads.

### 2.4.2. Agricultural Feeder

Agricultural feeders are usually away from the populations. Lengths of these feeders are usually much longer as the feeding points are spread out in large areas.

### 2.4.3. Industrial Feeder

Industrial Feeders are usually dedicated feeders for one industry with a large load or an area with a group of small industries.

An agricultural Rural and Tube-well dominated feeder is selected for Solarization on account of the availability of open land in rural areas and lengthy feeders resulting in high line loss and low voltage profile.

### 2.5. Peak Loading of Feeder in winter

11 kV Solarization initiative is taken to promote decentralized and distributed solar generation requiring no reinforcement of the existing distribution network. The size of the proposed Solar PV is selected such that the power generated is utilized locally without flowing back toward the transmission/ distribution system. Therefore, peak winter load is used for the selection of feeders and sizing of Solar PV.

## 3. Zafarwal Grid Stations

The main purpose of considering the above 100 A winter loading is that the power generated is utilized locally without flowing back toward the transmission/ distribution system. Therefore, peak winter load is used for the selection of feeders. These 11 kV feeders are emanating from 35 No. 132 kV G/Stations. To make this research work viable, 132 kV Zafarwal Grid station is selected as a case study whose 07 Number Feeders are suitable and fulfill the criteria for DG placements.

Table 1: Zafarwal Grid Station Feeders [19]

| Month      | 11KV<br>Raheem<br>Abad<br>feeder | 11KV<br>Non<br>ar | 11KV<br>Thor<br>o<br>Man<br>di | 11KV<br>sang<br>i<br>al | 11KV<br>Dham<br>t<br>hal | 11KV<br>Gag<br>ia<br>n | 11KV<br>King<br>ra |
|------------|----------------------------------|-------------------|--------------------------------|-------------------------|--------------------------|------------------------|--------------------|
| 01/12/2022 | 100                              | 100               | 110                            | 105                     | 115                      | 110                    | 120                |
| 01/11/2022 | 100                              | 90                | 90                             | 70                      | 100                      | 110                    | 100                |
| 01/10/2022 | 160                              | 140               | 180                            | 140                     | 200                      | 180                    | 190                |
| 01/09/2022 | 245                              | 210               | 240                            | 220                     | 260                      | 230                    | 250                |
| 01/08/2022 | 220                              | 225               | 270                            | 230                     | 160                      | 245                    | 290                |
| 01/07/2022 | 240                              | 215               | 260                            | 240                     | 260                      | 270                    | 330                |
| 01/06/2022 | 230                              | 245               | 305                            | 340                     | 390                      | 330                    | 290                |
| 01/05/2022 | 200                              | 220               | 240                            | 200                     | 265                      | 280                    | 280                |
| 01/04/2022 | 180                              | 230               | 230                            | 190                     | 250                      | 280                    | 290                |

|            |     |     |     |     |     |     |     |
|------------|-----|-----|-----|-----|-----|-----|-----|
| 01/03/2022 | 120 | 140 | 160 | 120 | 170 | 180 | 190 |
| 01/02/2022 | 70  | 90  | 90  | 70  | 100 | 100 | 100 |
| 01/01/2022 | 80  | 85  | 110 | 80  | 110 | 100 | 110 |

### 3.1. Data Collection

The required data carried out for the simulation has been collected from the 11-kV distribution network of GEPCO. The collected data is from 132 kV Zafarwal Grid station located in the vicinity of Narowal. The grid has been selected on the basis that it is a high loss and has a higher voltage drop, which is feeding to rural area tube well-dominated feeders. Most feeders are Agricultural. Data is collected through GPS device and Data sheet [20].

### 3.2. GPS Data (Coordinates)

GPS devices are used to take the waypoints of the poles. It captures signals from multiple satellites and uses the information to calculate the device's latitude, longitude, altitude, and sometimes speed and direction.

### 3.3. Data Entry Sheet

Details of waypoints/poles in entered on the Data entry sheet i.e. Date, group, waypoint number, pole height, conductor type, pole height, transformer detail, and number of circuits, etc. The Data entry sheet is shown in the figure 3.

### 3.4. Export through Garmin GPX file data

GPS data is exported through map source software from the GPS device into a GPX file for data joining purposes through Arc GIS software. The figure 4 shows the waypoints on map source software.

### 3.5. Data Entry of Data sheet

Data is entered in Access Base MDB files through data entry operators as mentioned on the data entry sheet for joining purposes through Arc GIS software. The figure 5 shows the view of data entry software like feeder name, group, date, grid station transformer detail, etc.

### 3.6. ARC GIS Software, Data Joining (GPX & MDB files)

Updated and latest GIS mapping of 11 kV feeders is crucial for accurate analysis and design of Solarization. Therefore, GIS mapping is considered as an input file for Synergee Electric software to conduct load flow studies and selection of optimal locations for placement of Solar PV generation.

| Data Table Form For HT                                                            |   |               |   |   |        |   |       |        |          |          |   |   |           |      |      |           |           |     |                                                                                     |          |          |                   |                    |  |
|-----------------------------------------------------------------------------------|---|---------------|---|---|--------|---|-------|--------|----------|----------|---|---|-----------|------|------|-----------|-----------|-----|-------------------------------------------------------------------------------------|----------|----------|-------------------|--------------------|--|
|  |   | Substation:   |   |   |        |   |       |        |          |          |   |   |           |      |      |           | DATE:     |     |  |          |          |                   |                    |  |
|                                                                                   |   | Feeder:       |   |   |        |   |       |        |          |          |   |   |           |      |      |           | GROUP:    |     |                                                                                     |          |          |                   |                    |  |
|                                                                                   |   | GIS ENGINEER: |   |   |        |   |       |        |          |          |   |   |           |      |      |           | SHEET NO: |     |                                                                                     |          |          |                   |                    |  |
| Survey Point Number                                                               |   |               |   |   |        |   |       |        |          | Pole     |   |   | Conductor |      |      | Equipment |           |     |                                                                                     |          |          |                   | Location & Remarks |  |
| Group                                                                             |   | Date          |   |   | GPS WP |   | Class | Height | End Type | Circuits | R | Y | B         | Type | Unit | Size      | Phase     | Use | Status                                                                              | Mounting | Manufctr | Type of Cross Arm |                    |  |
| 0                                                                                 | 1 | d             | d | m | m      | y | y     | 0      | 0        | 1        | * |   |           |      |      |           |           |     |                                                                                     |          |          |                   |                    |  |
|                                                                                   |   |               |   |   |        |   |       |        |          |          |   |   |           |      |      |           |           |     |                                                                                     |          |          |                   |                    |  |

Figure 3: Data Entry Sheet

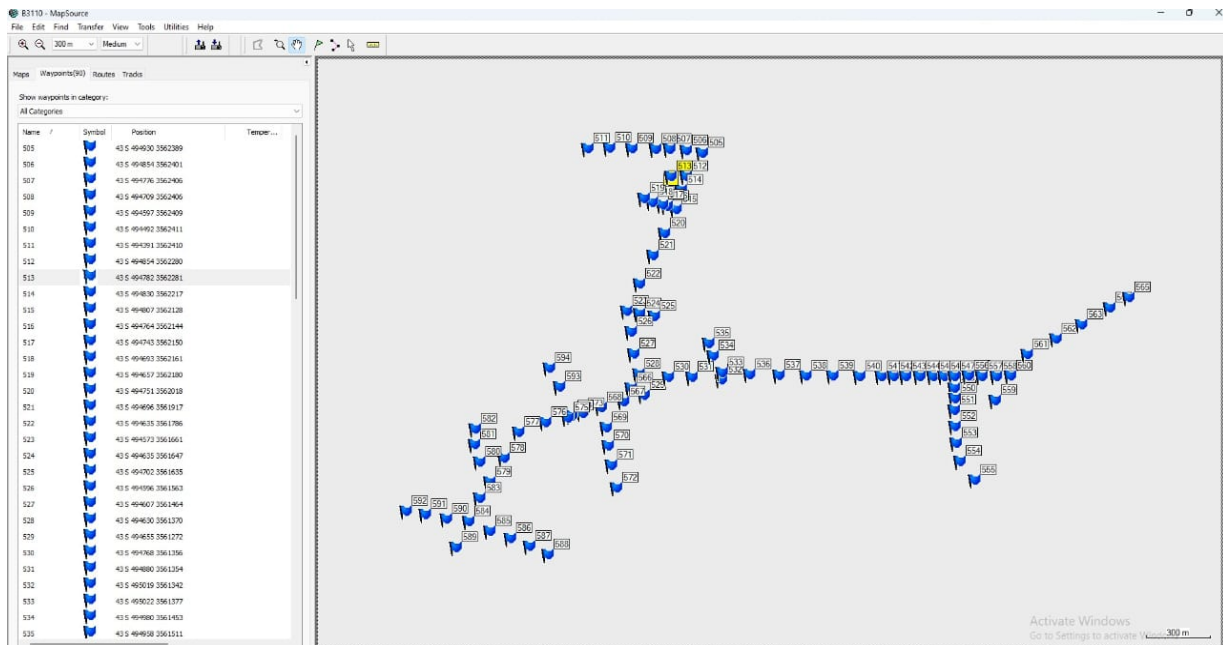


Figure 4: Way Point on Map

| Field Data                                                                                                                                               |  |                         |  |                |  |                    |  |                            |  |                |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------------------|--|----------------|--|--------------------|--|----------------------------|--|----------------|--|
| DISCO                                                                                                                                                    |  |                         |  |                |  |                    |  |                            |  |                |  |
| GEPCO                                                                                                                                                    |  |                         |  |                |  |                    |  |                            |  |                |  |
| Sub-Station                                                                                                                                              |  | Feeder                  |  | S/E            |  | Group              |  | Date                       |  |                |  |
| Zafarwal                                                                                                                                                 |  | Raheemabad              |  | E              |  | A                  |  | Tuesday, February 13, 2024 |  |                |  |
| GPS Wapoint#                                                                                                                                             |  | Pole Use                |  | Pole Class     |  | Pole Height        |  | End Type                   |  | Pole Phase     |  |
| 10                                                                                                                                                       |  | Primary Distribution    |  | PC Ordinary    |  | 36                 |  |                            |  | R-Y-B          |  |
| R                                                                                                                                                        |  | Y                       |  | B              |  | N                  |  | Equipment Type             |  | Equipment Unit |  |
| Dog                                                                                                                                                      |  | Dog                     |  | Dog            |  |                    |  | Transformer                |  | 1              |  |
| Equipment Size                                                                                                                                           |  | Equipment Phase         |  | Equipment Use  |  | Equipment Status   |  | Mounting                   |  |                |  |
| 25                                                                                                                                                       |  | R-Y-B                   |  | Dedicated      |  | Connected          |  | Single Pole                |  |                |  |
| Equipment Make                                                                                                                                           |  | Dedicated Consumer Name |  |                |  | Equipment Location |  |                            |  |                |  |
| Pel                                                                                                                                                      |  |                         |  |                |  | Jazz Tower         |  |                            |  |                |  |
| Equipment Number                                                                                                                                         |  |                         |  | No. Of Feeders |  | Pole Number        |  |                            |  |                |  |
| T-1130224010                                                                                                                                             |  |                         |  | 0              |  | 1130224010         |  |                            |  |                |  |
| <input type="checkbox"/> Angle Pole <input type="checkbox"/> Tap Pole <input type="checkbox"/> first secondary pole <input type="checkbox"/> Feeder Pole |  |                         |  |                |  |                    |  |                            |  |                |  |
| RS                                                                                                                                                       |  | RS1p                    |  | RS3p           |  | SC                 |  | LC                         |  | SI             |  |
| 0                                                                                                                                                        |  | 0                       |  | 0              |  | 0                  |  | 0                          |  | 0              |  |
| LI                                                                                                                                                       |  | PB                      |  | AG             |  | ST                 |  |                            |  |                |  |
| 0                                                                                                                                                        |  | 0                       |  | 0              |  | 0                  |  |                            |  |                |  |
| Remarks                                                                                                                                                  |  |                         |  |                |  |                    |  |                            |  |                |  |
| <input type="text"/>                                                                                                                                     |  |                         |  |                |  |                    |  |                            |  |                |  |
| <input type="button" value="Save"/> <input type="button" value="Exit"/>                                                                                  |  |                         |  |                |  |                    |  |                            |  |                |  |

Figure 5: View of Data Entry Software



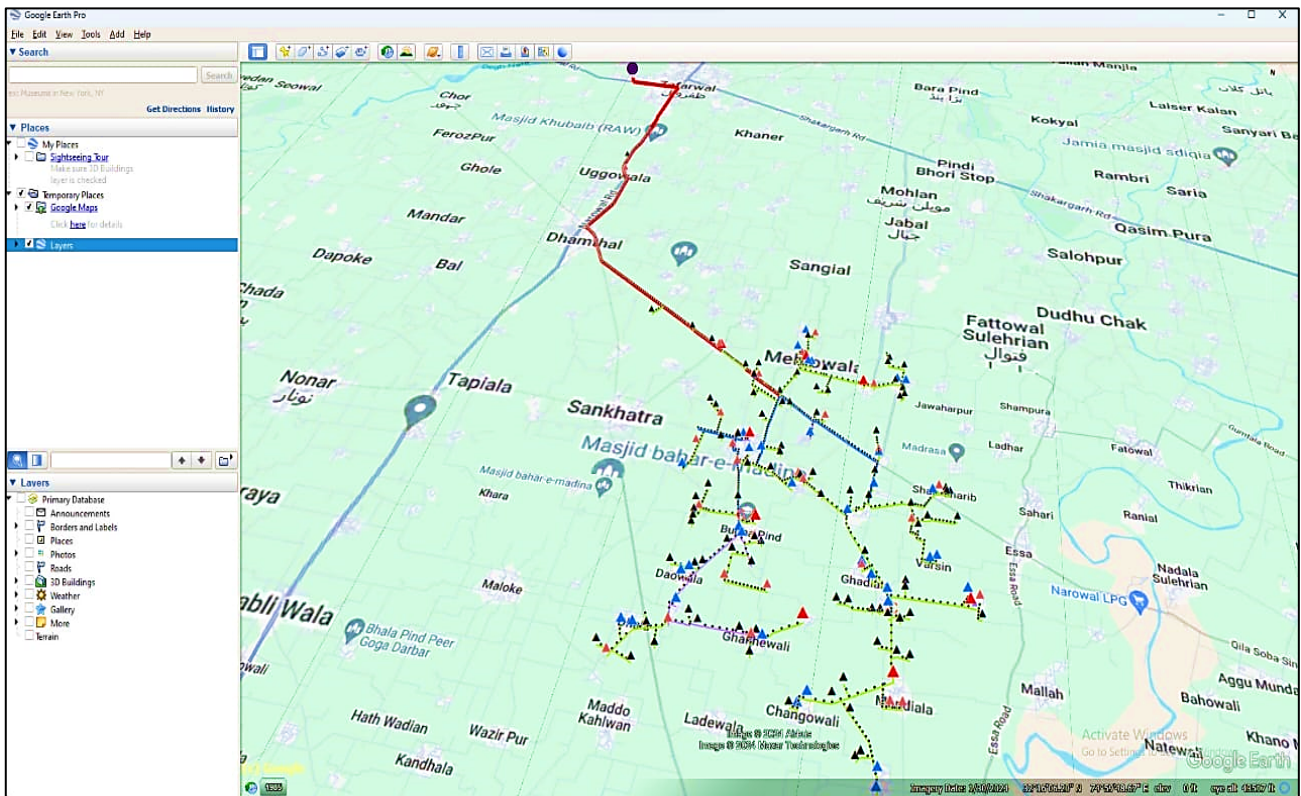


Figure 6: Google View using KML Files

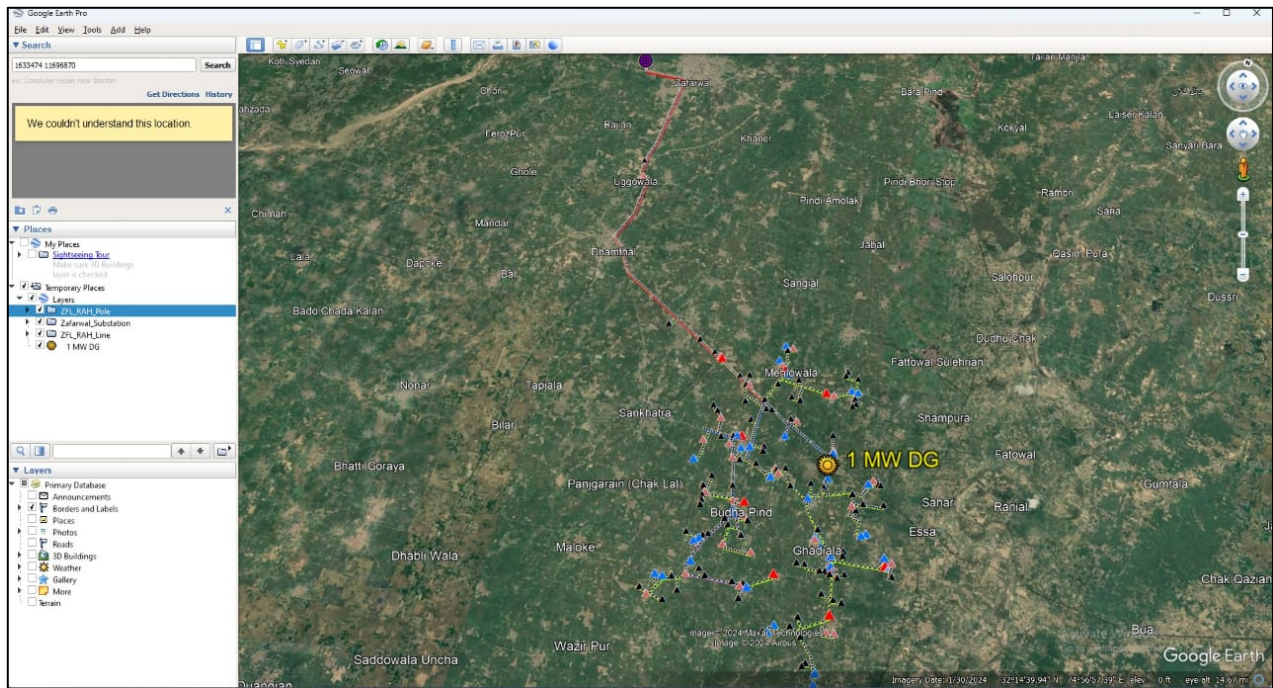


Figure 7: Google View of Raheem Abad Feeder 1MW DG placed

A geographic information system (GIS) is a system that creates, manages, analyzes, and maps all types of data. GIS connects data to a map, integrating location data (where things are) with all types of descriptive information (what things are like there) [21]. This provides a foundation for mapping and analysis that is used in science and almost every industry. GIS helps users understand patterns, relationships, and geographic context here we use GIS software for joining data both GPX data collected through a GPS device and MDB data collected through a data entry sheet [22]. The figure 6 and figure 7 shows the GIS map of

the 11 kV Raheemabad feeder emanating from 132 kV Zafarwal G/Station. GIS software provides us with different output files here we take two types of files MDB & KML files.

### 3.7. MDB & KML files

Arc GIS provides us with input files for synergee electric software for load flow studies and further DG placement. KML files are used to view the selected 11KV feeders on Google Maps to check the availability of land.



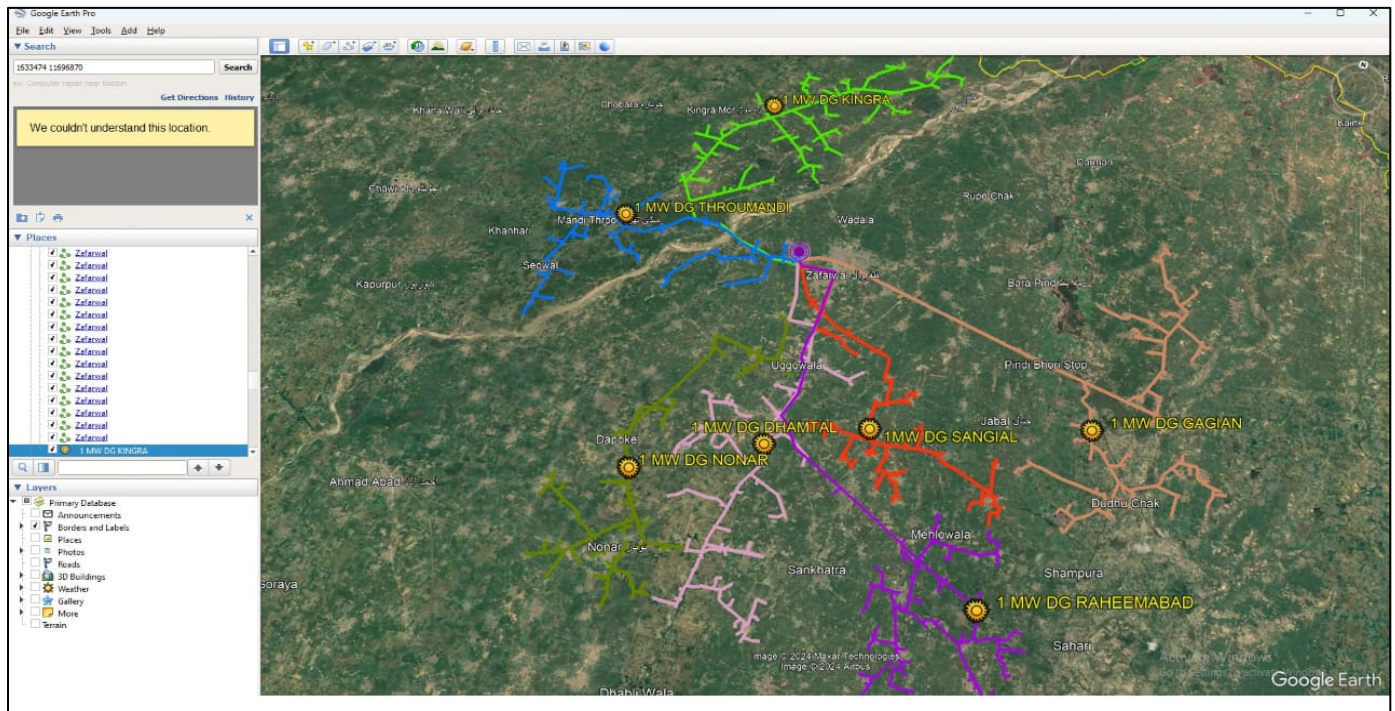


Figure 8: Google View after DG placement

The figure 6 shows the Google view using the KML file at Google map of the 11 kV Raheem Abad feeder emanating from 132 kV Zafarwal G/Station.

dominated feeders, and Domestic dominated feeders. Detail of these feeders is mentioned below mention Table 2.

### 3.8. Availability of Open Land

Site verification of selected feeders will be carried out through a physical visit to the site to ensure the DG placement at selected 11 kV feeders of 132 kV Zafarwal G/Station and predicts that open land is available at the site. Further after collecting the coordinates physically sites were also verified.

### 3.9. Site Verification

Installation of solar panels requires a large area of flat and clean land for installation; therefore, availability of excess open land (greater than 2.5 Acres for each 1MW Solar Park) is ensured while selecting feeders and sizing of Solar PV. The figure 7 shows the Google view of the 11 kV Raheem Abad feeder and shows that open land is available at the site.

The Flow Chart diagram of our research work is shown in Figure 9. All the steps of flow charts are explained in detail.

## 4. Data Joining (GPX & MDB files) ARC GIS Software

### 4.1. Modelling of Data

GEPCO has more than 60 no 132 kV Grid stations with 970 11 kV outgoing feeders. These feeders serve the public according to their requirements of load and area. There are four major categories of these feeders: Agricultural and rural feeders, Industrial dominated feeders, Commercial

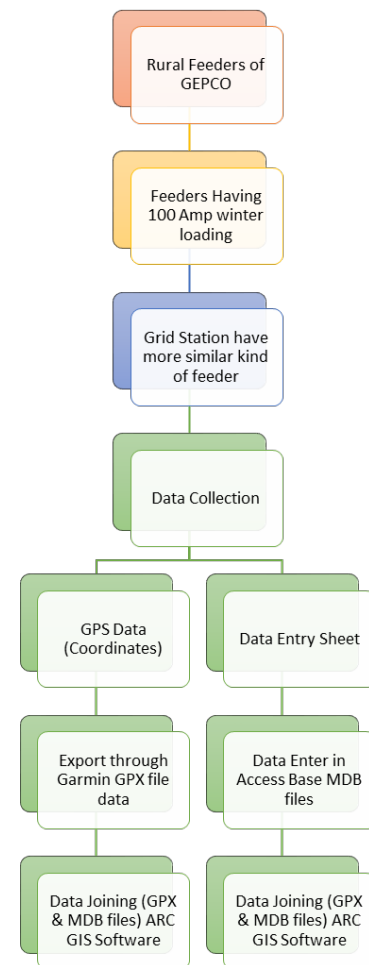


Figure 9: Flowchart of Proposed System.

Table 2: Detail of feeders

| SR. #                        | Description                  | Number of Feeders |
|------------------------------|------------------------------|-------------------|
| 1                            | Agricultural & Rural feeders | 337               |
| 2                            | Industrial dominated feeders | 259               |
| 3                            | Commercial dominated feeders | 69                |
| 4                            | Domestic dominated feeders   | 305               |
| Total Number of 11kv Feeders |                              | 970               |

GEPCO has a total of 970 feeders, and the main categories are Domestic feeders 305, commercial feeders 69, Industrial feeders 259, and Agricultural and rural dominated 337. Feeders are shown in Figure 10. The agricultural & rural-dominated feeders are considered for research work because 2.5-acre land is required for 1MW for placement of the DGs. These agricultural rural feeders are very lengthy, and they have a high line loss and high voltage drop.

The scrutiny will be further narrowed by considering the winter (Dec-2022) peak loading above 100 Amp, which resulted in a list of 137 candidate feeders from 337 agricultural & rural-dominated feeders. DG placement initiative is taken to promote decentralized and distributed solar generation, requiring no reinforcement of the existing distribution network. The main purpose of considering the above 100 A winter loading is that the power generated is utilized locally without flowing back toward the transmission/ distribution system. Therefore, peak winter load is used for the selection of feeders. These 11 kV feeders are emanating from 35 No. 132 kV G/Stations. To make this research work viable, 132 kV Zafarwal Grid station is selected as a case study whose 07 Number Feeders are suitable and fulfill the criteria for DG placements.

Figure 11 show the combined Loading detail for the year 2022 of 07 No. 11 kV feeders emanating from 132 kV Zafarwal G/Station) Maximum Summer loading in Amps and winter loading in December in Amps are shown. Real-time data is collected after a field survey of the selected feeders after a pole-to-pole survey through GPS devices and the waypoints of the poles with their details like height type and No of circuits on the poles.

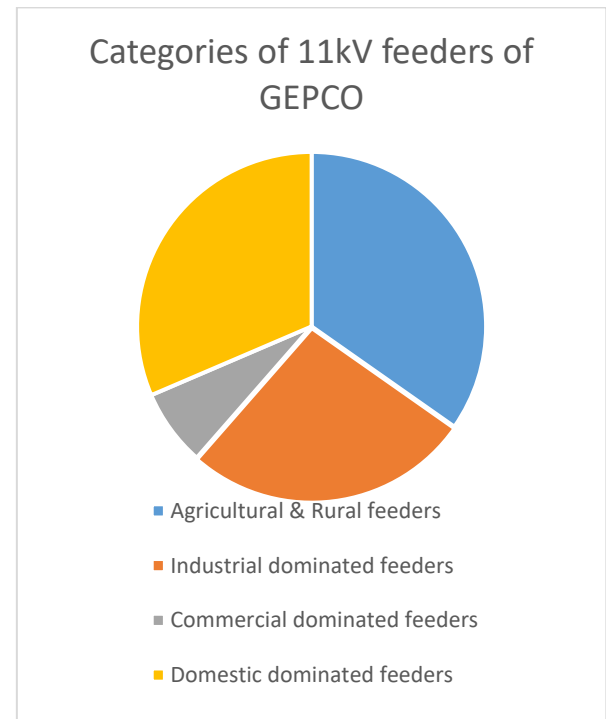


Figure 10: Categories of 11kV feeders of GEPCO

After completion of the site survey and completion of data entry, the entered data detail is attached with waypoints through Arc GIS Software for a geographical database of the electric network. Arc GIS gives us two types of files one for Synergee Electric software that is known MDB file and other one is KMZ file which is used to view real time data at Google Earth [12].

#### 4.2. Load Flow Analysis

Load flow studies by using MDB file of 11kV feeders under consideration is performed using "Synergee Electric" software of DNV GL based on GIS mapping, under following four scenarios as shown in figure 13.

The percentage voltage reduction is computed in Table 3 [23] and savings of electricity per KWh in Pakistani Rupees is computed in Table 4 [24].

#### 4.3. Electricity Price

Every distribution feeder contains transformers of commercial and domestic categories therefore rates of electricity per unit would be different for both types. GEPCO determined the Tariff rate for FY 2022-23 mentioned in the table 5 average rate of the Domestic load unit is Rs.23 and for commercial load fixed unit rate is Rs.60 hence average electricity price for overall loads can be considered as Rs.41.5 and would be used in the economic loss calculations.

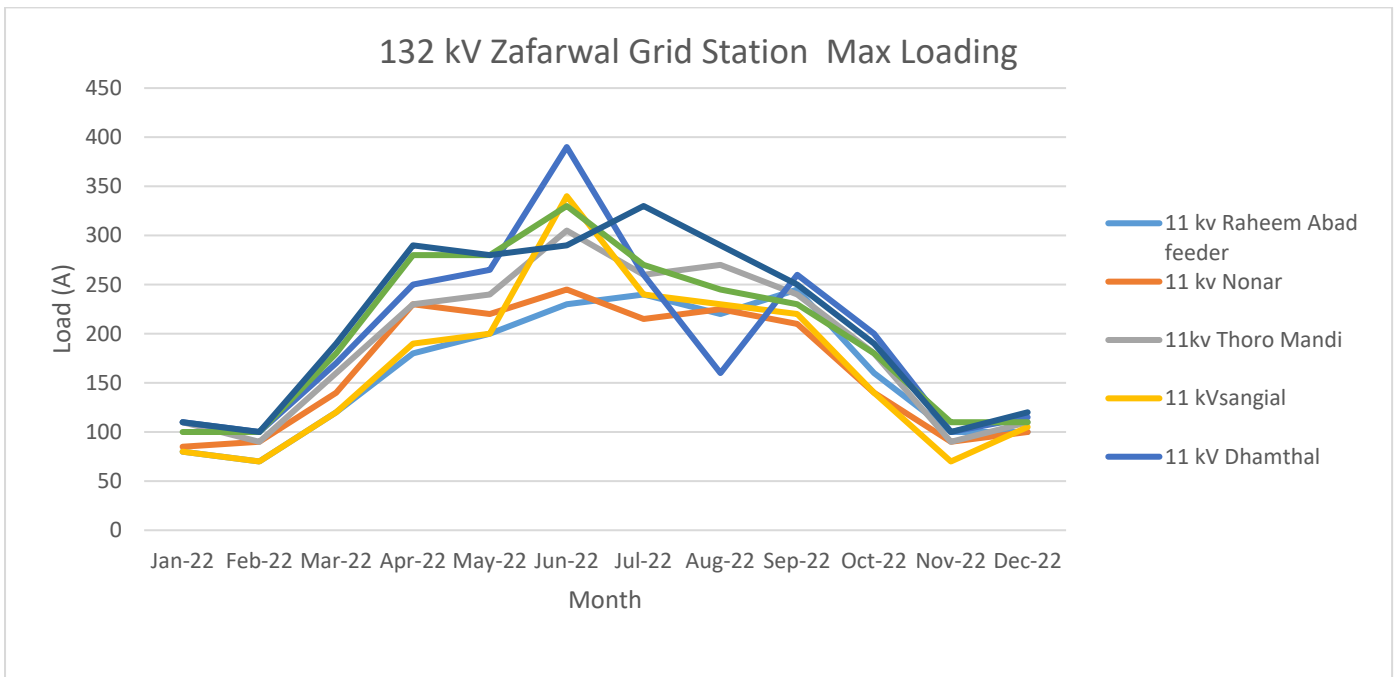


Figure 11: Max Loading of 132KV Zafarwal Grid Station

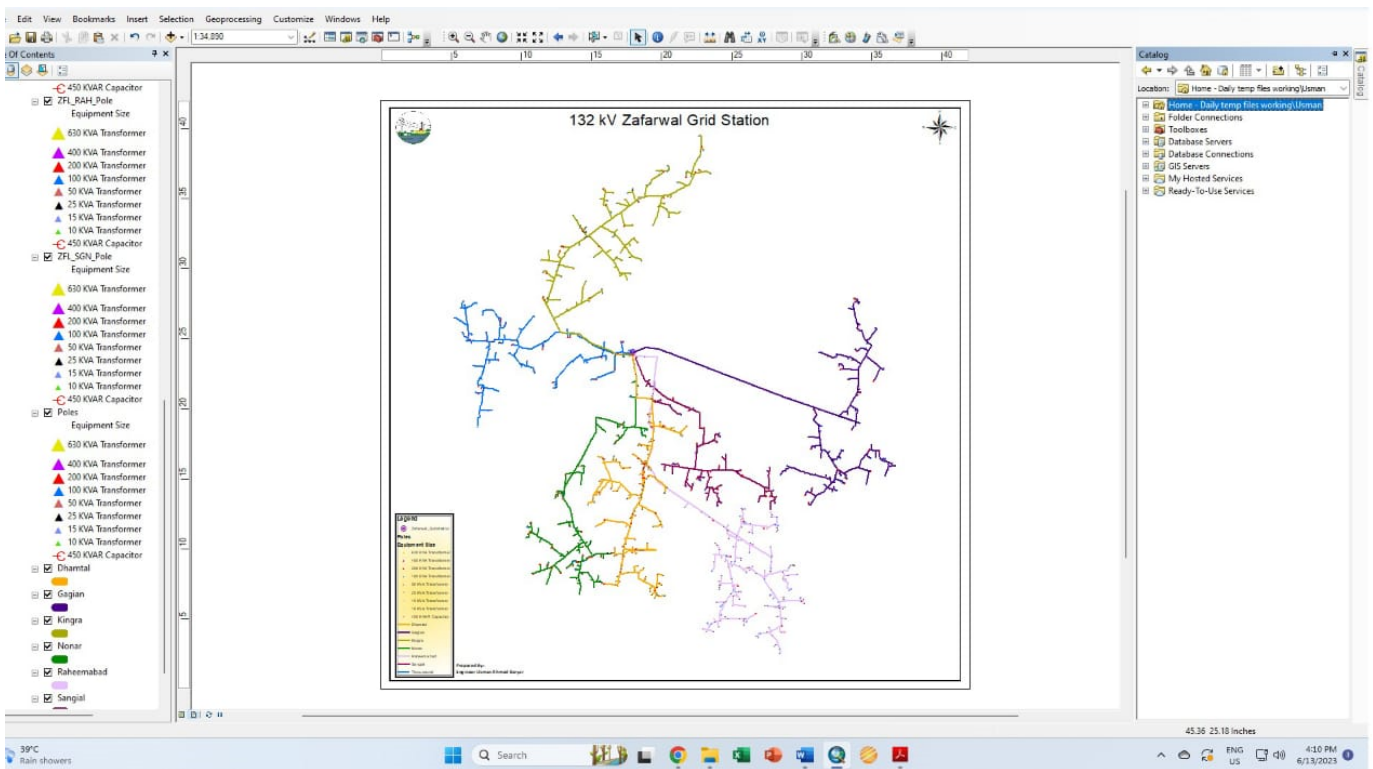


Figure 12: Arc GIS Software desktop view [12]



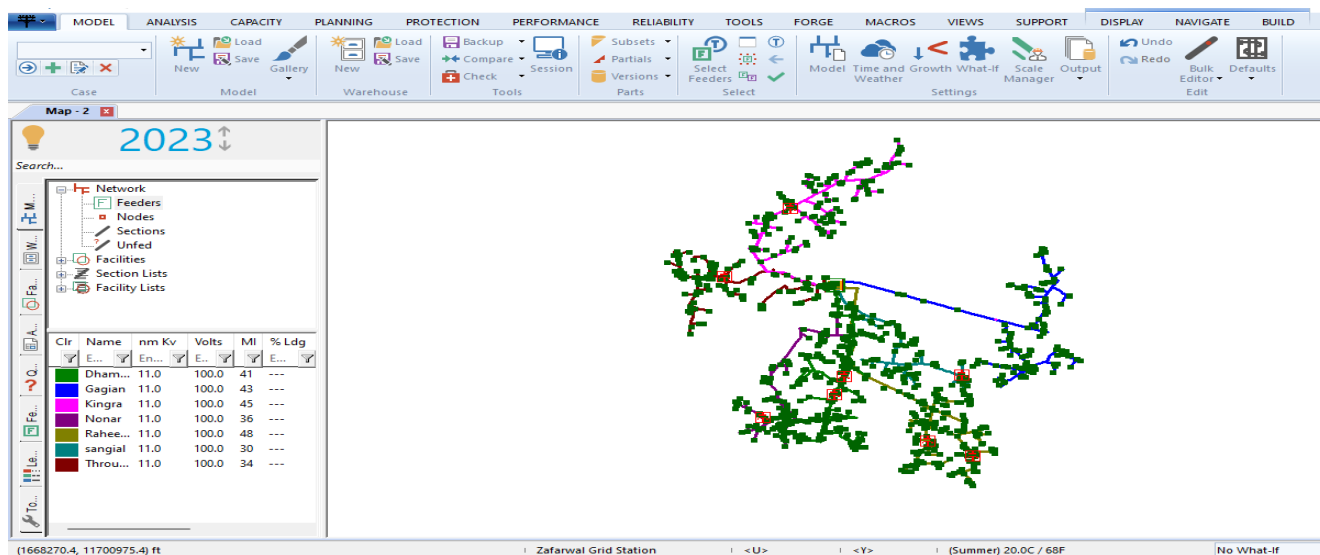


Figure 13: Overview of Synergee Software

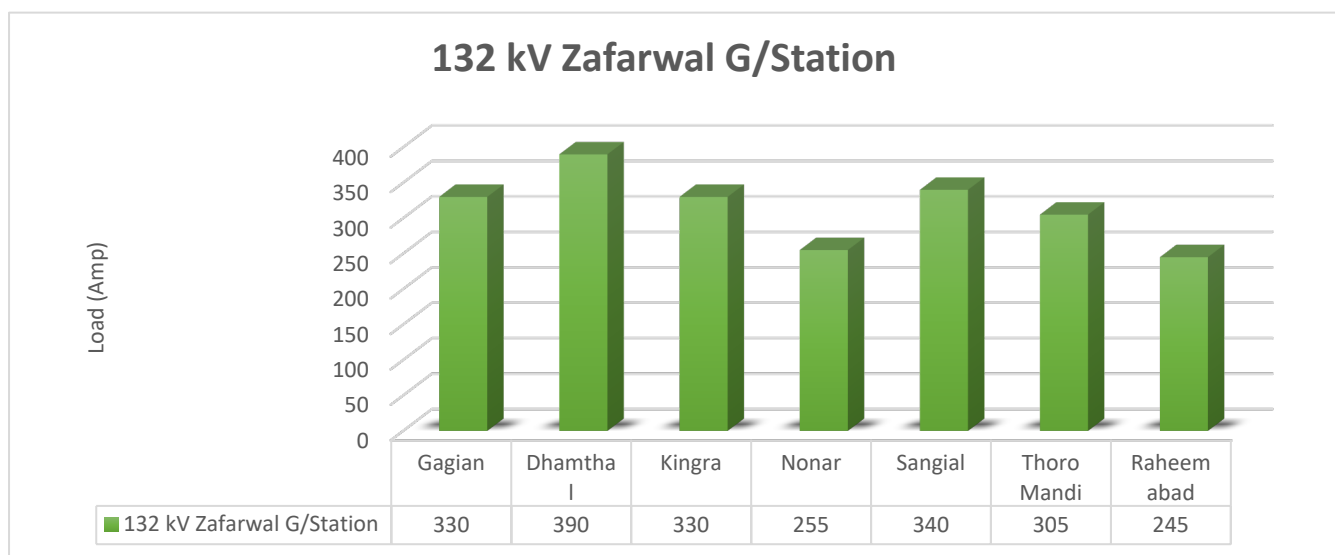


Figure 14: Load of 132 kV Zafarwal G/Station

Table 3: Solar PV installations on Rural &amp; Tube well Dominated Feeder emanating from 132 kV Zafarwal Grid Station.

| Sr. No | Name of Grid Station | Feeder Name | HT Length | Maximum Load in amp | PV Size (MW) | Load flow analysis Winter without PV |         | Load flow analysis Winter with PV |         | Savings KW | % V.D Reduction |
|--------|----------------------|-------------|-----------|---------------------|--------------|--------------------------------------|---------|-----------------------------------|---------|------------|-----------------|
|        |                      |             | (km)      | (Winter)            |              | kW Loss                              | V.D (%) | kW Loss                           | V.D (%) |            |                 |
| 1      | 132KV Zafarwal       | Throumandi  | 55.02     | 110                 | 1            | 64                                   | 6.2     | 17                                | 3.61    | 47         | 3               |
| 2      |                      | Nonar       | 56.97     | 100                 | 1            | 94                                   | 7.5     | 17                                | 3.07    | 77         | 4               |
| 3      |                      | Dhamthal    | 65.98     | 115                 | 1            | 47                                   | 4.7     | 16                                | 3.35    | 31         | 1               |
| 4      |                      | Kingra      | 71.73     | 120                 | 1            | 185                                  | 13.7    | 63                                | 8.91    | 122        | 5               |
| 5      |                      | Singial     | 47.52     | 105                 | 1            | 76                                   | 10      | 29                                | 4.46    | 47         | 6               |
| 6      |                      | Gagian      | 69.71     | 110                 | 1            | 96                                   | 7       | 45                                | 5.35    | 51         | 2               |
| 7      |                      | Raheemabad  | 76.18     | 100                 | 1            | 112                                  | 9.2     | 33                                | 4.74    | 79         | 4               |
|        |                      |             |           |                     |              | 674                                  | 8.3     | 220                               | 4.8     | 454        | 3.5             |

Table 4: DGs installations on Rural &amp; Tube well Dominated Feeders emanating from 132 kV Zafarwal Grid Station.

| Sr. No | Name of Grid Station | Feeder Name | HT Length (km) | PV Size (MW) (MW) | Load factor | Load flow analysis Summer without PV |         |                   | Load flow analysis Summer with PV |         |                   | Savings KW | Savings KW % | % V.D Reduction | Savings (kWh) |
|--------|----------------------|-------------|----------------|-------------------|-------------|--------------------------------------|---------|-------------------|-----------------------------------|---------|-------------------|------------|--------------|-----------------|---------------|
|        |                      |             |                |                   |             | kW Loss                              | V.D (%) | Annual Loss (kWh) | kW Loss                           | V.D (%) | Annual Loss (kWh) |            |              |                 |               |
| 1      | 132KV Zafarwal       | Throuman di | 55.02          | 1                 | 40          | 498                                  | 21.2    | 1012095           | 316                               | 18.4    | 642213            | 182        | 36.55        | 2.83            | 369882        |
| 2      |                      | Nonar       | 56.97          | 1                 | 40          | 604                                  | 24.2    | 1227521           | 334                               | 19.5    | 678795            | 270        | 44.7         | 4.64            | 548726        |
| 3      |                      | Dhamthal    | 65.98          | 1                 | 40          | 528                                  | 18.8    | 1073065           | 384                               | 17.8    | 780411            | 144        | 27.27        | 1.02            | 292654        |
| 4      |                      | Kingra      | 71.73          | 1                 | 40          | 1426                                 | 43.6    | 2898088           | 918                               | 37.5    | 1865670           | 508        | 35.62        | 6.11            | 1032419       |
| 5      |                      | Singial     | 47.52          | 1                 | 40          | 906                                  | 29.1    | 1841282           | 568                               | 25      | 1154358           | 338        | 37.31        | 4.11            | 686924        |
| 6      |                      | Gagian      | 69.71          | 1                 | 40          | 871                                  | 26      | 1770151           | 636                               | 24.6    | 1292556           | 235        | 26.98        | 1.42            | 477595        |
| 7      |                      | Raheemabad  | 76.18          | 1                 | 40          | 662                                  | 33.1    | 1345396           | 404                               | 28.5    | 821057            | 258        | 38.97        | 4.62            | 524339        |
|        |                      |             |                |                   |             | 5495                                 | 28      | 11167598          | 3560                              | 24.5    | 7235059           | 1935       | 35.21%       | 3.50%           | 3932539       |

Table 5: Average Rates of KWh Units for Domestic &amp; Commercial consumers

| S/No | Description                                              | Price (Rs)/Kwh |
|------|----------------------------------------------------------|----------------|
| A    | Average Domestic Tariff rate determined FY 2022-23       | 23.00          |
| B    | Fixed Commercial Tariff rate determined FY 2022-23       | 60.00          |
| C    | Average Rate for Domestic/ Commercial consumers= (A+B)/2 | (23+60)/2=41.5 |

#### 4.4. Calculations of Economic Loss and Pay Back Time Period

For calculating the economic loss first, we need to calculate the KWH losses with & without DG (PV) installation. After calculating the power loss in KWH multiply it by unit price which gives the annual economic loss of the selected feeders.

For example, for selected feeder's annually economic loss with & without DG (PV) placement can be calculated as

Annual Economic loss in Million for 07 feeders

$$= (\text{Annual Power loss for 07 feeders} \times \text{Average unit Rate}) / 1000000 \quad (1)$$

Annual loss in Million for 137 feeders

$$= (\text{Annual Power loss for 07 feeders} / 07 \times 137 \times \text{Average unit Rate}) / 1000000 \quad (2)$$

Annual Power loss without DG (PV) placement.

$$\text{Annual Power loss for 07 feeders without DG (PV) placement} = 11167598 \text{ KWh} \quad (3)$$

$$\text{Annual Economic loss in Million for 07 feeders} = \quad (4)$$

$$(11167598 \times 41.5) / 1000000 = 463.4 \text{ PKR}$$

$$\text{Annual loss in Million for 137 feeders} = ((11167598 / 7 \times 137) \times 41.5) / 1000000 = 9070.0 \text{ PKR} \quad (5)$$

Annual Power loss with DG (PV) placement.

$$\text{Annual Power loss for 07 feeders with DG (PV) placement} = 7235059 \text{ KWh} \quad (6)$$

$$\begin{aligned} \text{Annual Economic loss in Million for 07 feeders} & \quad (7) \\ &= (7235059 \times 41.5) / 1000000 \\ &= 300.25 \text{ PKR} \end{aligned}$$

$$\begin{aligned} \text{Annual loss in Million for 137 feeders} & \quad (8) \\ &= ((7235059 / 7 \times 137) \times 41.5) / 1000000 \\ &= 5876.32 \text{ PKR} \end{aligned}$$

Cost of DG (PV) including installation & operational charges.

$$\begin{aligned} \text{Cost per watt including installation \& operational charges} & \quad (9) \\ &= 90 \text{ PKR/watt} \end{aligned}$$

$$\begin{aligned} \text{Cost for 1 feeder 1 MW PV in Million} & \quad (10) \\ &= (90 \times 106) / 106 \\ &= 90 \text{ Million} \end{aligned}$$

$$\begin{aligned} \text{Cost for 7 feeders 7 MW PV in Million} & \quad (11) \\ &= 7 \times (90 \times 106) / 106 \\ &= 630 \text{ Million} \end{aligned}$$

$$\begin{aligned} \text{Cost for 137 MW PV in Million} & \quad (12) \\ &= 137 \times (90 \times 106) / 106 \\ &= 12330 \text{ Million} \end{aligned}$$

For finding the payback time of DG (PV) placement start with the initial price of DG (PV) placement and then add the cost of Annual Power loss of selected feeders. Repeat the process for both categories with & without DG (PV) placement and plotting the graph for a minimum 08 years will give the payback time of DG (PV) placement. Payback periods for selected feeders of GEPCO are given below

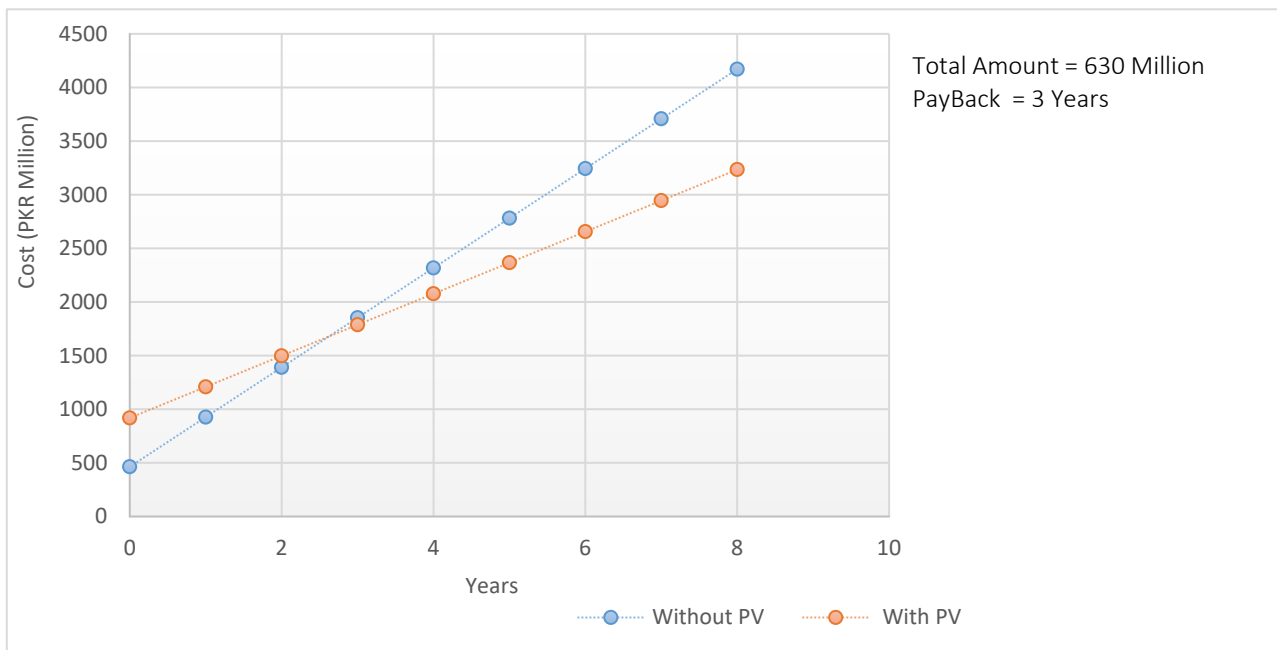


Figure 15: Payback Time Period of 7MW DG (PV) placement at selected 07 feeders

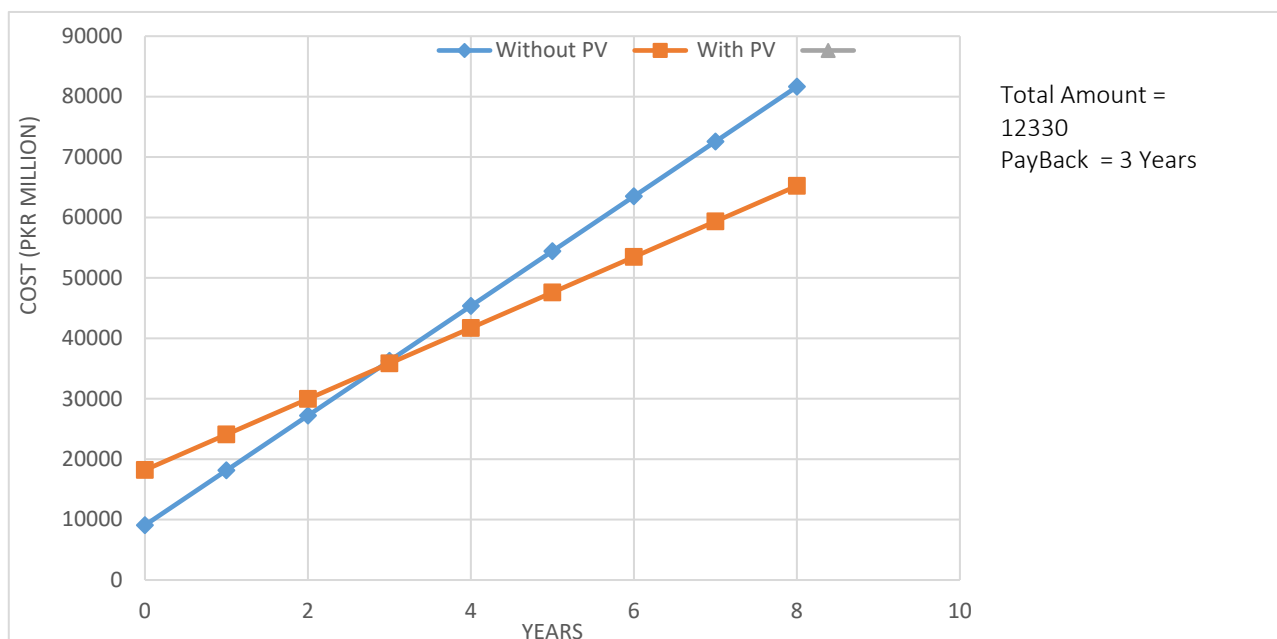


Figure 16: Payback Time Period of 7MW DG (PV) placement at 137 feeders



## 5. Conclusion

Currently, the power sector of Pakistan is facing the major challenge of controlling line losses and electricity theft, due to which load shedding is being applied on high-loss feeders. On the other hand, overall losses in power distribution systems are not only dropping the efficiency of the power system but also causing massive economic losses for the power distribution companies. According to the literature review, the power generation of Pakistan was 41557MW till 2022, of which 58% of power is generated from thermal resources as the cost of thermal generation is very high compared to other types of generations; therefore, for providing electricity to the consumers at affordable rates, Government of Pakistan has to bear the extra cost of thermal generation as compared to hydel & renewable generation. In such a situation, it is required to produce cheap electricity by installing new hydel & renewable energy projects; however, due to the present economic crisis in the country, it is difficult to attain the financial resources for hydel generation. Hence, the best strategy for the optimization of the power system is to encourage the public sector to invest and contribute to distribution loss reduction by installing DGs (Solar PV). Through their investment, they save the electric power losses and get financial benefits.

