EAI Endorsed Transactions
on AI and Robotics

Review Article

The Role of Biometric in Banking: A Review

Mehdi Marani[1,*], Morteza Soltani[2], Mina Bahadori[3], Masoumeh Soleimani[4], Mehdi Davari[5], Atajahangir Moshayedi[6]

[1]Department of Mechanical Engineering, Khomeinishahr Branch, Islamic Azad University, Isfahan, Iran
[2]Department of Industrial Engineering, Clemson University, SC, USA
[3]Department of Industrial Engineering, Clemson University, SC, USA
[4]Department of Mathematics and Statistical Sciences, Clemson University, SC, USA
[5]Department of Management, Isfahan Branch, Islamic Azad University, Isfahan, Iran
[6]School of Information Engineering, Jiangxi University of Science and Technology, No 86, Hong qi Ave, Ganzhou, Jiangxi, 341000, China

Abstract

Biometrics plays a pivotal role in enhancing security, ensuring accurate identification, and offering convenient solutions across diverse industries. Its uniqueness, reliability, and potential for future advancements establish it as a crucial and valuable field in today's digital landscape. Fingerprint authentication in ATMs presents primary advantages such as heightened security through distinctive identification and user convenience by eliminating the reliance on PINs or passwords. This research paper focuses on conducting a comprehensive review and comparative analysis of various approaches for fingerprint identification, aiming to contribute to the understanding of effective and efficient methods in the context of ATM authentication.

Received on 03 August 2023; accepted on 18 August 2023; published on 21 August 2023

Keywords: Fingerprint Sensor, Microcontroller, Identification Methods, Hardware

doi:10.4108/airo.3676

1. Introduction

Biometrics refers to the measurement and analysis of distinct physical or behavioral attributes unique to individuals, a concept that has gained prominence across various sectors. Notably, the integration of biometrics in the banking industry has emerged as a pivotal area of exploration. Biometric identification presents an innovative approach compared to traditional methods like passwords or identification cards, as biometric traits are immune to issues such as theft, replication, purchase, or forgery. This heightened level of dependability has spurred considerable interest in adopting biometric solutions within the banking domain, reflecting a notable step forward in bolstering security and reliability.

Numerous research studies have been undertaken to delve into the potential applications of biometrics within the banking domain, and this paper offers a compilation of selected investigations. A specific area of focus involves the exploration of fingerprint-based Automated Teller Machines (ATMs), an arena riddled with an array of intricate challenges. These challenges span a wide spectrum, encompassing factors like financial feasibility, concerns regarding device portability, the establishment of robust security measures, the acceptance of the technology among users, the efficiency of enrollment procedures, the resilience of the system, as well as issues related to privacy and defect rates.

However, the primary objective of this manuscript is to meticulously tackle the initial three challenges: namely, cost, portability, and security. The research endeavors outlined in this paper are meticulously designed to provide an all-encompassing evaluation and comparative analysis of various methodologies implemented in this sphere. The ultimate aim is to not only enhance the cost-efficiency, mobility, and

*Corresponding author. Email: msoleim@g.clemson.edu

security aspects of fingerprint-based ATMs but also to contribute significantly to elevating user experience and the overall operational effectiveness of the banking landscape.

By thoroughly examining the existing literature and synthesizing the information, the study identifies key research gaps and areas that warrant further examination. This research seeks to explore advancements and challenges in biometric authentication methods, specifically within the context of fingerprint identification devices employed in ATMs. The primary aim is to enhance the existing pool of knowledge and offer valuable input for the progress of the field in the future.

1.1. Research Contribution

1. Reviewing different approaches to fingerprint identification.
2. comparing the results of these methods to provide valuable insights for future researchers and contribute to the advancement of biometric authentication systems in ATM technology.

2. Review

T. Sabhanayagam et al. (2018) Offer a comprehensive overview of diverse biometric systems and their functional applications. Furthermore, the study concludes that while biometric recognition systems effectively address the limitations of traditional methods, it is important to consider potential challenges arising from the continuous evolution of biometric technology [1]. Khan et al. (2020) Involved in a separate endeavor that aimed to comprehend health data derived from wearable IoT technology. The team conducted an extensive review, discussion, and offered recommendations on utilizing this data as a biometric for computer security purposes. Several limitations were identified, including the ever-changing characteristics of the human body, sensor aging and deterioration, difficulties in selecting an appropriate population for biometric system assessment, sensor cost, effects on accuracy, lack of standardized techniques, and the inadequate security measures prevalent in biometric systems [2]. M. Gayathri et al. (2020) Conduct a comprehensive survey on the current state of biometric technology, covering various aspects such as different types of biometric traits, the techniques employed for extracting these traits' features, and the diverse application areas where various biometric traits find utility. The authors emphasize the paramount importance of safeguarding biometric data due to its sensitive nature. Despite biometric technology significantly reducing the problems associated with traditional forms of theft, it is acknowledged that certain vulnerabilities still exist. Hackers have demonstrated the ability to breach biometric data, underscoring the critical need for robust biometric template protection measures[3]. To illustrate the current trends in biometrics, the authors cite specific examples. These include the utilization of ECG biometrics control in cars for monitoring the health of drivers and passengers, as well as the adoption of palm recognition in smart panda buses Alsaadi (2021) summarized the existing behavioral biometrics systems and offers an exploration of the key advantages and disadvantages associated with popular behavioral biometrics technologies [4]. In a review paper by Yang et al. (2021), The researchers delve into a diverse array of strategies aimed at mitigating vulnerabilities in various layers of the Internet of Things (IoT) architecture. The authors underscore that every biometric trait, whether employed individually or in combination, exhibits unique strengths as well as notable limitations [5].

Biometric traits, such as fingerprints, iris patterns, and facial features, are distinctive to each individual. Among these biometric features, fingerprints have held the top position as the benchmark for individual identification for many years. In the 1990s, fingerprint scanning using optical, ultrasonic, and infrared imaging techniques was introduced, and measurements of pressure, temperature, and electric capacitance were used to detect patterns on the surface of the finger and convert them into electrical signals. The efficiency of a fingerprint recognition system is contingent on the accuracy of the algorithms used for feature extraction. Today, there are multiple approaches with acceptable results in fingerprint feature extraction. The problem arises when traditional methods fail to analyze fingerprint textures under low-quality conditions. Thus, various methods, including neural networks, traditional methods, and hybrid approaches, have been employed to extract features and match them with samples in the database [6].

Optimization algorithms play a significant role in enhancing the performance and effectiveness of biometric systems. Here, we introduce some papers that focus on optimization algorithms: Ansaripour et al. applied neural networks and optimization techniques to mitigate welding challenges and this approach can be analogous to improving biometric system performance and security [7]. Daniali et al. optimize a shell and tube heat exchanger for thermal efficiency and total cost using Copper oxide/Iranol refinery oil nanofluids. Employing natural base inspired algorithms, it generates a Pareto frontier curve, demonstrating the trade-off between efficiency and cost considerations [8]. Babajamali et al. explore multi-objective optimization of tandem cold rolling parameters using NSGA-II and Pareto-optimal front, aiming to enhance reductions and inter-stand tensions. The obtained optimized rolling schedules demonstrate improved performance, echoing biometric systems' pursuit of better accuracy and efficiency [9]. Barnoon et al. analyze proton exchange membrane fuel

cell (PEMFC) cooling, stress, and displacement under various conditions, utilizing multi-objective optimization to determine optimal plate thickness and number for temperature, stress, and displacement reduction. Similar to optimizing biometric systems, the research aims to enhance performance and longevity while considering factors like temperature control and stress management [10]. Khan et al. introduce a gait recognition framework employing deep learning and Bayesian optimization, analogous to biometric identification. The framework combines motion region extraction, hyperparameter optimization, and feature fusion, achieving high accuracy on public datasets similar to biometric systems' accuracy goals [11]. M Soltani presents a model for optimizing spare parts supply chains and condition-based maintenance, akin to the integration of components in biometric systems. This paper introduces innovative policies for spare part ordering based on system deterioration and optimizes decision variables for improved availability and cost efficiency, mirroring concerns in both logistics and biometric fields [12]. Soleimani et al. apply imbalanced data in medical classification, resembling the challenge of recognizing underrepresented traits in biometric systems. they propose a feature selection method using a support vector machine and wrapper approach, optimizing accuracy to %99.6 through neural network optimization, mirroring biometric systems' quest for accuracy in diverse trait recognition [13].

