INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

# Solution for Public Smart Dispenser Using Digital Payment Based on the Fingerprint Minutiae Algorithm

Jumadi Mabe Parenreng [a,*], Nur Fadiah [a], Irmawati Irmawati [b], Syahrul Syahrul [a], Abdul Wahid [c], M. Syahid Nur Wahid [a]

[a] *Informatics and Computer Engineering Department, Universitas Negeri Makassar, Makassar, Indonesia*
[b] *Accounting and Business Department, Universitas Patria Artha, Makassar, Indonesia*
[c] *English Department, Universitas Negeri Makassar, Makassar, Indonesia*

*Corresponding author: *jparenreng@unm.ac.id*

***Abstract*—Technological advancements have significantly focused on secure and efficient digital payments. In the context of Public Smart Dispensers (PSDs), using authentication and verification in payment transactions is crucial to address security concerns, enhance transaction efficiency, and provide a better user experience. This study employs minutiae algorithms for the fingerprint identification and verification process. Fingerprint identification utilizes the crossing number method, while fingerprint verification uses a validation score. If the validation score exceeds the threshold of >80, fingerprint verification is considered successful; conversely, verification is deemed unsuccessful if the validation score is <80. Through testing, biometrics as a payment method was conducted 100 times, resulting in an accuracy rate of 94% with an identification response time of approximately two or three seconds. The research findings demonstrate the practicality of implementing fingerprint biometric payment methods with minutiae algorithms on Public Smart Dispenser payment systems in the field of digital payments and technology. This enables fast and efficient transactions, significantly reducing the risk of fund misuse. Consequently, users can easily access water through Public Smart Dispensers, underscoring the real-world applicability and relevance of this solution. Implementing this technology can enhance user comfort and security while expediting the transaction process, which is crucial for public use. Therefore, this research makes a significant contribution to the advancement of fingerprint-based payment technology on public smart dispensers.**

***Keywords*— Public smart dispenser; biometric; transaction; minutiae.**

*Manuscript received 5 Apr. 2024; revised 29 Jul. 2024; accepted 12 Oct. 2024. Date of publication 30 Nov. 2024.*


## I. INTRODUCTION

A Public Smart Dispenser is a device that provides the general public with clean water. It gives customers who have already completed a transaction or payment access to drinking water. Electronic money, or e-payment, is used to make payments. Thanks to this, people can receive clean water more simply and conveniently. The swift progress of information and communication technology (ICT) has had a significant influence on many facets of human existence, especially when it comes to financial transactions [1], [2]. Debit cards, e-wallets, and other digital payment methods have become widely used as a result, completely changing the way we handle our money [3]. When it comes to digital payment methods, e-payment has become a popular option for consumers looking for non-cash transaction methods [4]. The process of making an electronic payment entails keeping money in an electronic wallet or e-wallet [5]. With every transaction, the value in the e-wallet decreases, but it may be added back up as needed [6], [7].

When compared to traditional banking methods[8], e-payments are more convenient and expedient in terms of transaction speed. In addition to saving consumers time, it gives them a sense of security and comfort when completing transactions whenever and wherever they choose [9], [10]. E-payments can also lower the expenses related to printing and distributing real currency, increasing its financial efficiency [11], [12], [13].

However, information security and privacy are critical with the surge in data breach cases and difficulties globally, including identity theft, credit card fraud, and cybercrime [14]. Uninformed individuals concerning information security leave room for careless parties to exploit someone's

personal information. Privacy and information security must, therefore, be appropriately safeguarded [15], [16].

E-wallets are a payment technique that is becoming increasingly common [17]. Maintaining e-money security techniques such as PINs, passwords, and cards are vulnerable to guesswork, human error, hacking, and physical card loss[18]. Biometric authentication—specifically, fingerprint recognition—is a viable way to improve e-wallet security to overcome these constraints. The use of fingerprint biometric authentication for e-wallet transactions is investigated in this study [19], [20], [21].

Fingerprint-based authentication techniques use the detection of distinct fingerprint features to confirm or validate a person's identity[22]. Every person has a distinct, permanent [23], and hard-to-copy fingerprint [24], [25], [18]. The patterns of ridges, valleys, and minutiae—tiny[26] points found on the surface of the fingers—give fingerprints their distinctiveness [27], [28]. Because minutiae differ in quantity and position between persons, they serve as a means of individual identification [29]. This study uses minutiae algorithms to extract and compare fingerprints based on minute traits. Because minutiae range in quantity and location among individuals, they act as a distinguishing factor between them [30], [31].

Biometric technology has made extensive use of fingerprint authentication methods in the context of digital payments[20], [32]. Compared to other biometric techniques, this method has several benefits, such as high accuracy, dependability, and simplicity of fingerprint acquisition. Fingerprint sensors allow for the fast and precise capturing of an individual's fingerprint [33], [34]. This fingerprint that has been taken acts as the person's only key or password [29], [35], [36]. The fingerprint identification verification process is quick to complete, taking only a few seconds [37], making transactions quick and easy [38], [39].

Previous research on the use of fingerprints as authentication for e-wallet usage. This research proves that digital wallet payment solutions can be improved with ease of access. The prototype evaluation results show that the fingerprint authentication mechanism performs securely and satisfies its users. In this study, an aspect assessment between the fingerprint model and the traditional model was conducted. The assessment results from the elderly show that the fingerprint model is more attractive than the traditional model in terms of usability, efficiency, satisfaction, memorability, and security. Meanwhile, the experts showed that the fingerprint model is better than the traditional model in terms of usability, efficiency, satisfaction, and security. The use of fingerprints as authentication also proves that the transaction process cannot proceed without the involvement of the actual owner [20]. Other studies are developing a multi-card smart card payment system that uses fingerprints to authenticate the card's PIN [40].