Installation of DGs (Solar PV) not only reduces the emission of greenhouse gases but also minimizes the losses of the distribution system by up to 35 % and improves the voltage drops also increases the quality of the distribution system through continuity of supply as compared to our conventional generation & distribution system.

Actual results presented in this research have shown that annual line losses of the GEPCO network for 07 feeders before DGs (Solar PV) are 11167598 KWh and voltage drops are 28.0%; after DGs (Solar PV), the losses are reduced to 7235059 KWh and voltage drops are 24.5 %. In short, 3932539 KWh units can be saved, and voltage drop can be reduced up to 3.5%. If we take the average unit rate as PKR 40.00/KWh, then we can save 157.3 Million PKR/Anum for these 07 No feeders if GEPCO implements this and if we enhance our research area till the other rural 137 feeders mentioned earlier in Chapter 04, then 3078.62 Million PKR can be saved through the installation of DGs (Solar PV) in our distribution system.

In light of the results obtained from the loss analysis and economic analysis, it is recommended that GEPCO and all the distribution companies in Pakistan should place the DGs (Solar PV) in their distribution system to achieve the goal of a highly efficient energy system in the country.

## Acknowledgement

I would like to express sincere gratitude to my parent department GEPCO and faculty of Electrical department under University of Sialkot for their guidance, motivations, ideas, and immense knowledge during the research process. They are always very helping in solving my reservations/ confusions and guided me to the completion of this study. On top of that, they are tolerant and progressive persons. This thesis could not be completed, without their continuous guidance, encouragement and support.

## References

- [1] M. C. V Suresh, J. B. Edward, "A hybrid algorithm based optimal placement of DG units for loss reduction in the distribution system", *Applied Soft Computing*, vol. 91, 106191–106191, 2020, doi:https://doi.org/10.1016/j.asoc.2020.106191.
- [2] R.-E. Precup, T. Kamal, S. Z. Hassan, *Solar Photovoltaic Power Plants*, Springer Singapore, 2019.
- [3] R.-E. Precup, T. Kamal, S. Z. Hassan, *Advanced Control and Optimization Paradigms for Wind Energy Systems*, Springer Singapore, 2019.
- [4] J. L. Holecek et al., "A Global Assessment: Can Renewable Energy Replace Fossil Fuels by 2050?", *Sustainability (Switzerland)*, vol. 14, no. 8, 1–22, 2022, doi:10.3390/su14084792.
- [5] Q. Wang, R. Li, G. He, "Research status of nuclear power: A review", *Renewable and Sustainable Energy Reviews*, vol. 90, no. February, pp. 90–96, 2018, doi:10.1016/j.rser.2018.03.044.
- [6] W. Wan et al., "Analyzing the Impact of Streamflow Drought on Hydroelectricity Production: A Global-Scale Study", *Water Resources Research*, vol. 57, no. 4, 2021, doi:10.1029/2020WR028087.
- [7] H. Hou et al., "Exploring the Role of Fossil Fuels and Renewable Energy in Determining Environmental Sustainability: Evidence from OECD Countries", *Sustainability (Switzerland)*, vol. 15, no. 3, 2023, doi:10.3390/su15032048.
- [8] N. Abas et al., "Techno-Economic Feasibility Analysis of 100 MW Solar Photovoltaic Power Plant in Pakistan", *Technology and Economics of Smart Grids and Sustainable Energy*, vol. 7, no. 1, 2022, doi:10.1007/s40866-022-00139-w.
- [9] B. Sultana et al., "Review on reliability improvement and power loss reduction in distribution system via network reconfiguration", *Renewable & Sustainable Energy Reviews*, vol. 66, pp. 297–310, 2016, doi:https://doi.org/10.1016/j.rser.2016.08.011.
- [10] Z. Nishtar, J. Afzal, "History of Emerging Trends of Renewable Energy for Sustainable Development in Pakistan."
- [11] G. M. Mufti et al., "Comparative analysis of the effects of renewable energy integration on the utility grid system", *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 1–5, 2018, doi:10.1109/ICOMET.2018.8346415.
- [12] P. R. Satpathy, R. Sharma, "Power loss reduction in partially shaded PV arrays by a static SDP technique", *Energy*, vol. 156, 569–585, 2018, doi:https://doi.org/10.1016/j.energy.2018.05.131.
- [13] G. M. Mufti et al., "Evaluating the Issues and Challenges in Context of the Energy Crisis of Pakistan", *Indian Journal of Science and Technology*, vol. 9, no. 36, 1–7, 2016, doi:10.17485/ijst/2016/v9i36/102146.
- [14] M. Arif et al., "Solar-Biogas Microgrid: A Strategy for

Development of Rural Communities in Pakistan", *SSRN Electronic Journal*, 2022, doi:10.2139/ssrn.4039931.

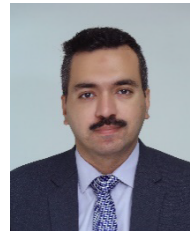
- [15] S. Giannelos et al., "Modelling Smart Grid Technologies in Optimisation Problems for Electricity Grids", *Energies*, vol. 16, no. 13, 2023, doi:10.3390/en16135088.
- [16] M. Farrokhhabadi et al., "Microgrid Stability Definitions, Analysis, and Examples", *IEEE Transactions on Power Systems*, vol. 35, no. 1, 13–29, 2020, doi:10.1109/TPWRS.2019.2925703.
- [17] N. Hatziaargyriou et al., "Definition and Classification of Power System Stability - Revisited & Extended", *IEEE Transactions on Power Systems*, vol. 36, no. 4, 3271–3281, 2021, doi:10.1109/TPWRS.2020.3041774.
- [18] U. Shahzad, "A Review of Challenges for Security - Constrained Transmission Expansion Planning", *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, no. 24, pp. 21–30, 2021.
- [19] R. S. Rao et al., "Power Loss Minimization in Distribution System Using Network Reconfiguration in the Presence of Distributed Generation", *IEEE Transactions on Power Systems*, vol. 28, no. 1, 317–325, 2013, doi:https://doi.org/10.1109/tpwrs.2012.2197227.
- [20] K. Mahmoud, N. Yorino, A. Ahmed, "Optimal Distributed Generation Allocation in Distribution Systems for Loss Minimization", *IEEE Transactions on Power Systems*, vol. 31, no. 2, 960–969, 2016, doi:https://doi.org/10.1109/tpwrs.2015.2418333.
- [21] B. Ismail et al., "A Comprehensive Review on Optimal Location and Sizing of Reactive Power Compensation Using Hybrid-Based Approaches for Power Loss Reduction, Voltage Stability Improvement, Voltage Profile Enhancement and Loadability Enhancement", *IEEE Access*, vol. 8, pp. 222733–222765, 2020, doi:https://doi.org/10.1109/access.2020.3043297.
- [22] A. A. A. El-Ela et al., "Optimal capacitor placement in distribution systems for power loss reduction and voltage profile improvement", *IET Generation Transmission & Distribution*, vol. 10, no. 5, 1209–1221, 2016, doi:https://doi.org/10.1049/iet-gtd.2015.0799.
- [23] A. Ehsan, Q. Yang, "Optimal integration and planning of renewable distributed generation in the power distribution networks: A review of analytical techniques", *Applied Energy*, vol. 210, pp. 44–59, 2018, doi:https://doi.org/10.1016/j.apenergy.2017.10.106.
- [24] A. Bayat, A. Bagheri, R. Noroozian, "Optimal siting and sizing of distributed generation accompanied by reconfiguration of distribution networks for maximum loss reduction by using a new UVDA-based heuristic method", *International Journal of Electrical Power & Energy Systems*, vol. 77, 360–371, 2016, doi:https://doi.org/10.1016/j.ijepes.2015.11.039.

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).



**Usman Asghar** has done his bachelor degree from University of Engineering and Technology in 2018. He has done his master's degree from University of Sialkot in 2014

His research interests include Load flow studies of Distribution power and its Utilization, Renewable Power Generation System and Distributed Power Management.



**Syed Zulqadar Hassan** received the PhD Degree from School of Electrical Engineering, Chongqing University, China in 2018. His active research includes modelling, control, designing, techno-economic analysis and energy management of alternative energy

power generation sources and microgrids with multiple power generation sources and electrical load management (demand response) for smart grid and microgrid. Till date he has published more than 65 publications in well reputed journals and in IEEE/Springer Nature international conferences on the application of fuzzy logic, artificial intelligence, neural networks, neuro-fuzzy, optimal control, adaptive control in renewable and energy storage systems (solar photovoltaic, wind, fuel cells, hydro, electric charging station, hydrogen, super-capacitor, battery, etc). Recently, he has edited two books titled 1) Solar Photovoltaic Power Plants: Advanced Control and Optimization Techniques, and 2) Advanced Control and Optimization Paradigms for Wind Energy Systems, both have been published by Springer Nature.



**Muhammad Ahmad** born in 1991 in Pakistan, completed his B.Sc. in Electrical Engineering with a specialization in Power System Engineering from the Swedish College of Engineering and Technology (SCET), Rahim Yar Khan, Pakistan. He

received scholarships from Shanghai Jiao Tong University (SJTU), China, for his M.Sc. and Ph.D. in Electrical Engineering, focusing on electrical drive systems and fault-current limiters (FCL) for VSC-HVDC transmission systems. He has published several high-impact papers in prestigious journals and conferences. Currently, he is a postdoctoral research fellow at the Interdisciplinary Research Center for Sustainable Energy Systems at King Fahd University of Petroleum and Minerals, Saudi Arabia. His research interests include, but not limited to, power electronics, motor drives, FCLs, hybrid circuit breakers for VSC-HVDC, renewable energy assessment, policies, and power markets.



**Arsalan Masood** received the M.S. degree from the Department of Electrical Engineering, COMSATS University Islamabad, Islamabad, Pakistan in 2016. He has done a Ph.D. degree in the School of Electrical and Electronic Engineering, North China

Electric Power University, Beijing, China. His research interests include distributed energy resource integration with a focus on electric vehicles, DER flexibilities and electricity markets.



**Muhammad Naqi Raza** has done his bachelor degree from University of Gujrat in 2018. He has done his master's degree from University of Sialkot in 2014

His research interests include distributed energy resources, hybrid power systems and machine learning optimization techniques.



**Tariq Kamal** holds doctorates in Energy and Sustainable Engineering from the University of Cadiz, Spain, and the Technical University of Munich, Germany, as well as a doctorate in Electrical Engineering from Sakarya University, Turkey. His

research interests encompass advanced intelligent control techniques, renewable energy systems, electric vehicles and their integration into power systems, distributed generation, smart grid applications, and the use of signal processing in power systems. Currently, he serves as an Assistant Professor of Electrical Engineering and the head of the Power Electronics and Control Group at the University of Vaasa, Finland. He is the author or co-author of more than 100 papers published in various international scientific journals and conference proceedings. Dr. Kamal has been involved in major collaborative projects across the globe, including in the USA, Germany, Belgium, Italy, Spain, Turkey, Australia, China, the UK, Finland, Sweden, and Estonia. He is also a regular reviewer for many leading international journals, including IEEE Transactions on Industrial Electronics and Applied Energy.

# The Dual Impact of AI in Clinical Trials: Perspective

Muhammad Yaqub, Lan He

School of Biomedical Sciences, Hunan University, Changsha, 410000, P.R China

\*Corresponding author: Muhammad Yaqub, Hunan University, [myaqub@hnu.edu.cn](mailto:myaqub@hnu.edu.cn)

**ABSTRACT:** The use of artificial intelligence in clinical trials opens the way for a period of transformation in which the potential to enhance efficiency, precision, and scope in clinical investigation is enormous. In this perspective, the promise and perils of AI regarding clinical trials are critically reviewed. On one hand, it's where AI can really make some revolutionary changes to the most critical aspects of trial design and execution—like patient recruitment, data management, and predictive analytics—which are now adaptive and more driven by data; on the other hand, AI applied in clinical trials also brings considerable problems related to data integrity, ethical considerations, and regulatory compliance. Such potential of AI to further biases, break patient confidences, and exacerbate already wide inequities in healthcare raises the need for vigilant oversight. As AI is rapidly evolving, so too are principles that guide transparency, fairness, and ethical rigors that guide their application in clinical trials. This work presents a case for strong AI frameworks that are subject to firm validation and ethical scrutiny, which will ensure that the benefits of AI are realized with reduced risks associated with it. If the field goes down this road, AI integration in clinical trials is going to be the real catalyst for innovation, which could translate into achieving better patient outcomes and expanding frontiers for medical science.

**KEYWORDS:** Artificial Intelligence, Clinical Trials, Patient Outcomes, Predictive Analytics, Healthcare Inequities

## 1. Introduction

One of the most extreme developments in medical research is the use of AI in clinical trials. Already available are emerging AI technologies offering enormous potential for efficiency, accuracy, and scalability in clinical trials.[1–3]. That promise is wrapped in a series of major challenges and key ethical concerns. There are many risks associated with implementing AI within clinical trials. Serious issues of data privacy, bias in algorithms, transparency, and the possible increase of inequities in health characterize a very difficult area of navigation. It also brings along several questions on the level of regulatory compliance, validity of the AI-driven outcomes, and whether healthcare is prepared to absorb full potential for AI while protecting the rights and well-being of the patient [4,5]. As summarized in Table 1, the literature highlights the transformative impact of AI on clinical trials, particularly in improving patient recruitment efficiency, enhancing data management, and addressing ethical and privacy concerns. These studies underscore both the potential benefits and the challenges that need to be navigated to fully integrate AI into clinical research.

It is therefore advanced in this paper that the dual-edged potential of AI in the context of clinical trials demands an appropriate and integrative perspective of the optimistic possibilities and potential risks concomitant with it. Current advancements in this area, related ethical considerations, and regulatory challenges were looked at in order to provide a balanced view in respect of the optimization of clinical trials using AI and the critical issues that have to be tackled for its successful integration. It contributes to the discussion on responsible and effective application of AI about medical research, and subsequently toward an innovation-sound and ethical future for AI-aided clinical trials. Figure 1 illuminating the promising role of AI in healthcare.

Table 1: Key Literature on the Integration of Artificial Intelligence in Clinical Trials

| Referen<br>ce | Year | Title                | Key<br>Findings                             | Relevance<br>to AI in<br>Clinical<br>Trials |
|---------------|------|----------------------|---------------------------------------------|---------------------------------------------|
| [6]           | 2019 | High-performan<br>ce | AI has the<br>potential to<br>significantly | Discusses<br>the overall<br>potential of    |



|      |      |                                                                      |                                                                                                                                     |                                                                                                      |
|------|------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
|      |      | medicine: the convergence of human and artificial intelligence       | enhance the accuracy, efficiency, and personalization of healthcare, including in clinical trials.                                  | AI in healthcare, highlighting its transformative impact on clinical trials.                         |
| [7]  | 2020 | The future of digital health with federated learning                 | Federated learning offers a way to leverage AI while preserving patient data privacy, a critical aspect of clinical trials.         | Provides insights into maintaining data privacy in AI-driven clinical trials, a key ethical concern. |
| [8]  | 2019 | Optimizing patient recruitment with AI                               | AI can streamline patient recruitment by analyzing electronic health records to identify candidates more efficiently.               | Focuses on how AI can address the significant challenge of patient recruitment in clinical trials.   |
| [9]  | 2020 | International evaluation of an AI system for breast cancer screening | Demonstrates the accuracy of AI in medical imaging, with potential applications in clinical trial monitoring and outcome prediction | Illustrates the practical applications of AI in diagnostic processes relevant to clinical trials.    |
| [10] | 2021 | Overview of deep learning applications in medical image analysis     | Reviews the state-of-the-art deep learning methods in medical image analysis, highlighting                                          | Provides a comprehensive review of AI applications in medical imaging, relevant for trials           |

|      |      |                                                                             |                                                                                                                                        |                                                                                                                 |
|------|------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|      |      |                                                                             | their potential in disease diagnosis and clinical trials.                                                                              | involving imaging-based outcomes.                                                                               |
| [11] | 2020 | Ethical considerations in the deployment of AI in healthcare                | Discusses the ethical implications of AI in healthcare, including issues of bias, transparency, and accountability.                    | Essential for understanding the ethical challenges AI presents in the clinical trial context.                   |
| [12] | 2017 | Dermatologist-level classification of skin cancer with deep neural networks | AI achieved dermatologist-level accuracy in skin cancer diagnosis, suggesting AI's potential to improve diagnostic accuracy in trials. | Demonstrates the effectiveness of AI in diagnostics, relevant for trials focusing on dermatological conditions. |
| [13] | 2017 | Artificial intelligence in healthcare : past, present, and future           | Explores the development of AI in healthcare and its potential future applications, including clinical trials.                         | Provides historical context and future outlook on AI's role in clinical trials.                                 |
| [14] | 2019 | The role of artificial intelligence in precision medicine                   | AI enables precision medicine approaches in clinical trials, allowing for more tailored treatment interventions.                       | Highlights how AI can enhance the personalization of clinical trials through precision medicine.                |
| [15] | 2018 | How artificial intelligence is changing                                     | AI accelerates the drug discovery                                                                                                      | Discusses AI's role in the early stages of clinical                                                             |

|  |  |                |                       |                                                     |
|--|--|----------------|-----------------------|-----------------------------------------------------|
|  |  | drug discovery | process, including in | trials, particularly in drug discovery and testing. |
|--|--|----------------|-----------------------|-----------------------------------------------------|

## 2. The Impact of AI in Medical Imaging

The effect of AI on clinical trials, even more so in the analysis of medical imaging, goes deep, as it helps in improving image analysis, smoothing trial workflows, and enhancing diagnostic precision. Speaking precisely, some of the ways AI can modify medical imaging in clinical trials include:

### 2.1. Automated Image Analysis and Interpretation

Medical imaging modalities, including but not limited to MRI, CT, and PET, are increasingly used in clinical trials for assessment of diseases process, treatment efficacy assessment, or biomarkers evaluation [16,17]. Traditional radiologist interpretation of images is very time-consuming and may be variable. Algorithms based on AI, especially those using deep learning techniques, can be programmed to look at medical imagery for patterns indicating lesions or other abnormalities that may well be too slight for the human eye to recognize. For example:

- AI-powered tools in an oncology trial can assist by automatic detection and quantification of tumor size, shape, and growth patterns in MRI or CT images, improving the assessment of treatment responses.
- AI in cardiology can analyze echocardiograms or cardiac MRIs to measure heart function, such as

ejection fraction, wall motion, and other variables that provide insight into drug effects on cardiovascular health.

AI-driven automation decreases interpretation time for images, enhances consistency in the review of images, and decreases the probability of human-related errors. The outcome is speedier trial results and more valid results, as the imaging biomarkers could be studied more precisely.

### 2.2. Enhanced Image-Based Biomarker Discovery

Biomarkers are important in a clinical trial in monitoring disease process or treatment response [18]. For imaging, this could involve the detection of slight structural or functional alterations in tissues, which are indicative of the disease. Artificial Intelligence has this phenomenal capability to discover new imaging biomarkers by analyzing huge datasets, with subtle patterns that may evade human eyes [19]. For instance:

- So far, these models have been applied in neurology for brain MRI reviewing, considering a number of biomarkers for various diseases, such as Alzheimer's disease and multiple sclerosis [20], which are grounded on different brain volume changes, cortical thickness, and white matter integrity.
- AI will find the radiomic features in oncology, such as microscopic variations either in tumor textures or shapes related to variations in patient outcomes, allowing early treatment efficacy predictions.

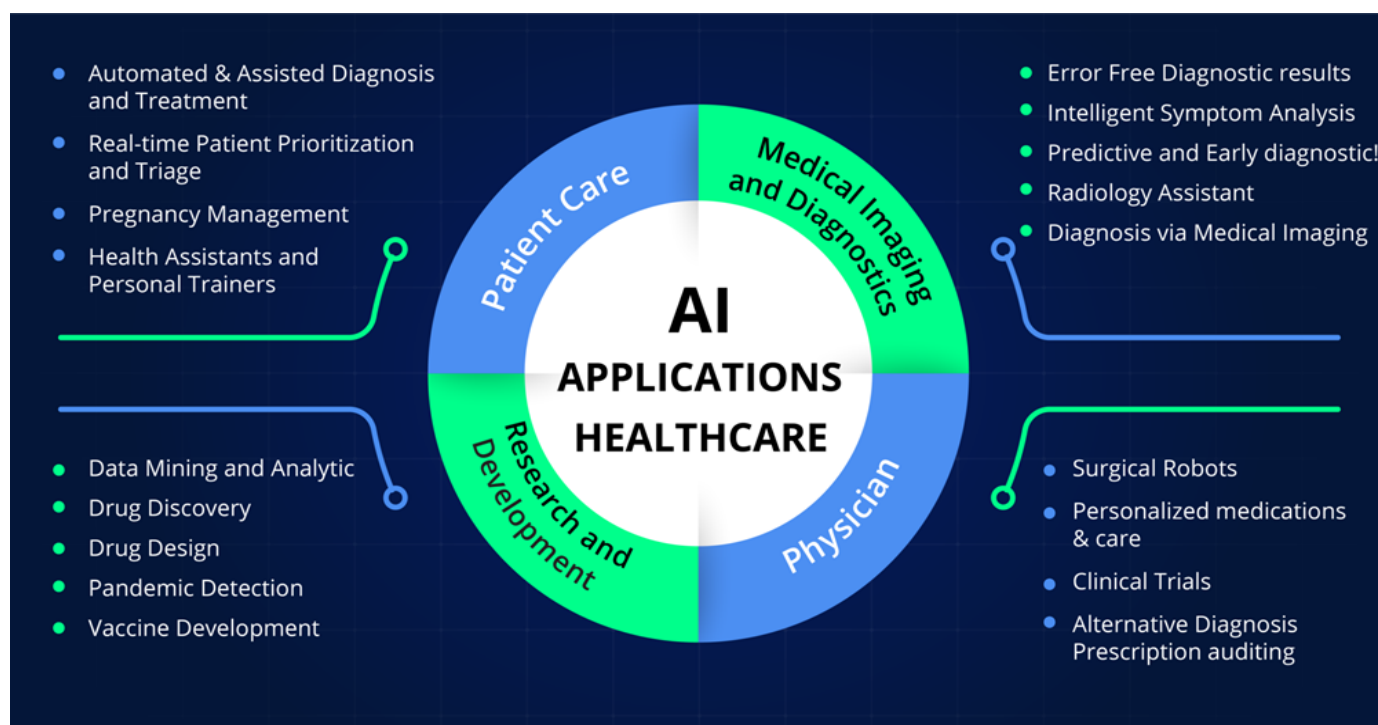


Figure 1: The promising role of AI in Healthcare

AI, therefore, applies to an improved ability in detection and quantification of complex biomarkers from imaging information, which enables better prediction of the progression of diseases and responses to pharmacological treatments. Consequently, this process has encouraged the formulation of more effective therapies and personalized ones during clinical trials, out of which comes the shortening of timelines for bringing efficacious therapies to market.

### *2.3. Real-Time Image Monitoring in Adaptive Trials*

AI represents the backbone of adaptive clinical trials, most seen in real-time image monitoring during trials, for which imaging is an enabler of response assessment in patients and modifications to trials [21]. Some decisions regarding dosage, continuing or modifying treatment, or even cohort adjustments depend mostly on scheduled reviews. AI can give data-driven insights at the exact moment by analyzing real-time imaging results. For example, in oncology trials, the AI system can track day-to-day changes in tumor size, density, and vascularity from MRI or CT scans continuously, which, based on a poor response of a patient, clinicians can alter the regimen of treatment immediately. This will save precious time in making critical adjustments, therefore offering the best possible care for a patient. AI-driven image analysis also cuts down on human error; hence, allowing more consistent and objective assessments across large cohorts of patients. AI makes clinical trials more flexible, meaning that faster and more precise assessments will enable the creation of better treatments.

### *2.4. AI in Image-Based Inclusion/Exclusion Criteria*

It often happens that medical imaging itself is crucial for the inclusion or exclusion of patients in clinical trials, depending on whether the extent of the disease, organic damage, or size of lesions meets the particular inclusion or exclusion criteria. Conventionally, radiologists would review such criteria manually by going through the imaging data; this is a very time-consuming process and may be prone to inaccuracies and inconsistencies. Artificial Intelligence solves this through automation of involved processes. It ensures the screening of the patients systematically and precisely based on the eligibility criteria brought about by the trial in mention [22].

For example, in neurological clinical trials, algorithms in AI can independently analyze MRI images to look for symptoms of brain atrophy or even lesions that will determine if a patient can be included or not. Similarly, AI in oncology research is able to evaluate the

dimensions and dissemination of tumors, classifying patients into the stages of investigation accordingly. This automation simplifies the process of screening, enhances the accuracy in patient selection, and thereby accelerates participants' recruitment, which has been a major bottleneck in many clinical trials.

### *2.5. Improved Patient Monitoring through Longitudinal Imaging*

Longitudinal imaging [23] is very often necessary in many clinical trials, especially those that target chronic or progressive diseases; this usually requires the repeated scanning of patients over time to monitor changes in disease progression or therapeutic effects. AI enhances this process by analyzing sequential imaging data and pointing out subtle changes that may pass undetected by the human eye. For example, in neurodegenerative disease trials, AI can quantify the change in brain volume between time points to give early signs of disease progression or response to therapy, while in oncology trials, the rate of tumor shrinkage or detection of new metastases in follow-up scans from AI can continuously provide feedback on treatment efficacy. The potential to automatically analyze complex imaging data over long periods ensures increased precision in monitoring, allowing for adjustments in trials based on real patient responses and therefore enabling rapid and true assessments of the efficacy of drugs.

### *2.6. Reducing Variability in Imaging Interpretations*

One major challenge facing clinical trials involving imaging modalities is the variation in the interpretation of the same image by different radiologists. Such variability leads to heterogenous data that might affect the outcome of such research. Artificial intelligence applications overcome this problem by applying uniform criteria to all image analyses, hence enabling uniform interpretation of images irrespective of the trial site or the personnel involved.

While artificial intelligence systems can, for example, measure such characteristics of lesions objectively for conditions like multiple sclerosis or cancers where the quantity and dimensions of lesions are a primary critical endpoint in clinical trials on all subjects. This permits a reduction of inter-reader variability and thus provides an assessment platform that is both standardized and reliable. The consistency of image reading is particularly essential in multisite clinical trials, where the results of image reading coming from different sites should be comparable. By mitigating the variability of humans,

artificial intelligence enhances the robustness and reliability of trial data, leading to a more exact conclusion.

### 2.7. AI for Enhanced Image-Guided Drug Delivery

The use of imaging in delivering drugs to a specific part of the body during most clinical targeted therapies, especially in cancer treatment, is critical. Artificial intelligence enhances the precision in such analyses of image data and hence could allow therapeutic agents to reach the sites with greater accuracy. The examples are that AI, in radiotherapy research, can analyze CT or MRI scans to delineate tumor margins with high precision so that radiation is delivered onto cancerous tissues while sparing other healthy ones. For example, in trials with nanoparticle or antibody-drug conjugates, AI can aid in determining optimum delivery sites and/or real-time drug dispersion with companion imaging techniques like PET or SPECT. Greater precision reduces the risk of unwanted off-target effects, improves the overall safety profile of these therapeutic interventions, and enhances the possibility of successful realization of the intended outcomes of the therapeutic interventions themselves. While AI-driven imaging guidance in drug delivery serves the dual purpose of enhancing effectiveness, the most important part is that it optimizes trial protocols by enhancing efficiency and productivity within clinical research [24].

## 3. Case Studies

The following are some case studies that give an idea of the realistic implementation of AI in clinical trials. It underlines and identifies real practical examples in order to explain exactly how AI impacted different stages of clinical research.

### 3.1. IBM Watson for Drug Discovery – Accelerating Cancer Research

IBM Watson for Drug Discovery has been employed by various pharmaceutical companies and research institutions to accelerate the identification of potential therapeutic targets and biomarkers for diseases like cancer. Working with the Barrow Neurological Institute, Watson [25] uncovered five new ALS-related gene candidates in less than two months' work that, if done by human researchers, would have taken years. Scanning through thousands of scientific papers and clinical trial records, AI was able to quickly create links between genes and ALS, accelerating the pathway to finding new medications.

The AI-driven literature and data mining of Watson reduced the time it took to sift through datasets that were

too complex; this hastened the early phases of clinical trials and hypothesis generation. This case underlines the capability of AI in manipulating large volumes of unstructured data, hence reinforcing trial design and biomarker identification, especially in complex diseases like ALS and cancer.

### 3.2. Tempus – Personalized Oncology Trials

Tempus is a Chicago-based technology company that uses AI to study clinical and molecular data to personalize cancer treatment. Its platform collates clinical data, including the genetic profile of patients, in order to match them with suitable clinical trials.

Tempus [26] has partnered with the University of Chicago Medicine to incorporate its AI platform into clinical trial matching at the hospital. In return, it analyzes the genomic sequencing data and clinical records to identify appropriate clinical trials for cancer patients and help match the right patients into the relevant oncology trials. This reduced the time taken by the system in matching patients with trials, while the trials the patients were being subjected to were more accurate. AI-driven patient matching works to improve enrollment rates, normally bottlenecks to oncology research. Additionally, this will enable the improvement of prospects for therapeutic success on account of the closer genetic profile alignment of a patient with trial parameters for more tailored and effective treatments.

### 3.3. Medidata – AI for Virtual Clinical Trial

Medidata is a company focused on cloud-based solutions for life sciences, having come up with an AI platform that allows the implementation of virtual clinical trials. The approach thereby minimizes physical visits and allows for remote data collection, which applies to rare diseases or pandemics, such as COVID-19. Medidata [27] conducted virtual trials of a candidate COVID-19 vaccine by implementing AI for remote monitoring of patient data. The AI-enabled platform collected data from wearables and patient-reported outcomes, while making the processing easier with a reduced administrative burden. This was interpreted as monitoring patients in real-time, without asking patients to travel to trial sites.

Virtual trials by Medidata removed geographical boundaries and allowed more patients to participate in parts of the world where access to clinical trial sites was at a premium. The integration of data from wearables enabled by AI also improved monitoring of patient health metrics, thus allowing quicker safety assessments and flexibility in the management of trials. That has been



particularly useful during the pandemic for running trials in a decentralized manner and finds wider application now.

### 3.4. AI in Adaptive Clinical Trials – Novartis and Microsoft

Novartis has allied with Microsoft to use AI in the design of adaptive clinical trials where real-time changes can be made to trial protocols based on intermediate outcomes [28]. This becomes particularly important in oncology, where patient responses can be highly variable. AI models, developed under the partnership between Novartis and Microsoft, predicted optimal dosing levels and signals of early treatment efficacy. For instance, AI models spotted subgroups of more responsive patients during a recent breast cancer trial, allowing for adaptive changes in the protocol of this trial focused on these subgroups.

Adaptation in trials-in fact, making changes according to responses-allows for efficiency in research and safety for the patient. AI enhances that ability to dynamically alter trial parameters, reducing time and cost it takes in new treatments. For example, in the case of this AI-driven trial on breast cancer, the number of patients exposed to ineffective treatments was reduced while hastening the approval process of successful therapies.

### 3.5. Benevolent AI – Accelerating Drug Repurposing

Benevolent AI applies the power of AI to find new drug candidates and indications that find new uses for already-approved drugs [29]. It reads through biomedical data like clinical trials, patents, and scientific literature to identify new potential uses for already-approved drugs. In the COVID-19 pandemic, Benevolent AI mentioned the use of baricitinib-a rheumatoid arthritis medication-as a likely candidate against COVID-19. The AI system curbed through mountains of data and suggested that the drug could reduce the cytokine storm that happens in serious cases of COVID-19, and hence it is an ideal candidate for repurposing.

Clinical trials started for baricitinib, and it proved very beneficial for COVID-19 patients. The drug was able to garner use authorization in emergency situations from the FDA. This is just one example in which AI accelerates a process that, without AI, involves tremendous time and resources: finding new uses for existing drugs. AI analyzes cross-domain datasets, driving much higher efficiency in drug repurposing.

### 3.6. Verge Genomics – AI for ALS Clinical Trials

Verge Genomics employs AI and machine learning to map the human genome for new treatments of

neurodegenerative diseases such as ALS [30]. In collaboration with the Cedars-Sinai Medical Center, Verge has fielded its AI platform against ALS patient data and surfaced novel targets for potentially informed clinical trials. In this respect, by applying AI to identify genetic patterns, Verge can accelerate the preclinical stages and move promising candidates into clinical trials more rapidly than would have otherwise been possible. The AI platform at Verge automated target identification and shaved huge margins off ALS drug development times and costs. The rapid pace from identification to clinical trials punts on AI's power for accelerating the initial parts of neurodegenerative disease clinical research, where advances usually take so much time.

These case studies epitomize how AI can transform everything from patient recruitment and data analysis to adaptive trial designs and drug repurposing within the clinical trial space. AI-driven tools enhance clinical research speed, efficiency, and precision-enabling better outcomes in oncology, neurodegenerative diseases, and pandemic response efforts. These examples demonstrate great strides that have been taken in real-world uses where AI makes the clinical trial more efficient, personalized, and accessible.

## 4. The Promise of AI in Clinical Trials

Clinical trials powered by AI can bring about a wealth of advantages to almost flip a new leaf in medical research and treatment. This starts from the patient selection stage and takes the shapes of the analysis, monitoring, and outcome prediction for clinical trials. document.

Table 2: Summary of the Promises and Perils of AI in Clinical Trials

| Aspect                         | Promises                                                                                    | Perils                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Efficiency</b> [31]         | Streamlines data analysis and patient selection.                                            | - Over-reliance on AI could lead to overlooking nuanced clinical insights. |
| <b>Accuracy</b> [32]           | - AI models can process large large datasets, identifying patterns beyond human capability. | - Potential for bias in AI algorithms due to biased training data.         |
| <b>Cost-Effectiveness</b> [33] | - Reduces costs by automating routine tasks and improving trial design.                     | - High initial costs for AI implementation and integration.                |

|                                    |                                                                                              |                                                                                                |
|------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <b>Patient Stratification</b> [25] | - Identifies optimal patient subgroups for targeted therapies.                               | - Risk of excluding underrepresented groups, leading to inequitable outcomes.                  |
| <b>Speed</b> [34]                  | - Accelerates the timeline of trials by predicting outcomes and optimizing processes.        | - Speed at the expense of thoroughness may compromise the trial's integrity.                   |
| <b>Regulatory Compliance</b> [35]  | - Assists in meeting regulatory requirements by maintaining accurate records and analysis.   | - Regulatory bodies may struggle to keep pace with rapidly evolving AI technologies.           |
| <b>Ethical Considerations</b> [36] | - AI can help ensure ethical trial designs by identifying potential issues in advance.       | - Ethical dilemmas around data privacy, consent, and the use of AI in decision-making.         |
| <b>Interpretability</b> [37]       | - Enhances understanding of complex data through advanced analytics and visualization tools. | - Black-box nature of some AI models may hinder transparency and trust in AI-driven decisions. |

#### 4.1. Enhanced Patient Recruitment and Retention

Patient recruitment and retention are the biggest challenges to clinical trials, namely, enrolling eligible patients or participants. The traditional model of doing things relies on manual efforts, which become time-consuming, prone to mistakes, and cumbersome. AI can fast-track patient recruitment by analyzing voluminous electronic health records and other medical data for suitable candidates with greater speed and accuracy. AI Algorithms can thus be trained to provide an estimate of the patient retention probability by detecting those factors

that could influence a participant's likelihood of completing a trial, thus improving retention rates and overall success of a trial.

#### 4.2. Improve how one manages and analyzes data

Clinical trials involve huge volumes of data, from patient demographics to clinical measurements, genomic data, and image data. Management and analysis operations for this kind of data are bulky and resource intensive. AI has the potential to innovate data management through automating means of processing and analyzing big datasets to researchers for them to find out hidden patterns and insights that, otherwise, would not be evident in the use of conventional statistical methods. Through machine learning algorithms, one is able to come up with the correlations, predict the outcome, and even hypothesize new hypotheses that enable researchers to fast track the processes in research activities, thereby increasing the accuracy of results realized in trials.

#### 4.3. Personalized Medicine and Adaptive Trials

AI also deepens analysis of datasets in ways that foster the development of personalized medicine approaches within clinical trials. In this regard, AI would be useful in developing treatment trials through integrating genomic, phenotypic, and clinical data in tailoring treatments to the characteristics of the individual patient. This customization will maximize the possibilities of success of the treatment while minimizing its side effects. Moreover, AI can support adaptive designs whereby the parameters of the trial are adapted based on the results of the interim analysis. A very key implication of adaptability is running quite a lot more efficient trials whereby treatments that promise much earlier are fast-tracked and less effective de-prioritized.

#### 4.4. Real-time monitoring and predictive analytics

Clinical trials monitoring may leverage the power of AI since such real-time analysis of patient data will be useful in quickly establishing safety problems and adverse events. Besides, predictive analytics, powered by AI, will project the outcome from early patient data so that one can decide wisely. This ability is most important for the early identification of possible risks and benefits during a trial process for more effective and safer treatments.

### 5. The Perils of AI in Clinical Trials

Although the potential benefits of AI in clinical trials are huge, so are the challenges to be addressed for its ethical and effective application in this context. Figure 2 presents the major perils of AI clinical trials.

### 5.1. Data Privacy and Security Concern

The application of AI in clinical trials presupposes the collection and analysis of large amount of personal health data. This gives more rise to concerns of privacy and data security, particularly, of sensitive medical information. Ensuring AI systems are compliant with data protection regulation, such as General Data Protection Regulation in Europe is critically important. There is also the risk that AI systems might be vulnerable to cyberattacks, which could lead to a breach in patient confidentiality and the data being misused.

### 5.2. Algorithmic Bias and Fairness

AI algorithms are only as good as the data on which they have been trained. If the training data is biased or unrepresentative, it can mean that AI systems produce biased outcomes, affecting differentially certain groups of patients. This will become of major concern in clinical trials, where biased algorithms could permit unequal access to treatment or inaccurate predictions about treatment efficacy for different demographic groups. Ensuring AI systems are trained on diverse and representative datasets is critical to mitigating these risks.

### 5.3. Transparency and Explainability

Such concerns also exist with regard to the fact that most AI systems, especially those involving deep learning, are often "black boxes" for which it can be pretty difficult to understand how they came up with certain decisions or predictions. This may then cause problems during clinical trials, where maximum effort is made to understand the logic behind treatment decisions and the subsequent results as clearly as possible. In that light, it is incumbent on researchers and regulators to commence the process of developing AI systems that are not only accurate but also explainable, so that use in clinical trials is transparent and hence trustable.

### 5.4. Algorithm

The infusion of AI into clinical trials will obviously raise a new dimension of regulatory challenges since prevailing frameworks may not be fully ready to face the challenge of the complexity of AI-driven research. This will require up-to-date guidelines to be developed, taking into account the specificity connected with the AI applications, such as algorithm validation, data governance, and ethical concerns. As shown in Table 2, the integration of AI in clinical trials presents a range of promises, including enhanced precision and efficiency, alongside significant perils, such as ethical dilemmas and data privacy concerns, highlighting the need for careful consideration in its application. Also, a series of ethical questions arise from the use of AI in clinical trials about

how automation might eventually substitute human judgment in areas critical to patient care and research. The challenge would be to balance the benefits of AI with the needs for human oversight and ethical accountability.

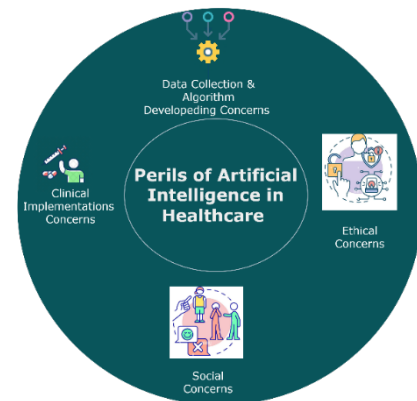


Figure 2: Perils of AI in Healthcare.

## 6. Recommendations for Future Research

1. Future research emphasis should be to enhance the interpretability and transparency of complex models, such as those dealing with deep learning, toward clinicians and regulators to instill trust in AI-driven decisions made during clinical trials.
2. Assess how AI integrates different types of data—imaging, genomics, clinical information—into one analysis that has the potential to advance personalized treatment strategies, and subsequently overall trial outcomes, for each data type.
3. Strive for models applying real-world evidence through artificial intelligence and wearables to EHRs and patient-reported outcomes to develop better generalizability and applicability of findings from clinical trials.
4. Design a framework directed towards the elimination of bias in artificial intelligence models in order to achieve equality regarding age, gender, and ethnicity. Further research works shall, therefore, be channeled towards the improvement of training datasets to make the AI assessment representative and inclusive.
5. The development of the AI framework should focus on international legislation requirements. Research is to be directed to make AI systems used in trials transparent and auditable, which again justifies that privacy and safety regulations from organizations such as the FDA and EMA are met.

## 7. Conclusion

Artificial intelligence might be very instrumental in changing clinical trials into medical research with the potential advantages of efficiency, accuracy, and scalability. Such benefits are hedged with major challenges that need to be navigated with care for

ensuring ethical and effective applications of AI. It is in the research community's best interest to address issues of data privacy, algorithm bias, transparency, and regulation to realize the power of AI in moving clinical trials forward without putting a patient's rights and well-being in jeopardy. In other words, AI in clinical research has a future if it is able to strike proper balance between innovation and ethical responsibility in ensuring that this technology gets used to its fullest for the betterment of all.

### Conflict of Interest

The authors declare no conflict of interest.

### References

- [1] S. Askin, D. Burkhalter, G. Calado, S. El Dakrouni, Artificial Intelligence Applied to clinical trials: opportunities and challenges, *Health and Technology*, vol. 13, no. 2, 2023, doi:10.1007/s12553-023-00738-2.
- [2] S. Piantadosi, Clinical trials: a methodologic perspective, John Wiley & Sons, 2024.
- [3] H. Saeed, I. El Naqa, Artificial intelligence in clinical trials, Springer: 453–501, 2022.
- [4] B.C. Stahl, Artificial Intelligence for a Better Future An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies, 2021.
- [5] W.H. Organization, Ethics and governance of artificial intelligence for health: large multi-modal models. WHO guidance, World Health Organization, 2024.
- [6] E.J. Topol, High-performance medicine: the convergence of human and artificial intelligence, *Nature Medicine*, vol. 25, no. 1, 2019, doi:10.1038/s41591-018-0300-7.
- [7] N. Rieke, J. Hancox, W. Li, F. Milletari, H.R. Roth, S. Albarqouni, S. Bakas, M.N. Galtier, B.A. Landman, K. Maier-Hein, S. Ourselin, M. Sheller, R.M. Summers, A. Trask, D. Xu, M. Baust, M.J. Cardoso, "The future of digital health with federated learning," *Npj Digital Medicine*, vol. 3, no. 1, 2020, doi:10.1038/s41746-020-00323-1.
- [8] M. Woo, "Trial by artificial intelligence," *Nature*, vol. 573, no. 7775, pp. S100–S102, 2019.
- [9] S.M. McKinney, M. Sieniek, V. Godbole, J. Godwin, N. Antropova, H. Ashrafian, T. Back, M. Chesus, G.C. Corrado, A. Darzi, M. Etemadi, F. Garcia-Vicente, F.J. Gilbert, M. Halling-Brown, D. Hassabis, S. Jansen, A. Karthikesalingam, C.J. Kelly, D. King, J.R. Ledsam, D. Melnick, H. Mostofi, L. Peng, J.J. Reicher, B. Romera-Paredes, R. Sidebottom, M. Suleyman, D. Tse, K.C. Young, et al., "International evaluation of an AI system for breast cancer screening," *Nature*, vol. 577, no. 7788, 2020, doi:10.1038/s41586-019-1799-6.
- [10] T. Dhar, N. Dey, S. Borra, R.S. Sherratt, "Challenges of Deep Learning in Medical Image Analysis—Improving Explainability and Trust," *IEEE Transactions on Technology and Society*, vol. 4, no. 1, 2023, doi:10.1109/tts.2023.3234203.
- [11] S. Gerke, T. Minssen, G. Cohen, Ethical and legal challenges of artificial intelligence-driven healthcare, 2020, doi:10.1016/B978-0-12-818438-7.00012-5.
- [12] A. Esteva, B. Kuprel, R.A. Novoa, J. Ko, S.M. Swetter, H.M. Blau, S. Thrun, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, 2017, doi:10.1038/nature21056.
- [13] F. Jiang, Y. Jiang, H. Zhi, Y. Dong, H. Li, S. Ma, Y. Wang, Q. Dong, H. Shen, Y. Wang, Artificial intelligence in healthcare: Past, present and future, *Stroke and Vascular Neurology*, vol. 2, no. 4, 2017, doi:10.1136/svn-2017-000101.
- [14] T.M. Maddox, Clinical Decision Support in Statin Prescription - What We Can Learn from a Negative Outcome, *JAMA Cardiology*, vol. 6, no. 1, 2021, doi:10.1001/jamacardio.2020.4756.
- [15] N. Fleming, "How artificial intelligence is changing drug discovery," *Nature*, vol. 557, no. 7707, 2018, doi:10.1038/d41586-018-05267-x.
- [16] F.Y. Chiu, Y. Yen, Imaging biomarkers for clinical applications in neuro-oncology: current status and future perspectives, *Biomarker Research*, vol. 11, no. 1, 2023, doi:10.1186/s40364-023-00476-7.
- [17] M. Yaqub, F. Jinchao, M.S. Zia, K. Arshid, K. Jia, Z.U. Rehman, A. Mehmood, "State-of-the-art CNN optimizer for brain tumor segmentation in magnetic resonance images," *Brain Sciences*, vol. 10, no. 7, 2020, doi:10.3390/brainsci10070427.
- [18] K.D. Davis, N. Aghaeepour, A.H. Ahn, M.S. Angst, D. Borsook, A. Brenton, M.E. Burczynski, C. Crean, R. Edwards, B. Gaudilliere, G.W. Hergenroeder, M.J. Iadarola, S. Iyengar, Y. Jiang, J.T. Kong, S. Mackey, C.Y. Saab, C.N. Sang, J. Scholz, M. Segerdahl, I. Tracey, C. Veasley, J. Wang, T.D. Wager, A.D. Wasan, M.A. Pellemounter, "Discovery and validation of biomarkers to aid the development of safe and effective pain therapeutics: challenges and opportunities," *Nature Reviews Neurology*, vol. 16, no. 7, 2020, doi:10.1038/s41582-020-0362-2.
- [19] A. Prelaj, V. Miskovic, M. Zanitti, F. Trovo, C. Genova, G. Viscardi, S.E. Rebuzzi, L. Mazzeo, L. Provenzano, S. Kosta, M. Favali, A. Spagnoletti, L. Castelo-Branco, J. Dolezal, A.T. Pearson, G. Lo Russo, C. Proto, M. Ganzinelli, C. Giani, E. Ambrosini, S. Turajlic, L. Au, M. Koopman, S. Delalogue, J.N. Kather, F. de Braud, M.C. Garassino, G. Pentheroudakis, C. Spencer, et al., Artificial intelligence for predictive biomarker discovery in immuno-oncology: a systematic review, *Annals of Oncology*, vol. 35, no. 1, 2024, doi:10.1016/j.annonc.2023.10.125.
- [20] B. Rossi, B. Santos-Lima, E. Terrabuo, E. Zenaro, G. Constantini, Common Peripheral Immunity Mechanisms in Multiple Sclerosis and Alzheimer's Disease, *Frontiers in Immunology*, vol. 12, 2021, doi:10.3389/fimmu.2021.639369.
- [21] E.T. Hébert, C.K. Ra, A.C. Alexander, A. Helt, R. Moisiuc, D.E. Kendzor, D.J. Vidrine, R.K. Funk-Lawler, M.S. Businelle, "A mobile just-in-time adaptive intervention for smoking cessation: Pilot randomized controlled trial," *Journal of Medical Internet Research*, vol. 22, no. 3, 2020, doi:10.2196/16907.
- [22] S. Prabhu, K. Prasad, A. Robels-Kelly, X. Lu, AI-based carcinoma detection and classification using histopathological images: A systematic review, *Computers in Biology and Medicine*, vol. 142, 2022, doi:10.1016/j.cmpbiomed.2022.105209.
- [23] W.M. van Oostveen, E.C.M. de Lange, "Imaging techniques in Alzheimer's disease: a review of applications in early diagnosis and longitudinal monitoring," *International Journal of Molecular Sciences*, vol. 22, no. 4, 2110, 2021.
- [24] W. He, Z. Zhang, Y. Luo, R.T.K. Kwok, Z. Zhao, B.Z. Tang, Recent advances of aggregation-induced emission materials for fluorescence image-guided surgery, *Biomaterials*, vol. 288, 2022, doi:10.1016/j.biomaterials.2022.121709.
- [25] A. Smart, P. Martin, M. Parker, Tailored medicine: Whom will it fit? The ethics of patient and disease stratification, *Bioethics*, vol. 18, no. 4, 2004, doi:10.1111/j.1467-8519.2004.00400.x.
- [26] Z. Chaudhary, C. Lungren, A. Shah, "Tempus: Reshaping the Landscape of Cancer Care with Revolutionary Artificial



Intelligence," *Teens in Health AI in Healthcare Summer 2023 Journal* *Teens in Health Is a Teen Led Organization That Aims to Provide Open Access to Biological Research Skill Development through Researching and Writing Articles*, 148, 2023.