In their research, Sun et al. address presentation attack detection (PAD) in fingerprint recognition systems, reflecting the challenge of distinguishing genuine users from fraudulent attempts in biometric systems. They introduce a novel method utilizing optical coherence tomography (OCT) features, achieving accurate attack detection with a %4 Equal Error Rate (EER), mirroring biometric systems' emphasis on precise identification [14].

Nowadays, considering the increasing need for security, this technology is being utilized in various applications such as attendance management, secure locks, ATMs, card reader devices, control and surveillance of agricultural machinery, vehicles, banking security system, and so on. Furthermore, to achieve each of the above objectives, it is necessary to utilize suitable hardware along with user-friendly programming specifically designed for it. This ensures complete monitoring and control of user equipment while maintaining security and minimizing the required time. It is worth mentioning that the hardware used in these systems should possess certain feathers such as simplicity, compactness, affordability, portability, ease of use, and, ideally be adaptable for various applications. To provide further illustration, Kumar et al. have developed a biometric-based security lock system utilizing fingerprint recognition, showcasing one of the practical applications of fingerprint technology [15]. This design incorporates a two-step identity verification process, consisting of credential authentication and fingerprint verification. Additionally, it has the capability to capture images of unauthorized users. The fingerprint is utilized as an identity verification system in this design. The operational steps of this design are, to enter your password using the keypad, and place your fingerprint on the fingerprint scanner. If the fingerprint is unauthorized, the image will be captured by the camera module and stored in the computer system, If the password and fingerprint belong to an authorized person, the entry door connected to the DC motor will be opened, now you can access your shelf. In this project, two microcontrollers, Atmega 16 and Pic16F877A, are employed. Both microcontrollers communicate with each other through various ports. Atmega 16 is connected to peripheral devices such as an LCD, keypad, and fingerprint module. Pic16F877A is connected to the DC motor, buzzer, and computer system. The fingerprint sensor used in this project is an optical type, and it scans the fingerprint using light-sensitive diodes, storing the signals as bright and dark pixels. An analog-to-digital converter is present in the scanner to convert the analog signals into digital form. This research indicates that designing a flawless security shelf can be an effective solution for addressing the significant problem of theft in today's world. KM and et al. have designed a security system based on fingerprint and RFID sensors. This system adopts a two-factor authentication method, leading to improved safety and effectiveness within the system. In this design, the RFID reader first reads a ten-digit code from the corresponding tag. These tags or labels contain microprocessors that store the ID or identifier of each object. It should be noted that when radio waves reach the RFID antenna, they create a magnetic field. The tags draw power from this magnetic field and become capable of transmitting information. The fingerprint sensor, on the other hand, compares the input image with the registered data and sends a verification signal to the computer. If both the RFID and fingerprint verification match, the microcontroller commands the motor associated with the doors, and they open by the motor's rotation. The hardware components used in this design include a pic microcontroller, fingerprint sensor, computer, RFID tags, electronic relay, and DC motor. The standard employed in the tags is based on the magnetic fields generated at close and far distances. LF (Low Frequency) and HF (High Frequency) frequencies are used for close distances, while UHF (Ultra-High Frequency) or microwave frequencies are used for far distances [16]. Figure 1 illustrates the tags and magnetic fields at far and close distances, respectively.

The researchers' findings point out that by developing and implementing a suitable and efficient security system in banks, it can foster a sense of trust among

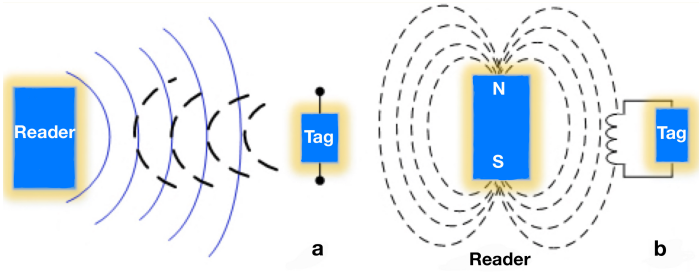

Figure 1. The magnetic fields created at close and distant distances

users, encouraging them to entrust their assets to the banking institutions. Gill KR, et al. [17] have designed a system for starting a car using a fingerprint. The first companies to adopt this system for vehicles were Mercedes-Benz and Volkswagen. In this design, the process begins with sampling the owner's fingerprint. The main identity verification core of the car's switch is a microcontroller. The fingerprint sensor captures the user's fingerprint and sends a signal to the microcontroller. The microcontroller performs a comparison between the scanned fingerprint and the one stored in its database. Once a successful match is detected, the car is activated and powered on. In this setup, a GSM module can also be used to fulfill an important role. Whenever an unauthorized user attempts to scan their fingerprint, a message is sent to all authorized users. Since the required power supply is 5 volts, while the car battery is 12 volts, an IC 7805 is used to obtain a 5-volt voltage. The hardware components used in this design include: The implemented setup includes the AT89S52 microcontroller, power supply, fingerprint sensor (R305), display, car ignition system, and GSM modem (SIM900A). The R305 fingerprint sensor is chosen for its low power consumption, affordability, superior performance compared to similar sensors, and easy implementation. Similarly, the SIM900A GSM module is a cost-effective and user-friendly module with messaging capabilities and, when equipped with a SIM card and internet connection, can also send emails. The design proposes the possibility of incorporating iris scanning or heartbeat detection as alternative identification methods in case of incomplete fingerprints or finger-related issues in the future. The researchers' findings indicate that the car ignition system using a fingerprint sensor leads to savings in traditional keys for starting the vehicle and can also be used when the user forgets to bring the car key, as the car can be turned on by authenticating the user's fingerprint using the sensor. Madhu R and others [18] have designed a method for remote communication with a device using fingerprint identification along with GSM and GPS capabilities. The software implementation process is as follows: initially, the user needs to place their finger on the fingerprint module. Then, the microcontroller compares the fingerprint image with its database and, if valid, sends a message to the device owner requesting access. If the device owner sends an access grant message, The end-user possesses the capability to control all the devices simultaneously. Table 1 presents a comprehensive comparison between the proposed design and other existing designs. The hardware components employed in this system comprise a GSM module, GPS module, and Arduino board [19], fingerprint sensor, display, and electronic relay with a junction box. The research indicates that this design enables multiple individuals to have access and control over the device's operation without necessarily being physically close to the device. The increased safety and flexibility for various applications, including agricultural machinery control, vehicle control, and theft detection of vehicles, are among the results of this design. In their 2016 paper, Singh et al. detailed the procedures of fingerprint verification and explored strategies to enhance the performance of the fingerprint biometric system, thus facilitating smooth access to the system. It resulted in higher security, and saves time, and solves several issues related to the input system [20]. In a 2018 study conducted by Manzoor, an in-depth analysis of various fingerprint biometric systems was presented, along with a detailed explanation of a fingerprint-based biometric system. The research demonstrated a trade-off between the security of biometric information and the overall system performance. Manzoor emphasized that achieving a secured biometric system with both lower equal error rates and higher identification accuracy continues to pose a significant challenge for researchers[21]. Sagayam et al. (2019) identify and classify fingerprint recognition by using the Euclidean distance and neural network classifier (NNC). This method improves the performance in some aspects like: time and accuracy. By Euclidean distance and NNC one can analyze the test image and the input image accuracy, but when the image is enrolled in different angles, the matching between the input image and the test image is not straightforward [22]. In their 2020 study, Ishak et al. designed software specifically catering to high-ranking officers in a security company, offering a range of ready-to-use formats. To ensure data security, all information is securely stored in a database. The system includes a unique fingerprint authentication feature for user access. Integrating the Secure Biometric Lock System for files and applications brings about several advantages, such as saving time and resources, minimizing paperwork, preventing errors, facilitating effective communication with senior staff or employees, ensuring proper etiquette, and providing other valuable benefits [23]. In their 2021 research, Marco Ferretti et