The following study examines how vending machine fingerprint payment methods are used to obtain user permission. His research's findings showed that two tests—user approval testing and payment system security testing—were conducted. The suggested method can pass security testing and avoid the risks associated with user top-ups, duplicate card usage, and card usage that does not belong to the user. The suggested solution demonstrates through user approval testing that consumers are at ease with the fingerprint payment technique [41]. Other studies also apply a security system to motorcycles [42]. The subsequent research implemented a minutiae score-matching algorithm on the .NET platform using 100 fingerprint images. The results of the study show that the developed algorithm is effective and has a high accuracy rate in matching fingerprint images by calculating the similarity score between the original image and the registered image [43]. other research on biometric identification systems. This research uses three biometrics, namely fingerprints, veins, and faces. This research performs fingerprint validation first, then vein validation, and then face validation. After that, the fusion level is carried out to determine the decision level of the validation results. The results of this study show superior performance in terms of accuracy [44].

From the discussion and previous research, digital payment using biometric fingerprints and the use of minutiae algorithms as a fingerprint authentication method can be the right solution to overcome the problem of fake fingerprints; easy and provide security in the payment transaction process so that this can be a solution for the public smart dispenser in transactions. The use of this fingerprint has a high level of accuracy, efficiency, and security. In addition, the minutiae algorithm is unique, difficult to imitate, and fast in minutiae extraction. These advantages should be considered when applying fingerprints as a payment method for Public Smart Dispenser. Thus, fingerprint payment is the right choice for the community to get drinking water efficiently, accurately, and safely through the Public Smart Dispenser.

## II. Materials and Method

This section describes implementing the payment method at PSD using fingerprints.

### *A. System Scheme*

Figure 1 shows the system scheme to determine the flow design of this system. First, the customer visits the Public Smart Dispenser and purchases drinking water. After that, the customer does a fingerprint for the transaction process. The fingerprint is used as a sample or input. Then, the minutiae algorithm extracts fingerprints that are later matched with fingerprints in the database.

After that, fingerprint matching is carried out between the fingerprint sample and the fingerprint in the database using the minutiae algorithm. If the fingerprint matches, verification is complete, which will later deduct the balance on the DANA payment, and the transaction is complete. Finally, the Public Smart Dispenser fills the water.

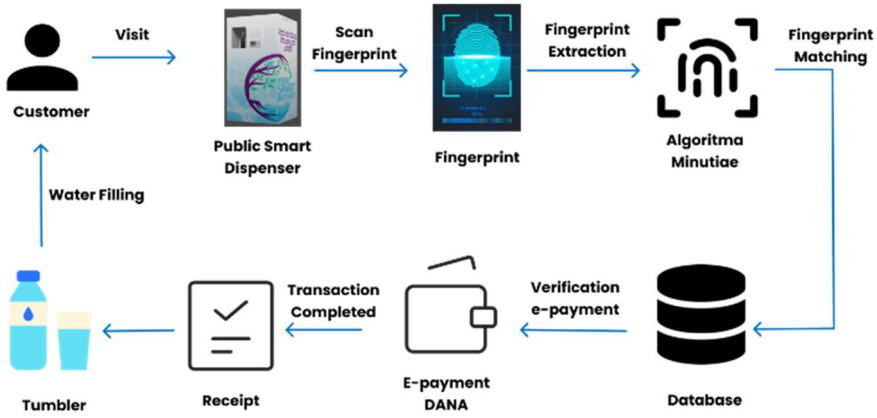


Fig. 1 System scheme

## B. Fingerprint System

Fingerprinting systems utilize the unique patterns on the skin surface of human fingertips for identification or authentication purposes, where fingerprint images are taken, fingerprint features are extracted, and then compared with data stored in a database to produce a match or mismatch [45]. Here is the workflow of a fingerprint biometric system [46], [47].

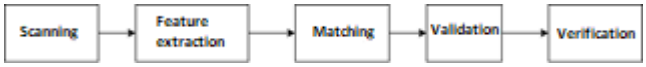


Fig. 2 Fingerprint system

Figure 2 shows the scheme of fingerprint biometrics. From the picture, it starts with scanning, which is inputting fingerprints using a sensor. Then, proceed with feature extraction, detecting fingerprint minutiae formed from skin streaks on fingerprints such as ridge ending and ridge bifurcation. Then, the matching process looks for the same fingerprint points between the stored fingerprints and the fingerprints inputted from the sensor [48]. In this study, the matching calculation process uses the crossing number method, where the crossing number value is taken from the ridge bifurcation and ridge ending values, as shown in Figure 3.

```
Algorithm: Ridge Detection

Input: Binary image matrix
Output: Detection of Ridge Bifurcation and Ridge Ending

1. For i ← 1 to rows do
2.   For j ← 1 to cols do
3.     If i = j then
4.       Examine neighboring pixels p1, p2, p3, p4, p5, p6, p7, p8, p9
5.       Set weight ← 0

6.       For each pixel p in {p1, p2, p3, p4, p5, p6, p7, p8, p9} do
7.         If pixel p = 255 then
8.           Increment weight by 1
9.         End If
10.      End For

11.      If weight = 3 then
12.        Mark pixel as Ridge Bifurcation
13.      End If

14.      If weight = 1 then
15.        Mark pixel as Ridge Ending
16.      End If
17.    End If
18.  End For
19. End For
```

Fig. 3 Pseudocode ridge detection

Then, the validation score calculation is carried out to verify the fingerprint. At the validation stage, the validation limit is checked to continue the verification process. The following is pseudocode in the extraction of ridge ending and ridge bifurcation of the crossing number method [49].

## C. Payment Mechanism

*1) Scanning Fingerprint*: Fingerprint scanning is done using image capture using a camera or fingerprint sensor [50]. In Figure 4 is a fingerprint image capture that has been converted to a gray color level or the process of changing to grayscale [51].

Fig. 4 Scanning fingerprint

*2) Fingerprint Minutiae Extraction*: In fingerprint extraction that will be used as a unique pattern of fingerprints, namely ridge ending and ridge bifurcation points [52]. The ridge ending is the end point of fingerprint strokes. While ridge bifurcation is the branching point of the fingerprint stroke [53]. These points will later be matched to the position of the ridge ending point and the ridge bifurcation point [54], [55]. A comparison process between existing fingerprints in the database and fingerprint input will carry out this matching [24]. For the fingerprint extraction process use the point end method and point bifurcation so that it can get a fingerprint trajectory line to find out the points of ridge ending and ridge bifurcation [56]. Figure 5 is a fingerprint extraction process where the ridge ending points and ridge bifurcation points are known.