- [27] K.H. Zou, C. Vigna, A. Talwai, R. Jain, A. Galaznik, M.L. Berger, J.Z. Li, The Next Horizon of Drug Development: External Control Arms and Innovative Tools to Enrich Clinical Trial Data, *Therapeutic Innovation and Regulatory Science*, vol. 58, no. 3, 2024, doi:10.1007/s43441-024-00627-4.
- [28] D. Hartl, V. de Luca, A. Kostikova, J. Laramie, S. Kennedy, E. Ferrero, R. Siegel, M. Fink, S. Ahmed, J. Millholland, A. Schuhmacher, M. Hinder, L. Piali, A. Roth, Translational precision medicine: an industry perspective, *Journal of Translational Medicine*, vol. 19, no. 1, 2021, doi:10.1186/s12967-021-02910-6.
- [29] M. Shanmuga Sundari, H.R. Penthala, A. Mogullapalli, M.M. Ammangatambu, "AI-Based Personalized Drug Treatment," *Artificial Intelligence and Machine Learning in Drug Design and Development*, 369–406, 2024.
- [30] J. Geraci, R. Bhargava, B. Qorri, P. Leonchyk, D. Cook, M. Cook, F. Sie, L. Pani, "Machine learning hypothesis-generation for patient stratification and target discovery in rare disease: our experience with Open Science in ALS," *Frontiers in Computational Neuroscience*, vol. 17, 2023, doi:10.3389/fncom.2023.1199736.
- [31] S.M. Williamson, V. Prybutok, Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare, *Applied Sciences (Switzerland)*, vol. 14, no. 2, 2024, doi:10.3390/app14020675.
- [32] R. Schwartz, R. Schwartz, A. Vassilev, K. Greene, L. Perine, A. Burt, P. Hall, Towards a standard for identifying and managing bias in artificial intelligence, US Department of Commerce, National Institute of Standards and Technology, 2022.
- [33] N. Hendrix, D.L. Veenstra, M. Cheng, N.C. Anderson, S. Verguet, "Assessing the Economic Value of Clinical Artificial Intelligence: Challenges and Opportunities," *Value in Health*, vol. 25, no. 3, 2022, doi:10.1016/j.jval.2021.08.015.
- [34] A. Jungbauer, G. Ferreira, M. Butler, S. D'Costa, K. Brower, A. Rayat, R. Willson, "Status and future developments for downstream processing of biological products: Perspectives from the Recovery XIX yield roundtable discussions," *Biotechnology and Bioengineering*, 2024.
- [35] P.G.R. de Almeida, C.D. dos Santos, J.S. Farias, "Artificial Intelligence Regulation: a framework for governance," *Ethics and Information Technology*, vol. 23, no. 3, 2021, doi:10.1007/s10676-021-09593-z.
- [36] A. Nassar, M. Kamal, "Ethical Dilemmas in AI-Powered Decision-Making: A Deep Dive into Big Data-Driven Ethical Considerations," *International Journal of Responsible Artificial Intelligence*, vol. 11, no. 8, 2021.
- [37] E. Nasarian, R. Alizadehsani, U.R. Acharya, K.-L. Tsui, "Designing interpretable ML system to enhance trust in healthcare: A systematic review to proposed responsible clinician-AI-collaboration framework," *Information Fusion*, 102412, 2024.



**Muhammad Yaqub** working as postdoctoral researcher at Hunan University. He received his Bachelor's and Master of Science in Computer Science from COMSATS University Islamabad, Pakistan, a top-ranked institution for IT education in Pakistan. He earned his Ph.D. in Electronic Science and Technology from Beijing University of Technology, China, in 2023, where he made significant contributions to the development of innovative deep learning-based schemes for medical image analysis, including segmentation, classification, and image reconstruction. With a strong academic background and a track record of over 30 publications in reputable international journals, Dr. M Yaqub is renowned for his expertise in applying cutting-edge technologies to advance cancer and oncology research. His work has consistently demonstrated a commitment to excellence in research and a keen analytical mindset.



**Lan He** working as associate professor at Hunan university, Changsha, China. She graduated from the School of Life Sciences of Northeast Normal University in 2010 and was later recommended to the Shanghai Institute of Biochemistry and Cell Biology, Chinese Academy of Sciences, where she received her Ph.D. in Science in 2016. In the same year, she entered Shanghai Tech University for postdoctoral research. She has published many papers as the first author or corresponding author in international authoritative journals, including *Advanced Science*, *Cellular & Molecular Immunology*, *PNAS*, etc. She has participated in the writing of two authoritative immunology books and one English book for Springer magazine. She is currently undertaking one National Natural Science Youth Fund, one Hunan Provincial Natural Science Youth Fund, and one Changsha Natural Science Fund.

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

# Fingerprint Bio-metric: Confronting Challenges, Embracing Evolution, and Extending Utility - A Review

Diptadip Maiti<sup>\*1</sup>, Madhuchhanda Basak<sup>2</sup>, Debashis Das<sup>3</sup>

<sup>1</sup>Department of CSE, Techno India University, West Bengal, 700091, India

<sup>2</sup>Department of CSE, Brainware University, West Bengal, 700125, India

<sup>3</sup>Department of CSE, Dr. Sudhir Chandra Sur Institute of Technology & Sports Complex, West Bengal, 700074, India

\*Corresponding author: Diptadip Maiti, Techno India University, West Bengal, 700091, India, Contact No & Email: +919433736910, [diptadip-maiti@gmail.com](mailto:diptadip-maiti@gmail.com)

**ABSTRACT:** As documented in recent research, this review offers a thorough examination of the intricate subject of fingerprint authentication, including a wide range of issues and applications. Addressing problems like non-linear deformations and enhancing picture quality, which are frequently reduced by sophisticated improvement and alignment techniques are important components of fingerprint image authentication. Countering security concerns such as spoofing is a major focus of Automated Fingerprint Identification Systems and necessitates the use of sophisticated cryptographic techniques and liveness detection. In order to accomplish speedier identification processes, the paper emphasizes the advancements made in fingerprint indexing and retrieval, with a focus on deep learning technologies and minutiae-based methodologies. Furthermore, fingerprint authentication is used for a variety of age groups, including neonates, where it is essential for identification verification and the management of medical records. The paper also highlights the wider uses of fingerprint technology, such as improved crime detection skills, insights into age-related features, and contributions to medical diagnostics. This review provides a thorough overview of the latest developments and potential future directions in fingerprint authentication by combining state-of-the-art methodologies and analysing technical details, implementation challenges, and security issues. This captures the dynamic and important role of this biometric technology.

**KEYWORDS:** Biometric Authentication, Fingerprint Identification System, Biometric Security, Biometric Application

## 1. Introduction

In the rapidly evolving landscape of biometric technology, fingerprint authentication has emerged as a cornerstone of identity verification and security systems. The intricate and unique ridge patterns present on human fingertips provide a reliable and convenient means of confirming individuals' identities. As societies transition towards digitalization and interconnectedness, the role of fingerprint biometrics becomes increasingly crucial in ensuring secure access to systems, facilities, and personal information. This paper delves into the intricate web of fingerprint biometric research, offering a comprehensive overview of the challenges faced, innovative solutions devised, and emerging trends that collectively shape the present and future of this dynamic field. Figure 1 depicts a few fingerprint images that have been collected through different technologies. Figure 1(a) represents fingerprint collected by ink and paper method, Figure 1(b) shows fingerprint collected by a digital scanner and Figure 1(c) shows fingerprint collected from a crime scene.

We will go through a number of fingerprint biometric dimensions in this exploration, each with its own opportunities and limitations. The challenge of authenticating unformatted fingerprint photos is significant because of

non-linear deformations, different pressures during acquisition, and a range of environmental factors. [1]. In response, researchers have developed intricate algorithms harnessing machine learning, convolutional networks, and auto encoders to enhance image quality and improve matching accuracy. Security vulnerabilities inherent in Automated Fingerprint Identification Systems (AFIS) call for advanced strategies to safeguard against threats such as spoofing and data tampering. Biometric cryptosystems and cancellable templates are among the innovative solutions that fuse cryptographic techniques with biometric data, forging new frontiers in secure authentication [2]. The realm of fast fingerprint indexing and searching is another pivotal arena, demanding the fusion of speed and precision in matching large datasets. Leveraging fingerprint features and deep learning algorithms, researchers have crafted strategies to expedite the matching process while ensuring accurate results. Furthermore, the application of fingerprint biometrics extends beyond traditional identity verification. From diagnosing medical conditions through changes in fingerprint patterns to detecting drug consumption and even determining handedness, the fingerprint's unique attributes are being harnessed for a diverse array of purposes. As this exploration unfolds, it underscores not only the strides made

in fingerprint biometrics but also the ethical considerations and societal implications that accompany the growing integration of biometric data into various aspects of modern life. As researchers continue to innovate and push the boundaries of what is possible, fingerprint biometrics remain a cornerstone in the pursuit of a secure and interconnected future [3].

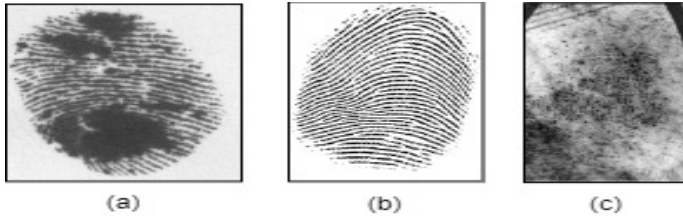


Figure 1: Different Source FP Images: (a) Rolled ink (b) Live scan (c) Latent

The objective of this review is to comprehensively explore the landscape of fingerprint authentication as documented in previous literature. It aims to delve into the technical challenges encountered in fingerprint image authentication, including addressing non-linear deformations, enhancing image quality, and implementing alignment methods. The review also seeks to examine the security considerations within Automated Fingerprint Identification Systems (AFIS), focusing on strategies to combat spoofing through liveness detection and advanced cryptographic measures. Additionally, it aims to analyse the methodologies and advancements in rapid fingerprint indexing and retrieval, particularly emphasizing minutiae-based approaches and the integration of deep learning techniques. Furthermore, the review intends to assess the diverse applications of fingerprint authentication, from identity verification in infants to its implications for medical history tracking, as well as its broader roles in medical diagnostics, age-related studies, handedness detection, and crime prevention. Through a thematic analysis of existing literature, this review aims to provide insights into the current state-of-the-art methodologies, implementation challenges, and security concerns within the field of fingerprint authentication.

To present a thorough overview of developments in the field of biometric authentication, we carefully reviewed publications published in the past ten years as part of the data collecting and analysis for this review study. Each study was methodically identified and categorized according to its purported benefits and drawbacks, accuracy measures, and procedures used. To comprehend these research methods to algorithmic processing, performance evaluation, and biometric data gathering, we carefully examined their techniques. The study aimed to evaluate the efficacy and accuracy rates of various biometric approaches, taking into account the advantages and disadvantages of each method. Through the consolidation of this data, we were able to identify patterns and breakthroughs, evaluate the development of biometric technologies, and provide perspectives on the condition of the technology sector at large. This comprehensive study seeks to offer a fair assessment of the advancements made, point out areas in need of development, and determine future paths for biometric authentication research.

In this study, we attempt to investigate various state-

of-the-art developments in finger print biometric practical application. The format of this essay is as follows: The difficulties and security risks associated with latent fingerprint authentication and automatic fingerprint authentication systems are discussed in Section 2. The method for all-purpose fingerprint user identification is described in Section 3. Fast fingerprint indexing and searching are covered in Section 4. The difficulties and solutions for analysing and identifying infants' fingerprints are described in Section 5. Multi-modal biometric techniques are discussed in Section 6. Comparative comparison of various approaches is the main topic of Section 7. Section 8 concludes with some final thoughts.

## 2. Challenges in Authentication

### 2.1. Authentication of Unformatted Fingerprint Image

In the field of fingerprint authentication, raw fingerprint images can be obtained from different sources, such as rolled ink prints, live scans, and latent prints. These images often suffer from non-linear deformations and poor quality, making authentication challenging. Non-linear deformations can arise due to variations in finger pressure and improper finger placement during image acquisition. These deformations can lead to unsatisfactory matching scores and impact the accuracy of fingerprint authentication systems. Low-quality fingerprint images can also result from factors like image scanner noise, partial prints collected from crime scenes (latent prints), and various skin conditions. These low-quality prints can be categorized as dry, wet, damaged, dotted, and blurred. Dry prints have minimal contact with the scanning surface, while wet prints result in smudged ridges and valleys due to extensive contact. Damaged prints may arise from scars or skin issues, while dotted prints are caused by excessive sweating. Blurred prints occur when motion or unclear ridges during scanning lead to image blurriness. To address these challenges, various techniques have been developed for fingerprint enhancement and alignment. Traditional methods such as Gabor filtering and adaptive boosted spectral filtering are commonly used for enhancing fingerprint images. Alignment techniques and cluster-based methods aim to rectify non-linear deformations, improving the accuracy of matching in automated fingerprint identification systems (AFIS). Figure 2 shows fingerprint feature extraction using convolution neural network, where three parallel CNN extract features from the fingerprint image and after the merging of the three features to form a unique feature descriptor, which is passed to a classifier for classification task.

Because of their high dimensionality, minutiae descriptors, which are widely used in fingerprint identification algorithms, face considerable hurdles. These descriptors are robust for fingerprint pattern identification because they capture fine features. However, the noise and volatility present in real-world settings might have a significant impact on their performance. Noise may cause mismatches during matching procedures by distorting minute points. This noise can originate from various sources, such as defective sensors or low-quality images. Accurate identification is made more difficult by unpredictable variations in fingerprint traits, such as ageing or changes brought on by injuries. Thus, even though minutiae descriptors are excellent at



collecting distinctive fingerprint features, their effectiveness depends on how well noise and unpredictability are handled to provide safe and dependable biometric identification systems.

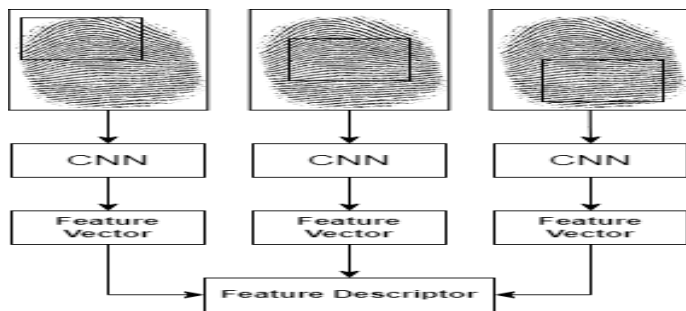


Figure 2: Extraction of Minutiae Descriptor using CNN

A novel latent fingerprint matching approach is presented by [4], which makes use of a descriptor-based Hough transform for latent prints together with a robust alignment technique. Their approach achieved a noteworthy rank-1 accuracy of 53.5% on NIST SD27, outperforming two commercial matchers and a non-commercial algorithm. Singular point-based alignment is a problem, as performance depends on the quantity of minutiae and the overall print quality. Refining features with top-down information from an exemplar print, in [5], the authors presented a feedback system for latent fingerprint matching. When combined with a cutting-edge matcher, it improved identification accuracy in the NIST SD27 and WVU databases by 0.5–3.5%. Finding a balance between the advantages of feedback and the complexity of the system, as well as the example print quality, is a challenge. Deformable Minutiae Clustering was proposed by [6] for latent fingerprint recognition, improving minutiae matching via cluster merging and Thin Plate Spline modelling. It outperformed previous techniques with up to 85.6% (Cylinder-Codes) and 83.3% (m-triplets) accuracy across different fingerprint databases. Scalability issues for latent-to-latent identification and algorithm speed are among the limitations. Using feature selection and random decision forest classification, the authors in [7] provided an adaptive latent fingerprint segmentation approach that achieved state-of-the-art performance on three databases. In order to balance accuracy and selection time, their method includes a unique SIVV-based metric for segmentation evaluation and modified RELIEF feature selection. Constraints about the applicability of the SIVV metric and assumptions about consistent ground truth are examples of limitations. A collaborative filtering paradigm for fingerprint enhancement was proposed by [8]. It involves pre-enhancing using Gabor filters and spatial patch-based enhancement utilizing spectral diffusion after that. Test findings on FVC2004 datasets showed that this approach was better than other approaches such as the Gabor filter and VeriFinger Algorithm Demo. The study is limited by fixed patch size effects and sensitivity to input fingerprint quality, which calls for additional investigation to fully evaluate resilience. FingerNet, a CNN-based method for latent fingerprint enhancement, was introduced by [9]. It has shared convolution and deconvolution layers for orientation guiding and noise reduction. It demonstrated potential for improvement with larger datasets and ground truth ROI an-

notations, as demonstrated by its top-1 matching accuracy of 47.7% when tested on NIST SD27 using data collected from SD4. Using Convolutional Neural Networks (ConvNets) for ridge flow estimation and minutiae descriptor extraction. In [10], the authors proposed an automated latent fingerprint recognition system that achieved rank 1 identification accuracies of 64.7% and 75.3% on NIST SD27 and WVU latent databases. Poor ridge quality, background noise, a tiny friction ridge area, reliance on manual ROI selection, long processing times, and scaling issues are some of the limitations. A technique to improve Automated Fingerprint Identification Systems (AFIS) by utilizing uncommon minutiae was suggested by [11]. This involves altering similarity scores that are based on least squares fitting mistakes in order to improve matching accuracy. It greatly improves the rank identification accuracy of minutiae-based matchers, as demonstrated by tests conducted on the GCDB forensic database. Future study on generalization and database size effects is suggested by the challenges of dataset restrictions and manual intervention for latent AFIS. An end-to-end latent fingerprint recognition system with automated ROI cropping, minutiae extraction based on deep learning, and texture template creation was promoted by [12]. Tested against a background of rolled prints on many datasets, yielding rank-1 retrieval rates varying from 7.6% to 69.4%. Among the drawbacks are difficulties in identifying fine details on low-quality photos, trimming dry latents, and the requirement for more varied operating databases for thorough training. By utilizing fine-coarse parallelism and asynchronous processing for latent fingerprint recognition. In [13], the authors invented ALFI and achieved a 22x speed gain over state-of-the-art approaches with equivalent accuracy. Tested on NIST SD27, they report accuracy using Equal Error Rate and F1-score, recognizing dataset size constraints, restricted classification strategies, and unknown uses beyond fingerprints, such as DNA analysis. LQMetric, an automated method for evaluating latent fingerprint quality and forecasting the probability of a rank-1 hit in the FBI's NGI AFIS system, was suggested by [14]. It produced a 61.4% match with human examiner assessments using local clarity maps and image analysis tools; it worked well for NGI searches but was not uniformly applicable to other AFIS methods. For improving latent fingerprint images. In [15], the authors provide a progressive GAN-based technique that consists of off-line training and repeated on-line testing phases. Based on CMC curve metrics, evaluation on the NIST SD27 dataset demonstrates better performance than previous models. Constraints on dataset quantity, processing cost, and possible inefficiency with subtle ridge features in latent prints are some of the limitations. An automated latent fingerprint identification system using DCNN-FFT augmentation for minutiae extraction and matching was described by [16]. It achieved 100% rank-1 identification on the FVC2002 and FVC2004 databases and 84.5% on the NIST SD27. The results show increased recall, F1 scores, and precision; however, computational time and dataset diversity are acknowledged as constraints. Using synthetic data for training. In [17], the author provide a deep nested UNets architecture for automated latent fingerprint segmentation and improvement. It performs better than current methods in fingerprint recognition and segmentation accuracy when tested on the NIST SD27 and IITD-MOLF



databases. One of the main drawbacks is the lack of high-quality and low-quality coupled fingerprint picture pairs in the current databases. This can be overcome by creating synthetic latent images for training. Using dense fingerprint patch alignment and matching. In [18], the authors promoted a non-minutia latent fingerprint registration method that outperformed previous techniques in registration when tested on the NIST27 and MOLF datasets. Its drawbacks include its dependence on 2D data, higher processing requirements, and possible inadequacy for poor-quality picture data. Using an algorithm based on Lindeberg's scale selection method. In [19], the authors revealed integrating pores (level 3 characteristics) alongside minutiae for latent fingerprint identification. When combined with pores, as opposed to just minutiae matching, greatly improves recognition rates on the IIITD Latent database. A small dataset size, a focus plane restriction for pore extraction, and computational costs that affect matching time are among the limitations. For latent fingerprint identification. In [20], the authors proposed the "Ratio of Minutiae Triangles" (RMT) algorithm, which makes use of local minutiae arrangements without pre-alignment. tested with Rank-1 recognition accuracy of 80% and 63.8% on the FVC2004 and NIST SD27 databases, respectively. Poor quality latent cases and the requirement for better feature extraction and matching phase integration for large databases are acknowledged constraints. In order to achieve accurate latent fingerprint enhancement and segmentation. In [21], the researchers proposed a hybrid model that combines the Chan-Vese approach for segmentation and Edge Adaptive Directional Total Variation (EDTV) for enhancement. Accurate Rank-1 identification was achieved with 61.24% and 70.16% on NIST SD27 and WVU DB databases, respectively. Restrictions include the size of the database and the requirement for additional testing on intricate latent fingerprints. Using Chan-Vese, an adaptive latent fingerprint segmentation and matching strategy based on the EDTV model was given by [22]. On the NIST SD27 dataset, this approach achieved AUCs of 72% and 70.59% for ROC and CMC curves, respectively. Limitation includes poor accuracy of existing techniques for latent fingerprint segmentation. Using scale and rotation invariant minutiae characteristics. In [23], the authors proposed an automatic latent fingerprint identification system that significantly improved Rank-1 identification accuracy on NIST SD27 and FVC2004 datasets. On NIST SD27, CLMP-NRS produced the maximum Rank-1 accuracy of 93.80%. Handling incomplete fingerprints with limited minutiae characteristics and relying on the quantity of retrieved minutiae for matching performance are two limitations. MinNet, a minutia patch embedding network for latent fingerprint identification that optimizes spatial and angular minutiae distribution, is introduced by [24]. Reaching cutting-edge outcomes, assessed on many public and private datasets, such as FVC-Latent and NIST SD27, with rank-1 accuracies of 85.88% and 92.39%, respectively. Its limitations include the inability to handle fingerprints that are partially or substantially deformed and its reliance on high-quality latent pictures for precise minutiae extraction. To achieve state-of-the-art accuracy and efficiency in latent fingerprint indexing, the authors in [25] offer a multi-scale fixed-length representation technique. performed better than other indexing techniques like PDC and DeepPrint

when tested on a variety of datasets, including Hisign and NIST SD27. possibility performance variance on simulated fingerprints and scope-limited optimization are among the limitations, indicating possibility for more improvements in feature representation. Using a residual encoder-decoder architecture and frequency-domain loss function optimization, the authors in [26] proposed a deep learning model for latent fingerprint enhancement. superior than current methods in terms of rank-25 and rank-50 accuracy when evaluated using the IIIT-Delhi MOLF database. The ridge-based approach of the technology and the requirement for additional refinement in deleting undesired portions of images and testing on a variety of databases are its limitations. With an emphasis on fairness in prediction and decision-making, the authors in [27] provided a technique to and reduce biases in automated algorithms working with latent fingerprint pictures. They evaluate the effect on automatic matching of latent fingerprints using covariate-specific ROC curves produced from regression models taking quality and demographics into account. Results demonstrate that, compared to assessments without quality, the suggested covariate-adjusted ROC curves conditioned on image quality and demographics offer a more informative assessment. The quality measurement algorithm's underlying assumptions and dataset restrictions are examples of limitations. It is believed that more research on a variety of datasets is crucial for method validation. ULPrint, a Universal Latent Fingerprint Enhancer, was introduced by [28], who used Mix Visual Transformer (MiT) SegFormer-B5 encoder architecture and Ridge Segmentation with UNet. By using directed blending of predicted ridge masks, the technique improves latent fingerprints and addresses issues with a variety of latent types. Tests conducted on both synthetic and actual datasets show notable gains in accuracy; nonetheless, there are still issues such as annotator subjectivity and limited databases. FingerGAN, a GAN-based technique for latent fingerprint enhancement, was presented by [29]. It optimizes minute information through adversarial, perceptual, and reconstruction losses. Tested on NIST SD27 and IIIT-Delhi MOLF, FingerGAN outperforms state-of-the-art techniques, however it has drawbacks such as computational complexity and dependence on high-quality rolled fingerprints for data production. For latent fingerprint recognition, the authors in [30] suggest a hybrid method integrating local (minutiae and virtual minutiae) and global features (AFR-Net embeddings). With a multi-stage matching paradigm and Squeeze U-Net CNN for augmentation, they attain an average rank-1 retrieval rate of 71.22% on multiple datasets. Failure instances including severe rotations and overlapping patterns are noted, as are challenges such as low contrast and occlusion. ACSACO, a hybrid approach combining Cuckoo Search and Ant Colony Optimization for latent fingerprint identification, was proposed by [31]. ACSACO beats individual algorithms when tested on the NIST SD-27 dataset, achieving excellent precision and recall for prints of good quality but lower accuracy for prints of poor or ugly quality. Complex backdrop problems and overlapping prints are among the limitations, indicating the need for additional optimization strategies and wider dataset validation. In order to enhance DeepPrint for recognition systems, in [32], the authors developed a CycleGAN-based technique to create artificial latent fingerprints. Their ap-

proach improves TDR at 0.01% FAR from 23.64% (MSP) to 45.45% (synthetic) when tested on NIST SD27. Reliance on a single matcher and the lack of functional latent databases are among the limitations.

Latent fingerprint identification is the painstaking process of locating and examining fingerprints from crime scenes, frequently with the aid of cutting-edge methods to improve their contrast and visibility. New levels of security are introduced when these latent prints are scanned and input into automatic fingerprint identification systems (AFIS). This meticulous manual process is essential for correct identification. Although AFIS significantly improves fingerprint matchings scalability and efficiency, it also brings with it potential vulnerabilities that were not as noticeable in manual systems. Problems like algorithmic flaws, spoofing attempts, and data breaches emphasize the necessity of strict security protocols to preserve the accuracy of fingerprint data. In order to guarantee that the improvements in fingerprint identification technology do not jeopardize its dependability and efficacy, it is crucial to comprehend the shift from manual latent fingerprint analysis to automated methods.

## 2.2. Security Threats in AFIS

Digital user authentication through fingerprint biometrics relies on Automated Fingerprint Identification Systems (AFIS) to verify individuals' identities. The concept of AFIS was initially developed by the US Federal Bureau of Investigation (FBI). The AFIS process can be divided into two phases: Enrolment and Identification. In the Enrolment phase, users' fingerprints are registered in the system. The Identification phase matches query fingerprints against stored templates for authentication. During Enrolment, fingerprint images undergo preprocessing, feature extraction, and template creation. In the Identification phase, query fingerprints are processed and matched against stored templates to identify valid users. Securing a biometric system is crucial due to the non-changeable nature of biometric traits. An AFIS needs robust security measures to safeguard user information from potential attackers. Various components within an AFIS can be exploited by attackers. These attack points include potential vulnerabilities in the biometric data acquisition process, template extraction, and communication channels. Several known attacks can compromise the security of an AFIS, including spoofing (presenting fake biometric data), exploiting similarity, zero-effort attempts (using attacker's own biometric to impersonate a legitimate user), physical destruction of the biometric sensor, replay attacks (intercepting and replaying biometric signals), communication channel attacks (cutting or altering channels), and more. These attacks can lead to unauthorized access, denial of service, and other security breaches.

### 2.2.1. Liveness Detection

To address these security challenges, researchers have developed preventive measures and countermeasures, such as liveness detection to determine if a fingerprint is from a living person or a spoof. Various methods have been proposed to detect spoof attacks that use materials like wood, glue, and gelatine to fabricate fingerprint spoofs. Figure 3 shows the process of liveness detection using auto encoder

where live and spoof fingerprint images are passed to an encoder to learn two different latent representation of the image and then it is passed to decoder to reconstruct the live and spoof fingerprint, this way the architecture knows the difference between a spoof and live image and can detect them.

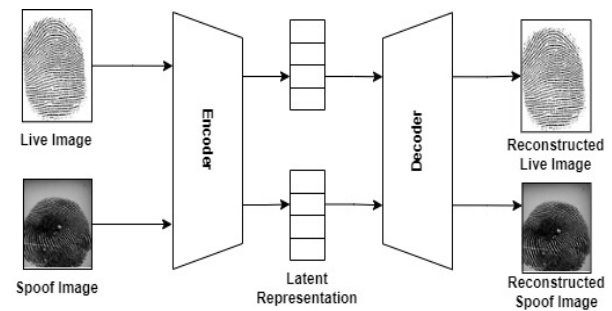


Figure 3: Process of Fingerprint Spoof Detection

In order to improve the resilience of biometric authentication systems against spoofing attacks, the authors in [33] present an approach that combines SURF, PHOG, and Gabor wavelets with low-level characteristics and shape analysis to detect liveness in fingerprint images. Achieving an average EER of 3.95%, their algorithm, which uses PCA for dimensionality reduction and various classifiers, such as SVM and Random Trees—beats above the previous record of 9.625%, validated across several databases, including LivDet 2011 and LivDet 2013. However, more testing on a range of sensors and materials is acknowledged for a thorough robustness assessment. A software-based fingerprint liveness detection technique is presented by [34]. It uses image gradient co-occurrence arrays for feature extraction and SVM classification. It attains greater accuracy on LivDet09DB and LivDet11DB datasets than state-of-the-art methods, in spite of drawbacks like quantization-induced information loss and high-dimensional feature vectors derived from higher-order co-occurrence arrays. Convolutional neural networks could improve gradient measurement; however, dimensionality reduction methods could be needed to handle higher-order arrays. In order to achieve state-of-the-art accuracy across LivDet datasets, the authors in [35] proposed a CNN-based technique for fingerprint spoof attack detection that makes use of local patches centred on minutiae for fine-grained analysis. The approach shows effectiveness against different spoof materials and testing settings, with an average accuracy of 99.03% on LivDet 2015, beating the 95.51% of competition winners. The need for more diverse datasets and ethical concerns about the use of biometric data are two acknowledged constraints, though. A fingerprint liveness detection technique using a BP neural network and difference co-occurrence matrices for improved textural features was suggested by [36]. The system builds input data based on these matrices and uses pre-trained networks to forecast classification accuracy, achieving higher detection accuracy on the LivDet 2013 database over earlier techniques. One of the limitations is the lack of diagonal direction difference co-occurrence matrices, which could more accurately represent the properties of the image. For real-time fingerprint liveness detection, the authors in [37] promoted a semi-supervised stacked autoencoder-based method that substitutes learnt representations for hand-



designed features. Exhibiting efficaciousness on the LivDet 2011 and 2013 datasets, the approach attains satisfactory performance, but with a recognition of constraints including dataset magnitude, model initialization, and difficulties with substandard quality, excessive brightness, or noisy images. Adversarial attacks on deep neural network-based fingerprint liveness detection were described by [38], exposing flaws in cutting-edge models. By applying FGSM, MI-FGSM, and Deepfool techniques, they illustrated how models might mistakenly identify phony fingerprints as real ones with minute variations. The evaluation of the LivDet 2013 and LivDet 2015 datasets made clear that deep learning applications require more reliable detection models and anti-adversarial techniques. With a score-level fusion approach that combines liveness detection and fingerprint matching, the authors in [39] took first place with 96.88% accuracy in the Fingerprint Liveness Detection Competition 2019. It was evaluated using the LivDet2015 and LivDet2019 datasets, taking into account restrictions on finger pressure and device time that may effect detection accuracy. It used ONNS for similarity, Slim-ResCNN for FLD score, and LR classifiers for fusion. A DenseNet optimized with a genetic algorithm was provided by [40] for fingerprint liveness detection, and it achieved 98.22% accuracy on a mixed Livdet dataset. Despite constraints in dataset size and computational cost for real-time applications, the method outperforms state-of-the-art efforts on LivDet 2009, 2011, 2013, and 2015 datasets by utilizing ROI extraction and specialized mutation operators. A liveness identification approach utilizing the Circular Gabor Wavelet (CGW) algorithm and SVM was presented by [41], which achieved 99.968% accuracy in differentiating between real and false fingerprints. The approach, which has been tested on 272 samples from optical and capacitive sensors, yields encouraging results but still needs to be assessed further against spoofing techniques used in the real world. A multi-modal liveness detection method incorporating fingerprint and iris inputs, leveraging statistical texture features and spatial analysis, was advocated by [42]. The approach outperforms sum-rule and product-based approaches with high precision (94.7%) for fingerprint detection and 97.8% accuracy for decision-level fusion. Recognizing its limits, such as its reliance on dataset size and its usefulness against particular attack types. Using the LivDet 2013 and 2015 datasets, the authors in [43] presented FLDNet, a lightweight CNN architecture for fingerprint liveness detection that achieves state-of-the-art performance. FLDNet solves problems such as accuracy on tiny size fingerprints and robustness against unknown spoof materials, and achieves 1.76% Average Classification Error (ACE) over all sensors with a redesigned dense block and attention pooling layer. A one-class convolutional auto encoder for fingerprint presentation attack detection is proposed by [44], and it achieves a D-EER of 2.00% on a dataset of 24,050 fingerprint images. Among the method's drawbacks include its inability to generalize to additional modalities, the requirement for distinct models for various attack substrates, and uncertainties about robustness and adversarial attacks. A weighted multi-modal CNN-based FLD technique was introduced by [45], which used ROI operation and feature fusion for improved performance. It achieves excellent accuracy in different evaluation circumstances, outperforming current approaches on LivDet 2011, 2013, 2015, and NUAA

datasets. Two drawbacks are the need for extensive training datasets and performance variability brought on by sensor diversity. EaZy learning, an adaptive ensemble learning model for fingerprint liveness detection, was suggested by [46]. On LivDet 2011, 2013, and 2015 datasets, it achieved average accuracies of 60.49% and 67.80%. It solves drawbacks such as reliance on clustering techniques and dataset size, as well as potential performance concerns in unknown contexts due to lack of variety in training data by clustering training data and integrating predictions using weighted majority voting. A novel approach using transformers and GANs to improve fingerprint presentation attack detection (PAD) generalization across sensors and materials was developed by [47]. With LivDet2015, the approach achieves an accuracy gain from 68.52% to 83.12%, addressing the limits of accuracy degradation in cross-sensor situations and inadequate generalization. Using a "transient liveness factor" (TLF) and picture quality measures, the authors in [48] suggest a person-specific FPAD technique that achieves 100% accuracy in spoof presentation detection. They admit constraints such as the short dataset size and the difficulty of generalizing across different materials while conducting experiments with a dataset of 30 live photos and 138 spoof samples from various attackers. In comparison to previous methods, the authors in [49] proposed a Fingerprint Liveness Detection (FLD) technique that improved accuracy by 1.0% on average by integrating AlexNet, VGG16, and ResNet CNNs with a genetic algorithm for feature weighting. Enhancing detection performance on several Livedet datasets, the strategy addresses the drawbacks of fixed-scale inputs and possible challenges in training the model due to over-abundance of features. A CNN-based fingerprint liveness detection technique was suggested by [50], which outperformed SVM and CNN+SVM hybrid techniques on the LivDet2015 dataset. Measured by precision, specificity, F1 score, and accuracy metrics, preprocessing approaches and feature extraction methods improve classification accuracy. Given that different materials provide different obstacles when it comes to creating false fingerprints, more study is necessary to improve classification performance in these scenarios. A multi-filter framework for fingerprint liveness detection utilizing hand-crafted features was promoted by [51], who achieved improved performance on LivDet test datasets. The method achieves an average accuracy of 99.15% and an average classification error of 0.85% on the LivDet 2015 dataset, outperforming state-of-the-art techniques. It involves procedures such as data augmentation, preprocessing, feature fusion, and dimensionality reduction. The authors recognize that lengthy processing times and complex parameter setting are real usability barriers. In order to counteract forced and phony fingerprint attacks, the authors in [52] introduced MFAS, a Micro-Behavioural Fingerprint Analysis System that records fingertip micro-behaviour throughout time. After being tested on 24 subjects, MFAS achieves 100% accuracy in identifying voluntary versus forced fingerprint placements, as well as 100% true positives. Though encouraging, the system can run into problems in realistic situations, requiring more study to improve technology and comprehend its application. The incremental learning model A-iLearn, proposed by [53], addresses the stability-plasticity conundrum in spoof fingerprint detection by adaptively integrating base

classifiers. A-iLearn increases accuracy on new fake materials by up to 49.57% without appreciable stability loss when compared to baseline models. It is tested on LivDet 2011, 2013, and 2015 datasets using a variety of spoof materials and sensors. Some drawbacks include the possibility of over fitting and the requirement for more research into feature integration techniques. By combining texture and sweating pore characteristics, the authors in [54] provided a static-based fingerprint liveness detection technique. An auto encoder minimizes feature dimensionality for binary classification using a softmax classifier by quantifying textural properties and pore activity. Testing the approach on LivDet 2013 and LivDet 2015, with an ACE of 0.11-0.24%, it recognizes the difficulties in maintaining several algorithms for hardware-based detection while addressing restricted pore feature-based techniques. A lightweight fingerprint liveness detection network called LFLDNet is proposed by [55]. It makes use of style transfer, foreground extraction, and an enhanced ResNet with MHSA. 95.27% accuracy on small-area fingerprints and 1.72% average classification error across sensors were achieved during evaluation on the LivDet2011, LivDet2013, and LivDet2015 datasets. The authors intend to investigate improved FLD technologies and GAN-based models for cross-sensor generalization against fingerprint deception assaults, while acknowledging the possibility of speed variations. Using CNNs and adversarial data augmentation, the authors in [56] proposed an FPAD technique and won the LivDet2021 competition. The method uses clean and adversarial fingerprints for a three-stage training process that yields good accuracy metrics and an EER of 0.036. The size restrictions of the dataset and possible susceptibilities to adversarial assaults are acknowledged by the authors. Using LPDJH image descriptors and deep learning, the authors in [57] introduced a fingerprint liveness detection technique that achieved good accuracy across LivDet datasets. Their approach shows competitive results on the LivDet 2011 dataset, with an average EER of 3.95%. Because there aren't enough test samples, the authors point out possible difficulties in identifying low-resolution fingerprints and calculating accuracy for particular sensors. A CNN-based fingerprint liveness detection technique was introduced by [58] using the Socofing dataset. The model performed well, achieving 98.964% accuracy with a FAR of 0.215% and a FRR of 7.251%. Computational limitations, inconsistent fingerprint quality, and unequal dataset distribution are some of the restrictions.

By addressing the crucial problem of separating real biometric samples from fake or artificial copies, fingerprint liveness detection makes sure that the system authenticates the submitted fingerprints. By stopping unauthorized access, this procedure is crucial for preserving the integrity of biometric systems. However, biometric cryptographic systems use biometric information like fingerprints to strengthen security by using cryptographic methods. This way, biometric identifiers are safely encrypted and shielded from unwanted access. The interdependence of liveness detection technologies and the efficacy of biometric cryptography systems highlights the relationship between these two domains. Robust liveness detection essentially acts as a cornerstone supporting the security of biometric cryptography systems, emphasizing the need for integrated solutions that handle biometric sample authenticity as well as biometric data

management securely.

### 2.2.2. Biometric Cryptosystem

Biometric cryptosystems are mechanisms that enhance the security of biometric systems by embedding biometric templates with secret keys or auxiliary data. This approach ensures protection against malicious use and data tampering. Figure 4 shows the block diagram of biometric cryptosystem, which consist of two parts one is for enrolment where template are generated from the fingerprint images and stored in the dataset and the second part is authentication where template is generated from a query fingerprint and matched with the stored template to provide access to a system.

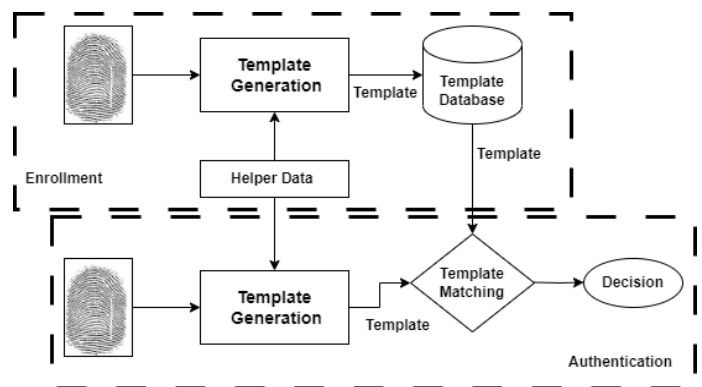


Figure 4: Biometric Cryptosystem

Pair-polar minutiae structures were used by [59] to present an alignment-free fingerprint cryptosystem. Their approach achieves robust security and improves privacy by changing minute structures. It has been tested on several databases and performs better than other systems in terms of Genuine Acceptance Rate (GAR) and False Acceptance Rate (FAR); nonetheless, a security risk arises from its dependence on the complexity of brute force attacks. In order to maximize security and efficiency, the authors in [60] suggest a feature-level sequential fusion algorithm for biometric cryptosystems. Experiments conducted on a finger vein database show that the algorithm performs better than the OR rule, decreasing input needs and obtaining a 1.47% False Acceptance Rate. Although the paper admits its limits in analysing some external security concerns, it shows that it is resilient to well-considered attacks. An ECC-free biometric key binding approach employing graph-based Hamming Embedding (GHE) and minutia-vicinity decomposition (MVD) for fingerprint minutiae-based representation was proposed by [61]. The strategy obtains GAR of 89% (FRR=11%, FAR=0.16%) for DB1 and GAR of 97% (FRR=3%, FAR=0.061%) for DB2, when tested on the FVC2002 datasets. The method balances security and performance trade-offs, but it is still susceptible to privacy attacks such as ARM and SKI, and it can only match fingerprint photos of the same finger taken under various circumstances or at different times. In [62], the authors provide a method to improve biometric template security that is based on a 2D logistic sine map (2DLSM). The technique employs diffusion and confusion processes, demonstrating effectiveness against a range of threats, by using chaotic streams from



2DLSM. Effectiveness has been evaluated on iris and fingerprint templates; nevertheless, real-time template production problems and noise sensitivity are among the constraints. A safe cryptographic authentication approach utilizing biometrics and the discrete logarithm problem was suggested by [63]. The approach produces cryptographic keys using a function  $F$  using iris codes, which allows it to handle mistake bits and achieve high accuracy rates. Promising results are shown by the CASIA iris database evaluation, which also notes that iris codes still require work in order to be improved in the future. BioKEY, a biometric-based cryptographic key generation technique based on convolution coding principles, was promoted by [64]. Unique cryptographic keys are created without saving templates by using fingerprint characteristics and applying convolution coding to specific locations. Tests conducted on common fingerprint databases such as MIAS, FVC2002, and FVC2004 show good accuracy and effectiveness; nevertheless, there are certain drawbacks such as difficulties with noisy or hazy fingerprints and a higher processing overhead in comparison to other techniques. ECC-based mutual authentication strategy for Smart Grid communications with biometric authentication integration for improved security and privacy was proposed by [65]. To safeguard against different types of security risks, the protocol consists of start-up, registration, and authentication stages. Notwithstanding its shortcomings, which include parameter sensitivity and vulnerability to certain assaults, the system shows efficiency through communication and computing cost comparisons with current protocols even if it does not offer precise accuracy measurements. In order to safeguard templates in multi-modal biometric systems, the authors in [66] provide a fuzzy vault technique that uses encryption to keep authentic templates safe from copycats. The approach satisfies optimal biometric security requirements with low FAR (0.1062) and zero FRR when tested on a simulated face and fingerprint database. In order to get the best security and accuracy, the authors recommend avoiding function creep attacks and balancing key length with chaff points. Hyper elliptic curve cryptography (HECC) for template encryption was used by [67] to introduce an improved iris recognition technique that achieves great security and accuracy. With the use of fuzzy logic matching and 2D Gabor filter for feature extraction, the system achieves 99.74% maximum accuracy and short identification time. Superior performance with reduced FAR, FRR, and EER measures is demonstrated by evaluation on the IITD and CASIA Iris V-4 iris datasets. A multi biometric cryptosystem for client-server network authentication is presented by [68], guaranteeing computation security and privacy. The approach enhances efficiency by achieving equivalent accuracy with less user input by using iris and fingerprint modalities from a dataset of 100 participants. The authors request protocol enhancements for increased security and verification speed, acknowledging the limitations in accuracy caused by biometric variability. A multi-biometric template security technique based on graph creation was proposed by [69] for cloud authentication. A branching factor graph with a low Equal Error Rate (ERR) of 0.66% is created using fingerprint and palm print features. The authors point out important benefits over conventional authentication techniques while also acknowledging limitations with regard to the encryption process and the quality

of the input sample. Using the Diffie-Hellman algorithm and minute characteristics, the authors in [70] proposed a fingerprint-based crypto-biometric system for secure communication. Tested using FVC2002 and the NIST special database 4, the system reports metrics such as FAR, FRR, GAR, and EER, demonstrating privacy protection. The authors have acknowledged the restrictions pertaining to the irreversibility of biometric data, possible data distortions, and key creation. A multi-modal biometric cryptosystem utilizing fingerprint and ear characteristics was promoted by [71], which included preprocessing, feature extraction, and classification stages. The approach achieves excellent accuracy (98.76%) with a dataset that includes photos of ears and fingerprints. Performance is analysed using metrics such as sensitivity, specificity, accuracy, false positive rate, and false negative rate. The lack of multi-modal databases and the dependence on multi-modal systems because particular biometrics, such as ear characteristics, are unreliable are among the limitations. However, the method offers an efficient fix for identity and security systems. A biometric cryptosystem using random projection and back propagation neural network (BPNN) for template protection is introduced by [72]. Original biometric traits are transformed into unlinkable projected vectors by random projection, and BPNN is then used to map these vectors to secure keys. Better security and performance than current techniques are demonstrated via experimental assessment on a variety of biometric datasets. The authors stress the necessity for more investigation into novel ciphers for biometric template security and the improvement of security through multiple-biometric template protection. A novel fingerprint biometric cryptosystem using fuzzy commitment and CNN-based automated texture descriptor discretization was presented by [73]. Tests conducted on the FVC2000 DB2-A database show encouraging outcomes: 1.25% for FAR, 1.15% for FRR, and 2.83% for EER. The restricted number of photos per identification class presents challenges, such as precisely identifying reference points and producing a bigger training set. An effective cancelable biometric authentication framework using a Genetic Encryption Algorithm (GA) for increased security is presented by [74]. The process entails using GA for increased security, choosing the best sub-images, and permuting biometric templates. Promising findings were obtained via evaluation on a variety of datasets, such as the face and fingerprint datasets; nevertheless, more validation on bigger and more diverse datasets is required to ensure generalizability. A cancellable biometric security system using sophisticated chaotic maps to improve fingerprint identification was provided by [75]. Using various chaotic maps, chaos-based picture encryption produces convolution kernels that are then used to construct encrypted biometric templates. With an EER of 0.593% and a high detection probability of 96.139%, the augmented quadratic map 3 performs best in the system. The invertibility of biometric transformations and the requirement to investigate cancellable recognition in alternative biometrics are among the limitations. The Cancelable Biometrics Vault (CBV) was introduced by [76], who used winnowing and chaffing to create safe biometric templates for cryptographic key encoding. Experimental results demonstrate that, regardless of key size, the CBV's use of an extended BioEncoding scheme is acceptable for bit strings such as iris-codes, and that its

decoding accuracy is equivalent to that of the underlying CB construct. The reliance on an appropriate CB scheme for the biometric representation and computational complexity unfit for real-time applications are among the limitations. A multi-biometric cryptosystem employing Modulus Fuzzy Vault, augmenting input data with BDPHE and segmenting pictures with MBIRCH, was proposed by [77]. Features are extracted by the bidirectional deer hunting optimization algorithm, fused using score level and normalized feature fusion, and then safely stored. The approach enhances revocability and security while producing superior ROC, FAR, FRR, and GAR metrics; nonetheless, it has drawbacks related to algorithm focus and dataset authenticity. A machine vision gait-based biometric cryptosystem using a fuzzy commitment strategy was invented by [78]. Robust bits are chosen for the fuzzy commitment scheme after gait characteristics are retrieved using LTP and GEL. Tested on the CASIA A and CMU MoBo datasets, obtaining 0% FAR and FRR under certain scenarios. One limitation is that it might be challenging to identify people with complicated backgrounds or occlusions. An asymmetric cryptosystem integrating the elliptic curve method and optical scanning cryptography (OSC) was proposed by [79]. Using ECC from biometric pictures, the approach encodes things into holograms, guaranteeing excellent decryption accuracy and key sensitivity. The technique has to be optimized for speed and handles vulnerabilities to ciphertext-only assaults, even though security and key management have improved. In order to pre-process biometric images, the authors in [80] promoted the use of a fuzzy extractor that leverages deep learning, together with code-based cryptosystems to generate robust keys utilizing face biometrics. Promising accuracy metrics are found while evaluating the LFW and CelebA datasets. There is need for improvement in data privacy and security, as evidenced by limitations such as storage requirements and attack vulnerability. ElGamal encryption and Shamir's secret sharing are two cryptographic algorithms that are used in the blockchain-based user re-enrolment approach for biometric authentication systems proposed by [81]. Key security characteristics are satisfied by simulations that show secure re-enrolment in a matter of seconds; nevertheless, scalability and adversarial assumptions are acknowledged limits. More research is needed to determine the implementation specifics and practical viability. Based on Lagrange's interpolation, the authors in [82] provide a secure multi-biometric template protection method that uses irreversible and unlinkable image transformation. By utilizing feature-level fusion, the technique combines the properties of the fingerprint, iris, and palm print, attaining a high accuracy of 99.9816% when applied to high-resolution picture datasets. Issues include growing database sizes and possible departures from ISO/IEC 24745 standards, and privacy protection is still a problem. Biometric attributes can be randomly shuffled using a 3D chaotic map, as proposed by [83], to create a safe cancellable biometric cryptosystem. Larger datasets and other attacks are needed for more research, however evaluation on the ORL, FVC, and LFW datasets demonstrates encouraging results with very low Equal Error Rates ( $6.2460 \times 10^{-13}$ ) and high average Area under the ROC curve (0.9998). A robust cancellable biometric authentication technique is introduced by [84], which makes use of DNA sequencing theory, PWLCM, logistic map, and

3D chaotic maps. Through dispersion and confusion, the technique produces biometric patterns that are completely undefined while achieving increased security. Although computational complexity is still a barrier, evaluation on a variety of face and palm print datasets shows encouraging results in terms of AROC, FAR, DH, SSIM, and PSNR. An Enhanced Biometric Cryptosystem (BCS) using iris and ear modalities with Binary Robust Independent Elementary Feature (BRIEF) was introduced by [85]. Although vulnerable to database-level assaults, experimental assessment on AMI and UBIPr databases shows better performance across several parameters compared to state-of-the-art approaches, suggesting its applicability for security applications. Using deep learning and crypto-mapping, the authors in [86] provided a multi-biometric secure-storage technique that generated cancellable biometrics from fused pictures of the face, fingerprint, iris, and palm. While ICUB results reveal greater error rates, experimental results on the CASIA V4, MICHE, and MobiFace datasets demonstrate good AUCROC and low EER. The limitations mentioned by the authors include the necessity to strike a compromise between security and recognition performance, hardware requirements, and potential over fitting. In an effort to improve security, the authors in [87] proposed a multi-round AES cryptosystem with hierarchical hardware pipelined structures and biometric key generation. The system outperforms traditional AES systems in terms of space and energy efficiency because to resource sharing and simultaneous XOR operations. The undefined dataset size and the restriction to area and energy efficiency measurements are among the limitations.