al. present a distributed solution for behavioral IoT fingerprinting. They recognize the scalability challenges posed by updating fingerprint models for device configuration variations in centralized solutions. To address this, they strategically target specific nodes, including gateways, as part of their distributed approach. Within the IoT ecosystem, a novel framework called H2O (Human to Object) has been proposed, designed to enable object monitoring through trained classification models, ensuring a scalable solution. Dedicated controller nodes integrated into the Internet Service Provider (ISP) efficiently conduct the training process. H2O introduces a mechanism to authenticate the identity of objects or humans based on their claims. The study includes a security analysis of the framework, which encompasses an attack model, demonstrating that the proposed solution effectively achieves its objectives even when faced with potential attacks [26]. In their latest research, Yin et al. (2021) introduce an IoT-oriented privacy-preserving fingerprint authentication system. This system incorporates four essential components: minutiae extraction, a cancelable binary template based on the minutia cylinder-code (MCC) generated using a novel normalized random projection technique, a lightweight, privacy-preserving template constructed through pairwise Boolean operations, and fingerprint matching. Notably, this groundbreaking system represents the first privacy-preserving, cancelable fingerprint authentication solution specifically designed to meet the demands of resource-constrained IoT environments [27]. In their 2022 study, Nonthaputha et al. explore an innovative IoT-based solution for a smart biometric fingerprint circular key storage cabinet. This advanced system empowers students to conveniently borrow and return machinery keys via a user-friendly touch screen and biometric fingerprint scan. All key transactions are efficiently recorded in the database, ensuring seamless tracking and management. The researchers have developed a user-centric software interface, ensuring students can effortlessly access the keys they need at any time, making the borrowing and returning process convenient and straightforward [28]. In their 2023 study, Siregar et al. endeavor to design a fingerprint sensor implementation system for a fingerprint reader prototype, incorporating a microcontroller. The central goal of this system is to achieve rapid and accurate attendance recording while ensuring its robustness against tampering and manipulation [29]. Lastra, et al. [30] conducted extensive research on efficient fingerprint identification using graphics processors (GPUs). Fingerprint recognition is widely utilized in various biometric identification systems. However, the fingerprint-matching process poses considerable computational challenges, requiring streamlined processing methods. With potentially large fingerprint databases, the scalability of models relies on the number of fingerprints and points in each fingerprint. To cater to the need for accelerated processing, the researchers put forth a unique fingerprint matching algorithm centered around minutiae, specially optimized for GPU-based massively parallel processing. The study's results highlight the minutiae-based fingerprint matching algorithm as one of the leading methods among biometric identification approaches. Hambalık et al. [31] conducted a research study focused on fingerprint recognition systems using Artificial Neural Networks (ANNs). Their investigation explored the potential integration of ANNs as feature extractors within the fingerprint recognition process. As a result of their investigation, the researchers created a complete and operational software system designed to perform fingerprint recognition, consisting of modules for high-resolution fingerprint sensors, image enhancement, feature extraction, and fingerprint matching. The study's results demonstrated the significant impact of neural networks on the overall detection rate, particularly in scenarios involving low-quality fingerprint images.

In recent times, certain banks have initiated trials of biometric ATM systems in specific regions or limited pilot programs. These initiatives require customers to enroll their biometric data (e.g., fingerprints) with the bank and utilize biometric authentication at designated ATMs. Biometric data is securely stored and utilized for subsequent ATM transactions, eliminating the need for physical cards or PINs. However, it's essential to acknowledge that the adoption and implementation of biometric ATMs may vary based on the country, financial institution, and regulatory requirements. While biometric authentication offers advantages in terms of security and convenience, it also brings challenges such as privacy concerns, technological integration, and cost implications [32].

In the realm of ATM security enhancements, various works have been explored, and some will be reviewed here. R. Murugesh (2012) introduced an innovative approach to bolster ATM security by replacing traditional ATM cards with fingerprints. Utilizing the AES 256 algorithm for PIN and OTP encryption, the study found that transitioning to a biometric system could streamline transactions, ensuring ease, reliability, and a stress-free experience without the need for physical cards. The robust AES 256 encryption provided solid security features, and the inclusion of a steganography mechanism further fortified the system against middleman attacks. With cost-effective biometric scanners readily available, this system promises users a seamless and secure experience, striking a perfect balance between convenience and safeguarding data integrity [33]. In their 2017 study, Taralekar et al. introduced an innovative "One touch multi-banking transaction system using biometric and GSM authentication" for ATM terminal customer

recognition. The proposed system effectively addresses the shortcomings of the traditional approach by introducing upgraded security features for seamless and secure transactions [34].

In their 2018 research, B. Saranraj et al. proposed a highly secure authentication system for ATMs. This system ensures that only the valid cardholder can access the ATM, and entering the ATM center requires both the account holder's ATM card and their knowledge. In case an unauthorized person tries to use the ATM card, the system sends an OTP to the account holder, and only upon entering this OTP into the ATM machine, the user is allowed to proceed with cash withdrawal. This advanced approach offers excellent efficiency while effectively preventing any illicit transactions [35]. In their 2019 study, Alzamel et al. proposed an innovative integrated fingerprint biometric authentication system designed specifically for securing the Point of Sale (POS) network. This new security option complements the use of ATM cards. The research findings revealed that this service offers customers a secure alternative for conducting daily transactions, reducing the reliance solely on the ATM card. The questionnaire results indicated a high demand among customers for a safer substitute for the card, indicating strong backing for the proposal, as it has the potential to mitigate issues associated with traditional ATM cards [36]. In 2019, Bataev published a paper aimed at evaluating the economic efficiency of specific devices. The study employed the Total Cost of Ownership (TCO) method, incorporating expert estimates of stolen funds in the Russian Federation to conduct the calculations. The findings demonstrated significant economic efficiency of these ATMs; however, they also highlighted the considerable expenses involved in implementing such ATMs within the banking systems of individual banks [37]. In 2022, T. Sangeetha et al. conducted research with a specific focus on incorporating a fingerprint-based method into the ATM system to bolster its security. The primary objective was to develop a more resilient security system using fingerprint-based ATMs. Their proposed system involved converting fingerprints into unique string values, which were then securely stored in a vast cloud memory within the EC2 database. During a transaction, the user's fingerprint was matched with the unique string in the cloud to facilitate authentication [38].

The ATM system based on fingerprint authentication was split into two stages: enrollment and authentication. In the enrollment phase, users were required to register up to 3-4 fingers to establish a protection threshold and accommodate various finger-related issues, such as wet, dry, skewed, dirty, cut, or worn fingers. The enrollment process ensured the system's flexibility and adaptability to real-life scenarios [39].