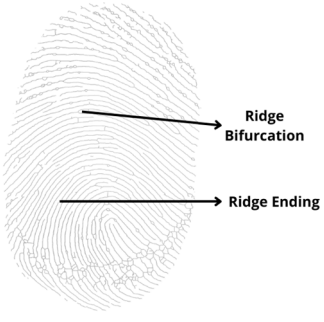


Fig. 5 Fingerprint feature extraction

*3) Matching Fingerprint*: The matching process is done by comparing the position of the extracted points in the database and fingerprints when doing fingerprints on the sensor [57]After that, the match is calculated, producing the validation score results. Here's an example of the fingerprint-matching process.

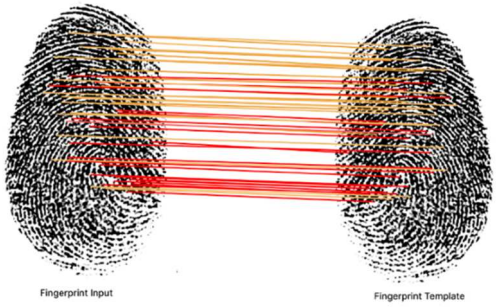


Fig. 6 Example of a matched fingerprint

Figure 6 shows the matching process for a matched fingerprint. The process is viewed from the position of the fingerprint points when taking the fingerprint and the fingerprint stored in the database during fingerprint registration. The position of the fingerprint points between the two fingerprints is said to be matched.

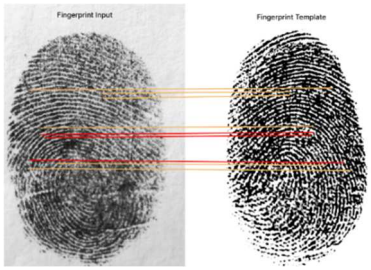


Fig. 7 Example of a mismatched fingerprint

The matching procedure for a fingerprint that does not match is shown in Figure 7. It is clear from this procedure that there is a notable difference in the way fingerprint minutiae (points) are arranged. Even when there are a few tiny points that match, the matching score is decreased by their small quantity. As a result of this disparity, the fingerprints are considered to be unmatched, and the fingerprint verification procedure is unsuccessful [58].

*4) Crossing Number*: The score calculation process is carried out after the scanning and feature extraction processes are completed. The crossing number calculation process can be observed in Figure 8. A ridge ending minutiae is assigned a value of 1, while a ridge bifurcation minutiae is assigned a value of 3 [49], [59], [60].

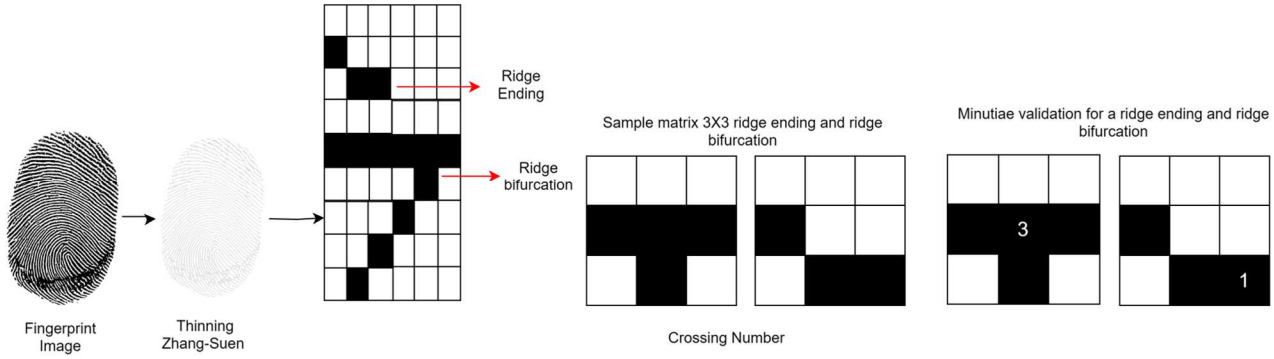


Fig. 8 Crossing number

Following the scoring of each detail, the following formula will be used to calculate the matching score [61], [62], [63]:

$$Match\ score = \frac{Number\ of\ matching\ minutiae}{Number\ of\ minutiae\ in\ template} \quad (1)$$

*5) Validation Fingerprint*: In the fingerprint validation process, the matching process is carried out first before it is said to be successful or the verification fails. then, a comparison is made by checking the suitability of the fingerprint. If the match score exceeds or exceeds 80, then the verification is successful and can continue the transaction. Still, if the match score is less than 80, then the verification fails and cannot continue the transaction. Factors that affect the fingerprint match score are minutiae points such as ridge ending and ridge bifurcation, and the number of matching minutiae at the same location in both prints can also increase the match scor e[27]. The following Figure 9 explains the flow of the decision-making process of the fingerprint matching process.

```
Algorithm: Fingerprint Validation

Input: user_fingerprint, database_fingerprints
Output: verification_result

1. Set Accuracy_threshold ← 0.80
2. user_fingerprint ← read_fingerprint_from_sensor()
3. user_fingerprint_features ← extract_features(user_fingerprint)
4. database_fingerprints ← read_database_fingerprints()
5. verification_result ← "Verification failed"
6. For each database_fingerprint in database_fingerprints do
7.    database_fingerprint_features ← extract_features(database_fingerprint)
8.    accuracy_level ← calculate_accuracy(user_fingerprint_features, database_fingerprint_features)
9.    If accuracy_level ≥ Accuracy_threshold then
10.       verification_result ← "Verification successful"
11.       Break
12. End For
13. If verification_result = "Verification successful" then
14.    Display "Verification successful. Proceeding with the transaction."
15.    Process_transaction()
16. Else If verification_result = "Verification failed" then
17.    Display "Verification failed. Transaction canceled."
```