Biometric characteristics are combined with cryptographic methods in biometric cryptography systems to protect authentication procedures, guarantee the privacy of biometric data, and prevent unwanted access. However, if the data is hacked, the intrinsic uniqueness of biometric features presents privacy problems. Cancellable biometrics are useful in this situation. In order to reduce the risk of prolonged exposure in the event of a data breach, cancellable biometric approaches convert biometric data into a non-reversible, pseudonymous form that can be updated or revoked as needed. The security architecture gains an extra layer of defence that improves user privacy and adaptability by incorporating cancellable biometrics into biometric cryptography systems. This addresses the reliability of authentication as well as the flexibility of maintaining biometric identifiers. This interaction emphasizes how crucial it is to combine cancellable biometric techniques with cryptographic security to offer a thorough and reliable solution to biometric data protection.

### 2.2.3. Cancellable Biometric

Cancellable biometric templates are introduced to enhance the security of biometric authentication systems by storing irreversible transformed versions of templates rather than original biometric templates. This approach prevents attacks and vulnerabilities while maintaining certain advantages, such as non-revocability. Techniques like mixing mechanisms and many-to-one transfer functions are commonly employed for generating cancellable biometrics. A basic block diagram of cancellable biometric is represented in Figure 5 where template is generated using transfer pro-

cess, if by any reason the template get compromise then it is very easy to replace the old template with a new one by changing the transformation process. Retaining identifiable biometric information despite transformation efforts aimed at unlinkability, potential mismatches due to lack of adaptation to temporal changes, increased computational demands, privacy risks from potential reconstruction, and usability issues regarding recognition reliability are some of the challenges associated with using high-quality initial biometric images for generating cancellable templates. In order to guarantee the security and usability of cancellable biometric systems in actual applications, it is imperative that these variables are balanced.

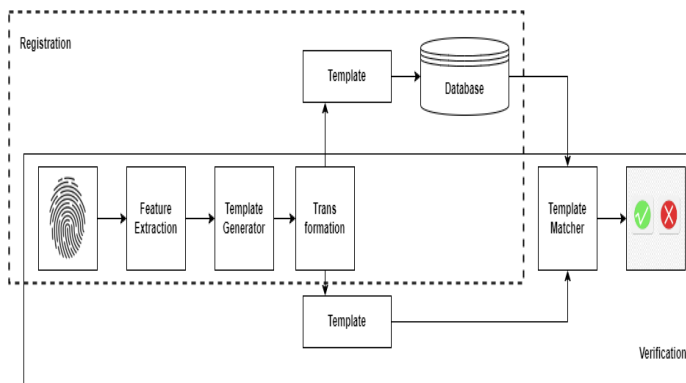


Figure 5: Cancellable Biometric

A fingerprint template protection technique utilizing fused feature-level structures that produce cancelable templates was presented by [88]. Improved performance was seen with EER ranging from 1.6% to 17.6% in the FVC 2002 and 2004 datasets. Two drawbacks are the expense of computing and the invertibility brought on by fusion. In order to take advantage of flaws in partial fingerprint-based authentication systems, the authors in [89] proposed creating "MasterPrints," which are artificial or actual partial fingerprints that match recorded templates for a large number of users. Their method proved that it was possible to impersonate users when tested on the FingerPass DB7 and FVC2002 DB1-A datasets; in some situations, Synthetic MasterPrints performed better than Sampled MasterPrints. Limitations include imbalanced datasets and limited application to minutiae-based systems, which have prompted more study into remedies. A one-factor cancellable biometric authentication technique using Indexing First Order hashing was suggested by [90]. It was assessed for accuracy performance, non-invertibility, renewability, and unlinkability. Tested on six datasets from the FVC 2002 and 2004 databases, yielding metrics for genuine-imposter distribution and Equal Error Rate (EER) that are adequate. Although it separates IDs from biometric templates, it assures unlinkability and is susceptible to standard symmetric key cryptosystem assaults. By using OIOM hash and MSH to create a pseudonymous identification, the authors in [91] promoted a one-factor cancellable palmprint recognition technique that achieved a recognition accuracy of 98.07%. although no specific limitations or restrictions are mentioned, experiments were conducted using the PolyU and TJU palmprint databases. A global multi-biometric system using deep neural networks for cancellable feature creation

was proposed by [92], which achieved good performance on iris datasets (IITD Iris and MMU2). The technique acknowledges constraints in sensitivity and adaptability and blends dimensionality reduction, adaptive fusion, and revocability. Aspects of security and privacy are explored, and some adversarial threats are illustrated. In order to provide maximum safety of sensitive data, the authors in [93] provided the Secure Triplet Loss method for training end-to-end deep learning models to build non-invertible and unlinkable biometric templates. The approach is tested on facial recognition and ECG tasks, showing that it can successfully modify pre-trained models or create secure models from scratch. The dataset utilized for experimentation is not stated, despite constraints being addressed, such as sensitivity to certain assaults and the effect of demographic characteristics on system accuracy. Constrained Optimized Similarity-based Attack (CSA) was introduced by [94] as an improvement over earlier similarity-based assaults. It incorporates algorithm-specific limitations to optimize pre-image production for impersonation. The usefulness of CSA is demonstrated through experiments using the labelled Faces in the Wild (LFW) dataset and Index-of-Max (IoM) hashing. The performance measures that are measured include the total success rate, the False Acceptance Impostor (FAI) rate, and the True Acceptance Impostor (TAI) rate. The success of CSA is contingent upon data leakage and constraint identifiability, which may restrict its application in certain biometric systems. In order to prevent unwanted access, the authors in [95] developed a non-invertible cancellable fingerprint template approach based on Delaunay triangulation of minutiae points. When evaluated against the FVC2002 database, the findings show promise in terms of identification accuracy, resilience against fingerprint distortion, and comparison to modern approaches. However, more research is necessary for wider validation due to concerns including hacked acquisition equipment and dataset size restrictions. A safe method for building fingerprint templates that are optimized was disclosed by [96]. This technique uses the quality of minutiae points to generate 3D shell-shaped templates. Tested on nine fingerprint datasets, the method yields a 0% Equal Error Rate (EER) and 100% accuracy in separating authentic individuals from imposters. Nevertheless, low-quality photos could be limiting its performance, indicating a possibility for improvement through multimodal biometric system integration. Using IoM hashing and BioHashing, the authors in [97] developed the first constrained-optimized similarity-based attack (CSA) against cancellable biometrics (CB). By optimizing preimage creation through algorithm-specific limitations, CSA outperforms Genetic Algorithm enabled similarity-based assaults (GASA). Success rate (SAR) and false acceptance index (FAI) of CSA, assessed on the LFW dataset, demonstrate the efficacy of CSA in breaking IoM hashing and BioHashing security. However, there are drawbacks to CSA due to its constant model complexity and dependence on hash code size. A cloud and Internet-of-things-ready method for cancellable biometric template generation was developed by [98]. By using the Greatest Common Divisor (GCD) between hazy biometric pictures, it guarantees authentication accuracy and non-recoverability. It is tested on several biometrics and achieves low EER values (down to 0.04%) and high AROC values (up to 99.59%), while it is recognized



to have limits with respect to pre-defined distortions and picture quality. A cancellable biometric authentication system with feature-adaptive random projection that includes feature extraction, transformation, and encrypted domain matching was presented by [99]. EER, GAR, and FAR metrics evaluation on the FVC2002 and FVC2004 databases revealed competitive performance. The need for more discriminating feature descriptors and investigation across a range of biometric features are acknowledged constraints. In order to provide biometric data safety and reliable authentication, the authors in [100] suggested a user authentication and key agreement system utilizing cancellable biometrics and PUF in multi-server settings. Their methodology beat state-of-the-art techniques when tested on the LFW dataset and assessed using the CMC, ROC, DIR, and DET curves. Recognized drawbacks include the requirement for assessment against complex assaults and scalability issues with larger data sets, indicating potential directions for further study. BioCanCrypto, a biocryptosystem using fingerprint cancellable templates that combines biocryptosystems and cancellable biometrics, was proposed by [101]. It takes cancellable templates and extracts cryptographic keys using a reusable fuzzy extractor with LDPC coding. tested using the FVC2002 dataset, showing encouraging outcomes despite low FRR and EER. The study is restricted to fingerprint data, though, thus it might be worthwhile to investigate alternative feature spaces or data modalities. A unique biometric template protection approach incorporating watermarking and cancellable transformation was suggested by [102]. The technique uses pair-polar coordinates with cancellable modification of minutiae and binary watermarking obtained from fingerprint minutiae. tested on the BioSecure and FVC2002 DB1 datasets, showing better EER and resilience to assaults than previous approaches. Investigating several biometric modalities to improve accuracy and robustness is one of the future research priorities. Absolute Value Equations Transform (AVET), a non-linear projection technique that ensures irreversibility by depending on the Absolute Value Equations issue, was promoted by [103]. AVET surpassed state-of-the-art approaches in bimodal circumstances and produced competitive performances in uni modal settings after being evaluated on eight datasets for different biometrics. A fixed sample size and susceptibility to brute-force attacks are two limitations. Using deep fusion and deep dream, the authors in [104] propose a multi-biometric cancellable system (MBCS) that creates tamper-proof templates using fingerprint, finger vein, and iris biometrics. It used a dataset with nine pictures per modality, outperforming comparable algorithms in EER, FAR, FRR, and AROC. All quantitative evaluations showed positive results. Larger datasets, high computing demands, and a drawn-out enrolment procedure are among the acknowledged limits. A cancellable multi-biometric identification system using ACM encryption and decimation to combine biometric data into a single template was presented by [105]. Performance measures, which were assessed using FVC 2002 and ICE 2005, included EER and ROC curve analysis. Its stated drawbacks were the need for better parameter estimate techniques and bigger databases. CSMoFN is a revolutionary cancellable multi-modal biometrics system that combines face and periocular data, as reported by [106]. It uses pairwise angular loss and ArcFace for training, and it achieves an EER of 6.67% on

average across six datasets and 2.12% on Facescrub. The authors warn against potential CB template inversion concerns while highlighting dual template-changeability and acknowledging difficulty in fair comparison. A new cancellable multi-biometric system combining deep learning-based fusion and selective encryption was developed by [107]. AES encryption, PRNG matrix XORing of a chosen ocular picture, and Viola-Jones facial segmentation are all used. Although constrained by the size of the dataset, it surpasses previous efforts with high entropy and low correlation, quicker enrolment, and better metrics like EER and AROC, indicating that medical imaging application is a promising area for future study. A unique cancelable biometric solution using deep learning for fingerprint and face biometrics on smart phones was presented by [108]. It improves security for Internet of Things applications by using Siamese networks with visual and text encoders. Prolonged testing shows improved performance compared to earlier approaches, surpassing ciphering-based systems in EER, FAR, FRR, and AROC, and attaining high accuracy metrics. MBFH, a unique cancellable biometric method that makes use of safe hashing and non-invertible transformations, was invented by [109]. Multi-biometric acquisition, feature extraction, Multi-Exposure Fusion (MEF), and SHA-3 hashing are all included in the process. Tests using retina, finger veins, palm, and dorsal vein pictures show high pairwise distances and good performance in generating text and visual templates, indicating flexibility for further improvements such as adding white Gaussian noise. A biometric template protection system for Euclidean and Cosine metrics was introduced by [110]. It used distance-preserving, one-way, and obfuscation modules with location-sensitive hash functions. Effectiveness against similarity-based and linear inequality attacks is demonstrated by evaluation on face datasets such as AR, CASIA, ORL, and LFW. However, this approach is not always the best option and requires pre-processing, which raises the computational costs significantly. Despite defences against assaults, the authors advise against assuming complete security in any situation. Using the chaotic Baker map to encrypt biometric templates, the authors in [111] provide a chaotic-based cancellable face recognition system that is highly accurate (98.43%) and adaptable to a variety of databases. The approach takes care of lighting, occlusion, and emotions, but it also recognizes the necessity for environmental adoption and trade-off between performance and user privacy. A cancellable biometric authentication system using image style transfer is proposed by [112]. During registration, users supply a face picture and a key image to create and store a template. In order to get high AUC values (>0.9) in most circumstances, authentication entails comparing freshly created templates with stored ones. Correlation coefficients and ROC curves are used to evaluate the results. One of the limitations is the possibility of authentication using marginally similar key images. This suggests that future research should put limitations on key image parameters.

Widely utilized in forensic and law enforcement settings, AFIS faces unique security issues such data breaches, spoofing attempts, and system flaws that could jeopardize the integrity and accuracy of fingerprint matching. In a similar vein, these vulnerabilities also affect general-purpose user authentication systems, which use fingerprints for iden-

tivity verification and access control in common applications. Consumer-grade fingerprint authentication systems can benefit from and benefit from the protective tactics included in AFIS security measures. Developers can better address similar risks in general-purpose systems by knowing the vulnerabilities and countermeasures relevant to AFIS. This will help to ensure that strong security mechanisms are put in place to protect user data and prevent unwanted access. In order to improve overall security and user trust in biometric technology, it is crucial to transfer high-security solutions from specialized applications to more commonly used fingerprint authentication systems.

### 3. General Purpose User Authentication

Automated Fingerprint Identification Systems (AFIS) commonly rely on minutiae-based fingerprint matching due to its strong evidential value, versatility, storage efficiency, and reliable matching performance. However, an emerging alternative approach in AFIS is pore-based fingerprint matching, which offers distinct advantages. Pore matching techniques can be broadly categorized into two main methods: (i) pore alignment-based matching and (ii) direct pore comparison-based methods. These techniques harness the unique characteristics of pores within fingerprints to enhance the accuracy and robustness of authentication systems. Figure 6 represents fingerprint image enhancement and reconstruction, where first the image is normalized, then ridge orientation is detected. After the ridge orientation detection ridge reliability is estimated and the frequency of the ridges are calculated. The above two step helps to find the region of interest and then the region is passed through Gabor filtering to remove noises to construct a higher quality fingerprint image from a low quality fingerprint image.

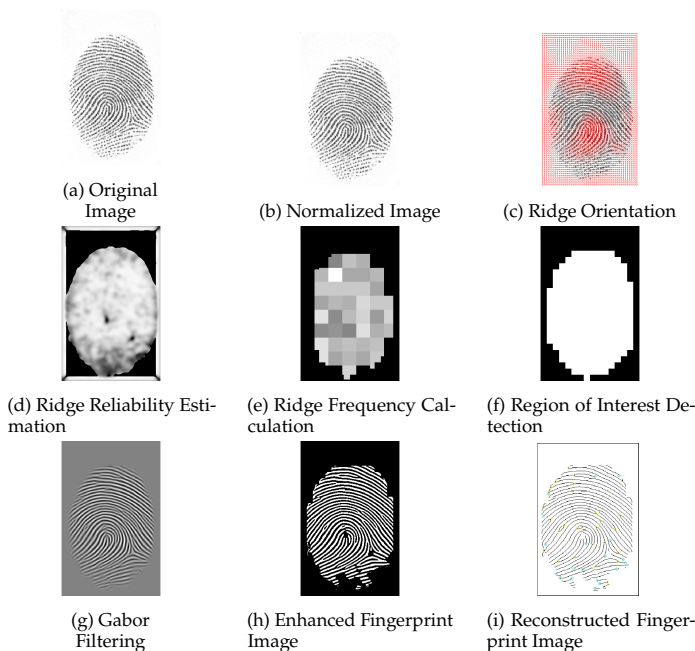


Figure 6: Fingerprint Image Enhancement & Reconstruction

Using global models, local analysis, and combination approaches, the authors in [113] provide techniques to improve fingerprint orientation extraction, obtaining an EER of 0.206% on the FVC2006 DB2 dataset. In addition to

parameter tuning, they seek to increase recognition accuracy by addressing the shortcomings of benchmark datasets through pre- and post-processing phases. Using the AMFM fingerprint model and binary ridge pattern generation, the authors in [114] proposed a method to reconstruct whole fingerprint pictures from discrete points. Experimental assessment on FVC 2002 datasets shows better results than state-of-the-art methods with >86% of Successful Match Rates at FAR=0.01%. Reduction in performance for templates with fewer detail points and sensitivity to orientation field estimate accuracy are some of the limitations. Using image quality assessment (IQA) for liveness detection spanning fingerprint, iris, and face recognition, the authors in [115] provide a software-based technique for identifying phony biometric features. With the use of 25 generic IQA features, the technique performs competitively when compared to state-of-the-art methods, exhibiting minimal complexity appropriate for real-time applications and classification error rates below 3% and 21.4% Half Total Error Rate (HTER) on fingerprint datasets. One limitation is that in order to defeat obfuscation attempts, access to the entire picture and the necessary processing resources are required. A local model-based fingerprint classification technique including core block extraction, area division, and classification phases that is capable of managing noisy and incomplete data was suggested by [116]. Assessment using the FVC 2000, 2002, and 2004 datasets demonstrates higher accuracy (96.7% and 96.5%) in comparison to current techniques; low-quality fingerprints are purposefully tested to gauge performance in difficult scenarios. Using FVC2002 DB1 as an example, the authors in [117] improved accuracy over previous techniques by using a two-stage process for partial fingerprint enrolment and a multi-scale texture-based A-KAZE strategy for matching. In light of the algorithm's reliance on enhancement techniques and small dataset circumstances, potential future research areas include synthetic fingerprint creation and resilience in real-world applications. One open-source and three commercial-off-the-shelf (COTS) extractors are used by [118] to evaluate fingerprint minutiae extraction performance and resilience against picture degradations. Assessment utilizes several measures on a dataset consisting of 40,000 artificially produced and 3,458 public-domain fingerprint photos. The evaluation recognizes obstacles such as noise, differences in finger location, and environmental conditions that affect the accuracy of the system. By merging global and local distance metric techniques, the authors in [119] proposed the Global-Local Distance Metric (GLDM) framework for improving bio-cryptosystem accuracy utilizing signature-based biometric features. Average classification error rates of around 7% and 17%, respectively, are obtained via experimental assessment on the PUCPR and GPDS-300 datasets. Challenges include limited positive samples for training and design restrictions in the signature system. A CNN-based pore extraction method for fingerprint pictures was provided by [120], making it easier to extract Level 3 features. Though it relies on high-resolution photos and has difficulties identifying pores in occluded or blurred images, the system outperforms previous algorithms and achieves excellent accuracy across touch-based, touch less, and latent fingerprint datasets. Future research may concentrate on creating matching algorithms for diverse fingerprint photos using derived pore properties. A new



technique for high-resolution fingerprint pore comparison using rotational invariant edge descriptors and Root-SIFT descriptors was introduced by [2]. EERs and FMR1000s for the FVC2002 datasets are 1.86% and 0.12%, respectively, according to the evaluation. The authors support direct pore comparison methods in spite of the possible loss of actual correspondences, acknowledging the drawbacks of comparing pores only on the basis of geometric distance. In order to improve ridge structures and remove false minutiae, the authors in [121] provide a fingerprint enhancement and reconstruction method based on orientation and phase reconstruction. Despite limitations such as age, dirt, and medical issues impacting picture quality, validation on the FVC2002 and FVC2004 datasets shows promise for enhancing interoperability among minutia encoders and matchers. DeepPoreID was created by [122], which achieved higher performance, especially with tiny picture sizes, by using deep convolutional networks for descriptive pore characteristics in fingerprint matching. Significant gains in EER and FMR100 are shown by evaluation on high-resolution fingerprint databases; nonetheless, there are certain drawbacks, such as a need for a sufficient number of pores and difficulties with occlusion. It is underlined that high-resolution fingerprint databases are available as open-source resources for more thorough testing. A homomorphic encryption-based fingerprint authentication system that guarantees access control while protecting biometric template data was investigated by [123]. Tested on FVC2002 DB2, the system shows an EER of 9.23%. The computational time issues that were found encourage research into more effective homomorphic encryption techniques. For a thorough assessment, more testing with bigger datasets and varied scenarios is advised. The Shark Smell Optimization (SSO) technique was used by [124] to study a fingerprint authentication system. Achieved FAR of 0.00%, FRR of 0.00666%, and CVR of 99.334% after evaluation on a dataset of 150 student fingerprint pictures. The size of the dataset, lack of variety, and exclusive dependence on the SSO algorithm are limitations. Future research into more swarm algorithms and bigger datasets is advised to get better results. Using fully homomorphic encryption (FHE) and the TFHE library, the authors in [125] created an effective fingerprint authentication system that preserves privacy while guaranteeing safe processing and storage of fingerprint data. Tested on NIST Special Database 9, the system reaches fingerprint matching in an average of 166 seconds, acknowledging the time consumption of the bootstrapping procedure and suggesting improvements for the future. BioSec, a biometric authentication system using fingerprint authentication for secure communication among edge devices, was introduced by [126]. AES-128 bit encryption is used to protect biometric templates while they are being sent and stored in databases. Assessed using the FVC-2004 DB3 dataset with 70% accuracy, they recognize the limitations of symmetric encryption vulnerability and propose improvements to privacy mechanisms, study of lightweight encryption methods, and investigation of other biometric markers such as iris for enhanced security and usefulness. In [127], the authors invented a blind and reversible fingerprint image watermarking method using the differential method and DCT domains. Assessed on the FVC2002 fingerprint database, the technique employs DCT-transformed sub-vectors to incorporate watermark bits,

facilitating direct watermark access throughout the extraction procedure. Evaluation measures included matching score and PSNR, which demonstrated a respectable level of fingerprint image security maintenance. The authors pointed out drawbacks like as noise sensitivity and compression, indicating that a bigger sample size would be necessary to increase performance. A set of two fingerprint matching methods, employing mtriplets and cylinder codes, fused with a supervised classifier for latent fingerprint recognition, was introduced by [128]. Achieved Rank-1 identification rates of 74.03% and 71.32% were evaluated on NIST SD27, GCDB, and MOLF DB4 databases. This work improves upon earlier approaches by evaluating matches using cumulative match characteristic (CMC) curves and plans to investigate other variables in further research for more accurate matching characterisation. Using attention mechanisms and Monte Carlo drop-out, the authors in [129] improved upon previous approaches by introducing an explainable fingerprint ROI segmentation model. High Jaccard similarity and Dice score measurements were obtained by testing on FVC datasets. Limitations include misclassification of background noise and performance changes caused by the size of the sample. An unsupervised technique for evaluating fingerprint quality based on minutiae detection confidence is called MiDeCon, and it was proposed by [130]. tested on FVC 2006 datasets; verification error and error-vs-reject curves showed superior performance compared to NFIQ1 and NFIQ2. The study did not address the limitations and limits of MiDeCon. ASRA, an Automatic Singular Value Decomposition-based Robust Fingerprint Image Alignment technique, was proposed by [131]. When tested on the FVC2002 and FVC2004 databases, ASRA demonstrated efficacy and efficiency in alignment, but with recognized shortcomings in terms of picture backgrounds and ROI extraction. For approach efficacy, more validation on bigger datasets is recommended. A unique fingerprint template protection and authentication method utilizing visual secret sharing (VSS) and super-resolution was suggested by [132]. The approach demonstrated security and resilience when tested on the FVC2002 DB1 dataset, while there are some acknowledged drawbacks, such as the requirement for higher-quality photos and the possibility of attacks on the super-resolution process. A dual-filter architecture and a novel texture descriptor, sDSIFT, were recommended by [133] to improve spoofing detection in fingerprint authentication systems. Tested using LivDet 2013 and 2015 datasets, the approach combines the dual-filter architecture with sDSIFT to achieve competitive accuracy. Nevertheless, shortcomings include the incapacity to distinguish between different filter kinds and spoofs created using materials that resemble real fingerprints. Three reliable methods utilizing fingerprint, iris, and voice characteristics for multi-modal biometric authentication were presented by [134]. The second technique, which used an SVM classifier and sum FFC, was evaluated on a dataset of 228 image and signal data, and it obtained a 100% classification rate; however, its scalability and real-world resilience were not evaluated. A secure online fingerprint authentication system with a cancellable fingerprint template design for privacy was provided by [135] for Industrial IoT devices over 5G networks. Tested on six public fingerprint databases, the system demonstrates competitive efficiency and performance, however it



recognizes the difficulties in preserving security while guaranteeing strong authentication over picture databases of poor quality. Using an Arduino Mega 2560 and a fingerprint sensor, the authors in [136] developed a fingerprint authentication system based on embedded systems. It generates templates using minutiae extraction and provides PIN and fingerprint combinations for smart home access. Although the accuracy is said to be high, low-end embedded systems' cost and durability against assaults present obstacles. CNN classification and Gabor filter-based feature extraction were used by [137] to investigate a fingerprint authentication technique. The approach beats other modern methods on the FVC2006 database, with a validation accuracy of 99.33%. Smaller training sets are still difficult to manage, despite results. A deep CNN model for fingerprint authentication was studied by [138], with 100% training and validation accuracy. One limitation is the diversity of datasets, which raises the possibility of strengthening robustness and generalizability. A multi-factor authentication approach was created by [139] to reduce False Acceptance Rates (FAR) and False Rejection Rates (FRR) in biometric systems. By combining several fingerprint sample permutations, their method increases system accuracy and fortifies it against impostor assaults. As opposed to single-factor authentication, experimental results on datasets like CASIA-FingerprintV5 and FVC2002 show lower mistake rates; nonetheless, the study admits several limitations, including addressing environmental deterioration and dataset size. InfinityGauntlet, a brute-force attack against smartphone fingerprint authentication (SFA) systems, was revealed by [140]. It uses SPI MITM to circumvent limit attempts and takes use of design flaws. They tested the assault on several devices using inexpensive equipment and a synthetic fingerprint generating technique, and they were able to detect four different types of attacks. One limitation is that security regulations demand the attack to be finished within 72 hours and that sensor hot plugging support be provided. A unified model for fingerprint authentication and spoof detection was developed by [141] using DualHeadMobileNet, a dual-head convolutional neural network. The model, using integrated datasets from FVC 2006 DB2A and LiveDet 2015, delivers low spoof detection error rates and good authentication accuracy. Computational effort and the requirement for bigger, more varied datasets for further studies are among the limitations. Blind-Touch, a privacy-preserving fingerprint authentication system using homomorphic encryption and machine learning, was introduced by [142]. Using PolyU and SOKOTO as benchmark datasets, the system attains great accuracy, with F1-scores of 93.6% and 98.2%, respectively. The influence of feature vector size on calculation time and the computational cost of constructing a traditional CNN with homomorphic encryption are among the challenges. The FingerPIN method, which combines PINs with fingerprints for multi-factor authentication, was proposed by [143]. According to a usability research, FingerPIN is more secure, quick, user-friendly, and efficient than conventional techniques. Restrictions include a limited sample size and a brief period of data collection, indicating the need for more study. An AVAAO-enabled Deep Maxout Network (DMN) for fingerprint-based person authentication was proposed by [144]. The technique obtained an accuracy of 0.927 on the CASIA Fingerprint Image Database by employ-

ing the AVAAO optimization algorithm of the method. The authors pointed out constraints such as the need for strong preprocessing and model training.

Fingerprints are being utilized more and more in general-purpose user identification to confirm identity on a variety of platforms, including secure facilities and mobile devices. This calls for quick and accurate verification procedures. Rapid fingerprint indexing and searching technologies are essential for fulfilling these expectations because they allow fingerprint records to be retrieved and matched quickly, improving system performance and user experience. The time needed for fingerprint verification can be greatly decreased by integrating sophisticated indexing and searching algorithms into general-purpose authentication systems, increasing the process's efficiency and scalability. This synergy emphasizes how crucial it is to optimize fingerprint search technologies to facilitate secure and seamless user authentication, guaranteeing that the speed and accuracy of the underlying verification procedures meet the convenience of biometric access.

#### 4. Fast Fingerprint Indexing and Searching

In various application domains, the rapid response and high efficiency of an Automated Fingerprint Identification System (AFIS) are paramount. To achieve swift results from large datasets, a common approach involves using a combination of fast and accurate algorithms. This entails employing a fast algorithm to generate a subset of candidate fingerprints, followed by a more precise but slower algorithm for final matching. Efficient fingerprint indexing predominantly revolves around two strategies: (i) utilizing Level-I features like ridge orientation and frequency maps, and (ii) leveraging minutiae features. The primary aim of fingerprint indexing is to reduce search space and time, especially when dealing with massive gallery image datasets. This section highlights several algorithms that exemplify this approach. Figure 7 shows the fingerprint processing and matching in distributed environment where the features from the fingerprint image is extracted at the client side and passed it to a server, where multiple feature matchers run in parallel to match the query feature in large fingerprint database. After matching the result is again send back to the client side.

To analyse huge databases efficiently, the authors in [145] created a distributed fingerprint matching system. The system achieves flexibility and scalability by using a two-level distributed design. Studies using NIST and synthetic fingerprint datasets showed that, when processing nodes and thread counts rose, execution times improved while accuracy remained similar to that of conventional AFIS. By parallelizing database searches, the authors in [146] introduced a GPU-based fingerprint recognition system that achieves fast processing rates. Although the approach can quickly identify millions of fingerprints per second, its practical use is limited by its 2% mistake rate. While highlighting the promise of GPU-based algorithms, the paper also notes that more development and integration into hybrid systems are required to achieve higher accuracy.

Using locality sensitive hashing (LSH) and minute cylinder-code SDK for effective indexing with pose lim-

itations, the authors in [147] developed an absolute registration method for fingerprint indexing. Experiments using databases such as the NIST Special Database 14 and a law enforcement fingerprint database shown increased efficiency and accuracy. Among the drawbacks are the high dimensionality of minutiae descriptors and the requirement for additional study to improve resilience against noise and unpredictability. In [148], the authors presented a fingerprint indexing technique that uses convex core points and minutiae pairs, combining candidate list reduction and k-means clustering to achieve effective indexing. The methodology outperforms state-of-the-art methods on six datasets by using coaxial Gaussian track coding and MBP representation for precise matching. One limitation is that the hardware and software utilized in the trials varied, and there is a lack of information on the values of the parameters.

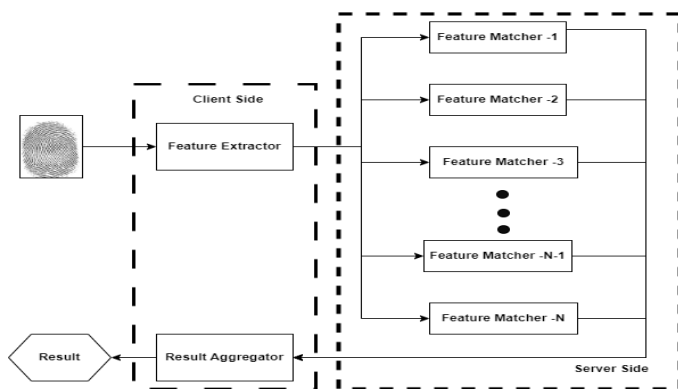


Figure 7: Fingerprint Processing & Matching In The Distributed Model

Improved retrieval efficiency was achieved by [149] using deep convolutional neural networks (DCNN) to build a minutiae-centred fingerprint indexing approach. They achieved superior results on five benchmark databases with their unique aggregating methodology that made use of 1-D CNN. Metrics for evaluation included penetration and error rates; higher penetration rates and lower error rates were noted. Two of the limitations were the high processing costs for MCC-based approaches and the low quality photos in FVC2000 DB3a. To address the shortcomings of minutiae-based approaches, the authors in [150] studied DeepPrint, a deep network for obtaining fixed-length fingerprint representations. Using the NIST SD4 and SD14 datasets, DeepPrint outperformed leading commercial off-the-shelf (COTS) SDKs in terms of accuracy and search speed. DeepPrint showed encouraging results in fingerprint identification, despite limits in benchmark saturation. CNNAI, a CNN-based technique for fingerprint recognition utilizing geometrical minutiae arrangements, was studied by [151], and it outperformed state-of-the-art algorithms in terms of identification rates. CNNAI demonstrated its abilities by achieving Rank-1 identification rates of 84.5% and 80% on the FVC2004 and NIST SD27 latent fingerprint datasets, respectively. Reliance on a minimum of eight minutiae points is one of the limitations, and using MINU-EXTRACTNET to extract all minutiae presents difficulties that might potentially impact identification rates. By developing a pore-based indexing technique for high-resolution fingerprints, the authors in [152] significantly reduced pre-selection error rates compared to previous approaches on a

variety of databases. The approach outperformed state-of-the-art minutiae-based algorithms on DBI and IITI-HRFP, according to tests conducted on datasets comprising DBI, DBII, IITI-HRFP, and IITI-HRF. Restrictions include decreased efficacy on databases with high-resolution whole fingerprints, which motivates more study into distortion correction methods. A latent fingerprint indexing technique integrating minutiae-based features, global and local matching, and machine learning-based segmentation was suggested by [153]. Up to 94.77% accuracy was shown in experiments on the IITI-D dataset, with indexing times varying from 5.29 to 25.92 seconds. Managing incomplete perceptions, background noise, inadequate ridge clarity, and nonlinear distortions are among the difficulties. An MCC-based indexing technique for latent fingerprint recognition was described by [154], beating competitors on the NIST SD4 and NIST SD14 databases by at least 1% and 3%, respectively. Although effective, it can have performance issues with different kinds of databases or with less-than-ideal detail extraction, and its temporal complexity prevents real-time applications. Employing graph-based algorithms for indexing and refining, the authors in [155] provided a pore-based fingerprint retrieval technique that outperformed previous approaches on databases DBI and DBII in terms of speed and accuracy. Its shortcomings, however, include the dependence of indexing precision on cluster accuracy and the computational cost that increases with the number of pores. Two fingerprint search strategies utilizing classic inverted index methods were proposed by [156]. They were examined on FVC2002 DB1a and a private dataset, with differences in document generation methodologies and minutiae handling. The second approach's scalability and sensitivity to low-quality minutiae were found to be limits, despite the fact that it produced reduced error rates. Using highly discriminative embeddings for constant-time identification and k-means or LSH index table generation, the authors in [157] present PalmHashNet, a palm print database indexing technique. Evaluation on four benchmark databases shows above 99% accuracy; nonetheless, there are several constraints, such as assumptions about the positioning of the palm area and unproven scalability on big datasets. By combining GIST descriptors from face, iris, and palm print biometrics, the authors in [158] developed an efficient multidimensional spectral hashing (MDSH) technique for data retrieval from multi biometric databases. Despite computational and memory constraints, experiments conducted on databases from IIT Delhi reveal enhanced accuracy measures that surpass tree-based indexing approaches and random hashing techniques. More efficiency improvements are proposed, such as lower memory use and processing costs, and investigating alternatives to local features. To lessen the computational burden in biometric identification systems, the authors in [159] proposed a nearest quality score-based intelligent search, which resulted in workload reductions of up to 38% for face, 31% for iris, and 29% for fingerprint databases. The technique, tested on the FERET, CASIA, and FVC2002 datasets, effectively indexes queries using sample quality scores that may be applied to a wide range of biometric features. Intraclass variability and susceptibility to various quality estimator techniques affecting the number of comparisons are challenges. FKIndexNet is an innovative approach for finger-knuckle-print (FKP) identification, de-

veloped by [160]. It uses customized autoencoder networks and similarity-preserving hash codes. The PolyU-FKP and IITD FKP databases show 100% hit rate in experimental findings at low penetration rates, indicating that index table creation approaches have limitations. A signal-based fusion approach for indexing biometric databases was presented by [161], which reduced computational effort by up to 70% without sacrificing biometric performance. Promising results are obtained when evaluated on benchmark databases such as FERET and FRGCv2, however these need the re-computation of indexes for new enrolments and high-quality face photos. By utilizing cancellable methods and DNN-based embedding extractors, the authors in [162] developed a novel approach to multi-biometric indexing that preserves privacy while improving biometric performance by 57%. Evaluation using a composite dataset reveals advancements but also points up extractor compatibility and dataset representation constraints. In their investigation of AFR-Net, an attention-driven fingerprint recognition network, the authors in [163] combined CNN-based and attention-based embeddings for improved performance. By utilizing a variety of datasets, AFR-Net surpasses baseline models and attains excellent accuracy metrics in verification and identification tasks. The lack of domain expertise in fingerprints and the requirement for better latent fingerprint preparation methods are among the limitations. An effective Gravitational Search Decision Forest (GSDF) method for fingerprint identification was created by [164] by merging the gravitational search algorithm (GSA) and random forest (RF). Comparing the GSDF technique to conventional machine learning classifiers, it yields higher identification rates for both entire and latent fingerprints. The authors agree that although the technique beats current methods, additional tuning is necessary for the recognition of low-quality latent fingerprints.

Infant fingerprint identification presents a unique set of challenges compared to adult fingerprint identification, which has a well-established sector with reliable techniques and tools for collecting and evaluating mature fingerprint patterns. Because of their fingers' quick growth and development, infants' fingerprints are more prone to distortion and have less defined ridges, therefore effective identification requires specific methods and modifications. It is necessary to modify fingerprint capture and processing technologies that have been developed for adults in order to address these issues with newborns. Researchers and practitioners can improve the overall efficacy and accuracy of fingerprint identification systems across all age groups by linking the methodology and technology utilized in both fields. This will guarantee that the systems remain accurate and dependable from infancy through adulthood. For comprehensive fingerprint identification systems that meet the needs of a wide range of demographics, this integration is essential.

## 5. Infants' Fingerprint Identification

Emerging as a challenging application, infants' fingerprint identification plays a crucial role in maintaining accurate records of a child's vaccination history, nutritional needs, and overall identity throughout their lifetime. Among various biometric options, fingerprinting emerges as one of

the most suitable choices due to its stability and uniqueness. While alternative biometrics like iris scanning or facial recognition are less feasible for infants due to practical challenges, fingerprints offer a reliable bio-marker. In the field of infants' fingerprint identification, limited research exists, but several notable contributions have been gathered from the literature. Figure 8 shows fingerprints of an infant at different age, which demonstrate the different density of ridges during different age of a infant.

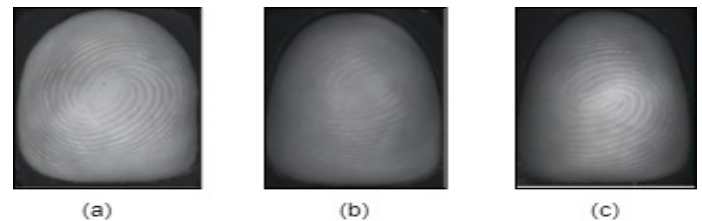


Figure 8: Fingerprints of an Infant at different age: a) 4 months b) 6 months c) 1 yr 3 months

A cost-effective, high-resolution fingerprint scanner for newborns was created by [165]. They achieved a rank-1 accuracy of 73.98% by building a database with pictures from 16,384 infants. In [166], the authors assessed the accuracy of child fingerprint recognition using NFIQ 2.0 measures in a follow-up research. Using a 500 PPI dataset, they were able to achieve TAR of 99.5% with FAR of 0.1% for children aged 12 months. An inexpensive newborn fingerprint identification system called InfantPrints was created by [167]. It consists of a high-resolution matcher and a specially designed fingerprint scanner. Assessed on a 315 baby longitudinal database, the system demonstrated excellent accuracy from enrolment at 2 months to authentication at 1 year. Among the drawbacks is the lack of a reliable automatic alignment technique for baby fingerprints. Using wavelet feature extraction and K-NN classification, the authors in [168] developed a baby's footprint identification system. Using a 200x500 pixel ROI and level 4 wavelet decomposition, the system obtained 99.30% accuracy with a dataset consisting of 600 footprint photos and 30 newborns. The modest sample size and the requirement for more testing on a bigger dataset for real-world application are acknowledged constraints. A newborn fingerprint identification technique using deep learning for fingerprint categorization was described by [169]. The approach obtained 78.4% classification accuracy compared to hand classification with a dataset consisting of 1,357 training photos, 166 validation images, and 1,181 test images. The requirement for significant computer resources and the difficulties in obtaining clear fingerprint pictures from some newborns are among the limitations. Using fingerprint, iris, and outer ear shape modalities, the authors in [170] created and assessed biometric recognition systems for babies. For the fingerprint and iris modalities, new hardware and software were created, but the outer ear shape modality made use of already-existing technologies. At a public clinic, data on newborns and young children under the age of one was gathered. FTA (failure to acquire) and equal error rate (EER) were used as accuracy measures. With an EER of 0.16%, the ear modality performed the best; nevertheless, inadequate reporting, inconsistent devices, and data



collection from newborns and young toddlers presented difficulties. A multi-instance contingent fusion approach for newborn fingerprint verification was presented by [171], which combined the left thumb and right index finger prints of infants ranging in age from one day to six months. The approach achieved 73.8%, 69.05%, and 57.14% accuracy for 1-month, 3-month, and 6-month intervals between enrolment and query prints, respectively, by using a 500 ppi fingerprint scanner and NIST feature extractor MINDTCT. Among the limitations were the requirement for fusion with increasing time intervals between photos and the lack of supplemental information in permission forms. M<sup>2</sup>BRTPC, a new Multi-modal Biometric Recognition for Toddlers and Preschool Children, is presented by [172]. Its goal is to identify children using minimum biometric characteristics such as fingerprints, faces, and iris. Their research, which acknowledged age range restrictions and the inherent difficulties in biometric identification, improved performance by  $14.75e^{18.75\%}$  using iris and fingerprint data from over 100 children ages 18 months to 4 years. Using a pre-trained ResNet-50 model, the authors in [173] investigated a fingerprint identification method for infants and toddlers, solving issues with image clarity and quality. The process entails cropping and enhancing images in order to precisely extract fingerprint traits. Using a dataset of 154 participants, the experimentation yielded an accuracy of 82.47%, a false rejection rate of less than 18%, and an authentication duration of about 2 seconds per fingerprint, while taking into account restrictions such as tiny fingerprint size and picture quality limits. Employing the CLCF dataset supplemented with a hybrid technique, the authors in [174] presented Child-CLEF, a CNN-based children detection system employing contactless fingerprints. The suggested Child-CLEF Net model outperforms current systems with 98.46% accuracy and 1.99% equal error rate by extracting minutiae and using BOZOROTH3 for identification. Larger datasets are required, as is the exploration of other enhancement and feature extraction techniques. Future developments should take patch-based newborn identification into consideration. These are some of the limitations.

Biometric identification systems for newborns and toddlers have advanced significantly in terms of accuracy and technological adaptability, but they still face significant obstacles in terms of data quality, moral issues, and practical implementation. Improving algorithms, expanding datasets, strengthening privacy protocols, and improving usability will be crucial in tackling these issues and boosting the dependability and relevance of these systems in paediatric healthcare and other fields.

A key component of biometric authentication is fingerprint identification, which uses distinctive ridge and valley patterns to confirm each person's identity. Though useful, it can have drawbacks such as spoofing, ambient conditions, and differences in fingerprint quality. In order to improve accuracy and reliability, multi-modal identification systems integrate various biometric modalities, such as voice prints, iris patterns, fingerprints, and facial recognition. Multi-modal systems are able to complement fingerprint data with other biometric identifiers, making up for any one modality's shortcomings and offering a more robust and all-encompassing authentication procedure. This integration makes biometric systems more flexible and user-friendly

while simultaneously enhancing overall security. Knowing how techniques might improve fingerprint recognition shows the possibility of developing more flexible and safe biometric systems that take advantage of several biometric properties.

## 6. Multi-modal Fingerprint Biometric

In [175], the author reported a multi-modal biometric system that combines face, fingerprint, and signature modalities with feature extraction techniques including Principal Component Analysis and Stationary Wavelet Transform. In order to address problems like spoof attacks and noisy data, they evaluate system accuracy on the YALE-FVC2002KVKR database by applying score and decision level fusion. Through the use of multi-modal strategies to overcome restrictions, the project aims to boost the dependability of biometric systems. In [176], the authors proposed improved uni modal and multi-modal biometric recognition systems using fingerprints and ECG signals using both traditional approaches and deep learning. When tested on virtual datasets like the FVC2004 fingerprint database and the MIT-BIH ECG database, multi-modal systems perform better than uni modal ones. Some of the drawbacks are the scarcity of ECG databases, the challenge of finding real-world datasets, and the high processing costs related to deep learning models. In [177], the authors have presented a deep learning-based multi-modal biometric fusion model that blends score, feature, and pixel layers to increase identification accuracy. Evaluation on a simulated dataset combining iris, fingerprint, and face data shows 99.6% accuracy using Euclidean distance metric learning and modality-specific network training for practicality. Limitations originating from the dataset's dependability may affect the accuracy rates. A 98.5% accurate HGSSA-bi LSTM model that combines fingerprint and iris biometrics is presented by [178]. When tested on the CASIA dataset, the model demonstrates excellent sensitivity and precision, but it also acknowledges the cost and complexity of multi-modal systems. In [179], the authors offers "Secure Sense," a multi-modal biometric system that incorporates face, fingerprint, and iris data and achieves 93% accuracy. The limitations of uni modal systems are addressed by decision-level fusion approach, which enhances strong authentication by utilizing real-time and web-based datasets.

## 7. Comparative Analysis

The Table 1 provides a comprehensive overview of unformatted fingerprint image authentication methods, encompassing various techniques aimed at enhancing the quality and recognition accuracy of latent fingerprints. Each method offers unique advantages and faces specific limitations, highlighting the need for ongoing research to address existing challenges and explore new avenues for improvement. Future research in this field should focus on several key directions. Firstly, there is a pressing need to develop robust and scalable algorithms capable of handling diverse and challenging latent fingerprints, including those with low quality, partial information, or distortion. This may involve further exploration of deep learning architectures, such

as convolutional neural networks (CNNs) and generative adversarial networks (GANs), to effectively enhance latent fingerprint images while preserving crucial details and minimizing noise. Secondly, efforts should be directed towards standardizing evaluation protocols and benchmark datasets to facilitate fair comparisons between different methods and promote reproducibility across studies. This includes the creation of large-scale, publicly available databases encompassing a wide range of latent fingerprint images captured under various conditions, which can serve as a common test bed for evaluating the performance of different algorithms. Additionally, research should address ethical considerations surrounding the deployment of unformatted fingerprint image authentication systems, including privacy concerns, algorithmic bias, and potential misuse of biometric data. Developing transparent and accountable frameworks for data collection, storage, and usage is essential to ensure the responsible and ethical implementation of these technologies in real-world applications. Furthermore, the integra-

tion of multi-modal biometric fusion techniques, such as combining fingerprint with other biometric modalities or contextual information, holds promise for enhancing the robustness and reliability of authentication systems, especially in challenging scenarios or under adversarial conditions. Lastly, advancements in hardware technologies, such as high-resolution sensors and efficient processing units, can significantly contribute to improving the accuracy and efficiency of unformatted fingerprint image authentication methods. Collaborative efforts between academia, industry, and regulatory bodies are essential to drive innovation, address emerging challenges, and ensure the continued advancement and responsible deployment of fingerprint authentication technologies in various domains. By pursuing these research directives, the field of unformatted fingerprint image authentication can continue to evolve and meet the growing demand for secure and reliable biometric authentication solutions.

