Available online at sjuoz.uoz.edu.krd

journals.uoz.edu.krd

Science Journal of University of Zakho

Vol. 11, No. 4, pp. 481–491, October-December, 2023

p-ISSN: 2663-628X
e-ISSN: 2663-6298

FINGERPRINTS TO AUTHENTICATE TRANSACTIONS IN CONTACTLESS CARDS

Soleen J. Ibrahim[a*], Ahmad B. Al-Khalil [b]

a College of Science, University of Duhok, Duhok, Kurdistan Region, Iraq - solin.jamalibrahim@gmail.com

b College of Science, University of Duhok, Duhok, Kurdistan Region, Iraq - ahmad.al-khalil@uod.ac

Received:21 Jun..,2023 / Accepted: 3 Sep.,2023 / Published:16 Oct.,2023. https://doi.org/10.25271/sjuoz.2023.11.4.1165

ABSTRACT:

The contactless bank card is a replica of the old fashion payment methods. The contactless card saves the customer a lot of time and effort because the cardholder can tap the card on the card reader instead of carrying a massive amount of cash or memorizing a long password. The transaction will be done in a few seconds, which is a magnificent technique for a very rush and speedy world like this. However, because the contactless card does not require a PIN or signature, it is vulnerable to different types of attacks, and the card can be used by every single person who has the card, even if they are not the real cardholder. Nevertheless, for each new problem, there is a unique solution. Hence this paper presents an innovative way to overcome this problem by embedding a fingerprint sensor into the contactless card to add an extra level of security by creating a virtual environment giving a contactless card and using a minutiae-based algorithm for fingerprint recognition in this contactless card. The work is evaluated based on accuracy using two metrics, false acceptance rate (FAR) and false rejection rate (FRR), algorithm's matching time, and transaction time. This work shows a good result regarding the transaction time and the possibility of integrating the fingerprint into the contactless card. It displays how fingerprint image quality and features affect fingerprint authentication results. However, it also shows that minutiae-based techniques are not adequate when the dataset is relatively small and has data with low-quality and/or noisy data.

KEYWORDS: Minutiae-based, Contactless card, Biometric, Security, Verification.

1- INTRODUCTION

The banking sector is experiencing a profound transformation due to globalization and evolving customer needs. In recent times, banking services have undergone significant changes in response to the rise of knowledge-based economies, the emergence of an information technology-driven society, and the consequent advancements in the field (Matyushok, Krasavina, Berezin, & García, 2021). Looking ahead, the key driving force behind the future evolution of banking lies in the ability of financial institutions to generate intricate financial products, enhance their infrastructure, and tap into geographically diverse and dispersed consumer markets (Aron & Muellbauer, 2019). Besides, over the past decade, customer demands have undergone tremendous evolution. Today, customers expect the convenience of accessing banking services anytime, anywhere, necessitating a greater emphasis on personalized banking products and services. Additionally, customers seek simplicity and ease in their day-to-day banking experiences, with those who have established a strong sense of trust in their bank being more inclined to consolidate their financial needs under a single provider of comprehensive financial services. Moreover, as cash usage declines and more transactions migrate online, the need for secure digital payment methods such as debit and credit cards becomes paramount. Protecting these payment instruments is crucial as individuals increasingly rely on digital payment channels for their day-to-day financial activities (Kandpal & Mehrotra, 2019).

In 2002, the new near-field communication (NFC) technology was introduced by Sony and NXP Semiconductors, a revolutionized retail payment method (Kang, Song, Kim, Lee, & Kim, 2021). These advancements have significantly enhanced the convenience and user-friendliness of traditional payment systems. By employing contactless payment methods, such as NFC-enabled payment cards, customers can securely make retail purchases by simply tapping their card near a POS terminal displaying the contactless wave symbol without entering a PIN code. With the integration of NFC technology into smartphones and payment cards, customers now have the ability to make in-store transactions without physically retrieving their credit cards, inputting PINs, or even extracting their wallets (Ali, Azad, Centeno, Hao, & Moorsel, 2019). While contactless transactions offer efficient and modernized transactions, studies (Gerpott & Meinert, 2018) (Zhao, Anong, & Zhang, 2019) suggested that the NFC technology is still in its early stages of global adoption. Market penetration varies across European countries, with varying degrees of acceptance for payment cards, mobile phones, and POS terminals capable of scanning contactless payments, all of which are increasingly integrating NFC technology. However, NFC's dominance as the universally recognized method for small retail payments seems unstoppable as it continues to gain traction worldwide. Accordingly, there are real concerns regarding the security of contactless cards.

Using radio frequency technology (RFID), contactless cards send data that unauthorized people can intercept if they are nearby the card. This makes potential eavesdropping and unauthorized access to cardholder data more likely. There is a chance of spying and illegal access due to the wireless nature of contactless card transactions (Al-Maliki & Al-Assam, 2021). Someone with nefarious intentions may try to intercept the radio signals and

* Corresponding author

grab the data transmitted between the card and the terminal if they are close to the card. Eavesdropping or sniffing is the term for this kind of attack. To intercept the radio signals and retrieve sensitive data on the card, such as the card number, expiration date, or even the cardholder's name, the attacker could utilize specialized equipment, such as an NFC reader or RFID skimmer. In addition, attackers might capture critical information like the card number or transaction details if they could intercept the transmission between the card and the payment terminal using specialized equipment. Alternatively, attackers may read card information from neighbouring cards using covert devices in congested areas or on transportation systems. Moreover, contactless cards may occasionally be vulnerable to fraudulent purchases if a stolen or lost card is in the wrong hands. One with the card may make illicit purchases without extra security measures, such as a PIN entry, particularly for small-value transactions when neither a signature nor a PIN is required. Alternatively, with stolen or compromised card data, attackers may try to clone or make fake cards, which could result in fraudulent transactions and financial loss (Klimek, 2020).

Therefore, this paper aims to propose an active method for embedding fingerprint technology in contactless banking cards. The focus will be on adding a third approach: the biometric-based approach to the contactless card, to add an extra layer of security during the transaction process. However, adding biometrics on a card is difficult since manufacturers must adhere to current thickness criteria to maintain compatibility with existing readers when swiping or inserting the card. Therefore, the work in this paper will be based on developing the method using a simulation platform in which we will virtually embed the fingerprint technique within a contactless card. This paper covers the biometric aspect of the fingerprint identifier since the ridges on the skin of cardholders' fingerprints are unique patterns. It is a dependable biometric characteristic because, unlike a password or ID, it cannot be stolen, borrowed, purchased, or forgotten.

The main contributions of this research are:

- Developing a virtual contactless card using the Java applet to embed a fingerprint recognition algorithm.
- The fingerprint recognition algorithm that has been developed is based on minutiae features.
- The proposed system has been tested and evaluated using poor-quality datasets to represent real-world scenarios.

The following sections in this article will adopt all the aspects to achieve its objective. In Section 2, the theories and background of the concepts this paper includes will be presented. The related work will be shown in Section 3. Section 4 will focus on the methods used in this work. At the same time, Section 5 will present the implementation results and discuss them. Finally, section 6 will introduce the conclusions and future work.

2- THEORIES AND BACKGROUND

The bank plays an essential role in the economy because it provides customers with financial services like facilitating payments, making loans, and accepting deposits. Facilitating payments allows money to be transferred from one party to another securely and efficiently. There are several types of payment: Cash, plastic cards, mobile payment, and online payment systems. The focus of this paper is on contactless plastic cards. Plastic cards make fast, easy purchases at the point of sale (POS). They are different types, and they can be Credit or Debit cards (Figure 1).