In the authentication phase, users could effortlessly conduct transactions by placing their finger on the biometric scanner. The fingerprint scan was then compared against the database containing all authenticated user fingerprints, ensuring a swift and secure transaction process. This novel approach aimed to strengthen the ATM system's security and provide users with a seamless experience through biometric authentication [40]. In their 2021 research, Hochwarter et al. conducted a study to examine the general attitudes and acceptance of biometrics within the Austrian public. The data was obtained through an online survey, revealing that while a notable minority showed resistance to the concept of ATMs with biometrics, a larger segment expressed a positive inclination towards such a system. However, the study did not indicate a strong preference for any specific biometric approach for ATMs among the Austrian populace [41].

Moshayedi et al, (2023) [42] proposed a novel system design called PFIB (Fingerprint-based ATM). They found The classification accuracy rate (CAR) is calculated to be 95%. This indicates that the fingerprint recognition system achieves a high level of accuracy, correctly classifying 95% of the samples. The true positive rate (TPR) is computed as 93.3%. By this method, ATMs can overcome challenges related to maintenance, cost, security, and efficiency, improving overall performance, and reducing operational expenses. Additionally, The design allows simultaneous or independent use of the card reader, potential cost savings by replacing existing card readers, a significant reduction in out-of-service ATMs, portability and compact size, versatility for various purposes, low manufacturing cost, high transmission speed, and enhanced security measures.

Upon reviewing these papers, it becomes evident that the majority of fingerprint recognition devices share several common components, as highlighted in Section 2.

3. The structure of a fingerprint recognition device

A cutting-edge fingerprint recognition device harmonizes hardware and software for meticulous identification. Its components, showcased in Figure 2, include fingerprint sensors capturing intricate details, while communication protocols ensure seamless data transmission. Processors analyze data, unveiling patterns, and the identification module employs algorithms for precise matches, echoed by the display module's outcomes. This symphony of elements defines the fingerprint recognition landscape's sophistication.In this harmonious integration, the device not only exemplifies technical finesse but also sets a benchmark for reliable and secure identity verification.

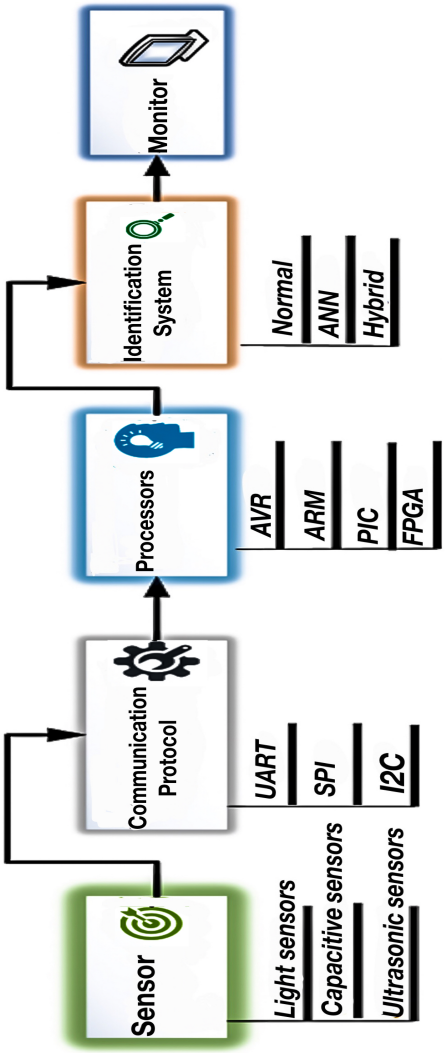

Figure 2. The design of a fingerprint recognition device

3.1. Sensor

Fingerprint registration devices are divided into two models based on the method of fingerprint acquisition: live scan and offline scan. In offline models, the process involves inking the fingers and pressing them onto paper to obtain fingerprints. Afterward, the paper is either captured or scanned to acquire the fingerprint images.

On the other hand, live scan methods work by digitally capturing the fingerprint when it touches the sensors. The primary use of offline methods is for identifying the fingerprints of criminals at the crime scene. Digital scanners are categorized based on resolution, pixel count, sensor area, accuracy, and other factors. Live scan digital scanners are divided into five categories: optical, capacitive, thermal, pressure-based, and ultrasonic.

There is a widespread application of fingerprint recognition sensors, they are used for identity confirmation in self-service kiosks [43], organizations, government agencies, universities, and educational institutions for attendance tracking [44], security systems for doors, vehicles, warehouses, and so on. In the following, we review some of these applications, and then we introduce some common types of sensors.

The most common types of fingerprint sensors used include optical, capacitive, and ultrasonic sensors we present a brief explanation about them here.

(i) Optical Sensors: This method is based on capturing an image and detecting specific patterns within it. This technology uses a series of default algorithms to examine the dark and light points present in the image, identifying the ridges and valleys on the skin. Optical sensors consist of a multitude of diodes, with some of them responsible for providing the necessary light for capturing the fingerprint. The advantages of these sensors include their simple manufacturing technology. However, they occupy a significant amount of memory, can only record two-dimensional images, and have lower security and higher production costs.

(ii) Capacitive Sensors: This technology is founded on an electronic circuit and an interconnected network of capacitors, forming the basis of its functionality. Instead of capturing an image, capacitive sensors use an array of capacitive circuits to record information related to the users' fingerprints. Since capacitors can store electric charges, their connection to conductive plates on the sensor surface allows for precise information retrieval regarding the ridges' placement and the number of stored charges within the capacitors. These sensors have higher security, and it is not possible to misuse the information from another fake image. However, due to different materials causing variations in the charge levels of the capacitors, the likelihood of compromising the system's security with other materials is almost negligible. Nonetheless, they are susceptible to software and hardware hacking.

(iii) Ultrasonic Sensors: This type of sensor utilizes a transmitter and receiver of ultrasonic waves to capture fingerprint information. When the finger is placed on the sensor, a high-frequency sound pulse is directed toward it. The skin absorbs certain segments of this pulse, while it reflects the remaining components. Based on the variations in the reflected waves due to the protrusions and depressions on the skin surface, the receiver of the sensor can obtain precise information about the

users' fingerprints by examining the intensity of the pulse at different points. These sensors have the capability to record three-dimensional images and provide high-level security. However, they have a more complex manufacturing technology compared to the previous two models.

Table 1 provides a comparison of these three sensor types.

Table 1. Comparison of Fingerprint Sensor Types

Sensor Type	Advantages	Disadvantages
(i)	Simple manufacturing technology	-excessive memory -Low cost production -Just two dimensional images -Higher error rates -Low security
(ii)	Higher security	-Susceptible to software and hardware hacking
(iii)	recording three dimensional -Higher security	-More complex manufacturing technology images

3.2. Communication Protocol

To connect and establish communication between the processor and the sensor, different protocols are used. The most common ones are I2C, SPI, and UART, which are all part of the serial communication set. Now, we introduce them as follows and then these protocols are compared to each other in Table 2.

The I2C protocol is a combination of the finest attributes of SPI and UART. With I2C, it is possible to connect multiple slaves to one master (like SPI) or use multiple masters to control one or more slaves. This feature becomes especially valuable when utilizing multiple microcontrollers to transmit data to a memory card or display it on an LCD. Components such as old displays, barometric pressure sensors, gyroscopes, and accelerometers use this protocol.

SPI (Serial Peripheral Interface) is a widely used communication protocol found in various modules, including SD card units, RFID card reader units, and 2.4 GHz wireless transceiver modules. Its primary function is to enable seamless data transfer, allowing continuous transmission or reception of any number of bits. Communication occurs in a master-slave relationship, with the master component (usually a microcontroller) sending commands to the slave component (such as a sensor, display, or Memory circuit). While the simplest SPI setup involves one master and one slave, it is also possible for one master to control multiple slaves.