Table 1: Comparative Analysis of Unformatted Fingerprint Image Authentication Methods

| Sl No | Paper | Year | Method                                                                                     | Dataset                                                        | Metric                                                       | Accuracy                                          | Limitation                                                                                                             |
|-------|-------|------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 1     | [4]   | 2012 | Robust alignment algorithm, descriptor-based Hough transform                               | NIST Special Database 27 (NIST SD27)                           | Rank-1 accuracy                                              | 53.5%                                             | Performance highly correlated with minutiae count and print quality. Not effective for singular point-based alignment. |
| 2     | [5]   | 2014 | Feedback mechanism from exemplar print                                                     | NIST SD27, WVU latent databases                                | Improvement in identification accuracy                       | 0.5-3.5%                                          | Trade-off between introducing feedback and system complexity. Effectiveness depends on exemplar print quality.         |
| 3     | [6]   | 2016 | Deformable Minutiae Clustering                                                             | NIST SD27, FVC2002, FVC2004, FVC2006, NIST SD4                 | Accuracy                                                     | Up to 85.6% (Cylinder-Codes), 83.3% (m-triplets)  | Slow speed, scalability issues, not effective for latent-to-latent fingerprint identification.                         |
| 4     | [7]   | 2017 | Adaptive latent fingerprint segmentation                                                   | NIST SD4, NIST SD 27, IITD CLF,                                | Rank 50 identification                                       | 78.7%,                                            | Assumption of consistent ground truth across examiners, limitations of SIVV based metric.                              |
| 5     | [8]   | 2018 | Collaborative filtering model for enhancing fingerprint image                              | FVC2004                                                        | EER, FMR100                                                  | 4.54, 7.5                                         | Fixed patch size limitation, sensitivity to input quality.                                                             |
| 6     | [9]   | 2018 | Convolutional neural network (CNN) FingerNet for latent fingerprint enhancement            | NIST SD27                                                      | Matching accuracy                                            | 47.7%                                             | Small dataset size, lack of ground truth for region of interest.                                                       |
| 7     | [10]  | 2018 | Automated latent fingerprint recognition system with ConvNets                              | NIST SD27, WVU latent databases                                | Rank 1 identification accuracies                             | 64.7%, 75.3%                                      | Poor ridge quality, background noise, dependence on manual ROI selection, long processing times.                       |
| 8     | [11]  | 2019 | Minutiae-based matcher improvement using rare minutiae                                     | GCDB                                                           | Rank-1 identification                                        | 92.72%                                            | Need for manual intervention, dataset size limitations.                                                                |
| 9     | [12]  | 2019 | End-to-end latent fingerprint identification system                                        | NIST SD27, MSP, WVU, N2N, background set of 100K rolled prints | Rank-1 retrieval rates                                       | 65.7%, 69.4%, 65.5%, 7.6%                         | Challenges in cropping algorithm, marking minutiae, and scalability.                                                   |
| 10    | [13]  | 2020 | Asynchronous processing for Latent Fingerprint Identification (ALFI)                       | NIST SD27, FVC 2004, FVC 2006                                  | F1-score, Equal Error Rate (EER)                             | 4.18%, 3.36%                                      | Limited test set, single classification approach, not tested on non-fingerprint latent features.                       |
| 11    | [14]  | 2020 | LQMetric: objective, automated tool for measuring the quality of latent fingerprints       | NIST ELFT-EFS-2 evaluation                                     | Clarity prediction, AFIS performance                         | 61.4%                                             | Performance not generally applicable to other AFIS algorithms or systems.                                              |
| 12    | [15]  | 2020 | Progressive GAN-based method for latent fingerprint enhancement                            | NIST SD27                                                      | CMC curve metrics                                            | 76%                                               | Computationally expensive, limited dataset size, may not work well with very weak features.                            |
| 13    | [16]  | 2020 | End-to-end automated latent fingerprint identification system using DCNN-FFT enhancement   | FVC2002, FVC2004, NIST SD27                                    | Precision, recall, F1 scores                                 | 100% for FVC2002 and FVC2004, 84.5% for NIST SD27 | Computational time for minutiae extraction, limited evaluation dataset.                                                |
| 14    | [17]  | 2020 | Deep nested UNets architecture for automatic segmentation and enhancement                  | NIST SD27, IITD-MOLF                                           | PA, MPA, MIoU                                                | 0.96, 0.96, 0.84                                  | Lack of publicly available databases with pairs of low-quality latent and high-quality fingerprint images.             |
| 15    | [18]  | 2020 | Non-minutia latent fingerprint registration method using dense fingerprint patch alignment | NIST27, MOLF                                                   | Deviation between matched minutiae, registration performance | 87.22%, 2.42                                      | Relying only on 2D information, computationally demanding.                                                             |

|    |      |      |                                                                                                         |                                                               |                                           |                       |                                                                                                                                                                          |
|----|------|------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 16 | [19] | 2021 | Fusion of pores and minutiae for latent fingerprint identification                                      | IIITD Latent database                                         | True detection rate, false detection rate | 82.89%,21.2%          | Limited database size, computational expense.                                                                                                                            |
| 17 | [20] | 2021 | Latent fingerprint identification using Ratio of Minutiae Triangles                                     | FVC2004, NIST SD27                                            | Rank-1 recognition accuracy               | 78.75%,86.82%         | Handling of partial fingerprint, computational complexity.                                                                                                               |
| 18 | [21] | 2021 | Hybrid model using EDTV for enhancement and Chan-Vese for segmentation                                  | NIST SD27, WVU DB                                             | Rank-1 identification                     | 72%                   | Limited database size, effectiveness in handling complex latent fingerprints.                                                                                            |
| 19 | [22] | 2021 | Adaptive latent fingerprint segmentation and matching using Chan-Vese based on EDTV                     | NIST SD27                                                     | RMSE                                      | 0.1837301             | Inadequate accuracy of existing techniques for segmentation.                                                                                                             |
| 20 | [23] | 2022 | Automatic latent fingerprint identification system using scale and rotation invariant minutiae features | FVC2004, NIST SD27                                            | Rank-1 identification accuracy            | 97.5%,88.8%           | Handling partial fingerprints, computational complexity.                                                                                                                 |
| 21 | [24] | 2022 | Minutia patch embedding network (MinNet) model                                                          | EGM Test Dataset, FVC-Latent Test Dataset, Tsinghua Distorted | Rank-1 Acc                                | 92.39%, 85.88%        | Limited success with partial or severely distorted fingerprints                                                                                                          |
| 22 | [25] | 2022 | Multi-scale fixed-length representation approach                                                        | Hisign, NIST SD27, MOLF, N2N                                  | Rank-1 Accuracy                           | 98.8%,99.81%          | Performance may vary on simulated fingerprints, optimization limited to study scope                                                                                      |
| 23 | [26] | 2022 | Residual encoder-decoder architecture                                                                   | IIIT-Delhi Multi Sensor Latent Fingerprint (MOLF) database    | Rank-25, Rank-50 Acc                      | 48.95%, 70.89%        | Ridge-based, limitations in reconstructing some parts of images, evaluation on different databases needed                                                                |
| 24 | [27] | 2022 | Analysis of fairness in latent fingerprint prediction                                                   | FBI WVU BioCop 2008 database                                  | AUC, SN, SP, PPV                          | 65.7%,69.4%           | Limited to FBI BioCoP database, quality measurements may not fully represent unbiased quality score, modelling assumptions of LFIQ algorithm may not always be satisfied |
| 25 | [28] | 2023 | Universal Latent Fingerprint Enhancer (ULPrint)                                                         | MSP database, NIST 302 database, Synthetic latent fingerprint | Rank-1 retrieval                          | 29.07%                | Scarcity of latent ,Challenges like occlusion, background variation, some failure cases mentioned                                                                        |
| 26 | [29] | 2023 | FingerGAN for latent fingerprint enhancement                                                            | NIST SD27, IIIT-Delhi MOLF                                    | Rank-1 accuracy                           | 76.36%                | Computational complexity, absence of true mates                                                                                                                          |
| 27 | [30] | 2023 | Combination of local and global features with automatic seg.                                            | NIST SD 27, NIST SD 302, MSP, MOLF DB1/DB4, MOLF DB2/DB4      | Rank-1 Retrieval Rate                     | 84.11%,70.43%,62.84%  | Challenges like low contrast, occlusion, varying backgrounds, some failure cases mentioned                                                                               |
| 28 | [31] | 2023 | Hybrid technique called AC-SACO for latent fingerprint recognition                                      | NIST SD-27                                                    | Precision, Recall, F-score                | 82.07%, 98.86%,89.68% | May not work well for complex backgrounds or overlapping latent fingerprints, need to explore other optimization techniques and datasets for validation                  |
| 29 | [32] | 2023 | Generation of synthetic latent fingerprints for data augmentation                                       | NIST SD27 ,MSP latent Database                                | True Detection Rate                       | 75.19%,77.02%         | Use of only one pre-trained fingerprint matcher, lack of publicly available operational latent fingerprint databases                                                     |

The Table 2 provides a detailed comparative analysis of various fingerprint liveness detection methods, encompassing a range of techniques such as feature extraction, machine learning, deep learning, and fusion approaches. Each method demonstrates different strengths and limitations in terms of accuracy, dataset applicability, and susceptibility to spoofing attacks. For instance, deep learning-based approaches, such as convolutional neural networks (CNNs) and stacked auto encoders, have shown promising results in achieving high detection accuracy. However, they often require large and diverse datasets for training to generalize well across different sensors and spoofing materials. Future research in fingerprint liveness detection should address several key challenges and explore new avenues for improvement. Firstly, there is a need to enhance the robustness and generalization capabilities of existing methods by leveraging larger and more diverse datasets that encompass various sensor types, image qualities, and spoofing materials. Additionally, researchers should focus on developing techniques capable of detecting low-resolution fingerprints and effectively handling imbalanced datasets to mitigate bias and improve overall performance. Secondly, the development of adaptive and resilient liveness detection systems that can dynamically adjust to evolving spoofing attacks is crucial. This may involve exploring novel approaches such as adversarial training, ensemble learning, and anomaly

detection to detect and adapt to emerging threats effectively. Moreover, incorporating multi-modal biometric fusion techniques, such as combining fingerprint with iris or face modalities, could further enhance the robustness and reliability of liveness detection systems. Furthermore, research efforts should concentrate on addressing ethical considerations related to the deployment of fingerprint liveness detection systems, including privacy concerns, algorithmic fairness, and transparency in decision-making processes. Developing standards and guidelines for evaluating and benchmarking liveness detection methods could also facilitate fair comparisons and promote reproducibility across different studies. Lastly, advancements in hardware technologies, such as improved sensor designs and embedded processing capabilities, can play a vital role in enhancing the efficiency and real-world applicability of fingerprint liveness detection systems. Collaborative efforts between academia, industry, and regulatory bodies are essential to drive innovation and ensure the responsible development and deployment of liveness detection technologies in various domains, including cyber security, law enforcement, and mobile authentication. By addressing these research directives, the field of fingerprint liveness detection can continue to evolve and meet the growing demand for secure and reliable biometric authentication solutions.



Table 2: Comparative Analysis of Fingerprint Liveness Detection Methods

| Sl No | Paper | Year | Method                                                                                  | Dataset                                            | Metric                             | Accuracy                                                             | Limitation                                                                                                         |
|-------|-------|------|-----------------------------------------------------------------------------------------|----------------------------------------------------|------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| 1     | [33]  | 2016 | Combination of low-level features, shape analysis, and PCA                              | LivDet 2011, LivDet 2013                           | EER                                | 3.95%                                                                | Need for more testing on different sensors and spoofing materials.                                                 |
| 2     | [34]  | 2017 | Co-occurrence array-based feature extraction and SVM classification                     | LivDet09DB, LivDet11DB                             | Average classification error       | 6.2%                                                                 | Loss of image information through quantization, large feature dimension.                                           |
| 3     | [35]  | 2018 | Deep CNN using local patches centred on minutiae                                        | LivDet 2011, LivDet 2013, LivDet 2015              | Average accuracy                   | 99.03% (LivDet 2015)                                                 | Need for more diverse datasets and ethical considerations.                                                         |
| 4     | [36]  | 2019 | BP neural network using difference co-occurrence matrices                               | LivDet 2013                                        | Classification accuracy            | 5.65%                                                                | Lack of diagonal direction difference co-occurrence matrices, challenge in distinguishing poor quality images.     |
| 5     | [37]  | 2020 | Semi-supervised stacked auto encoder-based hierarchical feature learning                | LivDet 2011, LivDet 2013                           | Average classification error       | 19.62%                                                               | Insufficient size of the dataset, difficulty in distinguishing poor quality images.                                |
| 6     | [38]  | 2020 | Adversarial attacks on deep learning-based liveness detection models                    | LivDet 2013, LivDet 2015                           | Error rate, FAR, FRR               | 4.3%, 3.7%                                                           | Limited diversity of fingerprint databases, simplicity of fingerprint liveness detection models.                   |
| 7     | [39]  | 2020 | Score-level fusion of fingerprint matching and liveness detection                       | LivDet2015, LivDet2019                             | Overall accuracy                   | 96.88% (LivDet2019)                                                  | Influence of finger pressure and duration on detection accuracy.                                                   |
| 8     | [40]  | 2020 | Genetic algorithm optimized DenseNet for liveness detection                             | LivDet 2009, LivDet 2011, LivDet 2013, LivDet 2015 | Accuracy                           | 98.22% (mixed Livdet dataset)                                        | Limited size of the dataset, requirement for specific sensor-matched datasets.                                     |
| 9     | [41]  | 2020 | Liveness detection using Circular Gabor Wavelet algorithm and SVM                       | -                                                  | Accuracy                           | 99.968% (FAR)                                                        | Limited experimentation on artificial spoofing methods.                                                            |
| 10    | [42]  | 2020 | Fingerprint and iris fusion-based liveness detection using statistical texture features | ATVS, LivDet2011                                   | Precision, accuracy                | 94.7% (fingerprint detection), 97.8% (decision-level classification) | Applicability to certain types of attacks, dependency on dataset size.                                             |
| 11    | [43]  | 2020 | FLDNet CNN                                                                              | LivDet 2013, 2015                                  | ACE                                | 1.76%                                                                | Improve accuracy on small fingerprints                                                                             |
| 12    | [44]  | 2021 | One-class Convolutional Auto encoder                                                    | -                                                  | D-EER                              | 2.00%                                                                | Lack of generality                                                                                                 |
| 13    | [45]  | 2021 | Weighted MCNN                                                                           | LivDet 2011, 2013, 2015, NUAA                      | Classification accuracy            | 2.42%                                                                | Diversity of sensors                                                                                               |
| 14    | [46]  | 2021 | EaZY Learning                                                                           | LivDet 2011, 2013, 2015                            | Accuracy                           | 60.49%, 67.80%                                                       | Dependence on clustering                                                                                           |
| 15    | [47]  | 2021 | Transformers + GANs                                                                     | LivDet 2015                                        | Accuracy                           | 68.52% - 83.12%                                                      | Poor generalization                                                                                                |
| 16    | [48]  | 2021 | Person-specific FPAD                                                                    | -                                                  | Accuracy                           | 100%                                                                 | Limited generalization                                                                                             |
| 17    | [49]  | 2021 | Multi-CNNs + Genetic Algorithm                                                          | Livedet datasets                                   | Accuracy                           | +1.0%                                                                | Fixed-scale input limitation                                                                                       |
| 18    | [50]  | 2022 | CNN                                                                                     | LivDet 2015                                        | Accuracy                           | 85.33%                                                               | Challenges with various materials                                                                                  |
| 19    | [51]  | 2022 | Multi-filter Framework                                                                  | LivDet 2009, 2011, 2013, 2015                      | ACC, ACE                           | 99.15%, 0.85%                                                        | Extensive parameter configuration                                                                                  |
| 20    | [52]  | 2022 | MFAS                                                                                    | 24 subjects                                        | Accuracy                           | 100%                                                                 | Limitations in real-life scenarios                                                                                 |
| 21    | [53]  | 2022 | A-iLearn model for incremental learning                                                 | LivDet 2011, LivDet 2013, LivDet 2015              | Overall Accuracy                   | Up to 49.57% improvement on new fake materials                       | Possibility of over fitting, need for further investigation of hand crafted and deep features                      |
| 22    | [54]  | 2022 | Static-based approach with fusion of pores perspiration and texture features            | LivDet 2013, LivDet 2015                           | Average Classification Error (ACE) | Biometrika: 0.11%, Italdata: 0.24%, Cross match: 0.21%               | Limited amount of pore feature-based algorithms, difficulty in maintaining and updating algorithms                 |
| 23    | [55]  | 2023 | Lightweight FLD network (LFLDNet) with CycleGAN and ResNet with MHSA                    | LivDet 2011, LivDet 2013, LivDet 2015              | Average Classification Error       | 1.72 across all sensors, 95.27% accuracy on small-area fingerprints  | Running speed affected by various factors, need for exploration of more effective FLD technology                   |
| 24    | [56]  | 2023 | FPAD based on adversarial data augmentation and CNNs                                    | LivDet2021                                         | EER, BPCER, APCER, Liv. ACC        | EER: 0.036, BPCER: 0.072, APCER: 0.000, Liv. ACC: 0.965              | Limited dataset size, generalizability to other presentation attacks, possibility of adversarial attacks           |
| 25    | [57]  | 2023 | Fingerprint liveness detection using deep learning with LPDJH descriptor                | LivDet 2009, LivDet 2011, LivDet 2013, LivDet 2015 | Average EER                        | LivDet 2011: 3.95%                                                   | Difficulty in detecting low-resolution fingerprints, estimation difficulty due to limited test samples             |
| 26    | [58]  | 2023 | Fingerprint liveness detection utilizing CNNs                                           | Socofing dataset                                   | Accuracy, FAR, FRR                 | Accuracy: 98.964%, FAR: 0.215%, FRR: 7.251%                          | Imbalanced distribution in dataset, varying quality and characteristics of fingerprints, computational constraints |

The Table 3 offers a comprehensive comparative analysis of various biometric cryptosystems, shedding light on different methods, datasets, metrics, accuracies, and limitations associated with these approaches. These biometric cryptosystems encompass a wide array of techniques such as fuzzy vault-based fingerprint cryptosystems, biometric key binding schemes, cryptographic authentication schemes based on discrete logarithm problems, and multi-biometric template security mechanisms, among others. Each method demonstrates specific strengths, including high accuracy,

robust security, and effectiveness in protecting biometric templates. However, they also encounter challenges such as susceptibility to privacy attacks, computational complexity, limitations in dataset availability, and reliance on specific biometric modalities. Several future research directives emerge from this analysis. Firstly, there is a pressing need for the development of more efficient and secure biometric cryptosystems capable of addressing emerging security threats and vulnerabilities, including adversarial attacks, privacy breaches, and database-level attacks. Secondly,

research efforts should focus on enhancing the scalability and usability of biometric cryptosystems, particularly in real-world applications such as secure communication, access control, and identity verification. Thirdly, the exploration of novel cryptographic primitives, deep learning techniques, and hardware implementations could lead to innovative biometric cryptosystems with improved performance and reliability. Moreover, future research should prioritize the development of biometric cryptosystems that are compliant with regulatory requirements such as GDPR and HIPAA, while also ensuring user privacy and data protection. Additionally, efforts should be directed towards

standardizing evaluation protocols and benchmarks to facilitate fair comparisons and reproducibility across different biometric cryptosystems. Furthermore, research should focus on the integration of biometric cryptosystems with emerging technologies such as blockchain and IoT to enhance security and interoperability in diverse application scenarios. By addressing these future research directives, the field of biometric cryptosystems can advance towards more secure, efficient, and user-centric solutions, thereby meeting the evolving needs of various domains including cyber security, healthcare, finance, and law enforcement.

Table 3: Comparative Analysis of Biometric Cryptosystems

| Sl No | Paper | Year | Method                                                                                                                     | Dataset                                                                                     | Metric                                                      | Accuracy                                     | Limitation                                                                                                                    |
|-------|-------|------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1     | [59]  | 2015 | Alignment-free fuzzy vault-based fingerprint cryptosystem using highly discriminative pair-polar (P-P) minutiae structures | FVC 2000 (DB1), FVC 2002 (DB1, DB2, DB3, DB4), FVC 2004 (DB2), FVC 2006 (DB2, DB3)          | GAR, FAR                                                    | 5.78%, 0.06%                                 | Security proof relies on complexity of brute force attack                                                                     |
| 2     | [60]  | 2016 | Feature level sequential fusion algorithm for biometric cryptosystems                                                      | Publicly available finger-vein database                                                     | FAR                                                         | 1.47% FAR                                    | Limited analysis of external security threats                                                                                 |
| 3     | [61]  | 2016 | ECC-free biometric key binding scheme using Graph-based Hamming Embedding (GHE) and Minutia Vicinity Decomposition (MVD)   | FVC 2002 (DB1, DB2)                                                                         | GAR, FRR, FAR                                               | GAR: 89%-97%, FRR: 3%-11%, FAR: 0.061%-0.16% | Vulnerable to privacy attacks like ARM and SKI, limited to matching fingerprint images of the same finger                     |
| 4     | [62]  | 2018 | Biometric template security mechanism based on two-dimensional logistic sine map (2DLSM)                                   | CASIA iris database, FVC 2002 (DB3)                                                         | Global shannon entropy                                      | 7.90                                         | noise sensitivity, inability to generate biometric templates in real-time                                                     |
| 5     | [63]  | 2018 | Secure cryptographic authentication scheme based on discrete logarithm problem                                             | CASIA iris database                                                                         | Inner and outer Hamming distance distributions, FA, FR, BER | 1.16%, 28.3%                                 | need for enhancing iris codes for better performance                                                                          |
| 6     | [64]  | 2019 | Biometric-based cryptographic key generation mechanism using convolution coding principles (BioKEY)                        | MIAS, FVC2002, FVC2004                                                                      | True positive rate                                          | 95.12%                                       | struggle with noisy or blurred fingerprints, significant computational time                                                   |
| 7     | [65]  | 2019 | ECC-based mutual authentication scheme for Smart Grid communications using biometric approach                              | Inhouse Dataset                                                                             | Computation cost                                            | 8.92 ms                                      | vulnerability to certain attacks                                                                                              |
| 8     | [66]  | 2020 | Fuzzy vault method for template security of multimodal biometric systems with face and fingerprint images                  | Virtual face and fingerprint database                                                       | GAR                                                         | 99%                                          | balancing security and accuracy                                                                                               |
| 9     | [67]  | 2020 | Enhanced iris recognition approach using hyperelliptic curve cryptography (HECC)                                           | CASIA Iris V-4, IITD iris datasets                                                          | Accuracy                                                    | 99.74%                                       | limitations with fuzzy extractor's parameters and potential attacks                                                           |
| 10    | [68]  | 2020 | Multibiometric cryptosystem for user authentication                                                                        | 100 subjects with iris and fingerprint modalities                                           | FRR, EER                                                    | 0.01, 0.005                                  | Limitations in accuracy and precision due to variability of biometric data                                                    |
| 11    | [69]  | 2020 | Multi-biometric template security method based on unique graph generation                                                  | CIE Fingerprints of IITD Database                                                           | ERR                                                         | Low ERR of 0.66%                             | Dependency on input sample quality                                                                                            |
| 12    | [71]  | 2020 | Multimodal biometric cryptosystem using fingerprint and ear                                                                | Fingerprint and ear image datasets                                                          | accuracy                                                    | 98.76%                                       | Reliance on systems for high accuracy                                                                                         |
| 13    | [72]  | 2021 | Biometric cryptosystem based on random projection and back propagation neural network                                      | NIST SD4, Faces94                                                                           | FNMR                                                        | 2.90%                                        | Time-consuming training process for off-line enhancement, need for further research on multiple-biometric template protection |
| 14    | [73]  | 2021 | Fingerprint biometric cryptosystem based on fuzzy commitment scheme and CNN                                                | FVC2000 DB2-A fingerprint database                                                          | FAR, FRR, EER                                               | FAR: 1.25%, FRR: 1.15%, EER: 2.83%           | Challenge of determining reference point precisely, need for larger training set                                              |
| 15    | [74]  | 2021 | Cancellable biometric authentication framework leveraging GA                                                               | ORL, FERET, LFW                                                                             | AROC                                                        | 0.9998                                       | Need for further validation on larger and more diverse datasets                                                               |
| 16    | [75]  | 2021 | Cancellable biometric security system based on advanced chaotic maps                                                       | In House                                                                                    | EER                                                         | 0.593                                        | Non-invertibility of biometric transformations, minor changes in biometrics affect hash functions                             |
| 17    | [76]  | 2021 | Cancellable Biometrics Vault (CBV) using chaffing and winnowing                                                            | CASIA-V3-Interval                                                                           | FRR, FAR                                                    | 6.92%, 0.001%                                | unsuitable for real-time applications due to computational complexity                                                         |
| 18    | [77]  | 2021 | Multi-biometric cryptosystem based on Modulus Fuzzy Vault algorithm                                                        | IIT Delhi Iris Database, IIT Delhi Palmprint Database, IIT Delhi Ear Database, NIST Special | ROC curve, FAR, FRR, GAR                                    | 0.96                                         | Limited focus on specific algorithms, need for experiments with natural image databases                                       |

|    |      |      |                                                                                                                                     |                                              |                           |                                                               |                                                                                                                                  |
|----|------|------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 19 | [78] | 2022 | Machine vision gait-based biometric cryptosystem using fuzzy commitment scheme                                                      | CMU MoBo, CASIA A                            | FAR, FRR                  | 0%                                                            | Recognition limitations due to variations like complex background and occlusions                                                 |
| 20 | [79] | 2022 | Asymmetric cryptosystem based on elliptic curve algorithm and optical scanning cryptography (OSC)                                   | Inhouse                                      | Information entropy       | 7.95                                                          | Speed limitations in encryption and decryption, vulnerability to cipher-text-only attacks                                        |
| 21 | [80] | 2022 | Fuzzy extractor for generating cryptographically strong keys from biometric images using deep learning and code-based cryptosystems | LFW, CelebA                                  | Accuracy                  | 93%                                                           | Requirement for large storage capacities with deep learning, susceptibility to attacks based on machine learning model inversion |
| 22 | [81] | 2022 | Block chain-based user re-enrolment scheme for biometric-based authentication systems                                               | Artificial dataset                           | Time complexity           | 0.1515                                                        | Computational complexity dependent on number of users, assumption of non-adversarial participants                                |
| 23 | [82] | 2022 | Secured multi-biometric template protection using Lagrange's interpolation                                                          | The Hong Kong Polytechnic University dataset | Accuracy                  | 99.9816%                                                      | Increase in database size, may not meet all ISO/IEC 24745 requirements                                                           |
| 24 | [83] | 2023 | Hardware design of secure cancellable biometric cryptosystem based on 3D chaotic map                                                | ORL, FVC, LFW                                | EER, AROC                 | EER of $6.2460 \times 10^{13}$ , AROC=0.9998                  | Needs further study on different types of attacks and larger datasets                                                            |
| 25 | [84] | 2023 | Cancellable biometric authentication mechanism using 3D chaotic maps, PWLCM, logistic map, and DNA sequencing theory                | Various face and palm print datasets         | AROC, FAR, DH, SSIM, PSNR | AROC = 1, AFAR of $6.2 \times 10^3$ , ADH=0.8755, PSNR=8.2061 | Increase in computational resources required                                                                                     |
| 26 | [85] | 2023 | Enhanced Biometric Cryptosystem (BCS) using ear and iris modalities based on BRIEF                                                  | AMI, UBIPr                                   | NRMSE                     | 1.7486                                                        | Susceptibility to database-level attacks, need for more sophisticated security techniques                                        |
| 27 | [86] | 2023 | Multi-biometric secure-storage scheme based on deep learning and crypto-mapping techniques                                          | CASIA V4, MICHE, ICUB, MobiFace              | AUCROC, EER               | 0.054                                                         | Need for hardware implementation, possibility of over fitting, trade-off between security and recognition performance            |
| 28 | [87] | 2023 | Biometric key generation and multi-round AES cryptosystem for improved security                                                     | Inhouse                                      | Energy efficiency         | 24.67 ms                                                      | Lack of dataset details, limited encryption techniques tested, limited performance metrics reported                              |

The Table 4 presents a comparative analysis of cancellable biometric methods, offering insights into various techniques, datasets, metrics, accuracies, and limitations associated with these approaches. These methods encompass a wide range of strategies such as protection methods for fingerprint templates, generating masterprints for impersonation, one-factor cancellable biometric authentication schemes, secure triplet loss for training deep learning models, and multi-server authentication using cancellable biometrics and PUF, among others. Each method exhibits specific strengths, including high recognition accuracy, robustness against attacks, and effectiveness in protecting biometric templates. However, they also face challenges such as computational complexity, vulnerability to specific attacks, dependence on dataset characteristics, and limitations in adaptability to diverse biometric modalities. Several future research directions emerge from this analysis. Firstly, there is a need for the development of more efficient and scalable cancellable biometric techniques, particularly in addressing computational complexity issues and improving performance across diverse biometric datasets. Secondly, research efforts should focus on enhancing the security and robustness of cancellable biometric methods against evolving threats and

sophisticated attacks, including template inversion attacks, brute-force attacks, and adversarial manipulations. Thirdly, the exploration of novel approaches such as deep learning-based fusion techniques, chaotic-based cancellable systems, and image style transfer for biometric authentication could lead to innovative solutions with improved performance and reliability. Moreover, there is a need for standardized evaluation protocols and benchmarks to facilitate fair comparisons and reproducibility across different cancellable biometric methods. Additionally, future research should prioritize the development of cancellable biometric techniques that are user-friendly, privacy-preserving, and compliant with regulatory requirements such as GDPR and HIPAA. Furthermore, efforts should be directed towards investigating the usability and acceptability of cancellable biometric systems in real-world applications such as access control, identity verification, and secure authentication. By addressing these future research directives, the field of cancellable biometric methods can advance towards more secure, efficient, and user-centric solutions, thereby meeting the evolving needs of various domains including cyber security, healthcare, finance, and law enforcement.

Table 4: Comparative Analysis of Cancellable Biometric Methods

| Sl No | Paper | Year | Method                                                                                          | Dataset                                       | Metric                     | Accuracy                                                                | Limitation                                                         |
|-------|-------|------|-------------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------|
| 1     | [88]  | 2017 | Protection method for fingerprint templates using fused structures at feature level             | FVC 2002 and 2004 databases                   | EER, separability, KS test | DB1: 2.19%, DB2: 1.6%, DB3: 6.14%; DB1: 11.89%, DB2: 12.71%, DB3: 17.6% | Computational cost for large-scale databases, non-invertibility    |
| 2     | [89]  | 2017 | Generating "MasterPrints" for impersonation in partial fingerprint-based authentication systems | FingerPass DB7 dataset, FVC2002 DB1-A dataset | Imposter Match Rate (IMR)  | 6.77%, 1.31%, 0.36%, 3.51%                                              | Dataset imbalance, applicability limited to minutiae-based systems |



|    |       |      |                                                                                                          |                                                                    |                                               |                                                                                       |                                                                                                                            |
|----|-------|------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 3  | [90]  | 2018 | One-factor cancellable biometric authentication scheme using Indexing First Order hashing                | FVC 2002 and FVC 2004                                              | EER, genuine-imposter distribution            | 4.26%, 2.67%                                                                          | Vulnerable to COA, KPA, CCA; identifier unlinkability                                                                      |
| 4  | [91]  | 2019 | One-factor cancellable palmprint biometric recognition scheme based on OIOM hash and MSH                 | PolyU and TJU palmprint databases                                  | Recognition accuracy                          | 98.07%                                                                                | No explicit mention of limitations                                                                                         |
| 5  | [92]  | 2020 | Universal solution for multi-biometric systems using deep neural networks                                | IITD Iris and MMU2                                                 | DI, EER                                       | DI: 10.35, EER: 0.12                                                                  | Limited adaptiveness, need for sensitive environment                                                                       |
| 6  | [93]  | 2020 | Secure Triplet Loss for training end-to-end deep learning models for cancellable biometric templates     | Off-the-person ECG and unconstrained face images                   | EER                                           | 12.56%, 13.99%                                                                        | Vulnerability under specific attack scenarios, impact of variability factors                                               |
| 7  | [94]  | 2020 | Constrained Optimized Similarity-based Attack (CSA) on cancellable biometrics using IoM hashing          | LFW dataset                                                        | Success rate, FAI rate, TAI rate              | 99.19%, 98.58%, 0.2866%                                                               | Dependency on protected template information                                                                               |
| 8  | [95]  | 2020 | Non-invertible cancellable fingerprint template based on Delaunay triangulation                          | FVC2002 database                                                   | EER                                           | 1.6%, 2.5%, 2.8%, 3.3%, 2.4%                                                          | Concerns about compromised acquisition device, need for larger dataset                                                     |
| 9  | [96]  | 2021 | Highly optimized user template construction for fingerprint-based authentication                         | Nine different fingerprint databases                               | EER                                           | 0%                                                                                    | Performance limited by image quality, suggestion for multi-modal system                                                    |
| 10 | [97]  | 2021 | Constrained-optimized similarity-based attack on cancellable biometrics using IoM hashing and BioHashing | LFW dataset                                                        | SAR, FAI                                      | 72.74%, 72.11%                                                                        | Fixed model complexity, over fitting reliance on IoM hash code size                                                        |
| 11 | [98]  | 2021 | Cancellable template using GCD                                                                           | Facial, fingerprint, iris, palm print                              | EER, AROC                                     | High AROC up to 99.59%, low EER down to 0.04%                                         | High-quality initial biometric images needed                                                                               |
| 12 | [99]  | 2021 | Feature-adaptive random projection                                                                       | FVC2002 DB1-DB3, FVC2004 DB2                                       | EER, GAR, FAR                                 | 1.0%, 2.0%, 4.0%, 11.0%                                                               | Need for more discriminatory feature descriptor                                                                            |
| 13 | [100] | 2021 | Multi-server authentication using cancellable biometrics and PUF                                         | LFW dataset                                                        | CMC curve, ROC curve, DIR curve, DET curve    | 18 <sub>th</sub>                                                                      | Lack of evaluation against sophisticated attacks                                                                           |
| 14 | [101] | 2021 | BioCanCrypto: biocryptosystem on fingerprint cancellable templates                                       | FVC2002 (DB1, DB2, DB3)                                            | EER, FRR                                      | 0.12%, 0.59%, 2.71%                                                                   | Limited exploration in different feature spaces                                                                            |
| 15 | [102] | 2021 | Watermarking reinforcement scheme                                                                        | BioSecure, FVC2002 DB1                                             | FMR, GMR, EER                                 | 1.98%                                                                                 | Limited to single biometric trait                                                                                          |
| 16 | [103] | 2022 | Absolute Value Equations Transform (AVET)                                                                | Eight datasets for various biometrics                              | GAR                                           | 93.22%, 91.91%, 96.2%                                                                 | Fixed sample size, vulnerability to brute-force attacks                                                                    |
| 17 | [104] | 2022 | Multi-biometric cancellable scheme using deep fusion and deep dream                                      | Nine images from each biometric modality                           | NPCR, PSNR, SSIM, UIQ, SD, UACI               | 99.158%, 24.523, 0.079, 0.909, 59.582, 23.627                                         | Computationally intensive, requires enrollment of all seven images                                                         |
| 18 | [105] | 2022 | Cancellable multi-biometric identification scheme using ACM                                              | FVC2002, ICE 2005                                                  | EER, ROC curve                                | 0.0005, 0.0019                                                                        | Lack of large-scale database, need for reliable parameter estimation                                                       |
| 19 | [106] | 2022 | Cancellable SoftmaxOut Fusion Network (CSMoFN)                                                           | AR, Ethnic, Face-scrub, IMDB, Wiki, YTF                            | EER                                           | 6.67%, 6.71%                                                                          | Risk of CB template inversion                                                                                              |
| 20 | [107] | 2022 | Selective encryption and deep learning-based fusion technology                                           | "Lena" image, face images                                          | Correlation, entropy, ROC curve, AROC         | 0.0008, 0.0019                                                                        | Limited size of the dataset                                                                                                |
| 21 | [108] | 2023 | Deep learning and style transfer for cancellable biometric system                                        | 1800 images dataset segmented into face and fingerprint biometrics | NCC, MSE, PSNR, SSIM, UIQ, SD, UBER           | Average NPCR: 99.26, PSNR: 23.28, SSIM: 0.0405, UIQ: 0.7492, SD: 60.442, UACI: 24.268 | Need for consistent physical condition, reduced reliability in certain environmental conditions                            |
| 22 | [109] | 2023 | Multi-Biometric Feature Hashing (MBFH)                                                                   | Retina, finger veins, palm, dorsal vein images                     | Hamming, Spearman, Jaccard pairwise distances | Average values over 0.9 in Spearman, Jaccard, and hamming distances                   | Applicability to adaptable and featherless biometric features, need for adaptability for adding white Gaussian noise       |
| 23 | [110] | 2023 | Biometric template protection scheme for Euclidean and Cosine metrics                                    | AR Face, CASIA FaceV5, ORL, LFW                                    | EER                                           | 8.559, 0.154                                                                          | Not optimal for other types of biometric authentication systems, slightly higher computational costs due to pre-processing |
| 24 | [111] | 2023 | Chaotic-based cancelable face recognition system using convolution kernels                               | AT&T, YALE, UFI, LFW, FERET                                        | Accuracy                                      | 98.43%                                                                                | Trade-off between system performance and user privacy, need for adaptation to environmental circumstances                  |
| 25 | [112] | 2023 | Biometric authentication system using image style transfer                                               | Face image database with key images                                | Correlation coefficients, ROC curves          | AUC values > 0.9 in most cases                                                        | Problem of key image similarity, need for restrictions in setting key images in future studies                             |

The presented Table 5 offers a comprehensive analysis of various general-purpose user authentication methods, covering a wide range of techniques, datasets, metrics, accuracies, and limitations. These methods encompass diverse

approaches such as orientation extraction, fingerprint reconstruction, fake biometric trait detection, local model-based classification, partial fingerprint matching, minutiae extraction evaluation, and multi-modal biometric authentication,

among others. Each method demonstrates specific strengths, including high accuracy rates, robustness against attacks, and efficiency in authentication processes. However, they also encounter challenges such as dataset limitations, computational resource requirements, dependence on specific features, and vulnerabilities to spoofing attacks. Several future research directions can be identified from this analysis. Firstly, there is a need for the development of more robust and secure authentication methods, particularly in addressing vulnerabilities to spoofing attacks and enhancing resistance against adversarial manipulations. Secondly, research efforts should focus on improving the scalability and efficiency of authentication systems, especially in handling large-scale datasets and reducing computational resource requirements. Thirdly, the exploration of novel biometric features, fusion techniques, and machine learning

algorithms could further enhance the accuracy and reliability of authentication methods across diverse modalities. Moreover, the development of privacy-preserving authentication techniques and the investigation of human-centric design principles could ensure the usability and acceptability of authentication systems in real-world scenarios. Lastly, efforts should be directed towards standardizing evaluation protocols and benchmarks to facilitate fair comparisons and reproducibility across different authentication methods. By addressing these future research directives, the field of general-purpose user authentication can advance towards more secure, efficient, and user-friendly authentication systems, thereby meeting the evolving needs of various applications such as cybersecurity, access control, and identity verification.

Table 5: Comparative Analysis of General Purpose User Authentication Methods

| Sl No | Paper | Year | Method                                   | Dataset                           | Metric                                              | Accuracy                              | Limitation                                         |
|-------|-------|------|------------------------------------------|-----------------------------------|-----------------------------------------------------|---------------------------------------|----------------------------------------------------|
| 1     | [113] | 2011 | Orientation Extraction                   | FVC2006 DB2                       | Average Error                                       | 0.206%                                | Limited benchmark dataset                          |
| 2     | [114] | 2012 | Fingerprint Reconstruction               | FVC2002 DB1A, DB2A                | Successful Match Rate                               | 86.48%, 86.96%                        | Performance limitations for certain scenarios      |
| 3     | [115] | 2013 | Fake Biometric Trait Detection           | Fingerprint, Iris, 2-D Face       | Classification Error Rate                           | <3%                                   | Computational resources, full image access         |
| 4     | [116] | 2015 | Local Model-based Classification         | FVC 2000, 2002, 2004              | Accuracy                                            | 96.7%, 96.5%                          | Allocation of low-quality fingerprints for testing |
| 5     | [117] | 2016 | Partial Fingerprint Matching             | FVC2000, FVC2002                  | EER                                                 | 1.17%, 1.4%                           | Dependence on enhancement algorithm                |
| 6     | [118] | 2017 | Minutiae Extraction Evaluation           | FVC 2002, FVC2004, Synthetic data | Average positional error, Average orientation error | 3.48%, 0.06%                          | Environmental variations                           |
| 7     | [119] | 2017 | GLDM for Bio-Cryptosystems               | PUCPR, GPDS-300                   | Classification Error Rate                           | 7%, 17%                               | Limited positive signature samples                 |
| 8     | [120] | 2018 | Pore Extraction using CNN                | Touch-based, Touchless, Latent    | Detection Rate, False Alarm Rate                    | 84.69%, 15.31%                        | Need for high-resolution images                    |
| 9     | [2]   | 2019 | Pore Comparison                          | FVC2002 DB I, II                  | EER, FMR1000s                                       | 1.86%, 0.12%                          | Dependence on alignment accuracy                   |
| 10    | [121] | 2020 | Fingerprint Enhancement & Reconstruction | FVC2002, FVC2004                  | TAR                                                 | 97.95%, 94.09%                        | Impact of dirt, age, medical factors               |
| 11    | [122] | 2020 | DeepPoreID Matching                      | DBI, DBII                         | EER, FMR100                                         | 35% increase in EER                   | Dependence on large quantity of sweat pores        |
| 12    | [123] | 2020 | Homomorphic Encryption                   | FVC2002 DB2                       | EER                                                 | 9.23% EER                             | Time-consuming encryption                          |
| 13    | [124] | 2020 | SSO Feature Extraction                   | 150 images                        | FAR, FRR, CVR                                       | FAR: 0.00, FRR: 0.00666, CVR: 99.334% | Small dataset size                                 |
| 14    | [125] | 2020 | FHE-based Authentication                 | NIST SD9                          | EER                                                 | 0.053%                                | Time-consuming encryption                          |
| 15    | [126] | 2020 | BioSec Framework                         | FVC-2004 DB3                      | Accuracy                                            | 70%                                   | Vulnerability of symmetric encryption              |
| 16    | [127] | 2020 | Reversible Watermarking                  | FVC2002                           | PSNR, Matching Score                                | 99.61%                                | Sensitivity to noise and compression               |
| 17    | [128] | 2021 | Ensemble Matching                        | NIST SD27, GCDB, MOLF DB1         | Rank-1 identification rate                          | 74.03%                                | Choice of supervised classifier                    |
| 18    | [129] | 2021 | DRUNet Segmentation                      | FVC Databases                     | Jaccard similarity, Dice score                      | 97.21%, 94.73%                        | Small training dataset                             |
| 19    | [130] | 2021 | MiDeCon Quality Assessment               | FVC 2006                          | FMR                                                 | 10 <sup>-1</sup>                      | Complex procedure                                  |
| 20    | [131] | 2021 | ASRA Image Alignment                     | FVC2002, FVC2004                  | Authentication accuracy                             | 99%                                   | Dependence on ROI extraction                       |
| 21    | [132] | 2021 | VSS & Super-resolution                   | FVC2002 DB1                       | Genuine match rate                                  | 94%,                                  | Need for higher quality fingerprint images         |
| 22    | [133] | 2021 | Dual-filter Framework                    | LivDet 2013, 2015                 | Accuracy                                            | 97.56%                                | Framework agnostic to filter type                  |
| 23    | [134] | 2021 | Multi-modal Biometric Authentication     | 228 image                         | signal data & EER, ROC curves                       | Classification rate of 100%           | Not tested on large scale dataset                  |
| 24    | [135] | 2022 | Secure Authentication                    | FVC2002 DB1-DB3, FVC2004 DB1-DB3  | EER                                                 | 0.99%, 3.28%                          | Balance between security and performance           |
| 25    | [136] | 2022 | Embedded System Authentication           | In-house                          | Accuracy                                            | -                                     | Robustness against attacks                         |
| 26    | [137] | 2022 | Gabor Filter & CNN                       | FVC2006                           | Validation accuracy                                 | 99.33%                                | Management of smaller training sets                |
| 27    | [138] | 2022 | Deep CNN Matching                        | In-house                          | Training & validation accuracy                      | 100%                                  | Lack of diversity in dataset                       |
| 28    | [139] | 2022 | Multi-factor Authentication              | CASIA-FingerprintV5, FVC2002 DB1  | FAR                                                 | 0.81%                                 | Limited size of dataset                            |

|    |       |      |                                        |                                  |                                    |                             |                                                     |
|----|-------|------|----------------------------------------|----------------------------------|------------------------------------|-----------------------------|-----------------------------------------------------|
| 29 | [140] | 2023 | Brute-force Attack                     | In-house                         | FAR                                | 4.1410 <sup>6</sup>         | Need for smartphones to support sensor hot plugging |
| 30 | [141] | 2023 | Joint Authentication & Spoof Detection | FVC 2006 DB2A, LiveDet 2015      | TAR, FAR, ACE                      | TAR = 100%, ACE = 1.44%     | Need for larger and more diverse datasets           |
| 31 | [142] | 2023 | Homomorphic Encryption & ML            | PolyU, SOKOTO                    | F1-score                           | PolyU: 93.6%, SOKOTO: 98.2% | HE-based computation challenges                     |
| 32 | [143] | 2023 | Multi-factor Authentication            | In-house                         | System Usability Scale             | 90%                         | Small sample size                                   |
| 33 | [144] | 2023 | AAVO enabled DMN                       | CASIA Fingerprint Image Database | Accuracy, Sensitivity, Specificity | 0.927, 0.938, 0.930         | Need for robust pre-processing                      |

The Table 6 offers a comprehensive comparative analysis of various fingerprint indexing methods, encompassing different approaches, datasets, metrics, accuracies, and limitations. Notable methodologies include distributed frameworks, GPU-based systems, absolute registration approaches, minutiae-based algorithms, deep learning-based models, and privacy-preserving indexing techniques. These methods exhibit diverse strengths, such as high processing speeds, improved accuracies, and workload reduction, while also facing challenges like hardware/software dependencies, scalability issues, and computational costs. Several future research directions emerge from this analysis. Firstly, there's a need for continued exploration of deep learning techniques in fingerprint indexing, especially in improving accuracy and reducing computational costs. Additionally, addressing scalability concerns and hardware dependencies

would be crucial for real-world deployment. Secondly, the development of privacy-preserving indexing methods is vital to ensure the security and confidentiality of biometric data, especially in light of increasing concerns regarding data privacy. Thirdly, research efforts should focus on enhancing the robustness and generalization capabilities of indexing algorithms, particularly in handling diverse datasets with varying quality and characteristics. Moreover, investigating novel features and descriptors, as well as exploring multimodal approaches, could further improve indexing performance and reliability across different biometric modalities. Lastly, efforts should be directed towards standardizing evaluation protocols and benchmarks to facilitate fair comparisons and reproducibility across different indexing methods.

Table 6: Comparative Analysis of Fingerprint Indexing Methods

| Sl No | Paper | Year | Method                                                                                     | Dataset                                                                                                  | Metric                                     | Accuracy                                                                        | Limitation                                                                                                             |
|-------|-------|------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 1     | [145] | 2014 | Two-level distributed framework for fingerprint matching                                   | Large synthetic database created with SFinGe, NIST databases                                             | Spdd up                                    | 312.8684 sec                                                                    | Distribution of synthetic fingerprint dataset, hardware resources, scalability of matching algorithms                  |
| 2     | [146] | 2015 | Fingerprint identification system using GPUs                                               | FVC2002, DB14                                                                                            | EER                                        | 2%                                                                              | Potential benefits of GPU-based algorithms, need for a two-stage system for practical applications                     |
| 3     | [147] | 2016 | Absolute registration approach with pose constraint                                        | Public domain fingerprint databases, NIST Special Database 14, database of 1,000,000 rolled fingerprints | Error Rate                                 | 2.33%                                                                           | High dimensionality of the Minutia Cylinder-Code (MCC) descriptor, need for further research on noise and variability  |
| 4     | [148] | 2017 | Fingerprint indexing algorithm based on minutiae pairs and convex core point               | FVC2000DB2A+B, FVC2000DB3A+B, FVC2002DB1A+B, FVC2004DB1A+B, NIST's DB4 and DB14                          | TPR                                        | 2.18                                                                            | Lack of detail regarding parameters, hardware/software differences                                                     |
| 5     | [149] | 2019 | Minutiae-centred fingerprint indexing method with deep convolutional neural network (DCNN) | FVC2002 DB2a, FVC2002 DB2b, FVC2004 DB1a, NIST special database 4, NIST special database 14              | Error rate, penetration rate               | 0.25%, 10%                                                                      | High computational cost for MCC-based method                                                                           |
| 6     | [150] | 2019 | DeepPrint: Deep network for learning fixed-length fingerprint representations              | NIST SD4, last 2,700 pairs of NIST SD14                                                                  | Rank-1 search accuracy                     | 98.80%                                                                          | Fixed length representation, Saturation of existing benchmarks                                                         |
| 7     | [151] | 2020 | CNN-based Combination of Nearest Arrangement Indexing (CNAI)                               | FVC2004, NIST SD27 latent fingerprint databases                                                          | Rank-1 identification rate                 | 80%, 85.4%                                                                      | Dependence on the availability of minutiae points, failure of MINU-EXTRACTNET                                          |
| 8     | [152] | 2020 | Pore-based indexing method for high-resolution fingerprints                                | Hong Kong PolyU high-resolution fingerprint databases (DBI and DBII), IITI-HRFP, IITI-HRF                | Pre-selection error rate, penetration rate | 67%, 49%, 42%, 28%, 10%                                                         | Effectiveness limited on databases of high-resolution full fingerprints                                                |
| 9     | [153] | 2020 | Latent fingerprint indexing using minutiae based rotational and translational features     | IITI-D latent fingerprint dataset                                                                        | Accuracy, indexing time                    | Accuracy up to 94.77%, average indexing time ranging from 5.29 to 25.92 seconds | Challenges with partial impression, background noise, poor ridge clarity, large non-linear distortions                 |
| 10    | [154] | 2021 | Indexing algorithm based on clustering of minutia cylinder codes (MCC)                     | Public data, proprietary data, synthetic data, NIST SD4, NIST SD14                                       | Error rate, Penetration Rate               | 53.9%, 0.01%                                                                    | Reduced search space, lower performance on databases with different characteristics or quality levels, time complexity |
| 11    | [155] | 2021 | Pore-based indexing and refinement                                                         | DBI, DBII                                                                                                | Accuracy                                   | 95.16%                                                                          | Computation increase with pores                                                                                        |



|    |       |      |                                                                  |                                    |                              |                                |                                       |
|----|-------|------|------------------------------------------------------------------|------------------------------------|------------------------------|--------------------------------|---------------------------------------|
| 12 | [156] | 2021 | Inverted index for minutiae-based search                         | FVC2002 DB1a, Private dataset      | Error rate                   | 0.42%                          | High search rates                     |
| 13 | [157] | 2021 | PalmHashNet for palm print indexing                              | CASIA, IIT Delhi, Tongji, PolyU II | Accuracy                     | Above 99% accuracy             | Not tested on large datasets          |
| 14 | [158] | 2021 | MDSH-based indexing for multi biometric retrieval                | IIT Delhi (iris, face, palm print) | Hit rate, Penetration rate   | 68%, 100%                      | Computational costs                   |
| 15 | [159] | 2022 | Quality score-based search for biometric identification          | FERET, CASIA, FVC2002              | Workload                     | Up to 38% reduction            | High intra-class variability          |
| 16 | [160] | 2022 | FKPIndexNet for finger-knuckle-print identification              | PolyU-FKP, IITD-FKP                | Error rate, Penetration rate | 0.32%, 100%                    | Limitations in index table generation |
| 17 | [161] | 2022 | Signal-based fusion for biometric database indexing              | FERET, FRGCv2, IJB-A               | Workload                     | Reduced workload by 30%        | Requires high-quality images          |
| 18 | [162] | 2023 | Privacy-preserving multi-biometric indexing                      | Composite dataset                  | Workload                     | Workload reduction by 57%      | Use of composite dataset              |
| 19 | [163] | 2023 | Attention-Driven Fingerprint Recognition Network                 | NIST SD4, NIST SD14                | Accuracy                     | 99.93%                         | Not using domain knowledge            |
| 20 | [164] | 2023 | Gravitational Search Decision Forest for fingerprint recognition | NIST SD27, FVC2004                 | Precision, Recall, F-measure | 93.90%, 96.25%, 95.06%, 96.25% | Recognition rate optimization         |

The Table 7 presents a comprehensive overview of various methodologies employed for infant and child biometric recognition, highlighting the diverse approaches, datasets, metrics, accuracies, and limitations associated with each method. Several studies focus on fingerprint recognition, utilizing techniques ranging from image enhancement and CNN-based ridge flow estimation to pre-trained CNN models. These approaches demonstrate promising accuracies, with [166] achieving up to 99.5% True Accept Rate (TAR) for infant fingerprints. However, challenges persist, such as the lack of automated alignment methods and issues with small fingerprint sizes and low image quality, as noted by multiple authors. Moreover, alternative biometric modalities like footprints, iris, and outer ear shape are explored, showing potential for high accuracy, as evidenced by [168] 99.30% accuracy in footprint identification and [170] low Equal Error Rate (EER) for outer ear shape recognition. Nonetheless, these methods encounter hurdles related to data collection challenges, limited dataset sizes, and transparency in processes and facilities. Future research in infant and child

biometric recognition could address these limitations by focusing on several key areas. Firstly, efforts should be directed towards developing automated alignment techniques to enhance accuracy and efficiency, especially for infant fingerprints. Secondly, there is a need for larger and more diverse datasets to ensure robust model performance and generalization. Thirdly, exploration of multi-modal biometric systems, as suggested by [172], could provide enhanced accuracy and reliability by combining different biometric traits. Lastly, advancements in image acquisition technologies and computing resources could facilitate the collection of high-quality images and alleviate challenges associated with low image quality and computing resource requirements, as highlighted by [169]. By addressing these research directions, future studies can contribute towards the development of more robust, accurate, and reliable infant and child biometric recognition systems, thereby enhancing their applicability in various domains such as healthcare, security, and childcare.