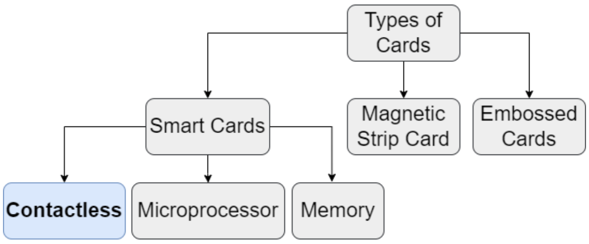


Figure 1. Types of Plastic Cards

2.1 Contactless Card

A form of payment called a contactless card uses contactless technology embedded with a plastic card to allow rapid and convenient transactions without directly touching a payment terminal, i.e., wirelessly communicating with the reader. There are three types of standards for contactless cards. Each operates with a specific range (Table 1).

Table 1. Contactless Cards Standards and Operating Range (Liu, 2013)

Contactless Card Type	Standard	Range
Close-coupling card (CICC)	ISO/IEC 10536	Up to 1 cm
Vicinity coupling card (VICC)	ISO/IEC 15 693	up to 1 meter
Proximity coupling card (PICC)	ISO/IEC 14 443	approximately 10 cm

Financial institutions often issue them as debit or credit cards. A tiny chip that provides the required hardware to establish wireless communication with suitable payment terminals is incorporated in contactless cards. The contactless chip on the card uses the radio frequency field that the terminal generates to power itself and communicate with the terminal. This is a speedy and straightforward mode of payment because the transaction is finished in a matter of seconds. This technology is often based on RFID or NFC (Al-Maliki & Al-Assam, 2021). NFC functions in both active and passive modes. The passive mode is utilized in contactless cards. A passive NFC chip that does not need its power source is present on the contactless card. The card's chip is powered by a radio frequency field produced by the payment terminal when brought close to one with NFC capabilities, enabling communication between the two devices. In contrast, contactless cards with RFID technology have an RFID chip built into the card. The RFID reader in a payment terminal generates radio waves that energize the card's chip when the card is brought close to it. Following that, radio frequency signals are used to exchange data between the card and the reader. NFC is a subset of RFID technology that is especially suited for close-quarters communication and safe transactions, despite the two technologies having many similarities. NFC is commonly used since it offers extra security features.

Regarding security, contactless cards use encryption methods to safeguard the cardholder's private information while it is transmitted (Kılınç & Vaudenay, 2018). Because of the encryption process, even if the transaction data is captured during transmission, it will still be unreadable and useless to outsiders. Only the authorized recipient, such as the card issuer or the payment terminal, can decrypt the encrypted data using the proper encryption keys (Furkan Altınok, Peker, Tezcan, & Temizel, 2022). Additionally, contactless cards frequently use tokenization, lowering the danger of hacking card information by substituting distinct tokens for the actual card details (Al-Maliki & Al-Assam, 2022). Instead of sending the factual card information when a contactless payment is made, the card's associated token is sent. A reputable third-party service provider or card issuer typically handles the tokenization procedure. Tokens cannot be used to carry out fraudulent transactions or obtain the original card information because they are useless outside the ecosystem of authorized payments. The secrecy and integrity of contactless payments are crucially protected by tokenization and encryption. A secure environment for using contactless cards in transactions is made possible by these security measures and other industry-standard procedures. Since their sensitive information is safeguarded during payment, they give cardholders peace of mind.

2.2 Threats and Security Concerns in Contactless Cards

Information security safeguards data and information from unauthorized access, use, destruction, or alteration. As technology continues to evolve, the concept of information security undergoes parallel advancements. Bank websites, in particular, hold critical and confidential information about their clients and customers. In today's world, information security concerns extend beyond technical aspects and encompass commercial considerations, often overlooked by many companies. Information security assurance is the paramount factor determining the success of any business. Evaluating a company's ability to protect private information has become a customary practice in the business realm. Therefore, we need to address security within contactless cards and payments by defining the types of attacks.

Although contactless cards offer users effortless, speedy, and straightforward transactions, they also open a new avenue to new attacks (Akinyokun & Teague, 2017). An "attack" on a contactless card is any intentional, malicious action taken by a person or a group intending to undermine the card's security or exploit loopholes in the contactless payment system (Ramesh, Jaunky, Roopchund, & Sigh, 2019). These assaults seek to influence the transaction process for fraudulent ends or gain unauthorized access to private cardholder data. This paper defines five types of attacks: relay attack, per-play attack, mafia attack, cloning and skimming attack, and eavesdropping attacks. In a relay attack, the attacker captures and sends the information that the POS and the contactless card are used to perfume a transaction without the customer's knowledge (Sportiello, 2019). Both the contactless card and the terminal exchange information with each other via the communication channel the attacker constructs, whereas both parties are made to believe it is a legit channel. Additionally, the pre-play attack occurs when the attacker collects sensitive data like PIN from the contactless card using a compromised POS terminal and then makes a fraudulent (unauthorized) transaction using the collected data (Lan, Xu, Zhang, Chen, & Luo, 2023). In contrast, in a mafia attack (aka mafia fraud), the attacker uses a malicious reader to conduct a contactless payment (Yang, Luo, Vijayalakshmi, & Shalinie, 2022). At the same time, in a cloning (skimming) attack, the attacker copies the contactless card information, like the card number stored in the chip, into another device (El Madhoun, Bertin, & Pujolle, 2018). Moreover, when the attacker can use the cloned card unlimited times, in a skimming attack, the attacker captures the potential information that can be used to commit fraud during communication between a contactless card and a terminal via skimmers. Furthermore, the attacker can read or modify the stored information. Finally, because the contactless card uses NFC and radio frequency signals to make a transaction and to exchange information with the reader, the attacker intercepts this signal from a distant location and records the transferred information, like card numbers and expiration dates. This attack usually happens when the communication protocol and encryption mechanisms are weak. This type of attack is also known as man-in-the-middle (Akter, et al., 2020).

2.3 Biometric Security Techniques

Researchers attempt to increase the security level of contactless cards using different techniques and methods. They focus on preventing skimming attacks on contactless cards using two-way challenge-response between the POS and contactless card without making any changes to the original card infrastructure (Al-Maliki & Al-Assam, 2021). In addition, they develop protocols and techniques to increase security by demanding a biometric scan before allowing access to the app or approving a transaction (Goode, 2018). Further safeguarding the user's privacy is the secure storage of biometric data on the user's device, which is not sent to or accessible by outside parties.

Biometrics is a biological or physical characteristic used to identify individuals uniquely. It is widely used worldwide for security, financial services, healthcare, travel, and retail. Biometrics have many advantages over the traditional password of endless characters and numbers due to their universality, uniqueness, and non-transferable (Suwald & Rottschäfer, 2019). Also, individuals do not need to memorize the biometrics. Biometrics is divided into two categories: biological and behavioural biometrics. Biological biometrics relies on human body characteristics such as fingerprints, iris, DNA, hand, face, etc. On the other hand, behavioural biometrics deals with human behaviour, such as signatures, keystrokes, voice, etc. Indeed, there are various types of biometrics, but some are more in use, like Face, Iris, Voice, and fingerprint. This work will focus on fingerprints, which will be explained in the next section.

The fingerprint is the oldest and most known biometric. There is no identical fingerprint in the world. Even in the case of identical twins, they share the same biometrics same DNA, but they have different fingerprint patterns. More importantly, this fingerprint remains unchangeable throughout life.