Fig. 9 Validation fingerprint algorithm

*6) Transaction in Public Smart Dispenser*: The following is the fingerprint transaction mechanism when the customer purchases.

```
Algorithm: Transaction PSD

input: ml_of_water
output : Messages indicating the status of the water purchase process, such as successful transaction,
insufficient balance, or fingerprint mismatch.

1. Input ml_of_water
2. Display "Step 1: Water Purchase Process"
3. Display "Select the number of ml of water: " + ml_of_water
4. Display "Step 2: Please place your finger on the PSD fingerprint sensor."
5. Read customer_fingerprint_data_from_sensor()
6. Verification_result ← Match_fingerprint_with_database(customer_fingerprint_data_from_sensor)
7. If Verification_result = "Fingerprint matches" then
8.    Display "Fingerprint matches. Proceeding to the next step."
9.    Display "Step 3: Checking balance and balance intersection."
10.   balance_check ← check_balance_and_balance_intersection()
11.   If balance_check = True then
12.       Display "Sufficient balance. Transaction successful."
13.       Open the dispenser faucet
14.       Fill the customer's drinking bottle
15.   Else
16.       Display "Insufficient balance. Transaction canceled."
17. Else
18.   Display "Fingerprint does not match. Please try again."
```

Fig. 10 Transaction psd algorithm

Figure 10 shows the transaction mechanism in PSD. First, the user enters the amount of water (ml) to be purchased. Then, fingerprinting is done for fingerprint reading. After that, fingerprint matching is done with those stored in the database. A balance check is carried out to see if the fingerprint matches and a balance deduction is made for drinking water payments. If the balance is insufficient, the transaction is canceled. However, if the fingerprint does not match, the user is again asked to fingerprint. The final stage of the water filling process. It should be noted that before making a transaction, the user needs to register an account first.

### *D. Hardware Prototype*

The following is a prototype of the tool that was built. the components used are esp32 [64], [65], fpm10a fingerprint [65], [66], [67] and breadboard.

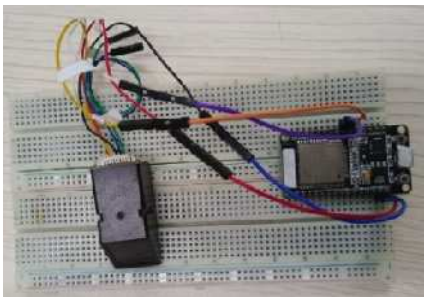

Fig. 11 Hardware prototype

The specifications of the tools used can be seen in the following table.

TABLE I
FINGERPRINT SENSOR MODULE SPECIFICATIONS

| Parameter | Values |
|---|---|
| power supply voltage | 3.6 – 6v |
| window size | 14x18 mm |
| template file | 512byte |
| storage capacity | 163 templates |
| fingerprint image input time | <1 second |
| search time | <1 second (Average 1:500) |

TABLE II
ESP 32 SPECIFICATIONS

| Parameter | Values |
|---|---|
| GPIO | 34 |
| Voltage | 3.3v |
| UART | 3 |
| 12C | 2 |
| SPI | 3 |
| ADC | 7 |
| RAM | 520K |

## III. RESULTS AND DISCUSSION

This research collected data from 10 individuals, each with 10 trials, resulting in 100 data points. Data collection was conducted using an FPM10A fingerprint sensor as the fingerprint scanner and an ESP32 as the microcontroller. Table 3 presents the collected fingerprint verification data. Data with a checkmark (√) indicates a matching fingerprint, a (X) indicates a non-matching fingerprint, and a dash (-) indicates an unregistered fingerprint. This data is based on the scores obtained each time a fingerprint is scanned. The fingerprint is considered matching if the matching score is greater than 80. Conversely, the fingerprint is considered non-matching if the score is less than 80. This can be seen in Table 4.

TABLE III
FINGERPRINT MATCHING DATA

| Id Fingerprint | Testing | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | `5 | 6 | 7 | 8 | 9 | 10 |
| #1 | √ | X | √ | √ | X | √ | √ | √ | √ | √ |
| #2 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #3 | √ | √ | √ | √ | X | √ | √ | √ | √ | √ |
| #4 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #5 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #6 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #7 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #8 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #9 | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| #10 | √ | - | - | √ | √ | √ | √ | √ | X | √ |

TABLE IV
FINGERPRINT MATCH SCORE DATA

| Id Fingerprint | Nama | Testing | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | `5 | 6 | 7 | 8 | 9 | 10 |
| #1 | akbar | 98 | 66 | 105 | 95 | 77 | 90 | 95 | 105 | 145 | 135 |
| #2 | fadiah | 178 | 117 | 335 | 150 | 155 | 135 | 119 | 145 | 156 | 178 |
| #3 | fahril | 168 | 182 | 142 | 162 | 80 | 160 | 211 | 95 | 214 | 229 |
| #4 | sasa | 102 | 117 | 131 | 150 | 91 | 115 | 150 | 127 | 141 | 114 |
| #5 | dafa | 263 | 318 | 160 | 164 | 151 | 305 | 228 | 123 | 115 | 151 |
| #6 | nurul | 287 | 247 | 313 | 361 | 416 | 328 | 308 | 238 | 430 | 258 |
| #7 | sahal | 202 | 493 | 309 | 432 | 462 | 196 | 205 | 142 | 131 | 163 |
| #8 | lalisa | 230 | 139 | 119 | 230 | 325 | 247 | 251 | 390 | 333 | 356 |
| #9 | upan | 262 | 221 | 297 | 112 | 105 | 128 | 140 | 121 | 298 | 238 |
| #10 | nanda | 249 | 0 | 0 | 219 | 203 | 141 | 195 | 186 | 76 | 222 |

Table 4 shows that there are fingerprints with matching scores below 80 and are not detected for several reasons. One reason is damaged fingerprints, such as peeling skin, wounds, or scratches. In addition, dirty fingerprints or differences in position during registration and validation and unregistered fingerprints can also cause non-detection. On the other hand, fingerprint data with validation scores above 80 is usually good, meaning it is not wet or dirty and is in the correct position during registration.

### A. Classification of Fingerprint Validity

*1) Valid*: As shown in Figure 12, valid fingerprint testing is performed on fingerprints that have validation scores more than 80. The procedure for taking a fingerprint image, which is then transformed or feature extracted, is depicted in the figure. Subsequently, it was discovered that the fingerprint, which had a validation score of 238, was on ID #9.

```
Image taken
Image converted
Fingerprint found.
Found ID #9 with confidence of 238
```

Fig. 12 Matching fingerprint test results

$$FAR = \frac{False\ Acceptance}{False\ Acceptance+True\ Rejects} \quad (2)$$

In the meantime, the system has accepted all fingerprints that should have been rejected, as indicated by the FAR of 0%. This shows how well the technology rejects erroneous fingerprints.