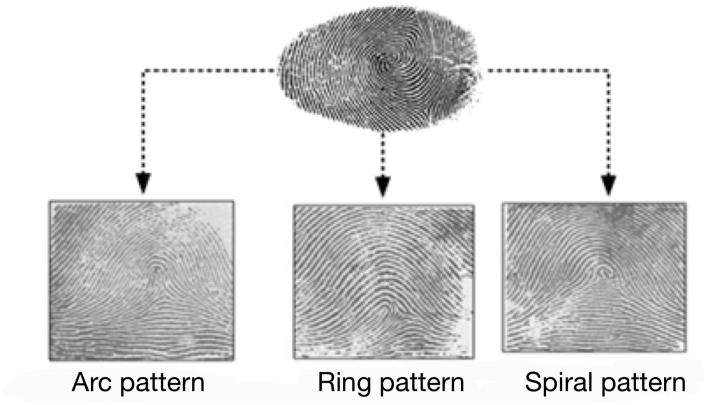

Figure 3. Fingerprint patterns

In contrast, UART communication involves a direct connection between two devices. The transmitting device receives parallel data from a control unit, such as a CPU, and converts it into a serial format before sending it to the receiving device. The receiving device subsequently converts the serial data back to parallel format, and the data is transmitted from the transmitting device's TX pin to the receiving device's RX pin.

For an extensive analysis and comparison of Communication Protocols, please refer to the accompanying Table 2.

3.3. Identification methods

In this section we explain the underlying principles and mechanisms of fingerprint recognition, firstly, then we review some of the methods used for fingerprint authorization and at the end we will compare various methods used in fingerprint recognition. a dynamic pattern of ridges and valleys characterizes the skin on the palm and sole of the foot. The whole extent of the palm and fingers is covered with continuous, thin lines, known as friction ridges. These friction ridges play a crucial role in increasing friction with objects, providing a stronger grip, and enhancing the sense of touch when in contact with various surfaces. In addition to these functions, the identity of individuals can be determined through these friction ridges. This is because these ridges are unique and unchangeable for everyone's fingers. Locations, where the friction ridges are suddenly interrupted or divided into two or more branches, are called minutiae. In general, the main fingerprint patterns are divided into three categories: arches, rings, and spirals, as shown in Figure 3, [45]. By analyzing these patterns, characteristics such as minutiae can be extracted.

By using local minutiae structures, one can quickly find relative matches between two fingerprint samples,

Table 2. Comparison of Communication Protocols

Communication Protocol	*Advantages*	*Disadvantages*
UART	•Use of only two wires •No need for a separate clock signal •Existence of parity bit for error checking •Data packet structure can be adjusted depending on the preferences set at both terminations •Availability of extensive documentation and widespread implementation methods	•The size of transmitted data is limited to a maximum of 9 bits •Absence of support for multiple masters (controllers) and multiple slaves (controlled devices) in the system •The baud rates of both sides can have a maximum variance of 10% from each other
SPI	•There are no start or stop bits, facilitating the continuous transfer of data •There is no sophisticated addressing mechanism for controlled devices, similar to the one present in I2C •Faster data transmission rate in comparison to I2C (approximately double the speed) •With separate lines for MISO and MOSI, simultaneous data reception and transmission are possible	•The use of four wires (compared to I2C and UART, which use two wires) •Absence of explicit indication for confirming the correct reception of data (unlike I2C, which possesses this capability) •Lack of error detection mechanism such as parity in UART •The presence of only one master is the only option provided
I2C	•Use of two wires •Support for multiple masters and multiple slaves •Capability to confirm or decline data transfer using ACK/NACK bits •Less complex hardware configuration in comparison to the UART approach •Familiar and extensively utilized protocol.	•Reduced data transfer speed in comparison to the SPI technique •Data length is restricted to a maximum of 8 bits •Hardware implementation may pose more complexities when compared to the SPI method

ensuring a complete match between them. Representing the minutiae as nodes and connecting them with edges, based on their proximity or spatial relationships allows the construction of a graph for each fingerprint sample. Various graph-based algorithms and techniques from graph theory can then be utilized to measure the similarity or dissimilarity between the two graphs, indicating the degree of match between the fingerprint samples [46], [47]. The general stages of a fingerprint are shown in Figure 4.

During the fingerprint registration process, a sensor scans the user's fingerprint and converts it into a digital image. Subsequently, the minutiae extractor analyzes the fingerprint image to identify distinct details known as minutiae points. In the user verification stage, the same sensor is touched again, and a new fingerprint image is created. This new image is called the query Print. The system extracts and compares the minutiae points from this image with the minutiae points stored in the database to find the number of common minutiae points. Due to differences in pressure, the query image and the database image need to be registered before comparison. Registration refers to aligning the two images to match the corresponding minutiae pairs. Then, the matching unit calculates the number of matching pairs between the two samples. Matching pairs refer to the minutiae points that have the same location and direction.

Upon completing the previous stage, the system determines the user's identity by calculating the matching score and comparing it to a predefined threshold value. This process allows for the determination of whether the user's fingerprint sufficiently matches the reference template for successful authentication. In this method, the direction of the ridges and their frequency are first determined, which improves the quality of the image and facilitates ridge extraction. After image enhancement, the main skeleton of the friction ridges is extracted, and finally an algorithm is used to identify and eliminate false minutiae using heuristics. Then, the matching phase begins. In the matching stage, as explained earlier, a score is calculated for the comparison of two fingerprints. One of the most challenging parts of fingerprint authentication is this matching stage because there are intra-class differences that indicate variations between different images of the same fingerprint, and there are inter-class similarities within the fingerprint. For example, factors such as finger pressure, finger placement, and rotation affect intra-class differences. Also, the existence of only

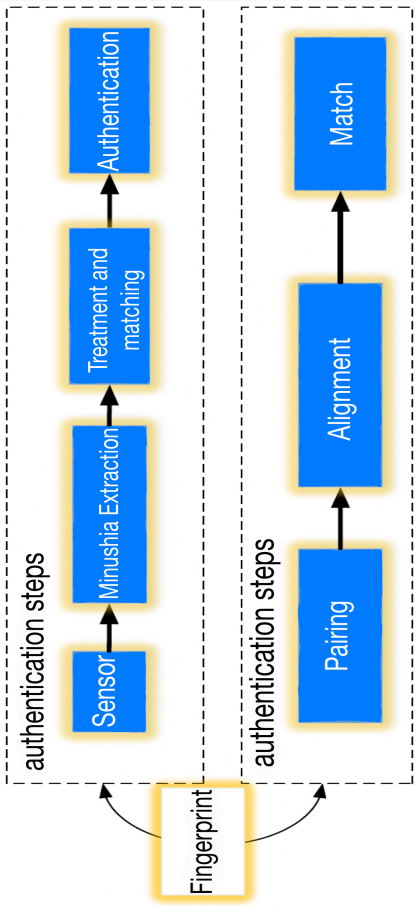

Figure 4. Stages of Identity Verification through Fingerprint

three general fingerprint pattern types (ring, spiral, and arch) creates similarities between different groups. In the following, we will examine the research presented in the field of identification methods, and at the end, we will compare them.

Yang, et al. [48] have conducted research on fingerprint matching based on maximum training. To match the fingerprint, this system uses ELM (Extreme Learning Machine) and R-ELM (Regularized Extreme Learning Machine). This approach is designed to address the shortcomings of conventional learning methods. The method involves several key steps, including efficient preprocessing, extraction of moment features, and principal component analysis for feature selection. The research findings demonstrate that this proposed method achieves superior matching accuracy, requiring less time compared to traditional approaches. The ELM and R-ELM methods introduced in this study prove to be more effective than the conventional methods.