Fingerprint recognition is an automated technique that compares fingerprints to comfier the individual's identity. According to (Yadav & Mathuria, 2015), there are two types of fingerprint recognition: one-to-one or to-many matches. In one-to-one matches, also known as verification, two fingerprints are compared to ensure a person's identity. In contrast, one-to-many, also known as identification, compares a fingerprint with the number of fingerprints usually applied at crime scenes. The patterns in each fingerprint are different and unique. These patterns can be divided into three categories Arch, Loop, and Whorl. Arch is the rarest pattern of a fingerprint. Only 5% of the world has an arch pattern. In comparison, the Loop pattern is the most common type among all patterns, as it can be found in 60%-70% of the population. Finally, the whorl pattern can be found in 25%-35% of the population. Furthermore, the characteristics of fingerprints are called minutiae, representing the ridge's characteristics. Ridges are the raised portion of the finger. Minutiae can be recognized, and they are of different shapes, directions, and sizes. Based on these features, researchers develop methods to match and identify fingerprints.

3- RELATED WORKS

Contactless payment is a touch-free transaction process in which the client purchases an identification token close to the vendor's point of sale (POS) scanner. The identification token can be a chip-enabled (contactless) bank card or a smartphone's digital wallet app (Bounie & Youssouf, 2020). However, with the scope of this paper, the focus is on manufacturing the contactless card embedded with biometrics and the authentication process.

From a banking perspective, A contactless payment card with an embedded fingerprint sensor was introduced by MasterCard and Zwipe in October 2014 (Biometric, 2014). The Zwipe MasterCard payment card is advertised as the first contactless payment card with fingerprint authentication in the world from this perspective. It has MasterCard's contactless application and a secure element that has received EMV certification. The card itself stores the cardholder's fingerprints, not a third-party database. The Zwipe MasterCard card can be used to make contactless purchases of any amount by scanning a fingerprint. The advantages, disadvantages, and challenges of embedding fingerprint biometric technology in contactless cards can be found in (Dommaraju, Kondaveeti, Katta, Devanaboina, & Cherukupalli, 2023).

Singh et al. suggested a biometric payment monitoring system based on distinctive fingerprints and faces (Singh, et al., 2021). The client's face is initially output by the system, which then processes it in accordance with the suggested computation to trim off facial highlights and sync it with the database. The customer must choose the conditional record from all the bank accounts connected to that particular person displayed in the window. It does not need any ledger information, such as PIN, a card number, or a bank account number. Setting a threshold value, however, is crucial until the procedures grow more reliable because facial recognition technology is not yet 100% accurate.

As a secure alternative to conventional passwords, Lavadkar, Thorat, Kasliwal, Gadekar, and Deshmukh suggested a method that advises using fingerprint authentication. The UID (Unique Identification) database, which is already connected to banks, has fingerprint biometrics used by the system. With this strategy, cashless payments are meant to be more secure, dependable, and simple to use. Following the same methodology, AliBabaee and Broumandnia (2019) presented their biometric authentication of fingerprints for banking users using a stream cipher algorithm.

Based on fingerprint recognition and matching, researchers attempt to enhance or develop algorithms to increase fingerprint-matching accuracy. Many researchers relied on minutiae points as features. When there is a high-quality or full fingerprint image, a minutiae-based technique is usually applied, showing a reliable result. In some conditions, the number of minutiae points needed for matching cannot be obtained, for instance, in the case of low-quality images, partial fingerprints, and latent fingerprints. Therefore, there is a demand for using features other than minutiae points for fingerprint matching. For the scope of this paper, the related work focuses on this research that used minutiae-based techniques.

The authors (Bhargava, Kumawat, & Bhargava, 2015) proposed a matching system that relies on Euclidian distance and minutiae points. Binarization, thinning, and normalization were applied to extract minutiae points. The extracted point's distance and angle from one another are calculated. Then the Euclidian distance of the new print and the template print were compared, and the system provided good accuracy when the required number of minutiae were available. Similarly, Babatunde (2015) proposed a robust minutiae-based method against various images and image orientations of fingerprints. The proposed method used Euclidian and spatial distance between minutiae points and core or delta (singular point). The matching score between the template and the new fingerprint was calculated using a correlation coefficient. The system gave a FAR of 0%, which shows the algorithm's efficacy in identifying fingerprints from various sources, but because of noise levels in datasets, it yielded a FRR range of 5%-10%. The comparatively high FRR indicated that the matching method could not be efficient with noisy fingerprint images. Then, (Boujnah, Jaballah, Khalifa, & Ammar, 2018) proposed another minutiae-based technique for a partial fingerprint which used minutiae-redefined characteristics. Additional features were recreated from minutiae against other minutiae, such as inter-minutiae distance, ridge number, and relative angles. The suggested method achieves recognition rates up to 98.06 % for the POLYU HRF database and 98.82% FVC 2004 database. This approach yields reasonable recognition rates, but the approach is impracticable if the number of minutiae points is fewer than two minutiae. In order to reduce the incorrect minutiae correspondences, the study of (Agarwal, Garima, & Bansal, 2021) proposes an approach that uses ridge contour points (level 3) with minutiae at the feature level. The ridge contour point set is near the minutiae involved in the matched minutiae pairings. The Iterative Closest Point (ICP) approach eliminates the erroneous correspondences by decreasing the Euclidean distance between the sets of ridge contour points connected to the minutiae pair. When applied to the FVC 2006 database, the suggested algorithm-based fingerprint matching achieves high identification accuracy and reduced error rates in contrast to minutiae-based fingerprint matching alone.

With machine learning, the author (Hambalık, 2016) proposed a fingerprint recognition based on a minutiae technique using two neural networks, the steps included in this system were image enhancement, feature extraction, and fingerprint matching. Two different types of databases were used to test the results; the first was the Crossmatch Verifier 300 database, which achieved a proper authentication rate value of 92% at the threshold where FNMR and FMMR were identical, which means that EER (equal error rate) reached 8%. The other database was the FVC2002 DB3A, which only attained a correct authentication rate of 67% with a 33% EER. However, the authors point out that the FVC2002 DB3A database's samples were far lower quality. Also, deep-learned features were utilized by the authors (Zhang, Xin, & Feng, 2019) to create deep learning for incomplete fingerprints. In order to learn both high-level global features and low-level minutia features, their model used two deep convolutional neural networks. However, their method did not consider the minutiae topologies structures during the learning process of the algorithms. In the same direction, (Chowdhury, Kirchgasser, Uhl, & Ross, 2020) constructed and trained a patch-based Siamese Convolutional Neural Network (CNN), which does not explicitly require the extraction of minutiae points. This network aims to discover the best features for matching fingerprint images. Gradient weighted Class Activation Mapping (Grad-CAM) was used to assess the features acquired by this network and see whether they correlate with the positions of minutiae points. Their research indicated that the suggested network automatically picks up on minutiae details when matching fingerprints. Therefore, the significance of minutiae points for fingerprint matching can be established using an automated learner without explicit domain knowledge.

4- METHODS

Dealing with money is a susceptible process. Therefore, there is "a must" to prove the user's identity during any transaction process via any payment channel. Authentication is verifying that a user's identity claim is valid. Based on advanced technology, the process of authentication is done automatically. Mainly, there are three approaches to a user's automatic authentication: knowledge-based (something the user knows, such as PIN), possession-based (something the user has, such as an ID card), and biometric-based (Zukarnain, Muneer, & Ab Aziz, 2022). The authorization process may involve more than one approach (sometimes three) to strengthen a secure transaction. In addition, an approach may include more than one/all of its authentication options, known as two/three-factor authentication.

4.1 Biometric Authentication

The biometric aspect in this paper presents the fingerprint identifier. The ridges (Minutiae) on the skin of users' fingerprints are unique patterns. It is a dependable biometric characteristic because, unlike a password or ID, it cannot be stolen, borrowed, purchased, or forgotten. The process of automatic authentication consists of four operations (Figure 2), as follows:

1. Data capture: the sensor will capture the biometric data (fingerprint).
2. Enrolment: the captured data should be analyzed, and its outstanding and unique features should be stored as a template.
3. Verification (authentication): When the cardholder wants to do a transfer, s/he needs to impress the sensor again to capture the new biometric data and compare it with the template created by the enrolment.
4. Matching: an algorithm should be implemented to compare the newly captured biometric data (in this case, the fingerprint) with the stored template. If there is a match, then the transaction is authorized. Otherwise, access is denied, and another layer of authentication must be considered, such as PIN or signature.