Table 7: Comparative Analysis of Infant and Child Biometric Recognition Methods

| Sl No | Paper | Year | Method                                                                                        | Dataset                                                                            | Metric                                           | Accuracy                                             | Limitation                                                                                  |
|-------|-------|------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 1     | [165] | 2016 | Image enhancement, CNN-based ridge flow estimation                                            | Infant fingerprint database                                                        | Rank-1 identification accuracy                   | 73.98%                                               | Lack of automated fingerprint alignment for infants                                         |
| 2     | [166] | 2016 | Evaluation of child fingerprint recognition using NFIQ 2.0 metric                             | Dataset of infants aged 0-5 years                                                  | True Accept Rate (TAR), False Accept Rate (FAR)  | TAR: 99.5% (500 PPI), 98.9% (1270 PPI)               | Piecewise linear model interpretation, dataset resolution variations                        |
| 3     | [167] | 2021 | InfantPrints system with custom-built fingerprint reader                                      | Longitudinal infant fingerprint database                                           | TAR, FAR                                         | 95.2%, 1.0%                                          | Lack of automated alignment method                                                          |
| 4     | [168] | 2021 | Footprint identification using wavelet feature extraction and K-NN                            | Dataset of 30 babies with footprint images                                         | Accuracy, Precision, Recall                      | 99.30% accuracy, 90.17% precision, 89.44% recall     | Small dataset size, single feature extraction method                                        |
| 5     | [169] | 2022 | Neonate fingerprint classification using deep learning                                        | Dataset with manual labelling of fingerprint images                                | Accuracy                                         | 78.4%                                                | Computing resource requirements, challenges in collecting high-quality images               |
| 6     | [170] | 2023 | Biometric recognition systems for infants (fingerprint, iris, outer ear shape)                | Dataset from volunteer infants and children                                        | Equal Error Rate (EER), Failure to Acquire (FTA) | EER: 0.16% (outer ear shape)                         | Challenges in data collection, limitations in facility and process transparency             |
| 7     | [171] | 2023 | Multi-instance contingent fusion technique for infant fingerprint verification                | Dataset of infant fingerprints                                                     | Verification accuracy                            | 73.8% (1 month interval), 57.14% (6 months interval) | Absence of ancillary information, greater time interval necessitates fusion                 |
| 8     | [172] | 2023 | Multi-modal Biometric Recognition for Toddlers and Pre School Children (M <sup>2</sup> BRTPC) | Dataset of iris and fingerprint modalities from children aged 18 months to 4 years | Accuracy                                         | 96.3%                                                | Restricted age range, improvements over existing methods without claiming absolute accuracy |
| 9     | [173] | 2023 | Pre-trained CNN model for newborn and toddler fingerprint recognition                         | Dataset of fingerprint images from 154 subjects                                    | Accuracy                                         | 82.47%                                               | Small size of fingerprints, low image quality                                               |

|    |       |      |                                                                       |                                  |                                  |                              |                                                                                          |
|----|-------|------|-----------------------------------------------------------------------|----------------------------------|----------------------------------|------------------------------|------------------------------------------------------------------------------------------|
| 10 | [174] | 2023 | CNN-based children recognition system using contact less fingerprints | CLCF dataset for experimentation | Accuracy, Equal Error Rate (EER) | Accuracy: 98.46%, EER: 1.99% | Need for larger datasets, exploration of different enhancement and extraction techniques |
|----|-------|------|-----------------------------------------------------------------------|----------------------------------|----------------------------------|------------------------------|------------------------------------------------------------------------------------------|

Several important conclusions can be drawn from a comprehensive analysis of the literature on latent fingerprint recognition and biometric identification systems. With a wide range of strategies being investigated, such as deep learning models, hybrid approaches, and sophisticated algorithmic techniques, these systems have undergone tremendous evolution. Due to this diversity, difficult fingerprint identification problems like partial prints, noise, and inconsistent quality have been significantly improved. The literature does, however, also highlight enduring difficulties. The comparison of various methods is made more difficult by the absence of standard evaluation methodologies, and algorithmic bias and generalizability are raised by the small size and lack of diversity of the datasets that are currently accessible. Moreover, a lot of sophisticated techniques, especially those centred on deep learning, have a high computational complexity, which makes real-time implementation challenging. Future work in this area has to concentrate on creating uniform benchmarks, growing datasets, maximizing computational effectiveness, and resolving moral issues with bias and privacy. Advantage, disadvantage, area of improvement and ethical implication of the fingerprint biometric studied in the manuscript are discussed below.

#### • Advantage:

- **Diverse Methodologies:** The literature study demonstrates the wide variety of approaches, such as hybrid approaches, descriptor-based tactics, deep learning models, and different algorithmic advancements, that are employed in fingerprint recognition and biometric systems. Due to the variety of methods available, researchers are able to tackle several facets of latent fingerprint recognition issues, including handling partial prints, noise, and quality differences. For instance, descriptor-based methods may provide computational efficiency, while deep learning models might enhance accuracy by discovering complex patterns in fingerprint data. The use of hybrid techniques, which blend conventional and cutting-edge methodologies, shows an effort to capitalize on each approach's advantages and advance latent fingerprint recognition technology.
- **Quantifiable Performance Metrics:** Numerous studies provide comprehensive performance indicators, like F1 scores, recall, precision, and rank-1 accuracy, which are essential for evaluating the efficacy of various techniques. Benchmarking these measures against popular datasets such as FVC2004 and NIST SD27 is common practice. Researchers and practitioners find it easier to compare the effectiveness of different techniques, evaluate advances, and pinpoint areas that require additional development when such measurements are transparently reported. Because of its transparency, the community is able to monitor advancements and set performance standards for systems to come.
- **Cutting-edge Techniques:** Numerous novel methods

have been presented, such as deep learning-based minutiae extraction, deformable minutiae clustering, and data augmentation using Generative Adversarial Networks (GAN). Especially for under-represented instances, GAN-based augmentation might artificially generate extra training data, hence improving the system's resilience. Latent fingerprint identification systems are becoming more accurate and scalable thanks to deformable minutiae clustering and deep learning techniques. This makes them more suitable for use in forensic applications, particularly in challenging situations where the prints are imperfect or deteriorated.

- **Real-world Testing:** The fact that numerous suggested techniques are evaluated on a range of databases and datasets, including NIST SD27 and FVC2004, is a noteworthy strength of the examined literature. This makes it possible to test the algorithms in a variety of scenarios, simulating the unpredictability of the actual world. By doing this, scientists may evaluate how reliable and broadly applicable their methods are, making sure they work effectively outside of carefully regulated lab environments. For technology meant to be used in actual applications, including forensic investigations and security systems, this real-world applicability is essential.

#### • Disadvantages:

- **Lack of Uniformity in Evaluation Standards:** Although a large number of research offer performance indicators, there is a notable deficiency in uniform assessment procedures between various inquiries. Direct comparisons between approaches are challenging because to variations in benchmarking procedures, quality criteria, and dataset sizes. Because of this, some accuracy statistics might be inflated, which makes it more difficult to determine whether strategy is better in an unbiased manner. A technique that works well on a small, clean dataset, for instance, might not translate as well to larger, messier real-world data. Additionally, because there isn't a single benchmark, reported accuracy gains may vary depending on the context and may not apply to different circumstances.
- **Dataset Limitations:** The small size and lack of diversity of datasets used for testing and training is a problem that keeps coming up in the literature. A lot of research papers admit that their datasets are too tiny or homogeneous to adequately capture the heterogeneity present in real-world circumstances, especially when it comes to latent print datasets. This suggests that the models may be over fitting to the unique features of these small datasets, which raises questions about their generalizability. A system that works well on the dataset it was trained on but has trouble with under-represented populations or situations, including various skin kinds, lighting settings, or sensor types, may also be introduced by a lack of diversity.

- **Computational Complexity:** There is a drawback to several of the sophisticated methods, especially those that depend on deep learning: higher computational demands. These techniques frequently call for additional processing power, memory, and time, but they may provide considerable accuracy gains. It is difficult to apply these techniques in real-time scenarios, such as live fingerprint recognition at security checkpoints or mobile devices with constrained computing power, due to the rise in computational complexity. For example, deep learning models can yield higher recognition rates, but their resource needs make them impractical for use in real-time, low-power devices.
- **Areas for Improvement:**
  - **Standardized Benchmarks and Evaluation Protocols:** The creation of uniform protocols for comparing fingerprint recognition algorithms across various datasets is among the most urgent need. This would entail defining testing settings, dataset properties, and consistent evaluation criteria. Researchers may more precisely compare the performance of various approaches when a consistent framework is in place, which helps them determine which techniques are actually improving the state of the art. Exaggerated performance claims might be lessened by using a consistent evaluation process, which would guarantee that all approaches are examined under comparable circumstances [118].
  - **Larger and More Diverse Datasets:** Future study should concentrate on increasing the amount and diversity of latent fingerprint databases in order to solve the limitations of the present investigations. This would include gathering information from a larger variety of sources and in a greater variety of settings, including various skin tones, ambient variables, and sensor kinds. By using larger, more representative datasets for algorithm training, researchers can improve system robustness and minimize bias. It would be easier to make sure that the algorithms can handle the whole range of real-world issues if more diverse latent prints were included, such as those with different levels of noise, distortion, and completeness [145].
  - **Improving Computational Efficiency:** Because many of the methods are computationally demanding, optimization is required to shorten processing times without compromising accuracy. For real-time applications, where speed is a crucial component, this is especially crucial. To lessen their processing footprint, researchers can concentrate on creating lightweight algorithms or improving already-existing deep learning systems. For example, the models could be deployed in resource-constrained contexts like mobile devices or edge computing platforms if they are optimized to perform well on GPUs or embedded systems [25].
  - **Integration with Other Biometric Modalities:** Integrating fingerprint identification systems with other biometric modalities, such facial recognition or iris scanning, is another possible avenue for advancement. When one modality is impaired (a partial fingerprint, for example), this multi-modal method may enhance overall accuracy and resilience. Combining information from several biometric sources may also improve security by making it more difficult for hackers to impersonate the system. Future developments may proceed in the direction of sensor fusion technique research and the creation of reliable multi-modal biometric authentication algorithms [42].
- **Ethical Considerations and Privacy:** Future research must also address ethical issues including privacy concerns, data protection, and algorithmic bias given the growing usage of biometric technologies in sensitive applications like security and forensics. Strong legal frameworks are especially necessary for forensic applications in order to guarantee the validity and acceptability of the data gathered using these systems. Researchers should investigate the moral ramifications of gathering and using biometric data, making sure privacy laws like GDPR are followed, and creating clear procedures for handling user consent and data [180].
- **Ethical Implications:**
  - **Privacy Concerns:** Fingerprint biometric systems create serious privacy concerns since they rely on the gathering, storing, and processing of private information. Biometric information, like fingerprints, is unchangeable after it is compromised, unlike passwords or other identity-related information. Biometric data is particularly susceptible to exploitation because of this. Identity theft, unapproved tracking, or monitoring might result from unauthorized access to fingerprint databases or data breaches. These worries are heightened by the collecting of biometric data, frequently without users' express or informed agreement. The collection, storage, and sharing of this data must adhere to strict processes in order to comply with data protection legislation, such as the General Data Protection Regulation (GDPR) in Europe. Crucial to ethical compliance are letting users know how their biometric data is being used and providing them with the choice to opt out. To reduce these concerns, biometric systems should place a high priority on openness, safe encryption, and privacy-preserving methods like homomorphic encryption or cancelable biometrics.
  - **Algorithmic Biases:** The possibility of algorithmic bias in fingerprint biometric technologies presents another ethical dilemma. Research has indicated that the accuracy of biometric systems can vary based on the demographic attributes of the people being scanned, including age, gender, and skin tone. For instance, under representation of particular populations in training datasets may result in reduced accuracy for those groups. Particularly in forensic or security scenarios, where a false match or inability to identify a legitimate individual can have dire effects, this bias can have catastrophic ramifications. Misidentification in forensic investigations may result in false allegations, and in security applications, specific populations may be unjustly singled out or denied access. In order to solve this problem, more diverse datasets must be used, and algorithms must be developed with fairness standards in place. These problems can be lessened by routinely



reviewing biometric systems for bias and including a variety of demographic groups in the testing process.

- **Legal Considerations:** Particularly in forensic and government use cases, fingerprint biometric technologies have a wide range of legal ramifications. The reliability and admissibility of biometric evidence in court is one of the main issues. Strict legal requirements must be met by forensic fingerprint identification systems in order for the evidence they produce to be trustworthy and supported by science. But many contemporary biometric algorithms are "black-box," especially those that rely on deep learning, which makes it challenging to understand how they arrive at a given judgement. This raises concerns about the accountability and transparency of these systems. Furthermore, there are jurisdictional differences in the legality of biometric data collecting, thus it is crucial to make sure local regulations are followed. While some nations have more permissive rules, others have tight legislation requiring express authorization for the use of biometric data. The ethical application of biometric technology must be covered by legal frameworks, with an emphasis on data protection, user permission, and making sure that systems are operated in a way that respects people's rights.

This review study on fingerprint biometrics has some major limitations, one of them being its scant discussion of recent developments in fingerprint sensing technology and their potential applications. Although the study thoroughly discusses the current state of the art in fingerprint recognition, it does not go into great detail into cutting edge advances like new capture methods, sophisticated sensing materials, or the effects of recent advancements in fingerprint sensor downsizing. The absence of these developments implies that the evaluation may not accurately reflect the state of the field today and in the future, given the potential impact they could have on the precision, usability, and integration of fingerprint biometrics in a variety of scenarios. This gap may allow significant technical trends to go unnoticed, along with the implications they have for research and real-world applications.

## 8. Conclusion

The adoption of creative solutions to current problems is essential to the future viability of biometric authentication. This entails creating reliable, scalable algorithms that can efficiently handle a variety of biometric data. It is imperative to establish uniform standards and evaluation procedures to guarantee impartial assessments of diverse authentication techniques. Strict ethical guidelines and openness campaigns are necessary to solve issues with algorithmic bias and data privacy in order to win over the public's trust. Multimodal fusion techniques that integrate various biometric features can greatly improve dependability. Furthermore, maximizing hardware technological developments is critical to increasing accuracy and productivity. The goal of research should be to develop biometric systems that are easy to use and prioritize both regulatory compliance and privacy protection. Collaboration between academic researchers, business personnel, and regulatory organizations is essential to spur innovation and guarantee the responsible

application of biometric technologies across various sectors. By implementing these tactics, biometric authentication will be able to advance, satisfy the increasing need for reliable and secure authentication methods, and improve security and user experience across a range of applications.

**Conflict of Interest** The authors declare no conflict of interest.

## References

- [1] R. Ramotowski, *Lee and Gaensslen's advances in fingerprint technology*, CRC press, 2012.
- [2] Y. Xu, G. Lu, Y. Lu, D. Zhang, "High resolution fingerprint recognition using pore and edge descriptors", *Pattern Recognition Letters*, vol. 125, pp. 773–779, 2019, doi:[10.1016/j.patrec.2019.08.006](https://doi.org/10.1016/j.patrec.2019.08.006).
- [3] P. Tertychnyi, C. Ozcinar, G. Anbarjafari, "Low-quality fingerprint classification using deep neural network", *IET Biometrics*, vol. 7, no. 6, pp. 550–556, 2018, doi:[10.1049/iet-bmt.2018.5074](https://doi.org/10.1049/iet-bmt.2018.5074).
- [4] A. A. Paulino, J. Feng, A. K. Jain, "Latent fingerprint matching using descriptor-based hough transform", *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 31–45, 2012, doi:[10.1109/ijcb.2011.6117483](https://doi.org/10.1109/ijcb.2011.6117483).
- [5] S. S. Arora, E. Liu, K. Cao, A. K. Jain, "Latent fingerprint matching: performance gain via feedback from exemplar prints", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 12, pp. 2452–2465, 2014, doi:[10.1109/tpami.2014.2330609](https://doi.org/10.1109/tpami.2014.2330609).
- [6] M. A. Medina-Pérez, A. M. Moreno, M. Á. F. Ballester, M. García-Borroto, O. Loyola-González, L. Altamirano-Robles, "Latent fingerprint identification using deformable minutiae clustering", *Neurocomputing*, vol. 175, pp. 851–865, 2016, doi:[10.1016/j.neucom.2015.05.130](https://doi.org/10.1016/j.neucom.2015.05.130).
- [7] A. Sankaran, A. Jain, T. Vashisth, M. Vatsa, R. Singh, "Adaptive latent fingerprint segmentation using feature selection and random decision forest classification", *Information Fusion*, vol. 34, pp. 1–15, 2017, doi:[10.1016/j.inffus.2016.05.002](https://doi.org/10.1016/j.inffus.2016.05.002).
- [8] W. Bian, S. Ding, W. Jia, "Collaborative filtering model for enhancing fingerprint image", *IET Image Processing*, vol. 12, no. 1, pp. 149–157, 2018, doi:[10.1049/iet-ipr.2017.0059](https://doi.org/10.1049/iet-ipr.2017.0059).
- [9] J. Li, J. Feng, C.-C. J. Kuo, "Deep convolutional neural network for latent fingerprint enhancement", *Signal Processing: Image Communication*, vol. 60, pp. 52–63, 2018, doi:[10.1016/j.image.2017.08.010](https://doi.org/10.1016/j.image.2017.08.010).
- [10] K. Cao, A. K. Jain, "Automated latent fingerprint recognition", *IEEE transactions on pattern analysis and machine intelligence*, vol. 41, no. 4, pp. 788–800, 2018, doi:[10.1109/tpami.2018.2818162](https://doi.org/10.1109/tpami.2018.2818162).
- [11] R. P. Krish, J. Fierrez, D. Ramos, F. Alonso-Fernandez, J. Bigun, "Improving automated latent fingerprint identification using extended minutia types", *Information Fusion*, vol. 50, pp. 9–19, 2019, doi:[10.1016/j.inffus.2018.10.001](https://doi.org/10.1016/j.inffus.2018.10.001).
- [12] K. Cao, D.-L. Nguyen, C. Tymoszek, A. K. Jain, "End-to-end latent fingerprint search", *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 880–894, 2019, doi:[10.1109/tifs.2019.2930487](https://doi.org/10.1109/tifs.2019.2930487).
- [13] A. J. Sanchez-Fernandez, L. F. Romero, D. Peralta, M. A. Medina-Pérez, Y. Saeys, F. Herrera, S. Tabik, "Asynchronous processing for latent fingerprint identification on heterogeneous cpu-gpu systems", *IEEE Access*, vol. 8, pp. 124236–124253, 2020, doi:[10.1109/access.2020.3005476](https://doi.org/10.1109/access.2020.3005476).
- [14] N. D. Kalka, M. Beachler, R. A. Hicklin, "Lqmetric: a latent fingerprint quality metric for predicting afis performance and assessing the value of latent fingerprints", *Journal of Forensic Identification*, vol. 70, no. 4, pp. 443–463, 2020.
- [15] X. Huang, P. Qian, M. Liu, "Latent fingerprint image enhancement based on progressive generative adversarial network", "Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops", pp. 800–801, 2020, doi:[10.1109/cvprw50498.2020.00408](https://doi.org/10.1109/cvprw50498.2020.00408).

- [16] U. U. Deshpande, V. Malemath, S. M. Patil, S. V. Chaugule, "End-to-end automated latent fingerprint identification with improved dcnn-fft enhancement", *Frontiers in Robotics and AI*, vol. 7, p. 594412, 2020, doi:[10.3389/frobt.2020.594412](https://doi.org/10.3389/frobt.2020.594412).
- [17] M. Liu, P. Qian, "Automatic segmentation and enhancement of latent fingerprints using deep nested unets", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1709–1719, 2020, doi:[10.1109/tifs.2020.3039058](https://doi.org/10.1109/tifs.2020.3039058).
- [18] S. Gu, J. Feng, J. Lu, J. Zhou, "Latent fingerprint registration via matching densely sampled points", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1231–1244, 2020, doi:[10.1109/tifs.2020.3032041](https://doi.org/10.1109/tifs.2020.3032041).
- [19] D. Agarwal, A. Bansal, "A utility of pores as level 3 features in latent fingerprint identification", *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23605–23624, 2021, doi:[10.1007/s11042-020-10207-x](https://doi.org/10.1007/s11042-020-10207-x).
- [20] U. U. Deshpande, V. Malemath, S. M. Patil, S. V. Chaugule, "Latent fingerprint identification system based on a local combination of minutiae feature points", *SN Computer Science*, vol. 2, no. 3, p. 206, 2021, doi:[10.1007/s42979-021-00615-7](https://doi.org/10.1007/s42979-021-00615-7).
- [21] S. M. Hilles, A. Liban, O. A. Miaikil, A. M. Altrad, Y. A. B. El-Ebiary, M. M. Hilles, J. Contreras, "Latent fingerprint enhancement and segmentation technique based on hybrid edge adaptive dtv model", "2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)", pp. 8–13, IEEE, 2021, doi:[10.1109/icscee50312.2021.9498025](https://doi.org/10.1109/icscee50312.2021.9498025).
- [22] S. M. Hilles, A. Liban, A. M. Altrad, O. A. Miaikil, Y. A. B. El-Ebiary, J. Contreras, M. M. Hilles, "Adaptive latent fingerprint image segmentation and matching using chan-vee technique based on edtv model", "2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)", pp. 2–7, IEEE, 2021, doi:[10.1109/icscee50312.2021.9497996](https://doi.org/10.1109/icscee50312.2021.9497996).
- [23] U. U. Deshpande, V. Malemath, S. M. Patil, S. V. Chaugule, "Automatic latent fingerprint identification system using scale and rotation invariant minutiae features", *International Journal of Information Technology*, vol. 14, no. 2, pp. 1025–1039, 2022, doi:[10.1007/s41870-020-00508-7](https://doi.org/10.1007/s41870-020-00508-7).
- [24] H. İ. Öztürk, B. Selbes, Y. Artan, "Minnet: Minutia patch embedding network for automated latent fingerprint recognition", "Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition", pp. 1627–1635, 2022, doi:[10.1109/cvprw56347.2022.00169](https://doi.org/10.1109/cvprw56347.2022.00169).
- [25] S. Gu, J. Feng, J. Lu, J. Zhou, "Latent fingerprint indexing: Robust representation and adaptive candidate list", *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 908–923, 2022, doi:[10.1109/tifs.2022.3154296](https://doi.org/10.1109/tifs.2022.3154296).
- [26] N. D. S. Cunha, H. M. Gomes, L. V. Batista, "Residual m-net with frequency-domain loss function for latent fingerprint enhancement", "2022 35th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI)", vol. 1, pp. 198–203, IEEE, 2022, doi:[10.1109/sibgrapi55357.2022.9991793](https://doi.org/10.1109/sibgrapi55357.2022.9991793).
- [27] E. Marasco, M. He, L. Tang, Y. Tao, "Demographic effects in latent fingerprint matching and their relation to image quality", "Proceedings of the 2022 7th International Conference on Machine Learning Technologies", pp. 170–179, 2022, doi:[10.1145/3529399.3529427](https://doi.org/10.1145/3529399.3529427).
- [28] A. B. V. Wyzykowski, A. K. Jain, "Synthetic latent fingerprint generator", "Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision", pp. 971–980, 2023, doi:[10.1109/wacv56688.2023.00103](https://doi.org/10.1109/wacv56688.2023.00103).
- [29] Y. Zhu, X. Yin, J. Hu, "FingerGAN: a constrained fingerprint generation scheme for latent fingerprint enhancement", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023, doi:[10.1109/tpami.2023.3236876](https://doi.org/10.1109/tpami.2023.3236876).
- [30] S. A. Grosz, A. K. Jain, "Latent fingerprint recognition: Fusion of local and global embeddings", *IEEE Transactions on Information Forensics and Security*, 2023, doi:[10.1109/tifs.2023.3314207](https://doi.org/10.1109/tifs.2023.3314207).
- [31] R. Jindal, S. Singla, "Latent fingerprint recognition using hybrid ant colony optimization and cuckoo search.", *Int. Arab J. Inf. Technol.*, vol. 20, no. 1, pp. 19–28, 2023, doi:[10.34028/iajit/20/1/3](https://doi.org/10.34028/iajit/20/1/3).
- [32] A. B. V. Wyzykowski, A. K. Jain, "A universal latent fingerprint enhancer using transformers", *arXiv preprint arXiv:2306.00231*, 2023, doi:[10.48550/arXiv.2306.00231](https://doi.org/10.48550/arXiv.2306.00231).
- [33] R. K. Dubey, J. Goh, V. L. Thing, "Fingerprint liveness detection from single image using low-level features and shape analysis", *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1461–1475, 2016, doi:[10.1109/tifs.2016.2535899](https://doi.org/10.1109/tifs.2016.2535899).
- [34] Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, Y.-Q. Shi, "Fingerprint liveness detection using gradient-based texture features", *Signal, Image and Video Processing*, vol. 11, pp. 381–388, 2017, doi:[10.1007/s11760-016-0936-z](https://doi.org/10.1007/s11760-016-0936-z).
- [35] T. Chugh, K. Cao, A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches", *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2190–2202, 2018, doi:[10.1109/tifs.2018.2812193](https://doi.org/10.1109/tifs.2018.2812193).
- [36] C. Yuan, X. Sun, Q. J. Wu, "Difference co-occurrence matrix using bp neural network for fingerprint liveness detection", *Soft Computing*, vol. 23, no. 13, pp. 5157–5169, 2019, doi:[10.1007/s00500-018-3182-1](https://doi.org/10.1007/s00500-018-3182-1).
- [37] C. Yuan, X. Chen, P. Yu, R. Meng, W. Cheng, Q. J. Wu, X. Sun, "Semi-supervised stacked autoencoder-based deep hierarchical semantic feature for real-time fingerprint liveness detection", *Journal of Real-Time Image Processing*, vol. 17, pp. 55–71, 2020, doi:[10.1007/s11554-019-00928-0](https://doi.org/10.1007/s11554-019-00928-0).
- [38] J. Fei, Z. Xia, P. Yu, F. Xiao, "Adversarial attacks on fingerprint liveness detection", *EURASIP Journal on Image and Video Processing*, vol. 2020, pp. 1–11, 2020, doi:[10.1186/s13640-020-0490-z](https://doi.org/10.1186/s13640-020-0490-z).
- [39] Y. Zhang, C. Gao, S. Pan, Z. Li, Y. Xu, H. Qiu, "A score-level fusion of fingerprint matching with fingerprint liveness detection", *IEEE Access*, vol. 8, pp. 183391–183400, 2020, doi:[10.1109/access.2020.3027846](https://doi.org/10.1109/access.2020.3027846).
- [40] W. Jian, Y. Zhou, H. Liu, "Densely connected convolutional network optimized by genetic algorithm for fingerprint liveness detection", *IEEE Access*, vol. 9, pp. 2229–2243, 2020, doi:[10.1109/access.2020.3047723](https://doi.org/10.1109/access.2020.3047723).
- [41] O. F. Onifade, P. Akinde, F. O. Isinkaye, "Circular gabor wavelet algorithm for fingerprint liveness detection", *Journal of Advanced Computer Science & Technology*, vol. 9, no. 1, pp. 1–5, 2020, doi:[10.14419/jacst.v9i1.29908](https://doi.org/10.14419/jacst.v9i1.29908).
- [42] R. Agarwal, A. S. Jalal, K. Arya, "A multimodal liveness detection using statistical texture features and spatial analysis", *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 13621–13645, 2020, doi:[10.1007/s11042-019-08313-6](https://doi.org/10.1007/s11042-019-08313-6).
- [43] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao, C. Gao, "Fldnet: Light dense cnn for fingerprint liveness detection", *IEEE Access*, vol. 8, pp. 84141–84152, 2020, doi:[10.1109/access.2020.2990909](https://doi.org/10.1109/access.2020.2990909).
- [44] J. Kolberg, M. Grimmer, M. Gomez-Barrero, C. Busch, "Anomaly detection with convolutional autoencoders for fingerprint presentation attack detection", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 2, pp. 190–202, 2021, doi:[10.1109/tbiom.2021.3050036](https://doi.org/10.1109/tbiom.2021.3050036).
- [45] C. Yuan, S. Jiao, X. Sun, Q. J. Wu, "Mffld: A multimodal-feature-fusion-based fingerprint liveness detection", *IEEE Transactions on Cognitive and Developmental Systems*, vol. 14, no. 2, pp. 648–661, 2021, doi:[10.1109/tcds.2021.3062624](https://doi.org/10.1109/tcds.2021.3062624).
- [46] S. Agarwal, C. R. Chowdary, V. Sourabh, "Eazy learning: An adaptive variant of ensemble learning for fingerprint liveness detection", *arXiv preprint arXiv:2103.02207*, 2021, doi:[10.48550/arXiv.2103.02207](https://doi.org/10.48550/arXiv.2103.02207).
- [47] S. B. Sandouka, Y. Bazi, N. Alajlan, "Transformers and generative adversarial networks for liveness detection in multitarget fingerprint sensors", *Sensors*, vol. 21, no. 3, p. 699, 2021, doi:[10.3390/s21030699](https://doi.org/10.3390/s21030699).
- [48] A. Verma, V. K. Gupta, S. Goel, A. K. Yadav, D. Yadav, et al., "Modeling fingerprint presentation attack detection through transient liveness factor-a person specific approach.", *Traitement du Signal*, vol. 38, no. 2, 2021, doi:[10.18280/ts.380206](https://doi.org/10.18280/ts.380206).

- [49] C. Yuan, Q. Cui, X. Sun, Q. J. Wu, S. Wu, "Fingerprint liveness detection using an improved cnn with the spatial pyramid pooling structure", *Advances in Computers*, vol. 120, pp. 157–193, Elsevier, 2021, doi:[10.1016/bs.adcom.2020.10.002](https://doi.org/10.1016/bs.adcom.2020.10.002).
- [50] Z. İ. Özkiper, Z. Turgut, T. Atmaca, M. A. Aydın, "Fingerprint liveness detection using deep learning", *2022 9th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 129–135, IEEE, 2022, doi:[10.1109/ficloud57274.2022.00025](https://doi.org/10.1109/ficloud57274.2022.00025).
- [51] R. C. Contreras, L. G. Nonato, M. Boaventura, I. A. G. Boaventura, F. L. Dos Santos, R. B. Zanin, M. S. Viana, "A new multi-filter framework for texture image representation improvement using set of pattern descriptors to fingerprint liveness detection", *IEEE Access*, vol. 10, pp. 117681–117706, 2022, doi:[10.1109/access.2022.3218335](https://doi.org/10.1109/access.2022.3218335).
- [52] A. Almeahmadi, "A behavioral-based fingerprint liveness and willingness detection system", *Applied Sciences*, vol. 12, no. 22, p. 11460, 2022, doi:[10.3390/app122211460](https://doi.org/10.3390/app122211460).
- [53] S. Agarwal, A. Rattani, C. R. Chowdary, "A-ilearn: An adaptive incremental learning model for spoof fingerprint detection", *Machine Learning with Applications*, vol. 7, p. 100210, 2022, doi:[10.1016/j.mlwa.2021.100210](https://doi.org/10.1016/j.mlwa.2021.100210).
- [54] D. Agarwal, A. Bansal, "Fingerprint liveness detection through fusion of pores perspiration and texture features", *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4089–4098, 2022, doi:[10.1016/j.jksuci.2020.10.003](https://doi.org/10.1016/j.jksuci.2020.10.003).
- [55] K. Zhang, S. Huang, E. Liu, H. Zhao, "Lfldnet: Lightweight fingerprint liveness detection based on resnet and transformer", *Sensors*, vol. 23, no. 15, p. 6854, 2023, doi:[10.3390/s23156854](https://doi.org/10.3390/s23156854).
- [56] A. Galli, M. Gravina, S. Marrone, D. Mattiello, C. Sansone, "Adversarial liveness detector: Leveraging adversarial perturbations in fingerprint liveness detection", *IET Biometrics*, vol. 12, no. 2, pp. 102–111, 2023, doi:[10.1049/bme2.12106](https://doi.org/10.1049/bme2.12106).
- [57] M. Nishanth, H. K. MR, K. N. MG, S. Kamal, T. Rao, K. Ashwini, "Fingerprint liveness detection using deep learning", *2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA)*, pp. 383–388, IEEE, 2023, doi:[10.1109/ciisca59740.2023.00079](https://doi.org/10.1109/ciisca59740.2023.00079).
- [58] Y. Myshkovskiy, M. Nazarkevych, "Robustness of fingerprint liveness detection based on convolutional neural networks", <https://ceur-ws.org/Vol-3550/short13.pdf>, 2023.
- [59] C. Li, J. Hu, "A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures", *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 543–555, 2015, doi:[10.1109/tifs.2015.2505630](https://doi.org/10.1109/tifs.2015.2505630).
- [60] T. Murakami, T. Ohki, K. Takahashi, "Optimal sequential fusion for multibiometric cryptosystems", *Information fusion*, vol. 32, pp. 93–108, 2016, doi:[10.1016/j.inffus.2016.02.002](https://doi.org/10.1016/j.inffus.2016.02.002).
- [61] Z. Jin, A. B. J. Teoh, B.-M. Goi, Y.-H. Tay, "Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation", *Pattern Recognition*, vol. 56, pp. 50–62, 2016, doi:[10.1016/j.patcog.2016.02.024](https://doi.org/10.1016/j.patcog.2016.02.024).
- [62] S. Rajendran, M. Doraipandian, "Biometric template security triggered by two dimensional logistic sine map", *Procedia computer science*, vol. 143, pp. 794–803, 2018, doi:[10.1016/j.procs.2018.10.387](https://doi.org/10.1016/j.procs.2018.10.387).
- [63] A. A. Al-Saggaf, "Secure method for combining cryptography with iris biometrics.", *J. Univers. Comput. Sci.*, vol. 24, no. 4, pp. 341–356, 2018.
- [64] G. Panchal, D. Samanta, S. Barman, "Biometric-based cryptography for digital content protection without any key storage", *Multimedia Tools and Applications*, vol. 78, pp. 26979–27000, 2019, doi:[10.1007/s11042-017-4528-x](https://doi.org/10.1007/s11042-017-4528-x).
- [65] A. A. Khan, V. Kumar, M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach", *Journal of King Saud University-Computer and Information Sciences*, 2019, doi:[10.1016/j.jksuci.2019.04.013](https://doi.org/10.1016/j.jksuci.2019.04.013).
- [66] S. Sapkal, S. Kakarwal, R. Deshmukh, "Template security of multimodal biometric system with face and fingerprint images using fuzzy vault method", *CSI Journal of Computing*, vol. 3, no. 3, pp. 36–40, 2020, doi:[10.21275/v5i3.nov162389](https://doi.org/10.21275/v5i3.nov162389).
- [67] V. Rajasekar, J. Premalatha, K. Sathya, "Enhanced biometric recognition for secure authentication using iris preprocessing and hyperelliptic curve cryptography", *Wireless communications and mobile computing*, vol. 2020, pp. 1–15, 2020, doi:[10.21203/rs.2.23196/v1](https://doi.org/10.21203/rs.2.23196/v1).
- [68] F. S. Babamir, M. Kirci, "A multibiometric cryptosystem for user authentication in client-server networks", *Computer Networks*, vol. 181, p. 107427, 2020, doi:[10.1016/j.comnet.2020.107427](https://doi.org/10.1016/j.comnet.2020.107427).
- [69] R. A. Rajan, P. Kumaran, "Multi-biometric cryptosystem using graph for secure cloud authentication", *Journal of Intelligent & Fuzzy Systems*, vol. 38, no. 5, pp. 6437–6444, 2020, doi:[10.3233/jifs-179724](https://doi.org/10.3233/jifs-179724).
- [70] R. Dwivedi, S. Dey, M. A. Sharma, A. Goel, "A fingerprint based crypto-biometric system for secure communication", *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1495–1509, 2020, doi:[10.1007/s12652-019-01437-5](https://doi.org/10.1007/s12652-019-01437-5).
- [71] P. S. Chanukya, T. Thivakaran, "Multimodal biometric cryptosystem for human authentication using fingerprint and ear", *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 659–673, 2020, doi:[10.1007/s11042-019-08123-w](https://doi.org/10.1007/s11042-019-08123-w).
- [72] J. Peng, B. Yang, B. B. Gupta, A. A. Abd El-Latif, "A biometric cryptosystem scheme based on random projection and neural network", *Soft Computing*, vol. 25, pp. 7657–7670, 2021, doi:[10.1007/s00500-021-05732-z](https://doi.org/10.1007/s00500-021-05732-z).
- [73] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, M. Gnjatović, "A novel fingerprint biometric cryptosystem based on convolutional neural networks", *Mathematics*, vol. 9, no. 7, p. 730, 2021, doi:[10.3390/math9070730](https://doi.org/10.3390/math9070730).
- [74] W. El-Shafai, F. A. H. E. Mohamed, H. M. Elkamchouchi, M. Abd-Elnaby, A. Elshafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm", *IEEE Access*, vol. 9, pp. 77675–77692, 2021, doi:[10.1109/access.2021.3082940](https://doi.org/10.1109/access.2021.3082940).
- [75] H. A. A. El-Hameed, N. Ramadan, W. El-Shafai, A. A. Khalaf, H. E. H. Ahmed, S. E. Elkhany, F. E. A. El-Samie, "Cancelable biometric security system based on advanced chaotic maps", *The Visual Computer*, pp. 1–17, 2021, doi:[10.1007/s00371-021-02276-2](https://doi.org/10.1007/s00371-021-02276-2).
- [76] O. Ouda, K. Nandakumar, A. Ross, "Cancelable biometrics vault: A secure key-binding biometric cryptosystem based on chaffing and winnowing", *2020 25th International Conference on Pattern Recognition (ICPR)*, pp. 8735–8742, IEEE, 2021, doi:[10.1109/icpr48806.2021.9412957](https://doi.org/10.1109/icpr48806.2021.9412957).
- [77] R. Sreemol, M. S. Kumar, A. Sreekumar, "Improvement of security in multi-biometric cryptosystem by modulus fuzzy vault algorithm", *2021 International conference on advances in computing and communications (ICACC)*, pp. 1–7, IEEE, 2021, doi:[10.1109/icacc-202152719.2021.9708136](https://doi.org/10.1109/icacc-202152719.2021.9708136).
- [78] L. A. Elrefaei, A. M. Al-Mohammadi, "Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme", *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 2, pp. 204–217, 2022, doi:[10.1016/j.jksuci.2019.10.011](https://doi.org/10.1016/j.jksuci.2019.10.011).
- [79] X. Chang, W. Li, A. Yan, P. W. M. Tsang, T.-C. Poon, "Asymmetric cryptosystem based on optical scanning cryptography and elliptic curve algorithm", *Scientific Reports*, vol. 12, no. 1, p. 7722, 2022, doi:[10.21203/rs.3.rs-1148931/v1](https://doi.org/10.21203/rs.3.rs-1148931/v1).
- [80] A. Kuznetsov, D. Zakharov, E. Frontoni, L. Romeo, R. Rosati, "Deep learning based fuzzy extractor for generating strong keys from biometric face images", *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, pp. 421–426, IEEE, 2022, doi:[10.1109/picst57299.2022.10238643](https://doi.org/10.1109/picst57299.2022.10238643).
- [81] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, S. M. Pournaghi, "Blockchain-based user re-enrollment for biometric authentication systems", *International Journal of Electronics and Information Engineering*, vol. 14, no. 1, pp. 18–38, 2022, doi:[10.6636/IJEIE.202206](https://doi.org/10.6636/IJEIE.202206).



- [82] S. D. Patil, R. Raut, R. H. Jhaveri, T. A. Ahanger, P. V. Dhade, A. B. Kathole, K. N. Vhatkar, *et al.*, "Robust authentication system with privacy preservation of biometrics", *Security and Communication Networks*, vol. 2022, 2022, doi:[10.1155/2022/7857975](https://doi.org/10.1155/2022/7857975).
- [83] L. A. Abou Elazm, W. El-Shafai, S. Ibrahim, M. G. Egila, H. Shawkey, M. K. Elsaid, N. F. Soliman, H. N. AlEisa, F. E. Abd El-Samie, "Efficient hardware design of a secure cancellable biometric cryptosystem", *Intell. Autom. Soft Comput.*, vol. 36, no. 1, pp. 929–955, 2023, doi:[10.32604/iasc.2023.031386](https://doi.org/10.32604/iasc.2023.031386).
- [84] H. A. A. Eldawy, W. El-Shafai, E. E.-D. Hemdan, G. M. El-Banby, F. E. A. El-Samie, "A robust cancellable face and palmprint recognition system based on 3d optical chaos-dna cryptosystem", *Optical and Quantum Electronics*, vol. 55, no. 11, p. 970, 2023, doi:[10.1007/s11082-023-04840-7](https://doi.org/10.1007/s11082-023-04840-7).
- [85] P. Kaur, N. Kumar, "Enhanced biometric cryptosystem using ear & iris modality based on binary robust independent elementary feature", "2023 6th International Conference on Information Systems and Computer Networks (ISCON)", pp. 1–6, IEEE, 2023, doi:[10.1109/iscon57294.2023.10112197](https://doi.org/10.1109/iscon57294.2023.10112197).
- [86] A. Sedik, A. A. A. El-Latif, M. A. Wani, F. E. A. El-Samie, N. A.-S. Bauomy, F. G. Hashad, "Efficient multi-biometric secure-storage scheme based on deep learning and crypto-mapping techniques", *Mathematics*, vol. 11, no. 3, p. 703, 2023, doi:[10.3390/math11030703](https://doi.org/10.3390/math11030703).
- [87] S. Nagaraju, R. Nagendra, S. Balasundaram, R. K. Kumar, "Biometric key generation and multi round aes crypto system for improved security", *Measurement: Sensors*, vol. 30, p. 100931, 2023, doi:[10.1016/j.measen.2023.100931](https://doi.org/10.1016/j.measen.2023.100931).
- [88] M. Sandhya, M. V. Prasad, "Securing fingerprint templates using fused structures", *IET Biometrics*, vol. 6, no. 3, pp. 173–182, 2017, doi:[10.1049/iet-bmt.2016.0008](https://doi.org/10.1049/iet-bmt.2016.0008).
- [89] A. Roy, N. Memon, A. Ross, "Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems", *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2013–2025, 2017, doi:[10.1109/tifs.2017.2691658](https://doi.org/10.1109/tifs.2017.2691658).
- [90] J. Kim, A. B. J. Teoh, "One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication", "2018 24th International Conference on Pattern Recognition (ICPR)", pp. 3108–3113, IEEE, 2018, doi:[10.1109/icpr.2018.8545565](https://doi.org/10.1109/icpr.2018.8545565).
- [91] X. Wang, H. Li, "One-factor cancellable palmprint recognition scheme based on oim and minimum signature hash", *IEEE Access*, vol. 7, pp. 131338–131354, 2019, doi:[10.1109/access.2019.2938019](https://doi.org/10.1109/access.2019.2938019).
- [92] G. S. Walia, K. Aggarwal, K. Singh, K. Singh, "Design and analysis of adaptive graph-based cancelable multi-biometrics approach", *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 54–66, 2020, doi:[10.1109/tdsc.2020.2997558](https://doi.org/10.1109/tdsc.2020.2997558).
- [93] J. R. Pinto, M. V. Correia, J. S. Cardoso, "Secure triplet loss: Achieving cancelability and non-linkability in end-to-end deep biometrics", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 2, pp. 180–189, 2020, doi:[10.1109/tbiom.2020.3046620](https://doi.org/10.1109/tbiom.2020.3046620).
- [94] H. Wang, X. Dong, Z. Jin, A. B. J. Teoh, M. Tistarelli, "Security analysis of cancellable biometrics using constrained-optimized similarity-based attack", *arXiv preprint arXiv:2006.13051*, 2020, doi:[10.1109/wacvw52041.2021.00012](https://doi.org/10.1109/wacvw52041.2021.00012).
- [95] A. K. Trivedi, D. M. Thounaojam, S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric", *Computers & Security*, vol. 90, p. 101690, 2020, doi:[10.1016/j.cose.2019.101690](https://doi.org/10.1016/j.cose.2019.101690).
- [96] U. Sharma, P. Tomar, S. S. Ali, N. Saxena, R. S. Bhadoria, "Optimized authentication system with high security and privacy", *Electronics*, vol. 10, no. 4, p. 458, 2021, doi:[10.3390/electronics10040458](https://doi.org/10.3390/electronics10040458).
- [97] H. Wang, X. Dong, Z. Jin, A. B. J. Teoh, M. Tistarelli, "Interpretable security analysis of cancellable biometrics using constrained-optimized similarity-based attack", "Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision", pp. 70–77, 2021, doi:[10.1109/wacvw52041.2021.00012](https://doi.org/10.1109/wacvw52041.2021.00012).
- [98] N. F. Soliman, A. D. Algarni, W. El-Shafai, F. E. A. El-Samie, G. Banby, *et al.*, "An efficient gcd-based cancelable biometric algorithm for single and multiple biometrics.", *Computers, Materials & Continua*, vol. 69, no. 2, 2021, doi:[10.32604/cmc.2021.016980](https://doi.org/10.32604/cmc.2021.016980).
- [99] W. Yang, S. Wang, M. Shahzad, W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection", *Journal of Information Security and Applications*, vol. 58, p. 102704, 2021, doi:[10.1016/j.jisa.2020.102704](https://doi.org/10.1016/j.jisa.2020.102704).
- [100] H. Zhang, W. Bian, B. Jie, D. Xu, J. Zhao, "A complete user authentication and key agreement scheme using cancelable biometrics and puf in multi-server environment", *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5413–5428, 2021, doi:[10.1109/tifs.2021.3128826](https://doi.org/10.1109/tifs.2021.3128826).
- [101] X. Dong, Z. Jin, L. Zhao, Z. Guo, "Biocrypto: An ldpc coded bio-cryptosystem on fingerprint cancellable template", "2021 IEEE international joint conference on biometrics (IJCB)", pp. 1–8, IEEE, 2021, doi:[10.1109/ijcb52358.2021.9484391](https://doi.org/10.1109/ijcb52358.2021.9484391).
- [102] B. Samira, R. H. Lamia, E. B. A. Najoua, "Biometric template security using watermarking reinforcement based cancellable transformation", "2021 International Conference on Cyberworlds (CW)", pp. 270–277, IEEE, 2021, doi:[10.1109/cw52790.2021.00052](https://doi.org/10.1109/cw52790.2021.00052).
- [103] T. M. Dang, T. D. Nguyen, T. Hoang, H. Kim, A. B. J. Teoh, D. Choi, "Avet: a novel transform function to improve cancellable biometrics security", *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 758–772, 2022, doi:[10.1109/tifs.2022.3230212](https://doi.org/10.1109/tifs.2022.3230212).
- [104] B. A. El-Rahiem, M. Amin, A. Sedik, F. E. A. E. Samie, A. M. Ilyasu, "An efficient multi-biometric cancellable biometric scheme based on deep fusion and deep dream", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2022, doi:[10.1007/s12652-021-03513-1](https://doi.org/10.1007/s12652-021-03513-1).
- [105] A. M. Ayoup, A. A. Khalaf, W. El-Shafai, F. E. A. El-Samie, F. Alrad-dady, S. M. S. Eldin, "Cancellable multi-biometric template generation based on arnold cat map and aliasing", *Computers, Materials & Continua*, vol. 72, no. 2, 2022, doi:[10.32604/cmc.2022.025902](https://doi.org/10.32604/cmc.2022.025902).
- [106] J. Kim, Y. G. Jung, A. B. J. Teoh, "Multimodal biometric template protection based on a cancelable softmaxout fusion network", *Applied Sciences*, vol. 12, no. 4, p. 2023, 2022, doi:[10.3390/app12042023](https://doi.org/10.3390/app12042023).
- [107] A. M. Ayoup, A. Khalaf, F. Alrad-dady, F. Abd El-Samie, W. El-Safai, S. Eldin, "Selective cancellable multi-biometric template generation scheme based on multi-exposure feature fusion", *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 549–565, 2022, doi:[10.32604/iasc.2022.024379](https://doi.org/10.32604/iasc.2022.024379).
- [108] A. Sedik, A. A. A. El-Latif, M. El-Affendi, H. Mostafa, "A cancelable biometric system based on deep style transfer and symmetry check for double-phase user authentication", *Symmetry*, vol. 15, no. 7, p. 1426, 2023, doi:[10.3390/sym15071426](https://doi.org/10.3390/sym15071426).
- [109] S. M. S. Eldin, A. Sedik, S. S. Alshamrani, A. M. Ayoup, "Cancellable multi-biometric feature veins template generation based on sha-3 hashing.", *Computers, Materials & Continua*, vol. 75, no. 1, 2023, doi:[10.32604/cmc.2023.030789](https://doi.org/10.32604/cmc.2023.030789).
- [110] Y. Jiang, P. Shen, L. Zeng, X. Zhu, D. Jiang, C. Chen, "Cancelable biometric schemes for euclidean metric and cosine metric", *Cybersecurity*, vol. 6, no. 1, p. 4, 2023, doi:[10.1186/s42400-023-00137-0](https://doi.org/10.1186/s42400-023-00137-0).
- [111] O. S. Faragallah, E. A. Naeem, W. El-Shafai, N. Ramadan, H. E.-d. H. Ahmed, M. M. A. Elnaby, I. Elashry, S. E. El-Khamy, F. E. A. El-Samie, "Efficient chaotic-baker-map-based cancelable face recognition", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–39, 2023, doi:[10.1007/s12652-021-03398-0](https://doi.org/10.1007/s12652-021-03398-0).
- [112] S. Yamamoto, H. Inaba, "Cancellable biometric authentication system by image style transfer", "2023 IEEE 12th Global Conference on Consumer Electronics (GCCE)", pp. 794–797, IEEE, 2023, doi:[10.1109/gcce59613.2023.10315291](https://doi.org/10.1109/gcce59613.2023.10315291).
- [113] F. Turrone, D. Maltoni, R. Cappelli, D. Maio, "Improving fingerprint orientation extraction", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1002–1013, 2011, doi:[10.1109/tifs.2011.2150216](https://doi.org/10.1109/tifs.2011.2150216).
- [114] S. Li, A. C. Kot, "An improved scheme for full fingerprint reconstruction", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1906–1912, 2012, doi:[10.1109/tifs.2012.2212012](https://doi.org/10.1109/tifs.2012.2212012).