Labati, et al. [49] have presented research on the extraction of minutiae in heterogeneous fingerprint images using artificial neural networks. In this method, sweat pores are utilized for quality assessment, and a technique for extracting minutiae coordinates from touch, touchless, and unstable fingerprint images is proposed. Specifically, neural networks are designed and trained to generalize the centrality of each minutia. The results of this study demonstrate that this approach achieves higher accuracy and better performance compared to other methods (such as extraction methods based on minutiae without neural network-based information classification).

FengJ et al. [50] have presented research on highly complex neural networks for enhancing latent fingerprints. This method utilizes two components, namely the ridge and non-ridge (smooth) regions. The ridge region is used for enhancing fingerprint feature extraction, while the non-ridge region is employed for orientation estimation and noise removal. The neural network is trained using a multitask and pixel-to-pixel approach. The results of this study demonstrate that this method achieves desirable outcomes for incompatible and latent fingerprints.

Khodadoust, et al. [51] have delved into a research endeavor centered around fingerprint representation, employing an innovative approach termed triangular expansion. In this pursuit, the method zeroes in on the utilization of triangular expansion for fingerprint representation, imparting a distinct and effective dimension to the study. By proposing an algorithm that leverages the power of a triple feature minutiae representation, the authors have set out to elevate the performance of fingerprint indexing. These three-dimensional feature vectors, which draw inspiration from molecules, serve as the foundation for generating indices that play a pivotal role in the intricate matching process. The heart of their approach rests upon the incorporation of an enhanced K-MEANS algorithm, a sophisticated mechanism that refines the process by which fingerprint candidates are selected for comparison. This strategic refinement paves the way for a significant reduction in the initial candidate list, ultimately culminating in the construction of a well-curated final candidate list that holds paramount importance during the matching phase.

On a parallel track, Zhao C. et al. [52] have contributed substantially to the realm of fingerprint verification, steering their research compass toward the integration of fuzzy noise fingerprints within the physical layer of wireless networks. This deliberate exploration is anchored in the notion of enhancing not only the security but also the overall efficiency of wireless network operations. By skillfully leveraging the concept of fuzzy noise fingerprints, the authors have harnessed the potential to fortify the security mechanisms of wireless networks, underlining their commitment to a more robust and resilient digital landscape.

Wireless communication systems face an ongoing challenge of unwanted data transmission from invalid sources, often due to unauthorized actors. In response, the authors present an innovative solution—an authentication algorithm using fuzzy noise fingerprints. This algorithm not only verifies identities but also ensures data integrity. By incorporating fuzzy noise fingerprints, it safeguards identity verification processes and defends against network attacks. The inclusion of combined PHY fingerprints enhances network stability, fortifying wireless communication systems against disruptions.In their independent research, Wang et al. [53] introduce a novel and inventive strategy for crafting non-cancelable fingerprint templates. The main objective of this approach is to develop templates that provide robust protection to the original fingerprint data, preventing any possibility of deletion or loss and ensuring that a new pattern or template for the fingerprint cannot be accepted.Unlike cancelable templates, which may require initial image alignment and can be susceptible to incorrect detection of specific points, non-cancelable templates offer distinct advantages. The proposed technique introduces a localized construction process where Minutiae structures are formed through semi-zone pairs, enabling the creation of removable fingerprints without the need for template alignment. Additionally, a discrete relative feature transformation based on the Fourier transform is proposed. These new templates fulfill the requirements of diversity, cancellability, and irreversibility. The performance evaluation of these templates includes testing on multiple public databases, demonstrating exceptional performance with the same error rate for lost fingerprints.

The research conducted by Zhao C. et al. and Wang S et al. makes a significant contribution to the advancement of fingerprint verification and template design. Their studies present innovative solutions to tackle vital challenges in wireless network security and safeguarding fingerprint data. The proposed algorithms and techniques provide promising results, highlighting the potential for improving the reliability and resilience of fingerprint-based authentication systems in various applications. A detailed review and comparison of fingerprint recognition methods are presented in Table 3.

3.4. Processor

In the field of embedded systems and microcontroller programming, there exist various types of protocols that facilitate communication and interaction between different components. Some of the commonly encountered protocols include ARM, AVR, PIC, and FPGA. A detailed review and comparison of these protocols are presented in Table 4.

AVR: AVR, short for Alf and Vegard's RISC processor, constitutes a family of microcontrollers created by Atmel (now owned by Microchip Technology). These microcontrollers are built on the principles of Reduced Instruction Set Computing (RISC) architecture and find extensive usage across diverse applications, including consumer electronics, industrial automation, and Internet of Things (IoT) devices. AVR microcontrollers are known for their low power consumption, high performance, and ease of use. They offer a range of features such as analog-to-digital converters, timers, serial communication interfaces, and programmable I/O pins. These microcontrollers offer a compelling combination of low power consumption, high performance, ease of use, and a rich set of features. These characteristics make them a preferred choice for a wide range of applications, where power efficiency, reliability, and flexibility are paramount. The AVR family continues to be a significant player in the microcontroller market, driving innovation and powering numerous electronic systems around the world.

ARM: ARM (Advanced RISC Machines) is a family of microprocessor architectures developed by ARM Holdings (now owned by NVIDIA). ARM processors are extensively utilized in mobile devices, embedded systems, and various other applications. Renowned for their energy efficiency, scalability, and adaptability, ARM processors have found their way into a diverse array of devices, such as smartphones, tablets, smartwatches, and automotive systems. They offer different cores and instruction sets to meet the requirements of different applications, ranging From energy-efficient IoT devices to high-powered computing systems. These kinds of processors offer a compelling combination of energy efficiency, scalability, and flexibility. Their widespread adoption in mobile devices, embedded systems, and diverse applications is a testament to their effectiveness. The ARM architecture continues to drive advancements in the industry, enabling efficient and powerful computing solutions for an increasingly connected world.

PIC: Microchip Technology's PIC (Peripheral Interface Controller) is a family of microcontrollers, known for their versatility and widespread use in embedded systems. These microcontrollers offer a diverse range of features, including timers, analog-to-digital converters, serial communication interfaces, and digital I/O pins. Renowned for their user-friendly nature, affordability, and the abundance of development tools and libraries, PIC microcontrollers are extensively applied in various domains such as industrial control, home automation, medical devices [54] , and consumer electronics.

FPGA: FPGA (Field-Programmable Gate Array) is a type of programmable integrated circuit that stands out for its flexibility, as users can configure and reconfigure it as needed after the manufacturing phase. FPGAs

Table 3. Comparison of Fingerprint Recognition Methods

Method	*Advantages*	*Disadvantages*
Ordinary	•Ease of execution •Extensive data classification is minimally required	•The process execution is lengthy •The accuracy during the alignment stage is low
Neural Network	•Increased accuracy in all stages •Increased efficiency in fingerprint registration and verification processes.	•Low fingerprint quality captured by the sensor can lead to detection issues. • High memory requirement for registration in different stages • Dependency on capturing all points of the fingerprint during scanning
Hybrid	•It maintains proper functionality in case of incomplete fingerprints. •High speed in recognition due to utilizing only a portion of the scanned image. •No need for extensive memory.	•Greater complexity compared to other techniques.