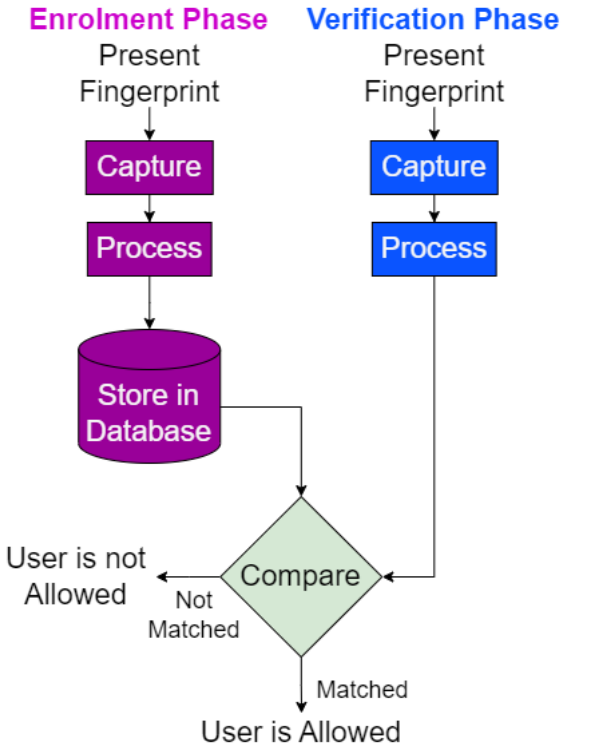


Figure 2. Block Diagram of a Biometric Authentication System

The automatic authentication procedure in a generic biometric system is divided into enrollment and verification (Figure 2). Data collection (fingerprint) and processing steps are all part of the enrolling phase. At the same time, the verification phase involves obtaining data (such as a fingerprint), processing it, and then matching it.

4.2 Enrolment Phase: Extracting Minutiae

The sensor initially collects the fingerprint when the biometric system is employed. Following processing, this data is entered into the system. When the data is analysed during enrolment, its distinctive and unique features should be saved as a template. This procedure is run when a contactless cardholder is registered for the first time. Minutiae have many shapes, which can be recognized using some traits, such as the location of minutiae, type, and direction (Yang, Wang, Hu, Zheng, & Valli, 2019). In the minutiae-based method, minutiae information is used to identify an individual. This method attempts to extract as much as possible minutiae from the finger impression to increase the accuracy of the matching process. The minutiae-based method is considered the best-recommended technique for comparing fingerprints among all techniques. The captured data (new fingerprint) must be recognized during verification to compare and match the template. Capturing the biometric feature is about extracting minutiae, which involves three stages: preprocessing, minutiae extraction, and creating and storing templates (vectors) (Figure 3).

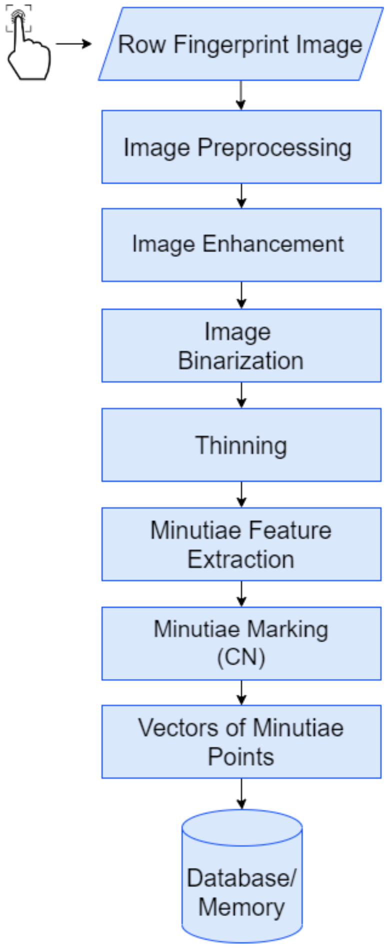


Figure 3. Stages of Capturing (extracting) Minutiae – Enrollment (Identification) Phase

4.3 Preprocessing Fingerprint Images

The preprocessing step consists of three stages: image enhancement, binarization, and thinning (Figure 3). Image enhancement is required to improve the quality of the fingerprint image. This can be assured by employing various methods and techniques to extract information from the image more effectively. This paper followed the work of (Hong, Wan, & Jain, 1998) to implement the enhancement of fingerprint images. While in the binarization step, the fingerprint image is converted from an 8-bit grey-level image into a 1-bit binary image (Patel, Parikh, & Patel, 2019). Binarization makes it easier to extract details since it improves the contrast between the ridges and non-ridges. The result will be an image with 0 for the ridges and 1 for the non-ridges (valleys). Then, the binarized fingerprint image moves to the next stage (thinning).

The enhanced fingerprint image goes through the thinning algorithm (Figure 3). Image thinning removes pixels from ridges until the ridges are just one pixel wide, also known as skeletonization. The thinning algorithm is applied to fingerprint images to simplify extracting minutiae. In this work, one of the most known thinning algorithms is used (Zhang & Suen, 1997). It is an effective method for applying parallel processing techniques to image thinning procedures. The enhanced fingerprint image is divided into smaller regions, which are processed simultaneously. The final thinning pattern is created by combining the results of the individual processing of each region. The method typically consists of repetitive steps in which pixels are evaluated and changed per predetermined guidelines or criteria. The technique may thin the pattern effectively while maintaining its structure and connection using parallelism. It can handle intricately structured complicated patterns, like fingerprint photos, in a computationally efficient form.

4.3.1 Minutiae Feature Extraction

Feature extraction is the process of obtaining a unique key feature from a fingerprint to be used in the fingerprint-matching stage to determine whether or not the two fingerprints are similar. This work focuses on the feature extraction of minutiae. Minutiae features are the best-recommended features for fingerprint recognition. However, in some cases, the number of correctly matched minutiae between two fingerprints cannot be achieved due to a low-quality image, a slight change in minutiae coordination, or its rotation, and it is vulnerable to deformations (Suwarno & Santosa, 2019). After skeletonizing the enhanced fingerprint image, the minutiae features are extracted. The crossing number (CN) approach is popular for extracting minutiae points (Kaur, Singh, Girdhar, & Sandhu, 2008). The difference between adjacent pixels is added to form the CN, which is then divided by two (Eq 1).

$$CN = 0.5 \sum_{i=1}^{8} (P_i - P_{i+1}) \qquad (1)$$

Furthermore, the minutiae points are extracted by scanning the local neighbourhood pixel using a 3x3 window. For the ridge end, the CN is equal to one, and for bifurcation, the CN is equal to three.

By now, the features and their characteristics, such as coordination of the feature, feature orientation, and its type, whether the endpoint or bifurcation, are stored as templates (Figure 3). In addition, each minutia is represented by the tuple mi = (x, y, θ, T), where x and y represent the coordinates of the minutiae, the direction of the minutiae is θ, and T is the type of the minutiae.

4.4 Verification Phase: Feature Matching

The authentication procedure must be carried out whenever the cardholder requests a transfer. This comes under the second (verification) phase. The cardholder must impress the sensor to record the new biometric information (Figure 2). The template stored during the enrolment process will be compared with the data that has been captured. Matching is a method of comparison that uses an algorithm. The transaction is approved if there is a match; otherwise, access is refused, and another layer of verification, such as a PIN or signature, must be considered.