- [115] J. Galbally, S. Marcel, J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition", *IEEE transactions on image processing*, vol. 23, no. 2, pp. 710–724, 2013, doi:[10.1109/tip.2013.2292332](https://doi.org/10.1109/tip.2013.2292332).
- [116] H.-W. Jung, J.-H. Lee, "Noisy and incomplete fingerprint classification using local ridge distribution models", *Pattern recognition*, vol. 48, no. 2, pp. 473–484, 2015, doi:[10.1016/j.patcog.2014.07.030](https://doi.org/10.1016/j.patcog.2014.07.030).
- [117] S. Mathur, A. Vjay, J. Shah, S. Das, A. Malla, "Methodology for partial fingerprint enrollment and authentication on mobile devices", "2016 International Conference on Biometrics (ICB)", pp. 1–8, IEEE, 2016, doi:[10.1109/icb.2016.7550093](https://doi.org/10.1109/icb.2016.7550093).
- [118] T. Chugh, S. S. Arora, A. K. Jain, N. G. Paulter, "Benchmarking fingerprint minutiae extractors", "2017 International conference of the biometrics special interest group (BIOSIG)", pp. 1–8, IEEE, 2017, doi:[10.23919/biosig.2017.8053498](https://doi.org/10.23919/biosig.2017.8053498).
- [119] G. S. E. Ekladious, R. Sabourin, E. Granger, "Learning global-local distance metrics for signature-based biometric cryptosystems", *Cryptography*, vol. 1, no. 3, p. 22, 2017, doi:[10.3390/cryptography1030022](https://doi.org/10.3390/cryptography1030022).
- [120] R. D. Labati, A. Genovese, E. Munoz, V. Piuri, F. Scotti, "A novel pore extraction method for heterogeneous fingerprint images using convolutional neural networks", *Pattern Recognition Letters*, vol. 113, pp. 58–66, 2018, doi:[10.1016/j.patrec.2017.04.001](https://doi.org/10.1016/j.patrec.2017.04.001).
- [121] R. Gupta, M. Khari, D. Gupta, R. G. Crespo, "Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction", *Information Sciences*, vol. 530, pp. 201–218, 2020, doi:[10.1016/j.ins.2020.01.031](https://doi.org/10.1016/j.ins.2020.01.031).
- [122] F. Liu, Y. Zhao, G. Liu, L. Shen, "Fingerprint pore matching using deep features", *Pattern Recognition*, vol. 102, p. 107208, 2020, doi:[10.1016/j.patcog.2020.107208](https://doi.org/10.1016/j.patcog.2020.107208).
- [123] W. Yang, S. Wang, K. Yu, J. J. Kang, M. N. Johnstone, "Secure fingerprint authentication with homomorphic encryption", "2020 Digital Image Computing: Techniques and Applications (DICTA)", pp. 1–6, IEEE, 2020, doi:[10.1109/dicta51227.2020.9363426](https://doi.org/10.1109/dicta51227.2020.9363426).
- [124] B. T. Ahmed, O. Y. Abdulhameed, "Fingerprint authentication using shark smell optimization algorithm", *UHD Journal of Science and Technology*, vol. 4, no. 2, pp. 28–39, 2020, doi:[10.21928/uhdjt.v4n2y2020.pp28-39](https://doi.org/10.21928/uhdjt.v4n2y2020.pp28-39).
- [125] T. Kim, Y. Oh, H. Kim, "Efficient privacy-preserving fingerprint-based authentication system using fully homomorphic encryption", *Security and Communication Networks*, vol. 2020, pp. 1–11, 2020, doi:[10.1155/2020/4195852](https://doi.org/10.1155/2020/4195852).
- [126] M. Golec, S. S. Gill, R. Bahsoon, O. Rana, "Biosec: A biometric authentication framework for secure and private communication among edge devices in iot and industry 4.0", *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 51–56, 2020, doi:[10.1109/mce.2020.3038040](https://doi.org/10.1109/mce.2020.3038040).
- [127] M. Lebcir, S. Awang, A. Benziane, "Reversible watermarking technique for fingerprint authentication based on dct", *IOP Conference Series: Materials Science and Engineering*, vol. 769, no. 1, p. 012070, 2020, doi:[10.1088/1757-899x/769/1/012070](https://doi.org/10.1088/1757-899x/769/1/012070).
- [128] D. Valdes-Ramirez, M. A. Medina-Pérez, R. Monroy, "An ensemble of fingerprint matching algorithms based on cylinder codes and mtriplets for latent fingerprint identification", *Pattern Analysis and Applications*, vol. 24, pp. 433–444, 2021, doi:[10.1007/s10044-020-00911-7](https://doi.org/10.1007/s10044-020-00911-7).
- [129] I. Joshi, R. Kothari, A. Utkarsh, V. K. Kurmi, A. Dantcheva, S. D. Roy, P. K. Kalra, "Explainable fingerprint roi segmentation using monte carlo dropout", "Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision", pp. 60–69, 2021, doi:[10.1109/wacv52041.2021.00011](https://doi.org/10.1109/wacv52041.2021.00011).
- [130] P. Terhörst, A. Boller, N. Damer, F. Kirchbuchner, A. Kuijper, "Midecon: Unsupervised and accurate fingerprint and minutia quality assessment based on minutia detection confidence", "2021 IEEE International Joint Conference on Biometrics (IJCB)", pp. 1–8, IEEE, 2021, doi:[10.1109/ijcb52358.2021.9484404](https://doi.org/10.1109/ijcb52358.2021.9484404).
- [131] F. Pandey, P. Dash, D. Samanta, M. Sarma, "Asra: Automatic singular value decomposition-based robust fingerprint image alignment", *Multimedia Tools and Applications*, vol. 80, pp. 15647–15675, 2021, doi:[10.1007/s11042-021-10560-5](https://doi.org/10.1007/s11042-021-10560-5).
- [132] A. Muhammed, N. C. Mhala, A. R. Pais, "A novel fingerprint template protection and fingerprint authentication scheme using visual secret sharing and super-resolution", *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10255–10284, 2021, doi:[10.1007/s11042-020-10095-1](https://doi.org/10.1007/s11042-020-10095-1).
- [133] R. C. Contreras, L. G. Nonato, M. Boaventura, I. A. G. Boaventura, B. G. Coelho, M. S. Viana, "A new multi-filter framework with statistical dense sift descriptor for spoofing detection in fingerprint authentication systems", "International Conference on Artificial Intelligence and Soft Computing", pp. 442–455, Springer, 2021, doi:[10.1007/978-3-030-87897-9\\_39](https://doi.org/10.1007/978-3-030-87897-9_39).
- [134] M. S. El Tokhy, "Robust multimodal biometric authentication algorithms using fingerprint, iris and voice features fusion", *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 1, pp. 647–672, 2021, doi:[10.3233/jifs-200425](https://doi.org/10.3233/jifs-200425).
- [135] A. Bedari, S. Wang, W. Yang, "A secure online fingerprint authentication system for industrial iot devices over 5g networks", *Sensors*, vol. 22, no. 19, p. 7609, 2022, doi:[10.3390/s22197609](https://doi.org/10.3390/s22197609).
- [136] A. Siswanto, A. Efendi, E. A. Kadir, "Fingerprint authentication in smart home environment based on embedded system", "2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)", pp. 1–6, IEEE, 2022, doi:[10.1109/iceccme55909.2022.9988711](https://doi.org/10.1109/iceccme55909.2022.9988711).
- [137] N. Pradeep, J. Ravi, "An revolutionary fingerprint authentication approach using gabor filters for feature extraction and deep learning classification using convolutional neural networks", "Innovations in Electronics and Communication Engineering: Proceedings of the 9th ICIECE 2021", pp. 349–360, Springer, 2022, doi:[10.1007/978-981-16-8512-5\\_38](https://doi.org/10.1007/978-981-16-8512-5_38).
- [138] A. F. Y. Althabhawee, B. K. O. C. Alwawi, "Fingerprint recognition based on collected images using deep learning technology", *IAES International Journal of Artificial Intelligence*, vol. 11, no. 1, p. 81, 2022, doi:[10.11591/ijai.v11.i1.pp81-88](https://doi.org/10.11591/ijai.v11.i1.pp81-88).
- [139] P. Singh, H. Samuel, F. Jaafar, D. Ameyed, "Enhancing biometric security with combinatorial and permutational multi-fingerprint authentication strategies", "2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)", pp. 1–7, IEEE, 2022, doi:[10.1109/picom/cbdcom/cy55231.2022.9927942](https://doi.org/10.1109/picom/cbdcom/cy55231.2022.9927942).
- [140] Y. Chen, Y. Yu, L. Zhai, "{InfinityGauntlet}: Expose smartphone fingerprint authentication to brute-force attack", "32nd USENIX Security Symposium (USENIX Security 23)", pp. 2027–2041, 2023.
- [141] A. Popli, S. Tandon, J. J. Engelsma, A. Namboodiri, "A unified model for fingerprint authentication and presentation attack detection", "Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment", pp. 77–99, Springer, 2023, doi:[10.1109/ijcb52358.2021.9484382](https://doi.org/10.1109/ijcb52358.2021.9484382).
- [142] H. Choi, S. Woo, H. Kim, "Blind-touch: Homomorphic encryption-based distributed neural network inference for privacy-preserving fingerprint authentication", *arXiv preprint arXiv:2312.11575*, 2023, doi:[10.1609/aaai.v38i20.30200](https://doi.org/10.1609/aaai.v38i20.30200).
- [143] E. Marasco, M. Albanese, V. V. R. Patibandla, A. Vurity, S. S. Sri-ram, "Biometric multi-factor authentication: On the usability of the fingerpin scheme", *Security and Privacy*, vol. 6, no. 1, p. e261, 2023, doi:[10.1002/spy.2.261](https://doi.org/10.1002/spy.2.261).
- [144] R. Deshmukh, P. Yannawar, "Avaio enabled deep learning based person authentication using fingerprint", "First International Conference on Advances in Computer Vision and Artificial Intelligence Technologies (ACVAIT 2022)", pp. 327–346, Atlantis Press, 2023, doi:[10.2991/978-94-6463-196-8\\_26](https://doi.org/10.2991/978-94-6463-196-8_26).

- [145] D. Peralta, I. Triguero, R. Sanchez-Reillo, F. Herrera, J. Benítez, "Fast fingerprint identification for large databases", *Pattern Recognition*, vol. 47, no. 2, p. 588–602, 2014, doi:[10.1016/j.patcog.2013.08.002](https://doi.org/10.1016/j.patcog.2013.08.002).
- [146] M. Lastra, J. Carabaño, P. D. Gutiérrez, J. M. Benítez, F. Herrera, "Fast fingerprint identification using gpus", *Information Sciences*, vol. 301, pp. 195–214, 2015, doi:[10.1016/j.ins.2014.12.052](https://doi.org/10.1016/j.ins.2014.12.052).
- [147] Y. Su, J. Feng, J. Zhou, "Fingerprint indexing with pose constraint", *Pattern Recognition*, vol. 54, pp. 1–13, 2016, doi:[10.1016/j.patcog.2016.01.006](https://doi.org/10.1016/j.patcog.2016.01.006).
- [148] J. Khodadoust, A. M. Khodadoust, "Fingerprint indexing based on minutiae pairs and convex core point", *Pattern Recognition*, vol. 67, pp. 110–126, 2017, doi:[10.1016/j.patcog.2017.01.022](https://doi.org/10.1016/j.patcog.2017.01.022).
- [149] D. Song, Y. Tang, J. Feng, "Aggregating minutia-centred deep convolutional features for fingerprint indexing", *Pattern Recognition*, vol. 88, pp. 397–408, 2019, doi:[10.1016/j.patcog.2018.11.018](https://doi.org/10.1016/j.patcog.2018.11.018).
- [150] J. J. Engelsma, K. Cao, A. K. Jain, "Learning a fixed-length fingerprint representation", *IEEE transactions on pattern analysis and machine intelligence*, vol. 43, no. 6, pp. 1981–1997, 2019, doi:[10.1109/tpami.2019.2961349](https://doi.org/10.1109/tpami.2019.2961349).
- [151] U. U. Deshpande, V. Malemath, S. M. Patil, S. V. Chaugule, "Cnnai: a convolution neural network-based latent fingerprint matching using the combination of nearest neighbor arrangement indexing", *Frontiers in Robotics and AI*, vol. 7, p. 113, 2020, doi:[10.3389/frobt.2020.00113](https://doi.org/10.3389/frobt.2020.00113).
- [152] V. Anand, V. Kanhangad, "Pore-based indexing for fingerprints acquired using high-resolution sensors", *Pattern Analysis and Applications*, vol. 23, pp. 429–441, 2020, doi:[10.1007/s10044-019-00805-3](https://doi.org/10.1007/s10044-019-00805-3).
- [153] H. P. Singh, P. Dimri, S. Tiwari, M. Saraswat, "Segmentation techniques through machine based learning for latent fingerprint indexing and identification", 2020, doi:[10.56042/jsir.v79i3.68640](https://doi.org/10.56042/jsir.v79i3.68640).
- [154] I. Pérez-Sánchez, B. Cervantes, M. A. Medina-Pérez, R. Monroy, O. Loyola-González, S. García, F. Herrera, "An indexing algorithm based on clustering of minutia cylinder codes for fast latent fingerprint identification", *IEEE Access*, vol. 9, pp. 85488–85499, 2021, doi:[10.1109/access.2021.3088314](https://doi.org/10.1109/access.2021.3088314).
- [155] Y. Xu, Y. Lu, F. Chen, G. Lu, D. Zhang, "High resolution fingerprint retrieval based on pore indexing and graph comparison", *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 226–236, 2021, doi:[10.1109/tifs.2021.3139219](https://doi.org/10.1109/tifs.2021.3139219).
- [156] J. M. S. Soares, L. Barbosa, P. A. L. Rego, R. P. Magalhães, J. A. F. de Macêdo, "Using inverted index for fingerprint search", *Journal of Information and Data Management*, vol. 12, no. 5, 2021, doi:[10.5753/jidm.2021.1918](https://doi.org/10.5753/jidm.2021.1918).
- [157] G. Arora, S. Kalra, A. Bhatia, K. Tiwari, "Palhashnet: Palmprint hashing network for indexing large databases to boost identification", *IEEE Access*, vol. 9, pp. 145912–145928, 2021, doi:[10.1109/access.2021.3123291](https://doi.org/10.1109/access.2021.3123291).
- [158] R. Balasundaram, G. F. Sudha, "Retrieval performance analysis of multibiometric database using optimized multidimensional spectral hashing based indexing", *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 110–117, 2021, doi:[10.1016/j.jksuci.2018.02.003](https://doi.org/10.1016/j.jksuci.2018.02.003).
- [159] D. Osorio-Roig, T. Schlett, C. Rathgeb, J. Tapia, C. Busch, "Exploring quality scores for workload reduction in biometric identification", "2022 International Workshop on Biometrics and Forensics (IWBF)", pp. 1–6, IEEE, 2022, doi:[10.1109/iwbf55382.2022.9794533](https://doi.org/10.1109/iwbf55382.2022.9794533).
- [160] G. Arora, A. Singh, A. Nigam, H. M. Pandey, K. Tiwari, "Fkpindexnet: An efficient learning framework for finger-knuckle-print database indexing to boost identification", *Knowledge-Based Systems*, vol. 239, p. 108028, 2022, doi:[10.1016/j.knosys.2021.108028](https://doi.org/10.1016/j.knosys.2021.108028).
- [161] P. Drozdowski, F. Stockhardt, C. Rathgeb, C. Busch, "Signal-level fusion for indexing and retrieval of facial biometric data", *IET Biometrics*, vol. 11, no. 2, pp. 141–156, 2022, doi:[10.1049/bme2.12063](https://doi.org/10.1049/bme2.12063).
- [162] D. Osorio-Roig, L. J. Gonzalez-Soler, C. Rathgeb, C. Busch, "Privacy-preserving multi-biometric indexing based on frequent binary patterns", *arXiv preprint arXiv:2310.03091*, 2023, doi:[10.1109/tifs.2024.3386310/mml](https://doi.org/10.1109/tifs.2024.3386310/mml).
- [163] S. A. Grosz, A. K. Jain, "Afr-net: Attention-driven fingerprint recognition network", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2023, doi:[10.1109/tbiom.2023.3317303](https://doi.org/10.1109/tbiom.2023.3317303).
- [164] M. Kumar, D. Kumar, "An efficient gravitational search decision forest approach for fingerprint recognition", *Kuwait Journal of Science*, vol. 50, no. 2A, 2023, doi:[10.48129/kjs.20635](https://doi.org/10.48129/kjs.20635).
- [165] A. K. Jain, S. S. Arora, L. Best-Rowden, K. Cao, P. S. Sudhish, A. Bhatnagar, Y. Koda, "Giving infants an identity: Fingerprint sensing and recognition", "Proceedings of the Eighth International Conference on Information and Communication Technologies and Development", pp. 1–4, 2016, doi:[10.1145/2909609.2909612](https://doi.org/10.1145/2909609.2909612).
- [166] A. K. Jain, S. S. Arora, K. Cao, L. Best-Rowden, A. Bhatnagar, "Fingerprint recognition of young children", *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1501–1514, 2016, doi:[10.1109/tifs.2016.2639346](https://doi.org/10.1109/tifs.2016.2639346).
- [167] J. J. Engelsma, D. Deb, K. Cao, A. Bhatnagar, P. S. Sudhish, A. K. Jain, "Infant-id: Fingerprints for global good", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 7, pp. 3543–3559, 2021, doi:[10.1109/tpami.2021.3057634](https://doi.org/10.1109/tpami.2021.3057634).
- [168] I. Widiatmika, I. N. Piarsa, A. Syafiandini, "Recognition of the baby footprint characteristics using wavelet method and k-nearest neighbor (k-nn)", *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*, vol. 12, no. 1, pp. 41–52, 2021, doi:[10.24843/lkjiti.2021.v12.i01.p05](https://doi.org/10.24843/lkjiti.2021.v12.i01.p05).
- [169] H. I. Yoshinori Koda, "Fundamental study of neonate fingerprint recognition using fingerprint classification", 2022, doi:[10.1109/biosig55365.2022.9897017](https://doi.org/10.1109/biosig55365.2022.9897017).
- [170] N. Nelufule, Y. Moolla, S. Ntshangase, A. de Kock, "Biometric recognition of infants using fingerprints", Tech. rep., EasyChair, 2023, doi:[10.1109/ictas56421.2023.10082749](https://doi.org/10.1109/ictas56421.2023.10082749).
- [171] T. O. Odu, T. Ogunfunmi, M. O. Olaniyan, I. A. Samuel, "Multi-instance contingent fusion for the verification of infant fingerprints", "World Conference on Information Systems for Business Management", pp. 197–207, Springer, 2023, doi:[10.1155/2024/7728707](https://doi.org/10.1155/2024/7728707).
- [172] M. Bahzad, L. M. Labib, M. Elhosseini, M. Badawy, "M<sup>2</sup>brtpc: A novel modified multimodal biometric recognition for toddlers and pre-school children approach", *Mansoura Engineering Journal*, vol. 48, no. 5, p. 5, 2023, doi:[10.58491/2735-4202.3069](https://doi.org/10.58491/2735-4202.3069).
- [173] M. Shabil, H. Fadewar, "Fingerprint recognition of newborns and toddlers using pre-trained model under convolution neural networks", *Journal of Data Acquisition and Processing*, vol. 38, no. 2, p. 234, 2023, doi:[10.5281/zenodo.7766329](https://doi.org/10.5281/zenodo.7766329).
- [174] K. Rajaram, N. B. Amma, S. Selvakumar, "Convolutional neural network based children recognition system using contactless fingerprints", *International Journal of Information Technology*, vol. 15, no. 5, pp. 2695–2705, 2023, doi:[10.1007/s41870-023-01306-7](https://doi.org/10.1007/s41870-023-01306-7).
- [175] M. Kazi, K. Kale, R. S. Mehsen, A. Mane, V. Humbe, Y. Rode, S. Dabhade, N. Bansod, A. Razvi, P. Deshmukh, "Face, fingerprint, and signature based multimodal biometric system using score level and decision level fusion approaches", *IETE Journal of Research*, pp. 1–20, 2023, doi:[10.1080/03772063.2023.2217784](https://doi.org/10.1080/03772063.2023.2217784).
- [176] S. A. El\_Rahman, A. S. Alluhaidan, "Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments", *Plos one*, vol. 19, no. 2, p. e0291084, 2024, doi:[10.1371/journal.pone.0291084](https://doi.org/10.1371/journal.pone.0291084).
- [177] H. Byeon, V. Raina, M. Sandhu, M. Shabaz, I. Keshta, M. Soni, K. Matrouk, P. P. Singh, T. Lakshmi, "Artificial intelligence-enabled deep learning model for multimodal biometric fusion", *Multimedia Tools and Applications*, pp. 1–24, 2024, doi:[10.1007/s11042-024-18509-0](https://doi.org/10.1007/s11042-024-18509-0).
- [178] J. Priyani, P. Nanglia, P. Singh, V. Shokeen, A. Sharma, "Hgssa-bilstm: A secure multimodal biometric sensing using optimized bi-directional long short-term memory with self-attention", *ECS Sensors Plus*, vol. 3, no. 1, p. 011401, 2024, doi:[10.1149/2754-2726/ad1b3a](https://doi.org/10.1149/2754-2726/ad1b3a).



- [179] J. Samatha, G. Madhavi, "Securesense: Enhancing person verification through multimodal biometrics for robust authentication", *Scalable Computing: Practice and Experience*, vol. 25, no. 2, pp. 1040–1054, 2024, doi:[10.12694/scpe.v25i2.2524](https://doi.org/10.12694/scpe.v25i2.2524).
- [180] D. A. Reid, M. S. Nixon, S. V. Stevenage, "Soft biometrics: Human identification using comparative descriptions", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, pp. 1216–1228, 2014, doi:[10.1109/tpami.2013.219](https://doi.org/10.1109/tpami.2013.219).

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).



**Diptadip Maiti**, is currently a research scholar in the department of Computer Science & Engineering at Techno India University, West Bengal. He did his B. Tech. in Computer Science & Engineering and M. Tech in Information Technology in 2005 and 2009 respectively.

His research interests are in Image Processing, Biometric Authentication, Machine Learning and Deep Learning.



**Madhuchhanda Basak**, is currently a research scholar in the department of Computer Science & Engineering at Techno India University, West Bengal. She did his B. Tech. & M. Tech. in Information Technology in 2006 and 2010 respectively.

Her research interests are in Image Processing, Biometric Authentication, Machine Learning and Deep Learning.



**Debashis Das**, is an Associate Professor in the department of Computer Science & Engineering at Dr. Sudhir Chandra Sur Institute of Technology & Sports Complex, West Bengal. He did his B. Tech. in Information Technology and M. Tech in Computer Science & Engineering in 2009 and 2012 respectively. He did his PhD in Computer Science & Engineering in 2017.

His research interests are in Image Processing, Biometric Authentication and Steganography.

# HivePool: An Exploratory Visualization System for Honey Beehive Data

Tinghao Feng\*, Sophie Columbia, Christopher Campell, Rahman Tashakkori

Computer Science Department, Appalachian State University, Boone, 28608, USA

E-mails: [fengt@appstate.edu](mailto:fengt@appstate.edu) / [columbiase@appstate.edu](mailto:columbiase@appstate.edu) / [campellcl@appstate.edu](mailto:campellcl@appstate.edu) / [tashakkorir@appstate.edu](mailto:tashakkorir@appstate.edu)

\*Corresponding author: Tinghao Feng, Computer Science Department, Appalachian State University, Boone, 28608, USA & Email: [fengt@appstate.edu](mailto:fengt@appstate.edu)

**ABSTRACT:** Honey bee health is crucial for global ecosystems, but traditional data analysis methods often struggle to capture the complex interplay between bee behavior and environmental factors. To bridge this gap, we developed HivePool, a novel data visualization and analysis tool designed to empower beekeepers and researchers with deeper insights into these interactions. This paper explores HivePool's functionalities, focusing on its interactive visualizations and innovative time-oriented pattern recognition for event prediction. By leveraging time series visualization techniques, HivePool allows users to explore not only static relationships between environmental variables but also how these variables change dynamically leading up to specific events within the hive. The paper showcases HivePool's effectiveness through two use cases: data-driven event exploration and example-driven event prediction. Overall, HivePool equips beekeepers and researchers with a powerful set of tools, facilitating a deeper understanding of bee behavior and environmental influences, ultimately leading to improved beehive health and management strategies.

**KEYWORDS:** Time Series Data Analysis, Event Visualization, Honey Beehive Data

## 1. Introduction

The alarming decline of honey bee colonies poses a significant threat, making it critical to unravel the mysteries behind Colony Collapse Disorder (CCD) [1]. Initiatives like the Appalachian Multipurpose Apiary System (AppMAIS) [2] have played a valuable role in collecting data on honey bee health. However, this data's sheer volume and complexity often create a roadblock for researchers trying to identify meaningful patterns. Existing analysis tools, while helpful, often fall short in their ability to uncover subtle correlations hidden within these intricate, multidimensional datasets [3].

To address this challenge, we developed HivePool, a groundbreaking visualization system that empowers users to delve deeper, exploring the intricate relationships between various time series data—temperature fluctuations, hive weight changes, and more—and specific events that occur within honey bee colonies, like swarming episodes. Unlike traditional analysis methods that may struggle to reveal these subtle connections, HivePool is specifically tailored to identify patterns between these diverse variables over time and how they relate to corresponding bee behavior.

The motivation behind HivePool stems from the recognition that existing data analysis tools often fail to illuminate the hidden connections within honey bee health datasets. Previous attempts, such as the visualization tool developed in our lab, provided some initial insights but lacked the sophistication needed to comprehensively analyze the richness of multidimensional time series data [3]. Similarly, Beevis, while offering a comparison of multiple time series alongside the video, lacked the capability to define events

specific to honey bee behavior and analyze how these multidimensional datasets influence or relate to bee activity [4]. HivePool builds upon these past efforts to bridge the gap and provide a more powerful platform for exploring the intricate temporal relationships within honey beehive data.

By providing a platform to define honey beehive data events and explore the intricate interplay between time series variables and bee behavior, HivePool offers researchers and beekeepers a powerful tool for gaining a deeper understanding of honey bee health and the factors that influence it. This paper delves into the functionalities of HivePool and showcases its effectiveness in uncovering hidden correlations within honey beehive data. By leveraging advanced visualization techniques and analytical tools, HivePool empowers users to extract valuable insights from these complex datasets, ultimately contributing to a more comprehensive understanding of honey bee health and paving the way for developing effective monitoring and management strategies. Through compelling case studies and feedback from domain experts, we demonstrate HivePool's ability to unlock hidden patterns within bee data, facilitating informed decision-making in both beekeeping practices and research endeavors. We conclude by highlighting the significance of HivePool in advancing our understanding of honey bee behavior and its implications for colony health, while also outlining exciting avenues for future research and development.

## 2. Related Work

### 2.1. Honey Beehive Data Analysis

Understanding honey bee behavior hinges on effective data collection and analysis from beehives. Here, we ex-

plore prior research that has significantly contributed to these efforts. The AppMAIS and Beemon projects [5, 6, 7, 8] serve as prime examples, collecting diverse data (humidity, temperature, weight, audio, and video recordings) from honey beehives in Western North Carolina over the past thirteen years. This data provides a valuable foundation for further analysis.

Researchers have increasingly utilized sensor data to analyze honey bee behavior in relation to environmental factors. In [9], the authors proposed a method using a supervised machine learning classification algorithm to estimate colony health status and predict imminent collapsing states for beekeepers. In [10], the authors introduced a honey bee colony state identification solution using temperature data and fuzzy logic. In [11], the authors developed a multi-sensor platform for real-time and long-term measurement of relevant hive parameters and environmental conditions. While these studies establish the groundwork for hive data collection and basic analysis, they often lack comprehensive data visualization capabilities.

Visualization techniques play a crucial role in assisting honey bee analysis by leveraging human visual perception to analyze biological features or behaviors. In [12], the authors developed an automated 3D visual system that utilized two video cameras to observe and output 3D space trajectories and inflight statistics of target honey bees. In [13], the researchers visualized honey bee activity at hive entrances to monitor hive conditions and predict honey bee behavior. However, these approaches often lack an efficient visualization system with a user-friendly interface and the capability for comprehensive visual analysis, motivating the development of HivePool.

Detection and prediction of honey bee swarms have also attracted significant research interest, further motivating HivePool's development. In [14], the authors presented a bee-condition-monitoring system incorporating a deep learning process to detect bee swarming. In [15], the authors proposed a method to detect swarming remotely. In [16], the authors disclosed a method for monitoring and predicting the swarming process within honey bee colonies using vibro-acoustic information, similar to the approach taken by Beemon.

HivePool builds upon these efforts by attempting to model the pattern using a time series of all variables preceding the swarm event. This enables prediction based on historical data and identified patterns.

## 2.2. Multivariate Time Series Visualization

Time series data visualization has garnered significant interest among researchers, inspiring the development of HivePool. Several existing visualization tools and techniques have influenced HivePool's design, particularly in the context of exploring multivariate time series data.

TimePool, a tool for visualizing multiple univariate time series, utilizes line charts – a concept similarly adopted by HivePool to represent time series of selected variables for multiple hives [17, 18, 19]. However, displaying numerous line charts can lead to clutter, hindering data comparison and individual item tracking [20, 21]. Variations like 3D line graphs and braided graphs offer minimal improvement and can be misleading with more data [22, 23]. ChronoLenses,

which applies data transformations and displays results in line charts, can also be more cluttered than the original data [24].

To address clutter from multiple line charts, HivePool employs juxtaposed techniques, projecting them onto a set of time lines for each hive [17]. Similar approaches include line graph explorers [25], two-tone pseudo coloring [26], Spark Cloud [27], and Horizon Graphs [28], all of which display time series side-by-side to avoid overlapping data. Works like Interactive Horizon Graphs [29] allow users to adjust the baseline for pattern discovery, while Qualizon graphs [30] incorporate qualitative categories with bands. In [31], the researcher present time series with multiple detail levels and abstractions, combining quantitative and qualitative representations. However, juxtaposed techniques become less effective as the number of displayed time series increases due to cognitive overload [23, 32, 33].

Juxtaposed timelines are commonly used for event exploration in various domains like news analysis [34], communication analysis [35, 36], and medical research [37, 38, 39]. HivePool leverages juxtaposed timelines to facilitate analyses of time series data for multiple hives, applying them in a different context than existing works. Similar to those used in the matrix or line-based visualizations, sorting techniques are also employed to reveal patterns within the data [40, 41].

EVIS serves as another significant inspiration for HivePool [42]. It visualizes a multivariate time series preceding an event on a RadViz space. HivePool borrows this concept to define the Event Leash on the scatter plot for two environmental variables.

In [43], the author presented a set of line charts, one for each dimension, to visually analyze multivariate time series. Selecting a series in one chart would highlight it in all charts, enabling interactive exploration. While intuitive, this approach doesn't explicitly reveal temporal relationships among the dimensions.

In [44], the authors employed a two-step dimension reduction process to project a group of multivariate time series as points in a 2D space. Users could examine feature contributions to clusters within the projection space. However, reducing each time series to a single point made it difficult to compare temporal trends in detail for a large number of series. In [45], the authors used animations and trajectories to show how values of multiple objects change over time in a shared 2D space. This approach can suffer from clutter and change blindness issues with many objects.

Specifically, several methods have been proposed to visualize a single multivariate time series. In [46], the author divided a multivariate time series into time slices and projected them onto an MDS plot based on their similarities. The temporal order was mapped to the color of the projections. Time Curves [47] projected high-dimensional temporal data points to a 2D space and connected them by temporal order with a time curve. Characteristics of the time curve were extracted to reveal patterns in the evolving data. In [48], the authors projected snapshots of a dynamic network to dots in a 2D space and connected them using a curve. However, visualizing a large number of time series was not a focus of these approaches.

The trajectory-based financial time series visualization [49] is relevant to HivePool's Event Leash concept. It plotted 2D time series as trajectories in a 2D space and clustered



them based on high-dimensional feature vectors using a Self-Organizing Map [50].

### 2.3. Trajectory Similarity Search

Calculating the similarities of trajectories is a common computational task in many domains [51]. For our application, trajectory similarity is key to revealing similar patterns of change in environmental variables preceding specific events within a hive. HivePool, utilizing a domain appropriate similarity metric, searches for times within beehives with similar changes selected measured variables.

In [52], the authors provide an overview of trajectory similarity measures. Popular approaches vary in complexity, susceptibility to noise, and whether they account for temporal differences [53]. Existing literature divides these measures into being either metric or nonmetric. A distance measure is considered metric if it is unique, symmetric, non-negative, and satisfies the triangle inequality [52]. Non-metric measures do not meet these requirements.

Euclidean distance is perhaps the simplest measure of quantifying similarity between trajectories [54]. However, it requires trajectories to be of equal length, which may be too primitive for some applications. Fréchet distance and Hausdorff distance both measure shape similarity [55, 56], though unlike Hausdorff, Fréchet is a metric measure [52]. Yet, none of these three distance measures account for temporal similarity.

Selected spatio-temporal similarity measures include Dynamic Time Warping and Longest Common Subsequence. Dynamic Time Warping performs a recursive search to locate the most similar points between trajectories [52, 57]. The longest Common Subsequence is a nonmetric measure that emphasizes robustness to noise [52, 58].

Similarity searching, finding the most similar trajectories within a large subset, can prove to be a computationally complex calculation. Searching large databases with many trajectories typically leads to a prohibitive runtime [59]. One attempt to devise an efficient searching algorithm is Wang and Liu's algorithm, which supports queries personalized to users [59]. Supporting such queries provides a tailored user experience, but this algorithm does not account for temporal differences.

Moreover, unlike in many real-world scenarios, notably with GPS data where trajectories may not be of the same length [60], the same number of points between compared trajectories can be guaranteed for our data. Searches that accommodate trajectories of varying lengths are unnecessarily complex for our application. Frentzos and Theodoridis proposed a novel algorithm to efficiently conduct an index-based similarity search, which utilizes R-trees [61]. Torch is a trajectory search engine that features a trajectory similarity search and utilizes R-trees [62]. Torch supports various search queries, allowing users to investigate patterns among trajectories. Likewise, HivePool supports two versions of similarity searching to find the most similar trajectories between all variables or two user-selected variables.

## 3. Domain Background And Data

### 3.1. Data Collection Methodology

This research utilizes data collected through the AppMAIS Beemon system [63]. Beemon functions by acquiring

data via a Raspberry Pi 4B (Rpi) and transmitting it to a designated server for primary analysis and visualization. Fig 1 provides a comprehensive view of the Beemon system's hardware configuration.

#### Beemon System Hardware:

The core components of the Beemon system include a Raspberry Pi 4B (Rpi), a Raspberry Pi Camera Model 2, and protective casing for both units.

#### Data Acquisition:

- *Environmental Sensors:* Data pertaining to scale readings, humidity, and temperature is collected by the Rpi through Field-Programmable Gate Array (FPGA) pins.
- *Audio Data:* A microphone connected to a USB port on the Rpi captures audio information.
- *Video Analysis:* Computer vision techniques are applied to video recordings to estimate bee activity levels (VideoFileSize) and bee traffic (departures and arrivals).

#### Data Used for HivePool:

Internal hive data:

- *RMSDb:* Noise level within the hive in Decibel scale
- *Temperature:* Internal hive temperature
- *Humidity:* Internal hive humidity

External hive data:

- *Hive Scale:* Weight of the hive
- *VideoFileSize:* Indicator of bee activity level

Derived data:

- *Arrivals:* How many bees come into the hive entrance within the video recording
- *Departures:* How many bees fly away from the hive entrance within the video recording
- *Difference:* The difference between Arrivals and Departures

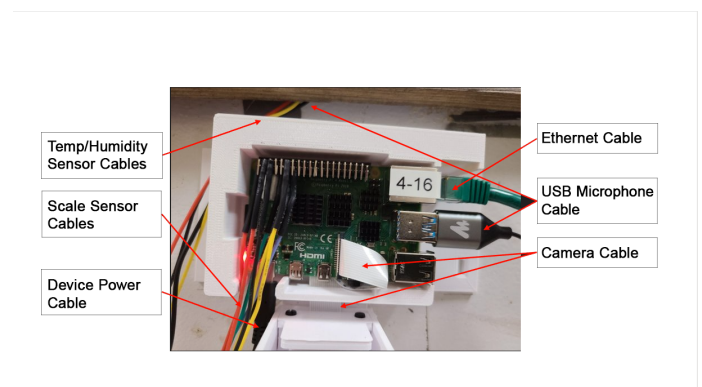


Figure 1: The Beemon system

This breakdown clarifies the data collection process and separates Beemon system details from the specific data used by HivePool for analysis.

### 3.2. Data Collection Timeframe

Our data collection focused on the active period of the hives, primarily daylight hours between 8:00 AM and 8:00 PM Eastern Standard Time (EST). For audio and video data, we captured one-minute segments at frequent intervals. Specifically, the Raspberry Pi (RPI) uploaded one-minute audio and video recordings every five minutes throughout the designated collection window, starting at 8:00 AM EST.

### 3.3. Challenges and Considerations

The Beemon system has undergone extensive testing for reliability under various weather conditions. However, occasional data gaps exist due to sensor malfunctions, power outages, or internet disruptions. Additionally, it's important to note that while video recordings capture the hive entrance, audio recordings come from within. This means they are not perfectly synchronized despite being captured simultaneously. Furthermore, propolis, a resin used by bees to seal their hives, can sometimes coat sensors and microphones, potentially affecting humidity, temperature, and audio data quality.

Despite these limitations, the data collected using the AppMAIS Beemon system provides a comprehensive snapshot of honey bee activity and environmental conditions. These datasets offer valuable insights into bee behavior and hive dynamics, even with inherent challenges. They serve as a strong foundation for developing advanced analytical and visualization techniques to unlock the complexities of honey bee ecosystems.

methods, however, often struggle to capture these subtle connections within complex, multidimensional datasets. Here, the rich data collected by the AppMAIS Beemon system presents a unique opportunity to delve deeper into these relationships.

While an initial scatter plot matrix (Fig 2) might not reveal clear correlations between independent variables like video file size, audio loudness (RMSDb), temperature, humidity, and hive weight, the potential to uncover hidden patterns remains significant.

This research is driven by two key motivations:

#### 4.1.1. Understanding the Impact of Environmental Changes

We aim to discover how fluctuations in environmental variables (e.g., temperature, humidity) influence honey bee behavior within the hive. By analyzing these relationships, we can gain valuable insights into bee health and colony well-being.

#### 4.1.2. Predicting Honey Bee Swarms

Swarming is a natural process where a portion of a colony leaves to establish a new one. Predicting swarm events is crucial for beekeepers as it allows proactive management and minimizes potential honey production losses. However, accurately predicting swarms remains challenging due to the complex interplay of factors involved.

### 4.2. Tasks

Addressing these motivations translates to two primary tasks for HivePool:

#### 4.2.1. Task 1: Data-Driven Event Exploration

This task explores user-defined events within the beehive data and identifies potential correlations with environmental factors. It comprises three subtasks:

- **(T1-1) Events Definition:** Since there are no predefined behavioral events within the data, users can leverage variables like VideoFileSize, RMSDb, and bee traffic data to define events of interest. This might involve investigating variable distributions across hives and time to identify potential inflection points or thresholds that could be considered events.
- **(T1-2) Environmental Pattern Definition:** Once an event is defined, the goal is to explore the environmental factors (temperature, humidity, etc.) and how they change leading up to the event. This involves identifying patterns in these variables that might be associated with the chosen event.
- **(T1-3) Potential Event Exploration:** HivePool then quantifies the relationship between defined events and the time series of independent variables through correlation analysis. Assessing the strength and direction of these correlations helps us understand the influence of environmental factors on bee behavior and hive dynamics.

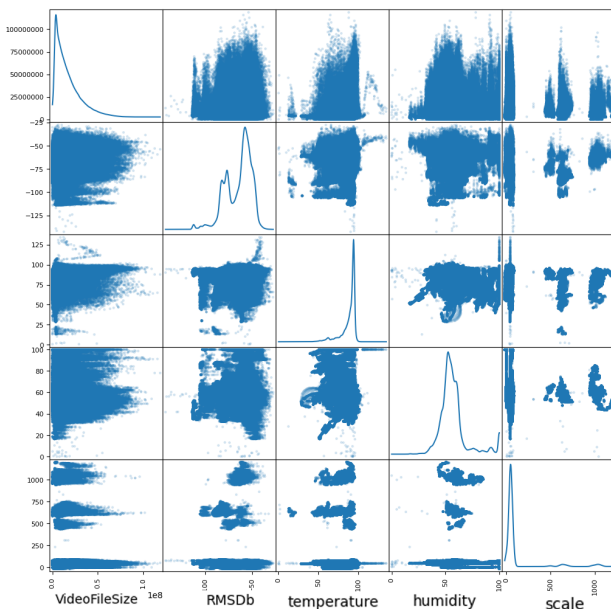


Figure 2: A scatter plot matrix with VideoFileSize, RMSDb, Temperature, Humidity, and hive Scale that shows no obvious relationships between these variables.

## 4. Motivation And Tasks

### 4.1. Motivation

Unveiling the intricate dance between honey bee behavior and environmental factors is critical for understanding colony health and dynamics. Traditional data analysis

#### 4.2.2. Task 2: Example-Driven Swarm Prediction

This task tackles the challenge of predicting honey bee swarms using historical data. It consists of the following subtasks:

- **(T2-1) Training and Test Set Splitting:** Swarm event data, typically collected by domain experts through video recordings, audio analysis, and direct observation, is the foundation for this task. The first step involves splitting these swarm samples into training and test sets. The training set defines the characteristic time series pattern preceding a swarm, while the test set is used to evaluate the prediction accuracy.
- **(T2-2) Multi-Variable Time Series Pattern Definition:** Since swarm samples are often limited, directly applying machine learning techniques might be impractical. To address this, HivePool utilizes the concept of a multi-variable time series pattern. This pattern, visualized using Detailed Leashes, depicts the changes in all relevant variables (temperature, humidity, etc.) leading up to a swarm event within the training set.
- **(T2-3) Similarity Search:** With the training pattern established, HivePool performs a similarity search across new datasets. This search identifies data points exhibiting similar patterns to the training swarm examples, potentially indicating upcoming swarms within the beehives.
- **(T2-4) Evaluation:** The effectiveness of these predictions is then evaluated using the predefined test set. By comparing the similarity search results with the known swarm events in the test set, HivePool can assess its accuracy in predicting future swarms.

This breakdown clarifies the importance of swarm prediction for beekeepers and highlights the challenges involved. It also details how HivePool addresses these challenges through its multi-variable time series pattern approach and evaluation using a test set.

### 5. HivePool Visualization

HivePool prioritizes user-friendliness with its comprehensive visualization design. This design allows users to gain intuitive insights into how honey bee behavior interacts with environmental variables. The toolbox offers a variety of components, including line charts for visualizing trends, time maps for spatial representation of events, hive time bar charts for activity breakdowns within the hive, scatter plots for exploring correlations, and a powerful algorithm for uncovering similar patterns within the data.

#### 5.1. Line Charts: Unveiling Trends in Bee Activity

Line charts are HivePool's workhorse for visualizing honey bee behavior. They offer a clear view of a chosen variable's time series data for each hive. Since bee data is time-oriented and often collected intermittently (typically 8 AM to 7 PM daily), HivePool employs a segmented timeline approach. Each day is represented by a continuous segment, allowing for scaling of daily data within it.

These line charts display the variable's basic line graph for each hive, typically the event under analysis. Users can observe how the variable changes over time, following its path across each day's segment as shown in figure 3 (1). To simplify the analysis, users can select individual hives to highlight their lines, isolating and comparing specific hive data to identify unique trends and patterns.

Interaction is key: users can zoom in or out to focus on specific timeframes or adjust the scale for different levels of detail. Hovering over data points reveals specific values, fostering deeper exploration. Ultimately, HivePool's line charts empower users to analyze time series data across multiple hives. By enabling the visualization of trends, patterns, and correlations in bee behavior over time, line charts become a powerful tool for understanding hive dynamics and informing beekeeping and research decisions.

#### 5.2. Time Maps: Decoding Bee Activity Throughout the Day

HivePool's time maps allow users to examine the daily distribution of a chosen variable more closely. They visualize this data using bubbles arranged along a vertical line within each day segment of the timeline.

Each bubble represents a specific data point, with its position on the y-axis indicating the time of day and its size reflecting the variable's value at that moment. This allows for a quick grasp of how the chosen variable fluctuates throughout the day within a hive.

Want to focus on a specific hive? No problem! Selecting a hive filters the time map, displaying only its data for focused analysis and pattern recognition across different days.

By visually depicting the variable's distribution within each day, the time map helps users understand how it changes over time. Identifying trends, peaks, and patterns in the variable's behavior provides valuable insights into hive dynamics and the influence of environmental factors.

Seamlessly integrated with the line chart, the time map allows for comparing the variable's daily distribution with its overall trend across multiple days. This lets users correlate specific time-based events with broader patterns observed in the line chart (See Fig 3 (2) for a sample: five-day line chart and time map for VideoFileSize in hive AppMAIS12R).

HivePool's time maps go beyond the line chart, offering a granular view of a variable's daily fluctuations. By providing a deeper understanding of bee activity patterns and environmental influences, the time map empowers users to make informed decisions and conduct insightful analyses.

#### 5.3. Hive Map: Spotlighting Activity Across Hives

HivePool's Hive Map takes a unique approach to visualizing time series data. Imagine a bar for each hive, divided into colored segments that mirror the line chart's threshold (think green for above threshold, orange for below, consistent across all visualizations).

These segments clearly show how the chosen variable is distributed across different hives over time, relative to the threshold. This makes it easy to identify periods when the variable exceeds or falls below the threshold for each hive, aiding in understanding hive dynamics and environmental influences.



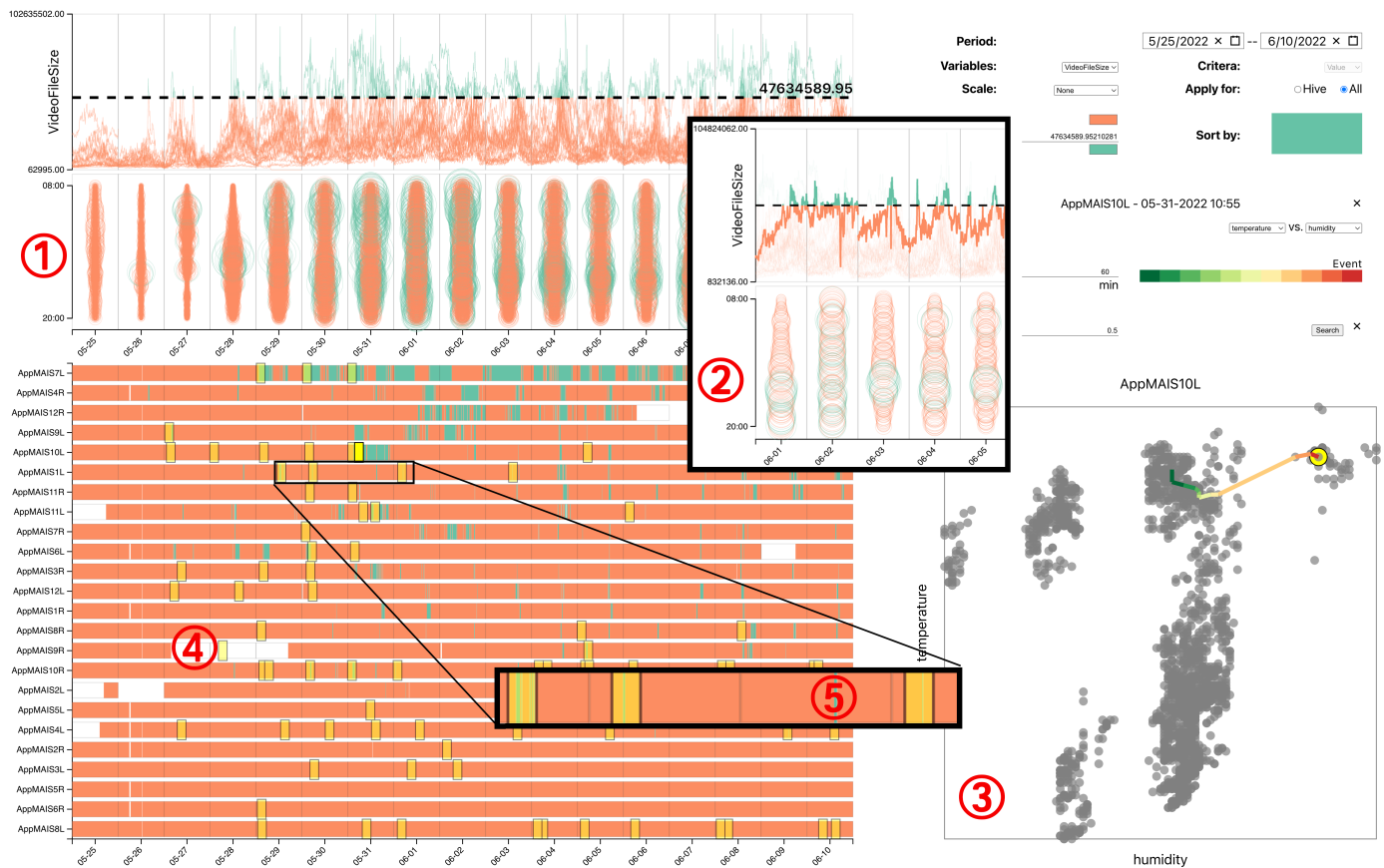


Figure 3: The layout of HivePool. (1) Line Charts and Time Maps. (2) Line Charts and Time Maps with a hive selected. (3) Scatter Plot with an Event Leash for a selected time point. (4) Hive Map. (5) Details of some data-driven event search results, which indicate the high VideoFileSize (green lines) are matched with the search results.