Table 4. Comparison of Microcontroller Types

Processor	*Subset size*	*frequency*	*Learning Sources*	*Price*	*General Power*	*Specialized power*	*Noise*	*Protocol*
AVR	Over 120	300 MHz	very high	affordable	moderate	low	high	Moderate
ARM	Over 200	over 1 GHz	moderate	moderate	high	high	low	Very good
PIC	Over 60	40 MHz	high	moderate	moderate	moderate	low	Good
FPGA	Over 200	over 1 GHz	moderate	moderate	moderate	high	low	Moderate

consist of programmable logic blocks and interconnects that can be configured to implement digital logic circuits. Unlike microcontrollers or microprocessors, FPGAs offer a high level of flexibility and can be customized to perform specific tasks or algorithms. They are used in applications that require high performance, parallel processing, and real-time data processing, such as digital signal processing, image and video processing, graph processing [55],[56], and scientific research. All these are different technologies used in the field of microcontrollers and digital logic design. Each has its own strengths and applications, some of which have been presented in Table 4.

4. Conclusion

In conclusion, this review paper has provided a comprehensive examination of the current state of fingerprint recognition devices in ATMs, shedding light on key research contributions in the field of biometric authentication. Through a thorough evaluation of fingerprint recognition algorithms, we have identified areas where improvements can be made, specificallywith regards to reliability, robustness, and proficiency.

Additionally, we have tackled the weaknesses connected with biometric authentication in ATMs, emphasizing the significance of bolstering security protocols. An avenue for potential improvement lies in employing transaction graphs and graph-based algorithms. Through constructing transaction graphs and applying such algorithms, researchers can efficiently identify suspicious activities, such as fraudulent transactions or unauthorized access attempts. These valuable findings can be harnessed to elevate the security measures integrated into ATM authentication systems [57], [58].

By bridging the gap between theoretical advancements and practical implementation, this review paper contributes to the broader understanding of fingerprint

recognition devices in ATMs. It provides a foundation for future researchers and industry professionals to build upon, working towards the common goal of enhancing the security and efficiency of ATM authentication systems [59], [60].

As the field continues to evolve, it is expected that further advancements will be made, both in terms of biometric technology and security measures. This review paper serves as a catalyst for future exploration and innovation in the realm of biometric authentication in the banking industry. By leveraging the insights gained from this review, researchers and industry experts can collaborate to develop more secure and reliable ATM authentication systems, ultimately safeguarding the interests of customers and financial institutions alike.

References

[1] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," International Journal of Applied Engineering Research, vol. 13, no. 5, pp. 2276-2297, 2018.

[2] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. Mcguire, "Biometric systems utilizing health data from wearable devices: applications and future challenges in computer security," ACM Computing Surveys (CSUR), vol. 53, no. 4, pp. 1-29, 2020.

[3] M. Gayathri, C. Malathy, and M. Prabhakaran, "A review on various biometric techniques, its features, methods, security issues and application areas," Computational Vision and Bio-Inspired Computing: ICCVBIC 2019, pp. 931-941, 2020.

[4] I. M. Alsaadi, "Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review," Int. J. Sci. Technol. Res, vol. 10, pp. 15-21, 2021.

[5] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," Sensors, vol. 21, no. 18, p. 6163, 2021.

[6] A. F. Y. Althabhawee and 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.

[7] Ansaripour N, Heidari A, Eftekhari SA. Multi-objective optimization of residual stresses and distortion in submerged arc welding process using Genetic Algorithm and Harmony Search. Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science. 2020 Feb;234(4):862-71.

[8] Daniali OA, Toghraie D, Eftekhari SA. Thermo-hydraulic and economic optimization of Iranol refinery oil heat exchanger with Copper oxide nanoparticles using MOMBO. Physica A: Statistical Mechanics and its Applications. 2020 Feb 15;540:123010.

[9] Babajamali Z, Aghadavoudi F, Farhatnia F, Eftekhari SA, Toghraie D. Pareto multi-objective optimization of tandem cold rolling settings for reductions and inter stand tensions using NSGA-II. ISA transactions. 2022 Nov 1;130:399-408.

[10] Barnoon P, Toghraie D, Mehmandoust B, Fazilati MA, Eftekhari SA. Natural-forced cooling and Monte-Carlo multi-objective optimization of mechanical and thermal characteristics of a bipolar plate for use in a proton exchange membrane fuel cell. Energy Reports. 2022 Nov 1;8:2747-61.

[11] Khan MA, Arshad H, Khan WZ, Alhaisoni M, Tariq U, Hussein HS, Alshazly H, Osman L, Elashry A. HGR-BOL2: human gait recognition for biometric application using Bayesian optimization and extreme learning machine. Future Generation Computer Systems. 2023 Jun 1;143:337-48.

[12] Soltani M. Joint optimization of opportunistic predictive maintenance and multi-location spare part inventories for a deteriorating system considering imperfect actions. arXiv preprint arXiv:1810.06315. 2018 Oct 15.

[13] Soleimani M, Forouzanfar Z, Soltani M, Harandi MJ. Imbalanced Multiclass Medical Data Classification based on Learning Automata and Neural Network. EAI Endorsed Transactions on AI and Robotics. 2023 Jul 24;2.

[14] Sun H, Zhang Y, Chen P, Wang H, Liu YP, Liang R. A New Approach in Automated Fingerprint Presentation Attack Detection using Optical Coherence Tomography. IEEE Transactions on Information Forensics and Security. 2023 Jul 7.

[15] M. N. Kumar, S. Raghul, K. N. Prasad, and P. N. Kumar, "Biometrically Secured ATM Vigilance System," in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, vol. 1: IEEE, pp. 919-922.

[16] K. M. Htwe, Z. M. M. Htun, and H. M. Tun, "Design and implementation of bank locker security system based on fingerprint sensing circuit and RFID reader," International Journal of Scientific and Technology Research, vol. 4, no. 7, pp. 6-10, 2015.

[17] K. R. Gill and J. Sachin, "Vehicle ignition using fingerprint sensor," Int. J. Innov. Res. Sci. Technol, vol. 2, no. 12, pp. 357-363, 2016.

[18] R. Madhu and U. Mahadevaswamy, "GSM/GPS based Device Switching with Fingerprint Module Integration using Arduino," International Journal of Computer Applications, vol. 149, no. 2, 2016.

[19] A. J. Moshayedi, M. Hosseinzadeh, B. P. Joshi, M. Emadi Andani,(2023). Recognition System for Ergonomic Mattress and Pillow: Design and Fabrication. IETE Journal of Research, 1-19.

[20] S. Singh, A. Singh, and R. Kumar, "A constraint-based biometric scheme on ATM and swiping machine," in 2016 international conference on computational techniques in information and communication technologies (icctict), 2016: IEEE, pp. 74-79.

[21] S. I. Manzoor and A. Selwal, "An analysis of biometric based security systems," in 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2018: IEEE, pp. 306-311.

[22] K. M. Sagayam, D. N. Ponraj, J. Winston, J. Yaspy, D. E. Jeba, and A. Clara, "Authentication of biometric system using fingerprint recognition with euclidean distance and neural network classifier," Int. J. Innov. Technol. Explor. Eng, vol. 8, no. 4, pp. 766-771, 2019.