The matching method is the core of the fingerprint authentication or recognition process. It is the process of checking whether or not fingerprint impressions are alike and measuring the similarity. The core model of this article is to develop a matching technique to increase the security of contactless cards by adding an extra level of security using fingerprint authentication. This feature-matching model will be embedded and tested on the virtual contactless card.

An essential step in a fingerprint authentication system is the verification phase (Figure 4), where a captured fingerprint is checked against a template that has been stored to see if it belongs to an authorized cardholder. Using a fingerprint scanner or sensor, the process starts by taking an image of the fingerprint. A digital fingerprint image is produced once the sensor recognizes the ridges and valleys in the fingerprint. Preprocessing and feature extraction procedures are applied to the newly acquired fingerprint image to improve quality, eliminate noise or artifacts, and create minutiae vectors, as in the enrolment phase (Figure 3). The newly obtained fingerprint picture is compared to the authorized user's previously saved template. Different matching methods assess how closely the collected fingerprint features match those of the stored template. Calculating a similarity score or distance measure is often required for this comparison. Accepting or rejecting the fingerprint as a match is based on the similarity score (Figure 4). The fingerprint is recognized as authentic, and the user is given access if the similarity score rises above a predetermined threshold or falls within an acceptable range. Otherwise, the fingerprint is disregarded as a non-match if the score is below the threshold, as displayed in Figure 4, followed by pseudo-code.

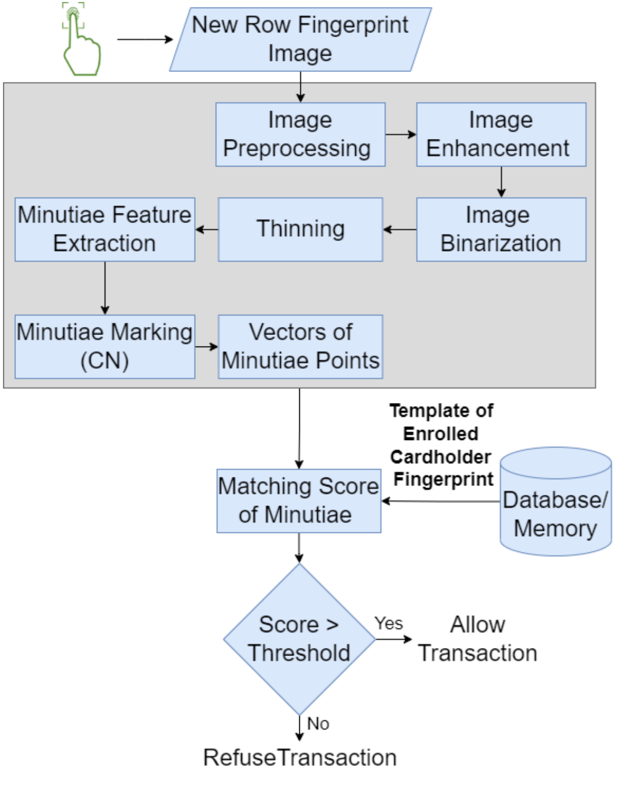


Figure 4. Minutiae Feature Matching - Verification (Authentication) Phase

Algorithm 1. Authentication Phase Pseudo Code.

```
Step 1: New row fingerprint image
Capture a new fingerprint using a capacitive sensor
Step 2: Image enhancement (Yang, Wang, Hu, Zheng, & Valli, 2019)
Enhance the image by applying
normalization
segmentation
ridge orientation
ridge frequency
morphologic operation
Step 3: Image binarization
```

```
Imgproc.threshold (Gabor_image, binarize_image, 0,255, Imgproc.THRESH_BINARY)
Step 4: Image thinning (Zhang & Suen, 1997)
While binarize_image is not thin
do
For     I in range (1, binarize_image_rows)
        For     j in range (1, binarize_image_columns)
                        calculate A (i, j)
                        calculate B (i,j)
                If      the first sub-iteration conditions are satisfied
                        binarize_image(I,j)=0
                End if
End for
End for
For     I in range (1, binarize_image_rows)
        For     j in range (1, binarize_image_columns)
                        calculate A (i, j)
                        calculate B (i,j)
                If      the second sub-iteration conditions are satisfied
                        binarize_image(I,j)=0
End if
End for
End for
image_thin= binarize_image
End while
Step 5: Minutiae feature extraction
minutiae_extraction_function (image_thin)
        For     I in range (1, image_thin.rows)
                For     j in range (1, image_thin.columns)
                        calculate CN
                        If      CN==3
        minutiae_vector=(I,j,angle(I,j),2)
                        Else if   CN==1
        minutiae_vector=(I,j,angle(I,j),1)
                        End if
                End for
        End for
Step 6: Matching score of minutiae
Match _list=Knnmatch(vector A, vector B, 2)
For      I in range (0, Match _list)
         Matches_array= Match _list
         If Matches_array[0]<threshold*Matches_array[0]
            GoodMatchList= Matches_array[0]
         End if
End for
similarity_score= GoodMatchList/ minimum (vector_A_Size, vector_B_Size)
Step 7: Comparing to the threshold (accept or refuse)
If similarity_score <50
   Refuse the transaction
Else
   Accept the transaction
End if
```

4.4.1 Minutiae-based Feature Matching

Minutiae-based matching is a method frequently used in fingerprint identification and authentication systems. It depends on locating and contrasting the distinctive fingerprint characteristics or the minutiae points. The retrieved details from the newly captured fingerprint (authenticated one) are compared with those kept in the reference (enrolled user's fingerprint) template) during the matching procedure. Different algorithms are employed to assess how similar or unlike the minutiae sets are to one another and calculate the score.

In this paper, the matching score measures how closely the newly acquired fingerprint's minutiae match those in the reference template (cardholder). The reference template's corresponding minutiae and each in the input fingerprint are compared. Calculating the distances and angles between the minutiae pairs is necessary for the comparison. Typically, Euclidean distance is used to calculate the separation between two minutiae. The distance here reflects the spatial gap between the minutiae points. Fast Library for Approximate Nearest Neighbors (FLANN) matcher based on Euclidean distance was applied for the matching process. FLANN is a collection of algorithms, and it has been designed for fast nearest-neighbor search (George & Gladston Raj, 2021). In this work, FLANN was designed to find the two best matches, k=2, in which k here refers to the number of nearest neighbors. In our case, the FLANN matcher calculates the distance between the point from vector A with all point from vector B and return the smallest two distance between them, and the process will be repeated until all the point from vector A compared with all's point from vector B. The Euclidian distance (Eq 2) measures the distance between the points.

$$d(x,y) = \sqrt{(x,y)^2} \qquad (2)$$

Then, Lowe's ratio test (Eq 3) from (Lowe, 2004) was used to find the best match between the two distances found by FLANN. For Lowe's threshold, 0.1 was selected for the minutiae matching score.

$$if\ distance1 < threshol * distance2 \qquad (3)$$

A predetermined cutoff (threshold) compares the derived similarity score. If the score exceeds the threshold (0.5), it indicates a match, and the fingerprint is verified as the registered user's (enrolled cardholder). A non-match is indicated if the score is below the cutoff (< 0.5) and the fingerprint is rejected as not belonging to the registered cardholder (Figure 4).

4.5 Simulation/Virtual Toolkits

This paper aims to integrate fingerprint technology into contactless banking cards to increase transaction security. However, including biometrics on a card is challenging because card producers must follow current thickness standards to keep their products compatible with readers already in use when swiping or inserting the card. Therefore, the work in this study focuses on creating the method utilizing a simulation platform that represents the virtual integration of the fingerprint methodology within a contactless card.