*2) Invalid*: Invalid fingerprint testing can be caused by several factors, such as a fingerprint that has yet to be registered or a validation score below the specified threshold of 80. This can be seen in Figure 13 for an invalid fingerprint due to lack of registration and Figure 14 for an invalid fingerprint due to a score below the validation threshold.

```
Image taken
Image converted
Fingerprint not registered
```

Fig. 13 Unregistered fingerprint test result

Figure 13 shows the results of testing unregistered fingerprints. Where there is an image taken that the fingerprint image is captured and then converted or feature extraction is carried out. Then there is fingerprint not registered information that the fingerprint is not registered. This is because the user has never done a fingerprint before.

```
Image taken
Image converted
Fingerprint not found
Found ID #1 with confidence of 66
```

Fig. 14 Fingerprint test results below the threshold

Figure 14 shows the results of the non-matching fingerprint test. For ID #1, there is information that the fingerprint was not found, with a validation score of 66. This is due to a damaged and dirty fingerprint.

$$FRR = \frac{False\ Rejection}{False\ Rejection+True\ Acceptance} \quad (3)$$

FRR= 0.06 was obtained at 6%, which indicates that 6% of fingerprints should have been accepted validly but were rejected by the system.

### B. Fingerprint Accuracy

Based on the experimental data in Table 3. There are 100 experimental data collected. This data calculates the accuracy level of using fingerprints as a payment method solution in public smart dispensers.

$$Accuracy = \frac{Amount\ of\ correct\ data\ x\ 100\%}{Amount\ of\ data} \quad (4)$$

Accuracy = 94 %; the calculation results show a system accuracy rate of 94%. This indicates the system's excellent ability to identify fingerprints from the total number of fingerprints tested correctly.

### C. Fingerprint Response Time

Table 4 displays the fingerprint trial data used to determine the fingerprint reading speed based on fingerprint usage. With an average reading speed of two seconds, the test result data demonstrates how quickly fingerprints may be detected. The high accuracy rate and the two-second average fingerprint reading speed demonstrate how simple it is for consumers to utilize fingerprints as a digital payment method.

TABLE V
RESPONSE TIME TESTING DATA

| Id Fingerprint | Computation Time | |
|---|---|---|
| | Detected | Speed |
| #1 | √ | 2 second |
| #2 | √ | 3 second |
| #3 | √ | 2 second |
| #4 | √ | 2.1 second |
| #5 | √ | 2 second |
| #6 | √ | 2 second |
| #7 | √ | 2.2 second |
| #8 | √ | 2 second |
| #9 | √ | 3 second |
| #10 | √ | 2 second |

### D. Comparison of Fingerprint Validation Algorithms

Here, in Table 5, several algorithms are comparable in fingerprint validation.

TABLE VI
COMPARABLE IN FINGERPRINT VALIDATION

| Algorithm | Accuracy Rate % |
|---|---|
| Siamese Rectangular Convolutional Neural Networks (SRCNN)[68] | <75% |
| minutiae matching algorithm[55] | 80% |
| Neural Network[69] | 91.10% |
| Hybrid Minutiae Feature Extraction Method[70] | 85.28% |
| Current Research Minutiae Algorithm Crossing Number Method and Score Match | 94% |

Table 5 shows the accuracy level of each other fingerprint validation algorithm in fingerprint detection. The table shows that the offered algorithm has a good level of accuracy compared to other algorithms. The offered algorithm performs ridge ending and ridge bifurcation fingerprint feature extraction. Then, the crossing number is done for weighting, and then the match score is calculated, exceeding the threshold of 80.

## IV. CONCLUSION

Based on the test results, it can be concluded that using a minutiae algorithm with the crossing number and confidence level method in fingerprint identification can provide a very high level of accuracy, reaching 94% of the total 100 data tested. This shows that this research has the potential to be a new solution in implementing payment methods on public smart dispensers. An analysis of the device's performance shows that the device has an error rate of 6% and a success rate of 94% in scanning fingerprints. In addition, the device shows a fast response, with a response time of between 2 and 3 seconds when tested. In conclusion, this fingerprint identification method is accurate and efficient, making it a viable choice for digital payment systems on public devices. Implementing this technology can improve user comfort and security and speed up the transaction process, which is very important in the context of public use. Thus, this research significantly contributes to developing fingerprint-based payment technology on public smart dispensers.

## ACKNOWLEDGMENT

This research was conducted through the collaboration of the Research Team and Research Student from Matching Fund Kedaireka, with the support of Makassar State University, Wahdah Water as the research partner, and the Ministry of Education under contract number 0219/E/KS.03.00/2023

## REFERENCES

[1] Vandana and N. Kaur, "A Study of Biometric Identification and Verification System," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 60–64. doi: 10.1109/ICACITE51222.2021.9404735.

[2] R. A. Kasri, B. S. Indrastomo, N. D. Hendranastiti, and M. B. Prasetyo, "Digital payment and banking stability in emerging economy with dual banking system," *Heliyon*, vol. 8, no. 11, Nov. 2022, doi:10.1016/j.heliyon.2022.e11198.

[3] K. Khando, M. S. Islam, and S. Gao, "The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review," *Future Internet*, vol. 15, no. 1, pp. 1–21, Jan. 2023, doi:10.3390/fi15010021.

[4] A. Chelvarayan, S. F. Yeo, H. Hui Yi, and H. Hashim, "E-Wallet: A Study on Cashless Transactions Among University Students," *F1000Res*, vol. 11, p. 687, 2022, doi:10.12688/f1000research.73545.1.

[5] A. R. Kurniawan, R. Imam, R. F. Zhalifunnas, A. R. Putra, F. L. Gaol, and T. Matsuo, "Use of E-Wallet as a Substitute for Physical Money in Transactions at Malls," in *Inventive Computation and Information Technologies*, S. Smys, K. A. Kamel, and R. Palanisamy, Eds., Singapore: Springer Nature Singapore, 2023, pp. 441–450.