For better comparison, hives can be sorted based on the total length of green or orange segments, depending on your preference. This sorting helps you see which hives experience the most or least time at a specific value, revealing patterns and trends across them.

The Hive Map also boasts interactive features to enhance user experience:

- **Hive Selection:** Clicking a hive's name highlights it in the line chart and filters the time map, allowing focused analysis of a single hive's data.
- **Event Selection:** Manually select an event and see similar events highlighted on the Hive Map. This lets you explore how hives behave similarly based on specific events or conditions, offering insights into hive dynamics and environmental factors.

By providing intuitive visuals and interactive features, the Hive Map empowers users to explore the chosen variable's distribution across hives over time. This facilitates in-depth analysis of hive dynamics and environmental influences, ultimately aiding informed decision-making and a deeper understanding of honey bee behavior. Fig 3 (4) shows the Hive Map right below the Line charts and Time Map.

#### 5.4. Scatter Plots & Event Leash: Unveiling Environmental Triggers

While line charts, time maps, and hive maps paint a vivid picture, HivePool goes beyond static visuals. It offers scatter

plots to explore relationships and distributions between two chosen environmental variables for each hive. However, scatter plots lack a time dimension. Enter the Event Leash, a novel feature that bridges this gap.

**Scatter Plots:** These plots allow users to visualize the correlation, distribution, and potential patterns between two selected environmental variables across different hives. This empowers users to identify potential connections between, say, temperature and humidity within each hive.

**Event Leash: Unveiling Time-based Triggers:** This innovative feature injects time-awareness into the scatter plot view. It displays a time series of the two environmental variables leading up to a selected event (visualized on the Hive Map). Imagine selecting a time point on the Hive Map – the Event Leash showcases the trajectory of both environmental variables right before that event.

The Event Leash's path reveals how these environmental variables changed before the event. To make interpretation easier, HivePool color-codes the time order – allowing users to see the sequence of changes clearly. (Imagine a rainbow, with earlier points closer to the event being red and transitioning to violet as you move backward in time.) Fig 3 (3) shows an Event Leash on the Scatter Plot.

By integrating the Event Leash, HivePool takes scatter plots to the next level. This innovative feature allows users to go beyond static correlations and delve into the temporal dynamics of hive behavior and environmental influences. It empowers users to understand how changes in environmental variables might precede specific events within the hive.

### 5.5. Detailed Leash: Diving Deeper into Pre-Event Changes

The Event Leash shows how environmental variables shift before an event. But what if you want to scrutinize each variable's individual story? Here's where the Detailed Leash steps in.

The Detailed Leash provides a zoomed-in view of the time series data for each environmental variable leading up to the selected event. This detailed view allows users to see each variable's specific patterns and trends and how they might contribute to the event's occurrence.

Imagine a vertical line marking the event's exact time. The Detailed Leash plots the time series data for each variable on either side of this line, showcasing their individual pre-event behavior. Fluctuations, trends, and anomalies become clear, allowing users to understand how each variable plays a role.

By examining the Detailed Leash, users can:

- Analyze how each variable evolves over time leading up to the event.
- Identify potential correlations and causal relationships between variables and the event.
- Discover potential predictive indicators associated with the event's occurrence.

This in-depth analysis empowers users to:

- Gain a deeper understanding of the factors influencing the event.
- Make informed decisions about beekeeping practices or research interventions.

The time-oriented pattern for swarm samples in Fig 4 are defined using the Detailed Leash.

The Detailed Leash elevates HivePool's analysis capabilities. Offering a granular view of individual variable behaviors facilitates a deeper understanding of the nuanced dynamics leading up to an event. This knowledge is crucial for informed decision-making and effective interventions in beekeeping and research.

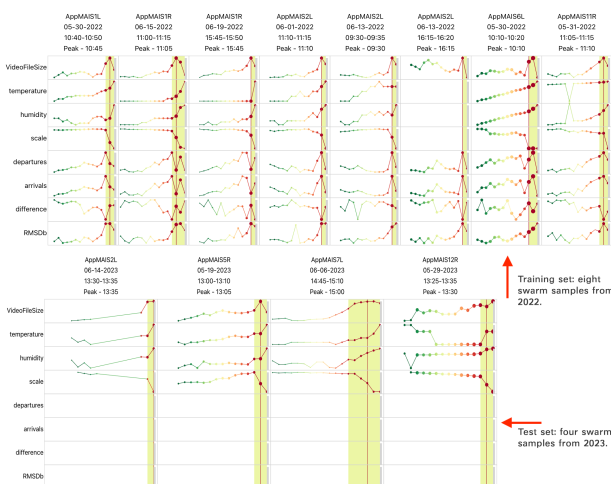


Figure 4: Detailed leashes for swarm samples. Eight samples from 2022 served as a training set and four samples from 2023 formed the test set.

### 5.6. Similarity Search: Unveiling Hidden Patterns in Bee Behavior

Behind the scenes, HivePool employs a greedy algorithm for similarity search. Within a user-defined date range and difference threshold, HivePool greedily searches for events with a set of leashes most similar to those of the swarm samples. An event, defined by the combination of its hive and leash start time, consists of a leash for each observed variable. By incrementally building the leashes and eliminating an event from consideration whenever its calculated difference exceeds the given threshold, HivePool avoids an expensive, exhaustive search.

#### 5.6.1. Similarity Metric

HivePool utilizes a similarity metric that accurately calculates similarities amongst time series trajectories. Consider two leashes of the same length, a swarm and an event leash of a single variable, for which we need to calculate their trajectory similarity. HivePool calculates a similarity score between 0 and 1, where higher scores indicate more similar trajectories. The similarity between two corresponding points at index  $i$  on a swarm ( $s$ ) and an event ( $e$ ) leash,  $a$  and  $b$  respectively, is calculated using the following equation:

$$\text{similarity}(i) = 1 - \frac{|a - b|}{\max(\max(e), \max(s)) - \min(\min(e), \min(s))} \quad (1)$$

To avoid unexpectedly high similarity scores, we penalized differences at the head of a leash higher than those at the tail of a leash by applying weights to the calculated similarity score at each index. Let  $D'$  be an array of length  $n$ , the length of both the swarm and event leashes, where the value at each index  $i$  is given by  $(i + 1)^2$ . The array of weights,  $D$ , is then calculated using the following formula:

$$D(i) = \frac{D'[i]}{\sum(D')} \quad (2)$$

The final similarity score, a value between 0 and 1, for two entire leashes is calculated using the following formula:

$$\sum_{i=0}^{n-1} \text{similarity}(i) * D(i) \quad (3)$$

#### 5.6.2. Greedy Algorithm

Since there could be an excessively large number of leashes in the similarity search, HivePool pursues a greedy approach where events with difference scores that exceed the user-defined difference threshold are immediately discarded. Then, at the termination of the search, HivePool identifies a list of events whose final similarity scores are guaranteed to be below the difference threshold.

In the first step, we consider only the first point, the head, of each variable leash for an event. We compare these to the first point of each corresponding swarm variable leash to calculate an initial similarity score. If the average difference between all swarms' leashes and the event leash is above the difference threshold, we eliminate the event from further consideration for each variable.

Once this initial search concludes, we may be left with numerous overlapping leashes, or leashes that contain the same time series data from the same hive. We remove overlapping events, greedily retaining only the event with the highest initial similarity score.

We repeat the similarity calculation for each point remaining in the leashes of the events still under consideration. Similarly, if any variable's average difference exceeds the difference threshold at any calculation step, we discard that event. Once the search concludes, the events remaining are returned with each variable's calculated final similarity score.

## 6. Analysis Cases

This section explores HivePool's effectiveness in achieving its two core functionalities: data-driven event exploration and example-driven swarm prediction.

### 6.1. Case 1: Data-Driven Event Exploration

Jerry, a curious and meticulous beekeeper who is interested in understanding how internal hive conditions, specifically temperature and humidity, might influence the bees' activity levels. To delve deeper into this question, Jerry decided to leverage the power of HivePool to unlock insights from beehive data. With HivePool at his disposal, Jerry embarked on a multi-step analysis process to explore the relationship between these environmental factors and bee activity.

#### 6.1.1. Exploring Activity and Setting the Stage

Having identified temperature and humidity as key environmental factors of interest, Jerry turned his attention to selecting a suitable indicator for bee activity within HivePool. Because a larger file size in the video recordings captured by the beehive sensors might correlate with a higher number of bees present, Jerry opted for VideoFileSize as his metric. Within HivePool, Jerry explored the VideoFileSize data using two key visualization elements: line charts and time maps. The line charts provided a detailed view of how VideoFileSize fluctuated over time for each beehive, allowing him to identify trends and patterns in bee activity across different days. The time maps, on the other hand, offered a broader overview, displaying the distribution of VideoFileSize values across the entire dataset. This visual representation enabled Jerry to quickly identify days with unusually high or low levels of bee activity.

By strategically adjusting a threshold line overlaid on the VideoFileSize line charts, Jerry could highlight specific time periods where the video file size exceeded a certain value, potentially indicating increased bee activity within the hive. This selection was then reflected on the Hive Map (Fig 3 (1) & (4)). Here, green segments represented these periods of high VideoFileSize activity for each individual hive. The hives were further sorted based on their total duration in these green segments, providing Jerry with a quick comparison of activity levels across his beehives.

However, a closer inspection of the Hive Map revealed a potential data collection bias. One particular hive (AppMAIS7L) displayed a disproportionately long green segment

compared to the others. This anomaly prompted Jerry to shift his focus to another hive (AppMAIS10L) that also exhibited a substantial period of high activity (bright yellow rectangle in Fig 3 (4)). He designated this specific time period, identified as T1-1, as the event of interest for further investigation within HivePool.

#### 6.1.2. Event Leash and Pattern Recognition

Continuing his exploration within HivePool, Jerry delved deeper into the relationship between the chosen indicator (VideoFileSize) and the environmental factors of interest (temperature and humidity). Two key visualizations offered valuable insights at this stage.

The Scatter Plot, a powerful tool for revealing correlations between variables, displayed the relationship between temperature and humidity specifically for the hive Jerry had selected (Fig 3 (3)). Each data point within the scatter plot represented a specific point in time, with its position determined by the corresponding temperature and humidity values. By visually examining the distribution of these data points, Jerry could identify potential patterns or trends in how these two environmental factors interacted.

Overlaid on top of the Scatter Plot was the Event Leash, a unique visualization element offered by HivePool (Fig 3 (3)). Represented by a rainbow line, the Event Leash served as a dynamic timeline, tracing the changes in both temperature and humidity leading up to the selected event of interest (T1-1) – the period of high VideoFileSize identified earlier. By simultaneously observing the scatter plot and the Event Leash, Jerry could gain a more comprehensive understanding of how temperature and humidity fluctuated in relation to each other and how they evolved in the lead-up to the identified period of high bee activity. In this specific instance, Jerry noticed a potentially interesting pattern – a decrease in temperature followed by an eventual rise, occurring alongside a continuous increase in humidity. This pattern, displayed prominently by the Event Leash, offered a valuable clue for Jerry to consider as he continued his investigation into the factors influencing bee activity within his hives.

#### 6.1.3. Similarity Search and Potential Events

With the high activity period (T1-1) identified for his chosen hive (AppMAIS10L), Jerry wasn't finished yet. HivePool offered an additional layer of analysis – the ability to search for similar environmental patterns across other hives. In the background, upon selecting the event, HivePool initiated a sophisticated similarity search. This search algorithm scanned the data from all the beehives, searching for data points where the Event Leashes exhibited patterns that closely resembled the one associated with T1-1. These similar patterns could indicate similar environmental changes leading to high bee activity in other hives.

The results of this search were then displayed on the Hive Map (Fig 3 (4)) using dimmed yellow rectangles. Each rectangle represented a potential high activity event in another hive, identified by the similarity search algorithm based on the environmental patterns observed in T1-1. This visual representation on the Hive Map allowed Jerry to see how the environmental changes (represented by the green



segments associated with high VideoFileSize in his initial event) aligned with the potential high activity events in other hives (represented by the dimmed yellow rectangles) (Fig 3 (5)). The spatial distribution of these potential events offered valuable insights into the potential influence of these environmental changes across his apiary.

Furthermore, HivePool's interactive nature allowed Jerry to delve deeper. By clicking on each potential event highlighted on the Hive Map, he could access the corresponding Event Leash for that specific data point. Examining these Event Leashes (Figure 5) provided a detailed view of how temperature and humidity evolved in those other hives leading up to their potential periods of high activity. Interestingly, all four potential event Leashes displayed a similar pattern to the one Jerry observed in T1-1: a drop in temperature followed by a rise, alongside a continuous increase in humidity. This remarkable consistency across multiple hives strengthened the potential connection between this specific environmental pattern and periods of high bee activity.

This exploration gave Jerry valuable insights into the potential relationship between temperature, humidity, and bee activity within his hives. HivePool's interactive visualizations and powerful similarity search functionality empowered him to analyze user-defined events and identify potential correlations with environmental factors across his entire apiary. This comprehensive approach offered by HivePool can be a valuable tool for beekeepers seeking to understand and manage the complex interplay between environmental conditions and bee behavior.

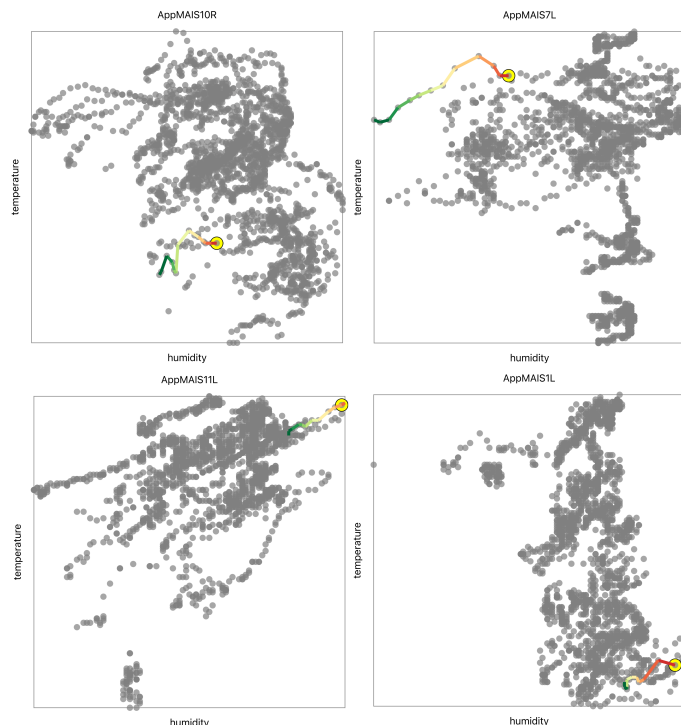


Figure 5: Four search results with high VideoFileSize for the Data-Driven Event Exploration. All the leashes show a similar pattern of continuous increasing humidity and a drop-first-and-rise-then temperature.

## 6.2. Case 2: Example-Driven Swarm Prediction

Gigi, a seasoned honey bee researcher, has meticulously documented honey bee swarm events for years. She has

identified some swarm occurrences across 2022 and 2023 through video recordings and on-site observations. Driven by a desire to manage beehive health and prevent disruptions caused by swarming proactively, Gigi embarked on a mission to develop a model capable of predicting future swarm events.

Her initial approach involved constructing a machine learning model. With this model in mind, Gigi meticulously loaded data specific to the identified swarm occurrences. The data encompassed precise timeframes relevant to each swarm event: May 30th, 2022, to June 20th, 2022, for eight samples identified in 2022, and May 15th, 2023, to June 15th, 2023, for four samples observed in 2023. Following these preparations, Gigi attempted to train the machine learning model using the 2022 dataset, evaluating its ability to predict swarms using the 2023 dataset.

However, a significant hurdle emerged during this process: extreme class imbalance within the labels. The positive labels signifying swarm samples constituted a minuscule fraction of the data. In the training set, only eight data points out of a staggering 75,628 (from 24 hives) were labeled as swarm events. Similarly, the test set has just four positive labels out of 147,351 data points (from 29 hives). This unbalanced distribution posed a substantial challenge for the machine learning algorithm. Due to the overwhelming presence of negative labels (representing non-swarm periods), the algorithm struggled to learn the intricacies of the positive class (swarm events) effectively. Recognizing this limitation and the potential for misleading results, Gigi explored alternative swarm prediction approaches. This led her to HivePool, a visualization-based analysis tool that facilitates swarm prediction using a visually-built precedent time series pattern. By leveraging HivePool's ability to identify similar environmental patterns preceding swarm events, Gigi hoped to gain valuable insights and improve her ability to predict future swarming occurrences.

### 6.2.1. Setting Up the Prediction Task

To initiate the analysis, Gigi first loaded the training set containing the swarm samples from 2022. HivePool responded by generating Detailed Leashes, one for each swarm sample (T2-1). These Detailed Leashes, serving as the foundation for predicting future swarms, visually represent the time series data for each swarm event. Unlike Event Leashes used in exploratory analysis, Detailed Leashes encompass all available environmental variables. This means each Detailed Leash displays a collection of time series line charts, one for every variable measured by the beehive sensors. By examining these charts, Gigi could gain a comprehensive understanding of how all environmental factors – temperature, humidity, video file size (indicating bee activity), scale (weight of the hive), honey bee traffic (if available), and RMSDb (a measure of hive vibration) – changed in the lead-up to each swarm event in the training data (Fig 4). However, a snag emerged when Gigi loaded the test set containing the 2023 swarm samples. Due to a data collection adjustment during that period, the 2023 samples lacked information on honey bee traffic and RMSDb. Fortunately, HivePool's design allows it to adapt. Despite missing some data, HivePool could still harness the remaining variables (VideoFileSize, Temperature, Humidity, and

Scale) to identify patterns within the data. These Detailed Leashes, encompassing all available variables for both the training and test sets, collectively define the multi-variable time series patterns that HivePool will utilize to predict potential swarm events (T2-2).

### 6.2.2. Performing the Similarity Search

Having loaded the training set, she initiated the search function. This prompted HivePool to embark on a similarity search across the 2023 data, utilizing the Detailed Leashes constructed from the eight training swarm samples from 2022 (T2-3). The search algorithm itself is designed to be adaptable. Recognizing that the 2023 data might have missing variables due to potential adjustments in data collection, the algorithm cleverly disregards missing entries. Instead, it focuses solely on the available variables that remained consistent across both datasets: VideoFileSize, Temperature, Humidity, and Scale. By comparing these four variables across the 2023 data points, the algorithm searched for instances that exhibited a high average similarity to the patterns observed in all eight training swarm Detailed Leashes. A user-defined threshold determined the level of similarity required for a data point to be considered a potential match. The outcome of this search yielded data points within the 2023 data that displayed a high degree of similarity to the environmental patterns that preceded swarm events in the training data from 2022. These identified data points, representing potential swarm events based on similar environmental changes, were then transformed into Detailed Leashes for Gigi's review. Additionally, these potential swarm events were highlighted on the Hive Map with dimmed yellow rectangles, providing a visual representation of the distribution of the hive and time. This combined visualization approach – Detailed Leashes and Hive Map markings – offered Gigi valuable insights into potential swarm occurrences within the 2023 data.

### 6.2.3. Evaluating the Results

Comparing these results to the actual 2023 swarm events, Gigi observed success. HivePool accurately predicted three out of four swarms (Fig 6). However, it also generated many false positives (Type I errors). 477 results points from the 147,351-point dataset were flagged, indicating potential algorithm refinement or threshold might be needed to better balance between accuracy and highlighting potential events. Despite this, Gigi was encouraged by HivePool's ability to identify actual swarms based on environmental patterns. This initial success suggests promise for beekeepers seeking to proactively manage hives and prevent disruptions caused by swarming (T2-4).

### 6.2.4. Future Refinement

While the high false positive rate necessitates further development, Gigi is encouraged by the three successful predictions. This case study highlights HivePool's ability to leverage historical data and time-oriented patterns to support proactive swarm management in beehives. By addressing the false positive issue through continued research,

HivePool can evolve into a valuable tool for beekeepers to predict and manage honey bee swarms more effectively.

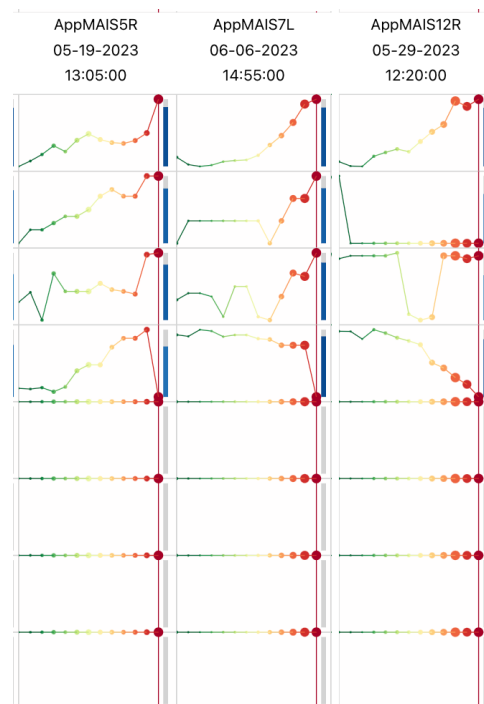


Figure 6: Swarm prediction based on data of 2023 (with missing variables) comparing to the training set successfully predict three out of four swarm samples in the test set, referring to Fig 4.

## 7. User Study

A user study assessed HivePool's effectiveness for beekeepers with limited data visualization experience. Participants, well-versed in honey beehive data, explored data exploration, environmental impact on bee behavior, and swarm prediction. This evaluated HivePool's accessibility and potential to empower beekeepers with data-driven insights for informed decisions, without requiring extensive training in specialized visualization techniques.

### 7.1. Study Design

The user study lasted approximately 30 minutes. The initial 20 minutes focused on a guided tour led by the developer to introduce participants to HivePool's core functionalities, including exploring beehive data, defining and finding potential events indicative of bee behavior, and even exploring its potential for swarm prediction. Following the guided tour, participants were empowered to take the reins for the remaining 10 minutes. This hands-on session allowed them to explore the system's features independently at their own pace. Participants were encouraged to ask questions throughout the study to ensure a productive learning environment. Finally, to gather valuable feedback on their experience, participants completed a five-question Google Form after wrapping up their exploration of HivePool.

### 7.2. Participants

A total of 10 participants were enrolled in the study. The group comprised 8 graduate students with a strong

background in honey beehive data and 2 experienced professors who brought their domain expertise to the table. A key characteristic shared by all participants was their lack of prior exposure to visual analytics tools. This selection process allowed us to simulate real-world scenarios where beekeepers, familiar with the intricacies of beehive data but new to visual analysis techniques, would be encountering HivePool for the first time. The user study allowed these participants to evaluate how HivePool's visual analytics approach could assist them in analyzing honey beehive data and extracting valuable insights.

### 7.3. User Feedback

The user study yielded valuable feedback through a Google Form survey, with questions focusing on:

- **(Q1) Did you find the system intuitive to understand?** (System Intuitiveness): This question gauged how easily participants understood HivePool's functionalities. Feedback was positive, with eight participants offering positive and one providing a neutral response. Here are some key quotes from participants: "Surprisingly intuitive for the number of different visualizations present." "I appreciated the connection between the graphs and how responsive the design was!" "The interface controls were very intuitive." "Once you understand the layout, it is extremely informative." "All the labels, graphs, and charts were clear and concise." There is one suggestion: "While this tool is going to be oriented towards professionals in the field, it might be helpful to add some more titles to provide quick context."
- **(Q2) Did you find the user interface of the visualization system easy to navigate?** (User Interface Navigation): This question assessed the user-friendliness of HivePool's interface for navigating and interacting with the data. Feedback was overwhelmingly positive. Here are some quotes: "The placement of user-determined options on the top right was very beneficial." "It gave the user very powerful tools to manipulate and browse the data." "Interactive items were labeled, which is good to see." There is also a suggestion: "Adding more descriptive labels to certain sections of the tool could greatly aid in navigation and usability."
- **(Q3) Did the visualization system provide valuable insights into honey beehive data and swarm prediction?** (Data Insights and Swarm Prediction): This question evaluated participants' perception of HivePool's effectiveness in providing valuable insights into beehive data and aiding in swarm prediction. Feedback was mostly positive, with seven participants offering praise and two providing neutral responses. Here are positive quotes: "Swarm prediction did very well compared to the limited data about existing swarms and the number of swarms." "I could see how this would be very helpful when investigating hive behavior or predicting swarms." "This system's visualization helped me have more insight into the trends of the honeybee data." Some suggestions for improvement: "The error rate is a little too high right now to be helpful in identifying swarms." "I would like it if the line plots in the swarm detection graphs had the

area under the curve colored in. This would make it a lot easier to compare the plots at first glance." "I would prefer that it includes a wider range of case studies on swarm events occurring."

- **(Q4) How useful did you find the visualizations in understanding the data and finding patterns?** (Visualization Utility): This question explored the perceived usefulness of the visualizations in helping participants comprehend the data and identify patterns. Feedback was very positive, with eight participants offering praise and one providing a neutral response. Here are positive quotes: "The use of similarity metrics was great." "Using leashes in general to find patterns was interesting and helpful." "The visualizations were easy to understand while retaining detailed information." "Users are able to make comparisons and draw conclusions from any of the contrasting data points." There are also some suggestions: "Some sort of outlier filter may be necessary." "It might be beneficial to aggregate all of the entries highlighted in blue into a visual carousel... Incorporating a search bar feature within this carousel would further improve functionality by enabling users to filter entries based on specific dates and times."
- **(Q5) Did the visualizations aid in making informed honey beehive data analysis decisions?** (Decision-Making Support): This question assessed how well the visualizations facilitated informed decision-making about honey beehive data analysis. Feedback was overwhelmingly positive. Here are some key quotes from participants: "(The interaction) would be very helpful in identifying sensor malfunction." "The similarity search seems to be very useful...I would look at times when the queen came out of the hive." "I see incredible potential in its ability to allow easy exploration through the data." "Analysis of the data becomes much more reliable and easier." "The visualizations are the best aid in making those decisions." "The insights provided by this tool would significantly boost my confidence in those choices."

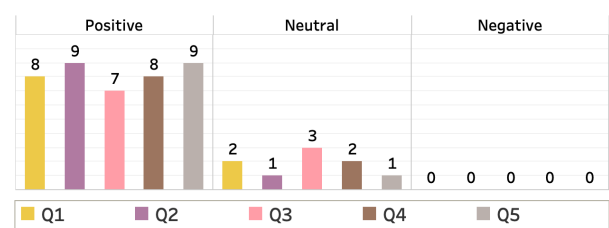


Figure 7: User feedback from the User Study.

By analyzing the survey responses and comments, we can gain valuable insights into user experience and identify areas for potential improvement within HivePool.

## 8. Conclusion

This work investigated the potential of HivePool, a visualization-based analysis tool, for exploring honey beehive data and predicting swarm events. We explored a case study where a beekeeper leveraged HivePool to investigate



the relationship between temperature, humidity, and bee activity within the hives. HivePool's functionalities empowered the beekeeper to visually analyze user-defined events, identify correlations between environmental factors and bee activity, and explore potential patterns across his apiary. Another case study indicates that a researcher attempted to apply machine learning for swarm prediction but encountered challenges due to class imbalance. HivePool offered an alternative approach by identifying similar environmental patterns preceding swarm events in historical data.

There is always room for improvement. Here are three key areas we will focus on in future development:

- **Incorporating Change Speed:** HivePool will incorporate "change speed" as a search criterion, allowing users to explore how rapidly environmental variables fluctuate within the hive, providing a more nuanced understanding.
- **Daily Time Series Generation:** HivePool currently uses data collected every five minutes (8am-8pm), creating time series gaps. This limits Event Leashes to the current day, hindering analysis of multi-day patterns. To address this, a daily version of HivePool will be introduced, aggregating data into daily points for continuous time series analysis of long-term environmental factors influencing bee behavior.
- **Mitigating Type I Errors:** The user study revealed high false positives in swarm prediction. To improve prediction accuracy, we'll refine the search algorithm or user thresholds, potentially incorporating additional data (honeybee traffic, RMSDb) or advanced similarity metrics.

By addressing these limitations and incorporating user feedback, HivePool will evolve into a robust, user-friendly tool that empowers beekeepers with data-driven insights into hive health, swarm prevention, and overall apiary management.

## 9. Acknowledgments

We gratefully acknowledge funding from the North Carolina General Assembly (NC ROI grant 2021-24) for the AppMAIS project. We also extend our appreciation to Lowe's Distinguished Professor Research Fund, relevant departments at Appalachian State University (Biology, Computer Science, Sustainability, Academic Affairs), and the undergraduate and graduate students who have contributed to the Beemon and AppMAIS data acquisition and hardware/software systems over the past eight years.

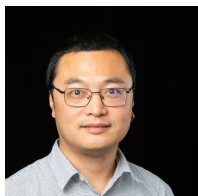
## References

- [1] O. US EPA, "Colony Collapse Disorder", 2013, doi:10.1007/springerreference\_123456.
- [2] "Appalachian Multipurpose Apiary Informatics Systems (AppMAIS)", doi:10.1007/springerreference\_654321, NC ROI 2021-24.
- [3] L. Richardson, C. Campell, R. Tashakkori, W. O'Brien, S. E. Davis, "Appmais simple data visualization app", "SoutheastCon 2023", pp. 366-370, 2023, doi:10.1109/SoutheastCon51012.2023.10114962.
- [4] T. Feng, S. Arkle, C. Campell, R. Tashakkori, "Bee vis: A comprehensive honey bee data visualization, exploration, and analysis system", "SoutheastCon 2024", pp. 1274-1281, 2024, doi:10.1109/SoutheastCon52093.2024.10500272.
- [5] R. Tashakkori, N. P. Hernandez, A. Ghadiri, A. P. Ratzloff, M. B. Crawford, "A honeybee hive monitoring system: From surveillance cameras to raspberry pi", "SoutheastCon 2017", pp. 1-7, 2017, doi:10.1109/SECON.2017.7925367.
- [6] R. Tashakkori, A. S. Hamza, M. B. Crawford, "Beemon: An iot-based beehive monitoring system", *Computers and Electronics in Agriculture*, vol. 190, p. 106427, 2021, doi:10.1016/j.compag.2021.106427.
- [7] D. J. Kale, R. Tashakkori, R. M. Parry, "Automated beehive surveillance using computer vision", "SoutheastCon 2015", pp. 1-3, 2015, doi:10.1109/SECON.2015.7132991.
- [8] R. Tashakkori, A. Ghadiri, "Image processing for honey bee hive health monitoring", "SoutheastCon 2015", pp. 1-7, 2015, doi:10.1109/SECON.2015.7133029.
- [9] A. R. Braga, D. G. Gomes, R. Rogers, E. E. Hassler, B. M. Freitas, J. A. Cazier, "A method for mining combined data from in-hive sensors, weather and apiary inspections to forecast the health status of honey bee colonies", *Computers and Electronics in Agriculture*, vol. 169, p. 105161, 2020, doi:10.1016/j.compag.2019.105161.
- [10] A. Kviesis, V. Komasilovs, O. Komasilova, A. Zacepins, "Application of fuzzy logic for honey bee colony state detection based on temperature data", *Biosystems Engineering*, vol. 193, pp. 90-100, 2020, doi:10.1016/j.biosystemseng.2020.03.011.
- [11] S. Cecchi, S. Spinsante, A. Terenzi, S. Orcioni, "A smart sensor-based measurement system for advanced bee hive monitoring", *Sensors*, vol. 20, no. 9, p. 2726, 2020, doi:10.3390/s20092726.
- [12] C. Sun, P. Gaydecki, "A visual tracking system for honey bee (hymenoptera: Apidae) 3d flight trajectory reconstruction and analysis", *Journal of Insect Science*, vol. 21, no. 2, p. 17, 2021, doi:10.1093/jisesa/ieab010.
- [13] T. Sledevič, V. Abromavičius, "Toward bee motion pattern identification on hive landing board", "2023 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream)", pp. 1-4, IEEE, 2023, doi:10.1109/eStream57549.2023.10123456.
- [14] G. Voudiotis, S. Kontogiannis, C. Pikridas, "Proposed smart monitoring system for the detection of bee swarming", *Inventions*, vol. 6, no. 4, p. 87, 2021, doi:10.3390/inventions6040087.
- [15] A. Zacepins, A. Kviesis, E. Stalidzans, M. Liepniece, J. Meitalovs, "Remote detection of the swarming of honey bee colonies by single-point temperature monitoring", *Biosystems engineering*, vol. 148, pp. 76-80, 2016, doi:10.1016/j.biosystemseng.2016.05.013.
- [16] M.-T. Ramsey, M. Bencsik, M. I. Newton, M. Reyes, M. Pioz, D. Crauser, N. S. Delso, Y. Le Conte, "The prediction of swarming in honeybee colonies using vibrational spectra", *Scientific reports*, vol. 10, no. 1, p. 9798, 2020, doi:10.1038/s41598-020-66836-2.
- [17] T. Feng, Y. Hu, J. Yang, T. Polk, Y. Zhao, S. Liu, Z. Yang, "Timepool: Visually answer "which and when" questions on univariate time series", "2023 IEEE Visualization and Visual Analytics (VIS)", pp. 201-205, 2023, doi:10.1109/VIS54172.2023.00049.
- [18] W. Aigner, S. Miksch, H. Schumann, C. Tominski, *Visualization of time-oriented data*, Springer Science & Business Media, 2011, doi:10.1007/978-0-85729-079-3.
- [19] W. Playfair, *The commercial and political atlas: representing, by means of stained copper-plate charts, the progress of the commerce, revenues, expenditure and debts of england during the whole of the eighteenth century*, T. Burton, 1801.
- [20] B. Ondov, N. Jardine, N. Elmquist, S. Franconeri, "Face to face: Evaluating visual comparison", *IEEE transactions on visualization and computer graphics*, vol. 25, no. 1, pp. 861-871, 2018, doi:10.1109/TVCG.2018.2865234.
- [21] A. Gogolou, T. Tsandilas, T. Palpanas, A. Bezerianos, "Comparing similarity perception in time series visualizations", *IEEE transactions on visualization and computer graphics*, vol. 25, no. 1, pp. 523-533, 2018, doi:10.1109/TVCG.2018.2865235.

- [22] L. Chittaro, C. Combi, G. Trapasso, "Data mining on temporal data: a visual approach and its clinical application to hemodialysis", *Journal of Visual Languages & Computing*, vol. 14, no. 6, pp. 591–620, 2003, doi:[10.1016/j.jvlc.2003.09.001](https://doi.org/10.1016/j.jvlc.2003.09.001).
- [23] W. Javed, B. McDonnel, N. Elmqvist, "Graphical perception of multiple time series", *IEEE transactions on visualization and computer graphics*, vol. 16, no. 6, pp. 927–934, 2010, doi:[10.1109/TVCG.2010.162](https://doi.org/10.1109/TVCG.2010.162).
- [24] J. Zhao, F. Chevalier, E. Pietriga, R. Balakrishnan, "Exploratory analysis of time-series with chronolenses", *IEEE Transactions on Visualization and Computer Graphics*, vol. 17, no. 12, pp. 2422–2431, 2011, doi:[10.1109/TVCG.2011.195](https://doi.org/10.1109/TVCG.2011.195).
- [25] R. Kincaid, H. Lam, "Line graph explorer: scalable display of line graphs using focus+ context", "Proceedings of the working conference on Advanced visual interfaces", pp. 404–411, ACM, 2006, doi:[10.1145/1133265.1133331](https://doi.org/10.1145/1133265.1133331).
- [26] T. Saito, H. N. Miyamura, M. Yamamoto, H. Saito, Y. Hoshiya, T. Kaseda, "Two-tone pseudo coloring: Compact visualization for one-dimensional data", "2005 IEEE Symposium on Information Visualization", pp. 173–180, IEEE, 2005, doi:[10.1109/INFVIS.2005.1532143](https://doi.org/10.1109/INFVIS.2005.1532143).
- [27] B. Lee, N. H. Riche, A. K. Karlson, S. Carpendale, "Sparkclouds: Visualizing trends in tag clouds", *IEEE transactions on visualization and computer graphics*, vol. 16, no. 6, pp. 1182–1189, 2010, doi:[10.1109/TVCG.2010.194](https://doi.org/10.1109/TVCG.2010.194).
- [28] J. Heer, N. Kong, M. Agrawala, "Sizing the horizon: the effects of chart size and layering on the graphical perception of time series visualizations", "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems", pp. 1303–1312, ACM, 2009, doi:[10.1145/1518701.1518897](https://doi.org/10.1145/1518701.1518897).
- [29] C. Perin, F. Vernier, J.-D. Fekete, "Interactive horizon graphs: improving the compact visualization of multiple time series", "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems", pp. 3217–3226, ACM, 2013, doi:[10.1145/2470654.2466441](https://doi.org/10.1145/2470654.2466441).
- [30] P. Federico, S. Hoffmann, A. Rind, W. Aigner, S. Miksch, "Qualizon graphs: Space-efficient time-series visualization with qualitative abstractions", "Proceedings of the 2014 International Working Conference on Advanced Visual Interfaces", pp. 273–280, ACM, 2014, doi:[10.1145/2598153.2598180](https://doi.org/10.1145/2598153.2598180).
- [31] R. Bade, S. Schlechtweg, S. Miksch, "Connecting time-oriented data and information to a coherent interactive visualization", "Proceedings of the SIGCHI conference on Human factors in computing systems", pp. 105–112, ACM, 2004, doi:[10.1145/985692.985707](https://doi.org/10.1145/985692.985707).
- [32] K. B. Schloss, C. C. Gramazio, A. T. Silverman, M. L. Parker, A. S. Wang, "Mapping color to meaning in colormap data visualizations", *IEEE transactions on visualization and computer graphics*, vol. 25, no. 1, pp. 810–819, 2018, doi:[10.1109/TVCG.2018.2865147](https://doi.org/10.1109/TVCG.2018.2865147).
- [33] J. Liu, A. Prouzeau, B. Ens, T. Dwyer, "Design and evaluation of interactive small multiples data visualisation in immersive spaces", "2020 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)", pp. 588–597, IEEE, 2020, doi:[10.1109/VR46266.2020.00079](https://doi.org/10.1109/VR46266.2020.00079).
- [34] M. Krstajic, E. Bertini, D. Keim, "Cloudlines: Compact display of event episodes in multiple time-series", *IEEE transactions on visualization and computer graphics*, vol. 17, no. 12, pp. 2432–2439, 2011, doi:[10.1109/TVCG.2011.179](https://doi.org/10.1109/TVCG.2011.179).
- [35] M. T. Fischer, D. Seebacher, R. Sevastjanova, D. A. Keim, M. El-Assady, "CommAID: Visual analytics for communication analysis through interactive dynamics modeling", *Computer Graphics Forum*, vol. 40, no. 3, pp. 25–36, 2021, doi:[10.1111/cgf.14256](https://doi.org/10.1111/cgf.14256).
- [36] M. L. Larrea, D. K. Urribarri, "Visualization technique for comparison of time-based large data sets", M. Naiouf, E. Rucci, F. Chichizola, L. De Giusti, eds., "Cloud Computing, Big Data & Emerging Topics", pp. 179–187, Springer International Publishing, Cham, 2021, doi:[10.1007/978-3-030-84825-5\\_16](https://doi.org/10.1007/978-3-030-84825-5_16).
- [37] M. Monroe, R. Lan, H. Lee, C. Plaisant, B. Shneiderman, "Temporal event sequence simplification", *IEEE transactions on visualization and computer graphics*, vol. 19, no. 12, pp. 2227–2236, 2013, doi:[10.1109/TVCG.2013.200](https://doi.org/10.1109/TVCG.2013.200).
- [38] D. Klimov, Y. Shahar, M. Taieb-Maimon, "Intelligent selection and retrieval of multiple time-oriented records", *Journal of Intelligent Information Systems*, vol. 35, no. 2, pp. 261–300, 2010, doi:[10.1007/s10844-008-0095-2](https://doi.org/10.1007/s10844-008-0095-2).
- [39] J. A. Fails, A. Karlson, L. Shahamat, B. Shneiderman, "A visual interface for multivariate temporal data: Finding patterns of events across multiple histories", "2006 IEEE Symposium On Visual Analytics Science And Technology", pp. 167–174, IEEE, 2006, doi:[10.1109/VAST.2006.261421](https://doi.org/10.1109/VAST.2006.261421).
- [40] B. L. Harrison, R. Owen, R. M. Baecker, "Timelines: an interactive system for the collection and visualization of temporal data", "Graphics Interface", pp. 141–141, Canadian Information Processing Society, 1994, doi:[10.20380/GI1994.18](https://doi.org/10.20380/GI1994.18).
- [41] C. J. Atman, "Design timelines: Concrete and sticky representations of design process expertise", *Design Studies*, vol. 65, pp. 125–151, 2019, doi:[10.1016/j.destud.2019.10.001](https://doi.org/10.1016/j.destud.2019.10.001).
- [42] T. Feng, J. Yang, M.-C. Eppes, Z. Yang, F. Moser, "Evis: Visually analyzing environmentally driven events", *IEEE Transactions on Visualization and Computer Graphics*, vol. 28, no. 1, pp. 912–921, 2022, doi:[10.1109/TVCG.2021.3114867](https://doi.org/10.1109/TVCG.2021.3114867).
- [43] P. Buono, A. Aris, C. Plaisant, A. Khella, B. Shneiderman, "Interactive pattern search in time series", "Visualization and Data Analysis 2005", vol. 5669, pp. 175–186, International Society for Optics and Photonics, 2005, doi:[10.1117/12.587256](https://doi.org/10.1117/12.587256).
- [44] T. Fujiwara, N. Sakamoto, J. Nonaka, K. Yamamoto, K.-L. Ma, et al., "A visual analytics framework for reviewing multivariate time-series data with dimensionality reduction", *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 2, pp. 1601–1611, 2020, doi:[10.1109/TVCG.2020.3030341](https://doi.org/10.1109/TVCG.2020.3030341).
- [45] R. Takami, Y. Takama, "Visual analytics interface for time series data based on trajectory manipulation", "2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)", pp. 342–347, 2018, doi:[10.1109/WI.2018.00-58](https://doi.org/10.1109/WI.2018.00-58).
- [46] S. Cheng, K. Mueller, W. Xu, "A framework to visualize temporal behavioral relationships in streaming multivariate data", "2016 New York Scientific Data Summit (NYSDS)", pp. 1–10, 2016, doi:[10.1109/NYSDS.2016.7747810](https://doi.org/10.1109/NYSDS.2016.7747810).
- [47] B. Bach, C. Shi, N. Heulot, T. Madhyastha, T. Grabowski, P. Dragicevic, "Time curves: Folding time to visualize patterns of temporal evolution in data", *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 1, pp. 559–568, 2016, doi:[10.1109/TVCG.2015.2467851](https://doi.org/10.1109/TVCG.2015.2467851).
- [48] S. van den Elzen, D. Holten, J. Blaas, J. J. van Wijk, "Reducing snapshots to points: A visual analytics approach to dynamic network exploration", *IEEE Transactions on Visualization and Computer Graphics*, vol. 22, no. 1, pp. 1–10, 2016, doi:[10.1109/TVCG.2015.2468078](https://doi.org/10.1109/TVCG.2015.2468078).
- [49] T. Schreck, T. Tekušová, J. Kohlhammer, D. Fellner, "Trajectory-based visual analysis of large financial time series data", *ACM SIGKDD Explorations Newsletter*, vol. 9, no. 2, pp. 30–37, 2007, doi:[10.1145/1345448.1345453](https://doi.org/10.1145/1345448.1345453).
- [50] T. Kohonen, *Self-organizing maps*, Springer Science & Business Media, 2012, doi:[10.1007/978-3-642-56927-2](https://doi.org/10.1007/978-3-642-56927-2).
- [51] K. Toohey, M. Duckham, "Trajectory similarity measures", *Sigspatial Special*, vol. 7, no. 1, pp. 43–50, 2015, doi:[10.1145/2811234.2811240](https://doi.org/10.1145/2811234.2811240).
- [52] N. Magdy, M. Sakr, T. Abdelkader, K. Elbahnasy, "Review on trajectory similarity measures", 2015, doi:[10.1109/IntelCIS.2015.7397286](https://doi.org/10.1109/IntelCIS.2015.7397286).
- [53] D. Hu, L. Chen, H. Fang, Z. Fang, T. Li, Y. Gao, "Spatio-temporal trajectory similarity measures: A comprehensive survey and quantitative study", *IEEE Transactions on Knowledge and Data Engineering*, 2023, doi:[10.1109/TKDE.2023.3241234](https://doi.org/10.1109/TKDE.2023.3241234).
- [54] C. Faloutsos, M. Ranganathan, Y. Manolopoulos, "Fast subsequence matching in time-series databases", *SIGMOD Rec.*, vol. 23, no. 2, p. 419–429, 1994, doi:[10.1145/191843.191925](https://doi.org/10.1145/191843.191925).
- [55] H. Alt, M. Godau, "Computing the fréchet distance between two polygonal curves", *International Journal of Computational Geometry & Applications*, vol. 5, no. 01n02, pp. 75–91, 1995, doi:[10.1142/S0218195995000064](https://doi.org/10.1142/S0218195995000064).

- [56] M.-P. Dubuisson, A. K. Jain, "A modified hausdorff distance for object matching", "Proceedings of 12th international conference on pattern recognition", vol. 1, pp. 566–568, IEEE, 1994, doi:[10.1109/ICPR.1994.576361](https://doi.org/10.1109/ICPR.1994.576361).
- [57] E. Keogh, C. A. Ratanamahatana, "Exact indexing of dynamic time warping", *Knowledge and information systems*, vol. 7, pp. 358–386, 2005, doi:[10.1007/s10115-004-0154-5](https://doi.org/10.1007/s10115-004-0154-5).
- [58] M. Vlachos, G. Kollios, D. Gunopulos, "Discovering similar multidimensional trajectories", "Proceedings 18th international conference on data engineering", pp. 673–684, IEEE, 2002, doi:[10.1109/ICDE.2002.994784](https://doi.org/10.1109/ICDE.2002.994784).
- [59] H. Wang, K. Liu, "User oriented trajectory similarity search", "Proceedings of the ACM SIGKDD International Workshop on Urban Computing", pp. 103–110, 2012, doi:[10.1145/2346496.2346515](https://doi.org/10.1145/2346496.2346515).
- [60] W. Zheng, R. Zhou, Z. Zhang, Y. Zhong, S. Wang, Z. Wei, H. Ji, "Understanding the tourist mobility using gps: How similar are the tourists?", *Tourism management*, vol. 71, pp. 54–66, 2019, doi:[10.1016/j.tourman.2018.09.011](https://doi.org/10.1016/j.tourman.2018.09.011).
- [61] E. Frentzos, K. Gratsias, Y. Theodoridis, "Index-based most similar trajectory search", "2007 IEEE 23rd International Conference on Data Engineering", pp. 816–825, IEEE, 2006, doi:[10.1109/ICDE.2007.367926](https://doi.org/10.1109/ICDE.2007.367926).
- [62] S. Wang, Z. Bao, J. S. Culpepper, Z. Xie, Q. Liu, X. Qin, "Torch: A search engine for trajectory data", "The 41st international ACM SIGIR conference on research & development in information retrieval", pp. 535–544, 2018, doi:[10.1145/3209978.3210047](https://doi.org/10.1145/3209978.3210047).
- [63] R. Tashakkori, A. S. Hamza, M. B. Crawford, "Beemon: An IoT-based beehive monitoring system", *Computers and Electronics in Agriculture*, vol. 190, p. 106427, 2021, doi:[10.1016/j.compag.2021.106427](https://doi.org/10.1016/j.compag.2021.106427).

**Copyright:** This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).



**Tinghao Feng** has completed his PhD in Computer Science from UNC Charlotte. He is an Assistant Professor in the Computer Science Department at Appalachian State University.

Tinghao's research primarily focuses on analyzing time-oriented data and developing visualization and analysis systems. He aims to create applications to explore temporal patterns and trends, drawing from his research experience in environmental science, healthcare, and finance. He has published numerous papers in reputable journals and conferences and has been recognized with several awards for his contributions.



**Sophie Columbia** completed her bachelor's degree from Appalachian State University in 2023. She completed her master's degree from Appalachian State University in 2024. Sophie worked as a Graduate Research Assistant on the AppMAIS project while she was a graduate student at Appalachian State University.



**Christopher Campell** has done his master's degree from Appalachian State University in 2020. He is currently a Research Associate in Machine Learning in the Computer Science Department at Appalachian State University.

Christopher Campbell leads the AppMAIS research group at Appalachian State University, focusing on innovative applications of machine learning and IoT technologies. His work includes developing advanced audio data labeling tools, estimating bee traffic using YOLO and optical flow, and creating comprehensive visualization systems for honey bee data. Chris's research also explores the health of honey beehives through cast ratio analysis at hive entrances, detecting honey bee piping with convolutional neural networks, and implementing IoT platforms for real-time beehive monitoring and alerting. Additionally, he has worked on non-invasive swarm detection methods, simple data visualization applications, and fleet management systems for apiaries using Jenkins. Through these diverse projects, Chris aims to enhance the understanding and management of honey bee populations and their environments.



**Rahman Tashakkori** received his bachelor's degree from Ahwaz University, Iran, in 1987. He completed two master's and PhD degrees at Louisiana State University, Baton Rouge, USA, in 1994, 1995, and 2001, respectively.

Rahman's main areas of research are in image processing, data science, honey bee monitoring systems, and computer science education. He has directed several NSF scholarship programs, including CSEMS, STEM, S-STEM, and LSAMP. He is a Senior Member of IEEE.