There are three applications in the system. The first application is a virtual reader that turns the card on and off and communicates with the virtual card using APDU. It is responsible for establishing the connection between the card and the reader. The reader sends a command to the virtual card to activate the card. In addition, it is responsible for card availability to receive/send data. It activates the card and makes it ready to receive commands and send the response, or deactivates the virtual card and stops receiving commands and sending the response. Moreover, it helps exchange the command and response between the virtual card and the virtual reader, where the reader sends the command APDU to the card, and the card sends the response APDU to the reader.

The second application (applet or Java card) is a fictitious contactless card applet with various features, including debit, credit, and PIN verification. Java cards can hold multiple applets for different applications, and each applet is identified uniquely by an application identifier (AID) (Kurnaz & Mohammed, 2020). Numerous industries and applications use it, including SIM cards, finance, EMV bank cards, and healthcare. A developer can test smart card apps quickly thanks to an object-oriented programming architecture. In addition to the previously mentioned objectives, the implementation of this work on the Java Card is motivated by the fact that it offers a practical and secure tool for working with smart cards, such as debugging and testing various applications in a virtual environment without the need for physical cards and readers.

The final one is the fingerprint algorithm, which determines an individual's authorization, and the similarity between fingerprints and recognizes them.

The contactless port 9026 is used for communication between the reader and the card. Once the card is powered on, the APDU command is sent to select the applet by its AID. A second command, APDU, is sent with the money required for the transaction to debit function. The fingerprint recognition will be triggered and begin matching between two fingerprints after the applet is chosen. The APDU will be sent to the card to complete the transaction if the fingerprint image similarity exceeds the threshold. If not, the cardholder must try again by placing their finger on the sensor. Each person has three chances. The PIN would be required if the attempt was made over three times. The card application will receive the PIN for verification. The card will be banned if the PIN is incorrect; otherwise, the APDU will be sent to the virtual card for the transaction.

5- RESULTS AND DISCUSSION

5.1 System Setup

The system has been developed virtually. We have a virtual card reader, a Java contactless card, and our proposed biometric system. The system has been run on an Intel Core i7 computer. The processor speed is 2.6 GHz, 8 GB RAM, and the OS used is Windows 10. The biometric system was developed using NetBeans 8.2. Java, the language used to develop this biometric authentication system, is supported by the integrated development environment (IDE). Various features and tools are available in NetBeans that might make the development process more manageable. Additionally, it supports several frameworks and libraries that can be used to implement biometric authentication systems, such as APIs specific to fingerprint recognition.

In order to test and evaluate the system, two fingerprint verification competition datasets (FVC2000 – DB2) and (FVC2002 – DB3) have been used. Comparatively speaking to more current fingerprint datasets, the FVC datasets are somewhat small. Ten fingerprints and eight imprints per finger make up each dataset. As a result, each dataset contains a total of 80 fingerprints. A cheap capacitive fingerprint sensor is used to capture DB2's fingerprint. The image size is 256x364 with a 500-dpi resolution. The DB3 has the same characteristics as the DB2, With a different image size of 300x300.

These two datasets cover a range of image quality since they attempt to depict real-world scenarios, which is a crucial point to make. While some images might have good clarity, high resolution, and little noise, others might have worse quality due to unfavourable image-capturing circumstances, incomplete fingerprint impressions, or image artifacts. Therefore, annotation errors that can occur in any dataset, including FVC datasets, must be noted.

Each database is split into two groups for evaluation. As a fingerprint template, the first group is utilized. The second one is employed to create freshly acquired fingerprints. Five impressions were saved as templates for each person, and three were used as test sets.

5.2 Evaluation Metrics

The proposed matching model's effectiveness is evaluated by the algorithm's precision utilizing the FAR, FRR, and matching and transaction time, respectively. The matching time can be calculated using a method known as nano time in NetBeans.

The FAR and FRR are metric approaches that employ biometric authentication to rate the biometric sensors' ease and the biometric system's security, respectively. These two metrics highlight the compromise between the system's ease and security (Kaur N. , 2021). FAR is a measure used in biometric authentication systems to calculate how frequently the system mistakenly accepts a fraud or unauthorized user as a legitimate user (Eq 4). It shows the system's susceptibility to false positive or false acceptance errors. A lower FAR denotes a higher degree of system security and accuracy.

$$FAR = \frac{\text{impostor scores exceeding threshold}}{\text{all impostor scores}} \qquad (4)$$

A cardholder sends their biometric sample (in this case, their fingerprint) to the system during the authentication process of a biometric authentication system, which compares it with the recorded templates to see if there is a match. The proposed approach compares five templates per person with three photos of each person. Ten fingerprints, each with eight impressions, are contained in each dataset. Five impressions were saved as a template, and three were used for the test. Except for the templates (templates belonging to the actual individual), which were 5x9=45. This article compared all of the individual tests' impression images, which were three for every 3x10=30 testes. For each dataset, a total of (30 x 45) comparisons were performed.

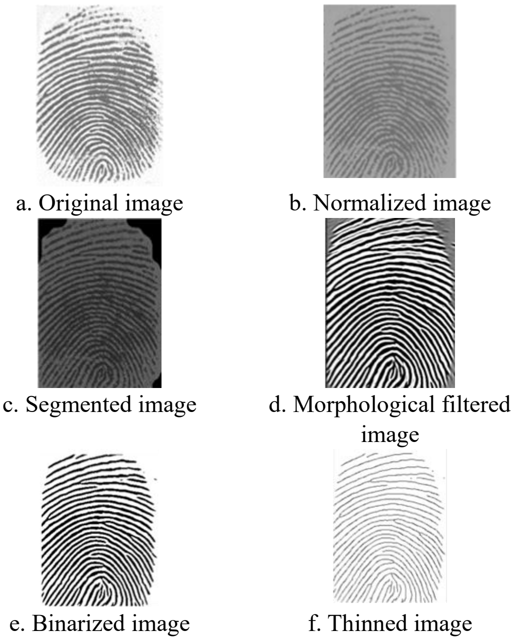
Following the calculation of the FAR value, the FRR is estimated. FRR is a measure used in biometric authentication systems to estimate how frequently the system mistakenly rejects a valid cardholder (Eq 5). It shows that the system has a propensity to generate erroneous rejections or false negative errors. A lower FRR denotes a higher level of user acceptance and system accuracy. The system compares the user's biometric sample—in the case of this paper, fingerprint—with the templates stored to determine whether there is a match during the authentication procedure.

$$FRR = \frac{\text{genuine scores were falling below threshold}}{\text{all genuine scores}} \qquad (5)$$

This proposed technique compared five templates and three photos for each cardholder. To calculate FRR, all individual testes impression images—three for every 3x10=30 testes—were compared to all templates—all save the right one (the one that belonged to the real individual), which was 5x9=45. For each dataset, 30x45 comparisons have been made in total.