[6] M. Yang, A. Al Mamun, M. Mohiuddin, N. C. Nawi, and N. R. Zainol, "Cashless transactions: A study on intention and adoption of e-wallets," *Sustainability (Switzerland)*, vol. 13, no. 2, pp. 1–18, Jan. 2021, doi: 10.3390/su13020831.

[7] A. Jiang, "The impact of digital finance on online shopping," *Financ Res Lett*, vol. 56, p. 104089, 2023, doi: 10.1016/j.frl.2023.104089.

[8] M. Al-Okaily, A. Lutfi, A. Alsaad, A. Taamneh, and A. Alsyouf, "The Determinants of Digital Payment Systems' Acceptance under Cultural Orientation Differences: The Case of Uncertainty Avoidance," *Technol Soc*, vol. 63, pp. 1–15, Nov. 2020, doi:10.1016/j.techsoc.2020.101367.

[9] A. L. Kilay, B. H. Simamora, and D. P. Putra, "The Influence of E-Payment and E-Commerce Services on Supply Chain Performance: Implications of Open Innovation and Solutions for the Digitalization of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 3, pp. 1–25, Sep. 2022, doi: 10.3390/joitmc8030119.

[10] M. N. M. Yunoh, N. S. M. Hashim, Z. C. Musa, M. Muhamad, A. A. M. Hassan, and N. Bahari, "Understanding the factors influencing the adoption of e-wallets by Malaysian youth," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 21, no. 6, pp. 1298–1307, 2023, doi: 10.12928/Telkomnika.v21i6.24082.

[11] T. Alameri, M. N. Hammood, K. Mezaal, and B. Eneizan, "E-Payment Model for The Iraqi Public Sector: A Passport Issuance E-System," *Journal of Engineering Science and Technology*, vol. 17, no. 1, pp. 435–0451, 2022.

[12] . Ekta, M. Mehta, and B. Sehgal, "Buying Practices of Homemakers through Cashless Transaction," *Adv Res*, vol. 21, no. 12, pp. 53–61, Dec. 2020, doi: 10.9734/air/2020/v21i1230284.

[13] T. K. Setor, P. K. Senyo, and A. Addo, "Do digital payment transactions reduce corruption? Evidence from developing countries," *Telematics and Informatics*, vol. 60, pp. 101577–101587, Jul. 2021, doi: 10.1016/j.tele.2021.101577.

[14] F. B. Orellana, "Traditional mediation versus e-mediation: does online technology have a negative impact in the effectiveness of mediation?," *Revista Chilena de Derecho*, vol. 50, no. 1, pp. 33–48, 2023, doi:10.7764/R.501.2.

[15] X.-M. Loh, V.-H. Lee, G. W. H. Tan, K. B. Ooi, and Y. K. Dwivedi, "Switching from cash to mobile payment: what's the hold-up?," *Internet Research*, vol. 31, no. 1, pp. 376–399, Feb. 2021, doi:10.1108/INTR-04-2020-0175.

[16] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A review on electronic payments security," Aug. 01, 2020, *MDPI AG*. doi: 10.3390/sym12081344.

[17] R. K. Singhal, P. Chauhan, and T. R. Pandey, "Exploration of Factors Affecting Adoption of Digital Wallet Among Indian Domestic Tourist: Study of Trust and Security Perception," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 1268–1271. doi:10.1109/ICRITO48877.2020.9197917.

[18] W. Yang, S. Wang, J. J. Kang, M. N. Johnstone, and A. Bedari, "A linear convolution-based cancelable fingerprint biometric authentication system," *Comput Secur*, vol. 114, p. 102583, 2022, doi:10.1016/j.cose.2021.102583.

[19] C. W. Lien and S. Vhaduri, "Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey," *ACM Comput Surv*, vol. 56, no. 1, pp. 1–37, Aug. 2023, doi:10.1145/3603705.

[20] S. Iqbal *et al.*, "A novel mobile wallet model for elderly using fingerprint as authentication factor," *IEEE Access*, vol. 8, pp. 177405–177423, 2020, doi: 10.1109/ACCESS.2020.3025429.

[21] S. S. Ali, V. S. Baghel, I. I. Ganapathi, S. Prakash, N.-S. Vu, and N. Werghi, "A Novel Technique for Fingerprint Based Secure User Authentication," *IEEE Trans Emerg Top Comput*, vol. 10, no. 4, pp. 1918–1931, 2022, doi: 10.1109/TETC.2021.3130126.

[22] M. Baskar, R. D. Rajagopal, B. V. V. S. Prasad, J. Chinna Babu, G. P. Bartáková, and T. S. Arulananth, "Multi-region minutiae depth value-based efficient forged finger print analysis," *PLoS One*, vol. 18, no. 11, pp. 1–16, Nov. 2023, doi: 10.1371/journal.pone.0293249.

[23] J. Preciozzi *et al.*, "Fingerprint Biometrics From Newborn to Adult: A Study From a National Identity Database System," *IEEE Trans Biom Behav Identity Sci*, vol. 2, no. 1, pp. 68–79, 2020, doi:10.1109/TBIOM.2019.2962188.

[24] S. Bakheet, S. Alsubai, A. Alqahtani, and A. Binbusayyis, "Robust Fingerprint Minutiae Extraction and Matching Based on Improved SIFT Features," *Applied Sciences (Switzerland)*, vol. 12, no. 12, pp. 1–17, Jun. 2022, doi: 10.3390/app12126122.

[25] G. M. Salama *et al.*, "Secure biometric systems based on bio-signals and DNA encryption of optical spectrograms," *Opt Express*, vol. 31, no. 3, pp. 3927–3944, Jan. 2023, doi: 10.1364/oe.478215.

[26] R. Gupta, M. Khari, D. Gupta, and R. G. Crespo, "Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction," *Inf Sci (N Y)*, vol. 530, pp. 201–218, 2020, doi:10.1016/j.ins.2020.01.031.

[27] A. Takahashi, Y. Koda, K. Ito, and T. Aoki, "Fingerprint Feature Extraction by Combining Texture, Minutiae, and Frequency Spectrum Using Multi-Task CNN," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020, pp. 1–8. doi:10.1109/IJCB48548.2020.9304861.