[23] Z. Ishak, N. Rajendran, O. I. Al-Sanjary, and N. A. M. Razali, "Secure biometric lock system for files and applications: a review," in 2020 16th IEEE International Colloquium on Signal Processing, Its Applications (CSPA), 2020: IEEE, pp. 23-28.
[24] H. Hoorfar, A. Bagheri, Minimum hidden guarding of histogram polygons. arXiv preprint arXiv:1708.05815. 2017 Aug 19.
[25] H. Hoorfar, Bagheri A. A New Optimal Algorithm for Computing the Visibility Area of a simple Polygon from a Viewpoint. arXiv preprint arXiv:1803.10184. 2018 Mar 27.
[26] M. Ferretti, S. Nicolazzo, and A. Nocera, "H2O: secure interactions in IoT via behavioral fingerprinting," Future Internet, vol. 13, no. 5, p. 117, 2021.
[27] X. Yin, S. Wang, M. Shahzad, and J. Hu, "An IoT-oriented privacy-preserving fingerprint authentication system," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11760-11771, 2021.
[28] T. Nonthaputha, M. Kumngern, S. Kaewwang, J. Phookwantong, N. Thepnarin, and K. Anontree, "A Design of Smart Biometric Fingerprint Key Storage Cabinet Based on IoT," in 2022 20th International Conference on ICT and Knowledge Engineering, 2022: IEEE, pp. 1-5.
[29] V. M. M. Siregar and N. F. Siagian, "The Implementation of Fingerprint Sensors for Fingerprint Reader Prototypes Using a Microcontroller," Internet of Things and Artificial Intelligence Journal, vol. 2, no. 1, pp. 47-59, 2022.
[30] M. Lastra, J. Carabaño, P. D. Gutiérrez, J. M. Benítez, and F. Herrera, "Fast fingerprint identification using GPUs," Information Sciences, vol. 301, pp. 195-214, 2015.
[31] P. M. A. Hambalık, "Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation," Tatra Mt. Math. Publ, vol. 67, pp. 117-134, 2016.
[32] A. J. Moshayedi, A. J. Li, N. Sina, Chen, X., Liao, L., Gheisari, M., Xie, X. (2022). Simulation and validation of optimized pid controller in agv (automated guided vehicles) model using pso and bas algorithms. Computational Intelligence and Neuroscience, 2022.
[33] R. Murugesh, "Advanced biometric ATM machine with AES 256 and steganography implementation," in 2012 Fourth International Conference on Advanced Computing (ICoAC), 2012: IEEE, pp. 1-4.
[34] A. Taralekar, G. Chouhan, R. Tangade, and N. Shardoor, "One touch multi-banking transaction ATM system using biometric and GSM authentication," in 2017 International Conference on Big Data, IoT and Data Science (BID), 2017: IEEE, pp. 60-64.
[35] B. Saranraj, N. S. P. Dharshini, R. Suvetha, and K. U. Bharathi, "ATM security system using Arduino," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020: IEEE, pp. 940-944.
[36] H. A. Alzamel, M. Alshabanah, and M. Alsmadi, "Point of Sale (POS) Network with Embedded Fingerprint Biometric Authentication," Hussah Adnan Alzame, Muneerah Alshabanah, Mutasem K. Alsmadi," Point of Sale (POS) Network with Embedded Fingerprint Biometric Authentication", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN, 2019.
[37] A. V. Bataev, "The Model of Assessing Economic Efficiency of Biometric ATMs," in 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019: IEEE, pp. 1365-1370.
[38] T. Sangeetha, M. Kumaraguru, S. Akshay, and M. Kanishka, "Biometric based fingerprint verification system for atm machines," in Journal of Physics: Conference Series, 2021, vol. 1916, no. 1: IOP Publishing, p. 012033.
[39] Moshayedi AJ, Roy AS, Liao L, Lan H, Gheisari M, Abbasi A, Bamakan SM. Automation Attendance Systems Approaches: A Practical Review. BOHR International Journal of Internet of things, Artificial Intelligence and Machine Learning. 2022 May 11;1(1):25-34.
[40] M. N. Kumar, S. Raghul, K. N. Prasad, and P. N. Kumar, "Biometrically Secured ATM Vigilance System," in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, vol. 1: IEEE, pp. 919-922.
[41] C. Hochwarter, D. Jahnel, and A. Uhl, "Public Perceptions, Preferences and Legal Aspects towards ATMs with Biometric Authentication in Austria," in 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), 2019: IEEE, pp. 1-6.
[42] A. J. Moshayedi, M. Soleimani, M. Marani, Sh.Yang, A.Razi, M. Emadi Andani, (2023) Fingerprint Identification Banking(FIB); Affordable and Secure Biometric IOT Design. Paper presented at the International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT 2023), China.
[43] K. O. Okokpujie, F. Olajide, S. John, and C. G. Kennedy, "Implementation of the enhanced fingerprint authentication in the ATM system using ATmega128 with GSM feedback mechanism," 2016.
[44] P. Subpratatsavee and N. Pubpruankun, "A Design and Implementation of Attendance System Using Smallest Wireless Fingerprint with Arduino Yún Embedded Board," in Applied Mechanics and Materials, 2015, vol. 752: Trans Tech Publ, pp. 1057-1061.
[45] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of fingerprint recognition. Springer, 2009.
[46] Soleimani M, Naderi MH, Ashrafi AR. Tensor product of the power graph of some finite rings. Facta Universitatis, Series: Mathematics and Informatics. 2019 Mar 13:101-22.
[47] Mahmudi F, Soleimani M. Some results on Maximal Graph of a Commutative Ring, 2016.
[48] J. Yang, S. Xie, S. Yoon, D. Park, Z. Fang, and S. Yang, "Fingerprint matching based on extreme learning machine," Neural Computing and Applications, vol. 22, pp. 435-445, 2013.
[49] R. D. Labati, A. Genovese, E. Munoz, V. Piuri, and F. Scotti, "A novel pore extraction method for heterogeneous fingerprint images using convolutional neural networks," Pattern Recognition Letters, vol. 113, pp. 58-66, 2018.
[50] J. Li, J. Feng, and C.-C. J. Kuo, "Deep convolutional neural network for latent fingerprint enhancement," Signal Processing: Image Communication, vol. 60, pp. 52-63, 2018.
[51] J. Khodadoust and A. M. Khodadoust, "Fingerprint indexing based on expanded Delaunay triangulation," Expert Systems with Applications, vol. 81, pp. 251-267,

2017.
[52] C. Zhao, M. Huang, L. Huang, X. Du, and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks," Computer networks, vol. 128, pp. 164-171, 2017.
[53] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," Pattern Recognition, vol. 66, pp. 295-301, 2017.
[54] A. J. .Moshayedi, D. C. Gharpure, (2017, May). Evaluation of bio inspired Mokhtar: Odor localization system. In 2017 18th international carpathian control conference (ICCC) (pp. 527-532). IEEE.
[55] M. Soleimani, F. Mahmudi, M. H. Naderi, On the Maximal Graph of a Commutative Ring. Mathematics Interdisciplinary Research. 2021 Jul 2.
[56] Soleimani M, Mahmudi F, Naderi MH. Some results on the maximal graph of commutative rings. Advanced Studies: Euro-Tbilisi Mathematical Journal. 2023 Mar;16(supp1):21-6.
[57] Moshayedi AJ, Roy AS, Liao L, Lan H, Gheisari M, Abbasi A, Bamakan SM. Automation Attendance Systems Approaches: A Practical Review. BOHR International Journal of Internet of things, Artificial Intelligence and Machine Learning. 2022 May 11;1(1):25-34.
[58] Boroujeni SP, Pashaei E. A Hybrid Chimp Optimization Algorithm and Generalized Normal Distribution Algorithm with Opposition-Based Learning Strategy for Solving Data Clustering Problems. arXiv preprint arXiv:2302.08623. 2023 Feb 16.
[59] Mehrabi N, Boroujeni SP. Age estimation based on facial images using hybrid features and particle swarm optimization. In2021 11th International Conference on Computer Engineering and Knowledge (ICCKE) 2021 Oct 28 (pp. 412-418). IEEE.
[60] Boroujeni SP, Pashaei E. Data clustering using chimp optimization algorithm. In2021 11th international conference on computer engineering and knowledge (ICCKE) 2021 Oct 28 (pp. 296-301). IEEE.