5.3 Implementation Results

As mentioned in subsection 4.2, the fingerprint image must be pre-processed before moving to the following steps, either during the identification or verification phases (subsection 4.3). Figure 5 shows an instance of the pre-processed data (fingerprint image). Enhancing the quality, clarity, and distinctiveness of the biometric characteristic under analysis is the goal of the fingerprint image preprocessing phase. Each stage advances the precision, dependability, and effectiveness of succeeding biometric processing algorithms, resulting in more reliable and potent biometric authentication or identification systems.



a. Original image b. Normalized image

c. Segmented image d. Morphological filtered image

e. Binarized image f. Thinned image

Figure 5. The stages of Preprocessing the Original Fingerprint Image

The fingerprint's orientation, scale, and position are intended to be uniformly represented in the normalized image (Figure 5.b.), a processed version of the original image. With the help of this preprocessing procedure, fingerprint images obtained from various individuals or sources are guaranteed to have uniform features and precise comparisons. At the same time, the region of interest (ROI) in the normalized fingerprint image, which is often the fingerprint ridge area, is isolated to create the segmented image (Figure 5.c.). The image's foreground (ridge region) is separated from the background (non-ridge region) using the segmentation technique (Chaudhari, Lade, & Pande, 2014). This stage assists in decreasing the impact of noise and unnecessary information and focusing further processing on the essential fingerprint elements, such as ridge patterns and minutiae points. Then, to enhance the quality and clarity of the segmented fingerprint ridges, local ridge orientation, ridge frequency, and morphological filters techniques are applied to create the Morphological image (Figure 5.d.) by suppressing artifacts or distortions, filtering aids in lowering noise, improving ridge visibility, and ensuring the correctness of future processing steps. Then, the grayscale-filtered image is converted into a binary image (Figure 5.e.). Binarization facilitates extraction and analysis of ridge features, such as ridge ends and bifurcations, by simplifying the fingerprint image and separating the ridge structures. Finally, the binarized fingerprint image has been further processed to create the thinned image, in which the ridge lines are shrunk to a single pixel width (Figure 5.f.). The skeleton of the ridge patterns is extracted using thinning techniques, but the vital topological characteristics are kept. For fingerprint matching and identification, minutiae points (the distinctive features of the fingerprint), ridge ends, bifurcations, and other ridge structures must be extracted.

The fingerprint images initially obtained (during the enrollment phase) and recently acquired (during the verification phase) are enhanced and thinned. The minutiae points of the enhanced-thinned image are retrieved during the enrolling step and saved as a vector in memory. The minutiae points of the newly obtained enhanced-thinned image are recovered during the verification step, and the similarity score is computed by comparing them to the stored vector.

Table 2. The outcome of Implementing the proposed method based on the Evaluation Metrics

Database	FAR	FRR	Time to Create One Template	1:1 Matching	1:1 Matching with a Transaction
DB2	1	0	1-2 sec	2 sec	3 sec
DB3					

The FAR and FRR values show a balanced system performance regarding false acceptance and rejection rates (Table 2). In other words, there is an equal chance that the system will make errors in both directions. This shows that the suggested solution cannot efficiently discriminate between authorized and legitimate users. This system is at the chance level and can be explained why it is there. The fingerprint images used for authentication could be poor quality, noisy, or imperfect. Higher error rates can result from less accurate minutiae extraction and matching due to poor image quality. As mentioned earlier, a cheap capacitive fingerprint sensor captures DB2's fingerprint. In addition, a small or unrepresentative dataset was used to train and test the system, which may not have sufficiently captured the variety of fingerprints that might be seen in real-world circumstances. Moreover, the algorithm used to compare and match the extracted minutiae is unreliable enough to match the characteristics precisely. It lacks the intelligence needed to deal with variances in fingerprint patterns and accept slight variations between samples.

In the proposed system, processing speed is a crucial factor. Customers have very high expectations for the quickness of the transaction when using contactless cards. They anticipate a quick and secure transaction. As a result, this article assessed the system's matching time and transaction time for speed. The time it takes to validate the transaction and check the cardholder's details is called the "time of matching" in a contactless card transaction. The system design and implementation details will determine how this matching time affects cardholder notification. In general, for a seamless and practical user experience, the matching time should be as quick as possible. The cardholder anticipates a timely response to complete the transaction when they initiate a contactless card transaction. The cardholder may experience delays and inconveniences due to excessively long matching times, which may frustrate them and alter how they see the transaction process. Fast matching times guarantee the cardholder can complete their transaction quickly and easily, with little waiting. It is crucial to remember that the authentication process' security and correctness should not be jeopardized by the matching time. While speed is desirable, the accuracy and efficiency of the matching process should not be sacrificed in the name of speed. To guarantee convenience and security for contactless cardholders, it is essential to balance quick matching and strong authentication.

6- CONCLUSIONS AND FUTURE WORK

In order to prevent unauthorized access and fraudulent transactions, this research studied the integration of fingerprint authentication using minutiae-based feature extraction and matching approaches with contactless banking cards. Contactless banking cards now have an extra level of protection through fingerprint authentication. Additionally, a convenient and smooth user experience is provided by combining fingerprint authentication with contactless banking cards to validate their identity rather than using PINs or passwords. Therefore, cardholders can complete contactless transactions quickly, increasing efficiency and reducing terminal wait times.

The proposed system in this paper has been developed virtually. In order to test and evaluate the system, two fingerprint verification competition datasets have been used. These two datasets cover a range of image quality since they attempt to depict real-world scenarios. Each database is split into two groups for evaluation. As a fingerprint template, the first group is utilized. The second one is employed to create freshly acquired fingerprints. Minutiae points, ridge ends, bifurcations, and other ridge structures must be extracted for fingerprint matching and identification. Therefore, in both the enrolment and verification processes, the images need to be pre-processed to enhance the quality, clarity, and distinctiveness of the biometric characteristic (fingerprint). The FAR and FRR values show a balanced performance of the system in terms of false acceptance and false rejection rates. This means there is an equal chance that the system will make errors in both directions. This showed that the suggested solution cannot efficiently discriminate between authorized and legitimate users. The algorithm used to compare and match the extracted minutiae is unreliable enough to match the characteristics precisely. It lacks the intelligence needed to deal with variances in fingerprint patterns and accept slight variations between samples. However, in the proposed system, processing speed is a crucial factor. When it comes to using contactless cards, customers have very high expectations for the speed of the transaction. They expect the transaction to be fast and safe.

It is possible to investigate more sophisticated and reliable feature extraction methods. Beyond minutiae points, such as ridge orientation, texture, and pores, new fingerprint traits are being looked into. The system's ability to discriminate between data sets and increase matching accuracy can be improved using various attributes. In addition, for more accurate matching, fingerprint image quality can be improved. Preprocessing approaches that solve typical problems such as inadequate image resolution, noise, distortion, and incomplete or overlapping fingerprints can be developed through future work. It is possible to investigate denoising algorithms, image-enhancing methods, and image completion strategies to enhance the overall quality of fingerprint images.

Furthermore, accessing large-scale and diverse fingerprint databases can facilitate the developing and evaluating of more precise matching algorithms. Matching algorithms can be trained and tested more successfully by gathering extensive datasets covering various demographic characteristics, ambient circumstances, and sensor variations. This makes it possible to generalize and evaluate performance in diverse real-world settings more accurately.

7- REFERENCES

Matyushok, V., Krasavina, V., Berezin, A., & García, J. S. (2021). The global economy in technological transformation conditions: A review of modern trends. *Economic Research-Ekonomska Istraživanja, 34*(1), 1471-1497.

Aron, J., & Muellbauer, J. (2019). *The Economics of Mobile Money: harnessing the transformative power of technology to benefit the global poor.* Oxford: Centre for the Study of African Economies.

Kandpal, V., & Mehrotra, R. (2019). Financial Inclusion: The Role Of Fintech And Digital Financial Services In India. *Indian Journal of Economics & Business, 19*(1), 85-93.

Kang, S.-G., Song, M. S., K. J., Lee, J. W., & Kim, J. (2021). Near-field communication in biomedical applications. *Sensors, 21*(3), 703.

Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & Moorsel, A. v. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100*, 408-427.

Gerpott, T. J., & Meinert, P. (2018). Termination notice of mobile network operator customers after a tariff switch: An empirical study of postpaid subscribers in Germany. *Telecommunications Policy, 42*(3).

Zhao, H., Anong, S., & Zhang, L. (2019). Understanding the impact of financial incentives on NFC mobile payment adoption. *International Journal of Bank Marketing, 37*(5), 1296-1312.