[28] K. Castillo-Rosado, M. Linortner, A. Uhl, H. Mendez-Vasquez, and J. Hernandez-Palancar, "Minutiae-based Finger Vein Recognition Evaluated with Fingerprint Comparison Software," in *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2020, pp. 1–5.

[29] D. L. Andreea-Monica, S. Moldovanu, and L. Moraru, "A Fingerprint Matching Algorithm Using the Combination of Edge Features and

Convolution Neural Networks," *Inventions*, vol. 7, no. 2, pp. 1–13, Jun. 2022, doi: 10.3390/inventions7020039.
[30] S. S. Ali, V. S. Baghel, I. I. Ganapathi, and S. Prakash, "Robust biometric authentication system with a secure user template," *Image Vis Comput*, vol. 104, pp. 1–14, Dec. 2020, doi:10.1016/j.imavis.2020.104004.
[31] R. Donida Labati and F. Scotti, "Fingerprint," in *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, and M. Yung, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 1–6. doi: 10.1007/978-3-642-27739-9_740-2.
[32] F. Liébana-Cabanillas, Z. Kalinic, F. Muñoz-Leiva, and E. Higueras-Castillo, "Biometric m-payment systems: A multi-analytical approach to determining use intention," *Information & Management*, vol. 61, no. 2, p. 103907, 2024, doi: https://doi.org/10.1016/j.im.2023.103907.
[33] M. S. Niazy, N. Ahmad, Z. Habibi, B. Niazi, and Nasrullah, "Comparative Analysis of Different Biometric Techniques for Security Systems," *Australian Journal of Engineering and Innovative Technology*, vol. 5, no. 3, pp. 141–153, Jun. 2023, doi:10.34104/ajeit.023.01410153.
[34] E. Nnaemeka Uchenna, O. Obikwelu Raphael, and A. Theophilus Leonard, "Overview of Technologies and Fingerprint Scanner Used for Biometric Capturing," *Innovation*, vol. 1, no. 1, pp. 1–5, 2020, doi:10.11648/j.innov.20200101.11.
[35] B. Mróz-Gorgoń, W. Wodo, A. Andrych, K. Caban-Piaskowska, and C. Kozyra, "Biometrics Innovation and Payment Sector Perception," *Sustainability (Switzerland)*, vol. 14, no. 15, pp. 1–23, Aug. 2022, doi:10.3390/su14159424.
[36] H. W. Noh, C. G. Ahn, S. H. Chae, Y. Ku, and J. Y. Sim, "Multichannel Acoustic Spectroscopy of the Human Body for Inviolable Biometric Authentication," *Biosensors (Basel)*, vol. 12, no. 9, Sep. 2022, doi: 10.3390/bios12090700.
[37] F. Hidayanti, F. Rahmah, and A. Wiryawan, "Design of Motorcycle Security System with Fingerprint Sensor using Arduino Uno Microcontroller," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 4374–4391, 2020.
[38] G. Dahia, L. Jesus, and M. Pamplona Segundo, "Continuous authentication using biometrics: An advanced review," Jul. 01, 2020, *Wiley-Blackwell*. doi: 10.1002/widm.1365.
[39] H. Adnan Alzame, M. Alshabanah, and M. K. Alsmadi, "Point of Sale (POS) Network with Embedded Fingerprint Biometric Authentication," *Int J Sci Res Sci Technol*, vol. 6, no. 5, pp. 95–111, Sep. 2019, doi: 10.32628/ijsrst119659.
[40] N. Badovinac and D. Simic, "E-Payment Systems Using Multi-card Smartcard," in *Advances in Operational Research in the Balkans*, N. Mladenović, A. Sifaleras, and M. Kuzmanović, Eds., Cham: Springer International Publishing, 2020, pp. 237–249.
[41] S. Hutomo, P. Sukarno, and R. Yasirandi, "How Can Fingerprint Improves The Payment Experience of a Drink Vending Machine?," in *2020 8th International Conference on Information and Communication Technology (ICoICT)*, 2020, pp. 1–6. doi:10.1109/ICoICT49345.2020.9166181.
[42] E. Jajuli, M. R. Effendi, L. Kamelia, R. Mardiati, D. Miharja, and E. A. Zaki Hamidi, "The Implementation of Motorcycle Security System Using Voice Commands and Fingerprint Sensors," in *2021 15th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2021, pp. 1–6. doi:10.1109/TSSA52866.2021.9768232.
[43] D. and P. J. Patel Ronakkumar B. and Hiran, "Biometric Fingerprint Recognition Using Minutiae Score Matching," in *Data Science and Intelligent Applications*, V. and S. H. N. and P. R. Kotecha Ketan and Piuri, Ed., Singapore: Springer Singapore, 2021, pp. 463–478.
[44] E. M. Cherrat, R. Alaoui, and H. Bouzahir, "A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 1562–1570, 2020, doi: 10.11591/ijeecs.v18.i1.pp1562-1570.
[45] S. Bakheet, A. Al-Hamadi, and R. Youssef, "A Fingerprint-Based Verification Framework Using Harris and SURF Feature Detection Algorithms," *Applied Sciences (Switzerland)*, vol. 12, no. 4, Feb. 2022, doi: 10.3390/app12042028.
[46] S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System," in *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE*, Institute of Electrical and Electronics Engineers Inc., Feb. 2020, pp. 1–4. doi: 10.1109/ic-ETITE47903.2020.342.
[47] Z. Liu, Y. Niu, and Q. Qu, "Fingerprint Identification using Ridge Lines," in *3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA)*, 2022, pp. 732–735. doi: 10.1109/CVIDLICCEA56201.2022.9825387.
[48] N. Bhuvaneswary, C. V. Reddy, C. Aravind, and K. H. Prasad, "Smart Voting Machine using Fingerprint Sensor and Face Recognition," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2022, pp. 1159–1166. doi:10.1109/ICAAIC53929.2022.9792643.
[49] Z. Alqadi, M. Abuzalata, Y. Eltous, and G. M. Qaryouti, "Analysis of Fingerprint Minutiae to Form Fingerprint Identifier," *International Journal on Informatics Visualization*, vol. 4, no. 1, pp. 10–15, 2020, doi: 10.30630/joiv.4.1.332.
[50] A. Alotaibi, M. Hussain, and H. A. Aboalsamh, "Cross-Sensor Fingerprint Recognition Using Convolutional Neural Network and Canonical Correlation Analysis," *IEEE Access*, vol. 12, pp. 84738–84751, 2024, doi: 10.1109/access.2024.3413975.
[51] W. Lei and Y. Lin, "A Novel Dynamic Fingerprint Segmentation Method Based on Fuzzy C-Means and Genetic Algorithm," *IEEE Access*, vol. 8, pp. 132694–132702, 2020, doi:10.1109/access.2020.3011025.
[52] M. Gao, Y. Tang, H. Liu, and R. Ma, "Statistics of fingerprint minutiae frequency and distribution based on automatic minutiae detection method," *Forensic Sci Int*, vol. 344, p. 111572, 2023, doi:10.1016/j.forsciint.2023.111572.
[53] L. Makni and C. Charrier, "Minutia Confidence Index: A new framework to qualify minutia usefulness," in *Proceedings - 2020 International Conference on Cyberworlds, CW 2020*, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 257–264. doi:10.1109/CW49994.2020.00048.
[54] N. Alsharman, A. Saaidah, O. Almomani, I. Jawarneh, and L. Al-Qaisi, "Pattern Mathematical Model for Fingerprint Security Using Bifurcation Minutiae Extraction and Neural Network Feature Selection," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1–16, 2022, doi: 10.1155/2022/4375232.
[55] G. Raj M., S. Rakshitha, S. Priya S., S. Vaishnavi, and A. Sivaranjani, "Latent Fingerprint Enhancement for Investigation," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 644–648. doi:10.1109/icaccs48705.2020.9074191.
[56] S. Socheat and T. Wang, "Fingerprint Enhancement, Minutiae Extraction and Matching Techniques," *Journal of Computer and Communications*, vol. 08, no. 05, pp. 55–74, 2020, doi:10.4236/jcc.2020.85003.
[57] M. A. Wani, F. A. Bhat, S. Afzal, and A. I. Khan, "Supervised Deep Learning in Fingerprint Recognition," in *Advances in Deep Learning*, M. A. Wani, F. A. Bhat, S. Afzal, and A. I. Khan, Eds., Singapore: Springer Singapore, 2020, pp. 111–132. doi: 10.1007/978-981-13-6794-6_7.
[58] A. J. Mohamed Abdul Cader, J. Banks, and V. Chandran, "Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges," *Sensors*, vol. 23, no. 14, pp. 1–28, Jul. 2023, doi:10.3390/s23146591.
[59] Y. Surajkanta and S. Pal, "A Digital Geometry-Based Fingerprint Matching Technique," *Arab J Sci Eng*, vol. 46, no. 4, pp. 4073–4086, Apr. 2021, doi: 10.1007/s13369-021-05390-4.
[60] J. K. Appati, P. K. Nartey, E. Owusu, and I. W. Denwar, "Implementation of a Transform-Minutiae Fusion-Based Model for Fingerprint Recognition," *Int J Math Math Sci*, vol. 2021, no. 1, pp. 1–12, 2021, doi: 10.1155/2021/5545488.
[61] K. Y. Qureshi, S. A. Khan, and J. M.Y, "Effectiveness of assigning confidence levels to classifiers and a novel feature in fingerprint matching," in *Conference Proceedings - IEEE International Conference on Applied Computational Science*, 2009, pp. 181–186. doi: 10.1109/ICSMC.2009.5346241.
[62] S. K. D. R., R. K. Chhotaray, K. B. Raja., and S. Pattanaik, "Fingerprint Verification based on fusion of Minutiae and Ridges using Strength Factors," *Int J Comput Appl*, vol. 4, no. 1, pp. 1–8, Jul. 2010, doi: 10.5120/799-1136.
[63] A. M. Bazen and S. H. Gerez, "Fingerprint matching by thin-plate spline modelling of elastic deformations," *Pattern Recognit*, vol. 36, no. 8, pp. 1859–1867, 2003, doi: 10.1016/S0031-3203(03)00036-0.
[64] A. Budijanto, S. Winardi, and K. E. Susilo, *Interfacing ESP32*. Surabaya: Scopindo Media Pustaka, 2021.
[65] Lady Ada and K. Rembor, "Adafruit Optical Fingerprint Sensor," adafruit. Accessed: Jan. 20, 2024. [Online]. Available: https://learn.adafruit.com/adafruit-optical-fingerprint-sensor?view=all