Al-Maliki, O., & Al-Assam, H. (2021). Challenge-response mutual authentication protocol for EMV contactless cards. *Computers & Security, 103*, 102186.

Klimek, L. (2020). Misuse of contactless payment cards with radio-frequency identification. *Masaryk University Journal of Law and Technology, 14*(2), 259 - 274.

Kılınç, H., & Vaudenay, S. (2018). Secure contactless payment. *Information Security and Privacy: 23rd Australasian Conference, ACISP 2018, Wollongong, NSW, Australia, July 11-13, 2018, Proceedings 23., Springer International Publishing.*

Furkan Altınok, K., Peker, A., Tezcan, C., & Temizel, A. (2022). GPU accelerated 3DES encryption. *Concurrency and Computation: Practice and Experience, 34*(9), 36507.

Al-Maliki, O., & Al-Assam, H. (2022). A tokenization technique for improving the security of EMV contactless cards. *Information Security Journal: A Global Perspective, 31*(5), 511 - 526.

Akinyokun, N., & Teague, V. (2017). Security and privacy implications of NFC-enabled contactless payment systems. *Proceedings of the 12th international conference on availability, reliability and security*.

Ramesh, V., Jaunky, V. C., Roopchund, R., & Sigh, O. H. (2019). Customer satisfaction', loyalty and 'adoption'of e-banking technology in Mauritius. *Embedded Systems and Artificial Intelligence: Proceedings of ESAI 2019* (pp. 861-873). Fez, Morocco: Springer Singapore.

Sportiello, L. (2019). "Internet of Smart Cards": A pocket attacks scenario. *International Journal of Critical Infrastructure Protection, 26*, 100302.

Lan, X., Xu, J., Zhang, Z., Chen, X., & Luo, Y. (2023). A systematic security analysis of EMV protocol. *Computer Standards & Interfaces, 84*, 103700.

Yang, M.-H., Luo, J.-N., Vijayalakshmi, M., & Shalinie, S. M. (2022). Contactless Credit Cards Payment Fraud Protection by Ambient Authentication. *Sensors, 22*(5), 1989.

El Madhoun, N., Bertin, E., & Pujolle, G. (2018). An overview of the EMV protocol and its security vulnerabilities. *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ).* IEEE.

Akter, S., Chellappan, S., Chakraborty, T., Khan, T. A., Rahman, A., & Al Islam, A. A. (2020). Man-in-the-middle attack on contactless payment over NFC communications: design, implementation, experiments and detection. *IEEE Transactions on Dependable and Secure Computing , 18*(6), 3012 - 2023.

Goode, A. (2018). Biometrics for banking: best practices and barriers to adoption. *Biometric Technology Today, 10*, 5 - 7.

Suwald, T., & Rottschäfer, T. (2019). Capacitive fingerprint sensor for contactless payment cards. *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)* (pp. 241 - 245). IEEE.

Yadav, S., & Mathuria, M. (2015). Fingerprint recognition based on minutiae information. *International Journal of Computer Applications, 120*(10).

Bhargava, N., Kumawat, A., & Bhargava, R. (2015). Fingerprint matching of normalized image based on Euclidean distance. *Int. J. Comput. Appl , 120*(24), 20 - 23.

Babatunde, I. G. (2015). Fingerprint matching using minutiae-singular points network. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 8*(2), 375 - 388.

Boujnah, S., Jaballah, S., Khalifa, A. B., & Ammar, M. L. (2018). Person's Identification with Partial Fingerprint Based on a Redefinition of Minutiae Features. *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)* (pp. 1- 5). IEEE.

Agarwal, D., Garima, & Bansal, A. (2021). A utility of ridge contour points in minutiae-based fingerprint matching. *Proceedings of International Conference on Computational Intelligence and Data Engineering: ICCIDE 2020.* Springer Singapore.

Hambalık, P. M.—A. (2016). Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation. *Tatra Mt. Math. Publ, 67*, 117 - 134.

Zhang, F., Xin, S., & Feng, J. (2019). Combining global and minutia deep features for partial high-resolution fingerprint matching. *Pattern Recognition Letters, 119*, 139 - 147.

Chowdhury, A., Kirchgasser, S., Uhl, A., & Ross, A. (2020). Can a CNN automatically learn the significance of minutiae points for fingerprint matching? *In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, (pp. 351 - 359).

Zukarnain, Z. A., Muneer, A., & Ab Aziz, M. K. (2022). Authentication securing methods for mobile identity: Issues, solutions and challenges. *Symmetry, 14*(4), 821.

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry, 11*(2), 141.

Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence , 20*(8), 777 - 789.

Patel, M. B., Parikh, S. M., & Patel, A. R. (2019). Performance improvement in preprocessing phase of fingerprint recognition. *Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2018. 2.* Springer Singapore.

Zhang, T. Y., & Suen, C. Y. (1997). A fast parallel algorithm for thinning digital patterns. *Communications of the ACM, 27*(3), 337 - 343.

Suwarno, S., & Santosa, I. (2019). Simple verification of low-resolution fingerprint using non-minutiae feature. *Journal of Physics: Conference Series, 1196*(1), 012062.

Kaur, M., Singh, M., Girdhar, A., & Sandhu, P. S. (2008). Fingerprint verification system using minutiae extraction technique. *International Journal of Computer and Information Engineering, 2*(10), 3405 - 3410.

George, J., & Gladston Raj, S. (2021). Leaf Identification using Harris Corner Detection, SURF Feature and FLANN Matcher. *Int. J. Innov. Technol. Explor. Eng, 8*(8).

Kurnaz, S., & Mohammed, H. (2020). Secure pin authentication in java smart card using honey encryption. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1 - 4). IEEE.

Kaur, N. (2021). A study of biometric identification and verification system. *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE).* IEEE.

Chaudhari, A. S., Lade, S., & Pande, D. S. (2014). Improved Technique for Fingerprint Segmentation. *Int. J. Adv. Res. Comput. Sci. Manag. Stud, 2*, 402 - 411.

Liu, L. M. (2013). A RFID controller with contactless cards for internet of things. *Applied Mechanics and Materials., 336*, 2521 - 2524.

Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International journal of computer vision, 60*, 91 - 100.

Bounie, D., & Youssouf, C. (2020). Card-sales response to merchant contactless payment acceptance. *Journal of Banking & Finance, 119*(105938).

Singh, G., Kaushik, D., Handa, H., Kaur, G., Chawla, S. K., & Elngar, A. A. (2021). BioPay: A Secure Payment Gateway through Biometrics. *Journal of Cybersecurity and Information Management (JCIM), 7*(2), 65 - 76.

Lavadkar, M. A., Thorat, P. K., Kasliwal, A. R., Gadekar, J. S., & Deshmukh, D. P. (n.d.). Fingerprint Biometric Based Online Cashless Payment System. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 27 - 32.

AliBabaee, A., & Broumandnia, A. (2019). Biometric authentication of fingerprint for banking users, using stream cipher algorithm. *Journal of Advances in Computer Research, 9*(4), 1-17.

Biometric. (2014). Mastercard And Zwipe Launch Fingerprint Payment Card As Alipay Looks To Biometrics. *Biometric Technology Today., 11*(1).

Mehr Nezhad, M., & Hao, F. (2021). OPay: an Orientation-based Contactless Payment Solution Against Passive Attacks. *Annual Computer Security Applications Conference.*

Dommaraju, B. T., Kondaveeti, D. S., Katta, S., Devanaboina, V. N., & Cherukupalli, N. L. (2023). Fingerprint Sensor based Biometric Payment Cards. *2023 7th International Conference on Computing Methodologies and Communication (ICCMC).* IEEE.