[66] D. and J. A. K. and F. J. Maltoni Davide and Maio, “Fingerprint Sensing,” in *Handbook of Fingerprint Recognition*, Cham: Springer International Publishing, 2022, pp. 63–114. doi: 10.1007/978-3-030-83624-5_2.

[67] W.-C. Lin, C.-T. Hsieh, and M.-C. Chang, “Design and implementation of pixel-based adjustable ESD protection circuits for capacitive fingerprint biometric sensors,” *International Journal of Circuit Theory and Applications*, vol. 51, no. 3, pp. 991–1006, Mar. 2023, doi: https://doi.org/10.1002/cta.3477.

[68] H. Zhengfang, A. J. P. Delima, I. K. D. Machica, J. C. T. Arroyo, S. Weibin, and X. Gang, “Fingerprint Identification based on Novel Siamese Rectangular Convolutional Neural Networks,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 5, pp. 28–37, May 2022, doi: 10.46338/ijetae0522_04.

[69] G. Awasthi, H. S. Fadewar, A. Siddiqui, and B. Gaikwad, “Analysis of Fingerprint Recognition System Using Neural Network,” in *2nd International Conference on Communication & Information Processing (ICCIP)*, 2020, pp. 1–11. [Online]. Available: https://ssrn.com/abstract=3648835

[70] R. Raghavan and K. John Singh, “An enhanced and hybrid fingerprint minutiae feature extraction method for identifying and authenticating the patient’s noisy fingerprint,” *International Journal of System Assurance Engineering and Management*, vol. 15, no. 1, pp. 84–97, 2024, doi: 10.1007/s13198-022-01674-6.