Secure Bio-Cryptographic Authentication System for Cardless Automated Teller Machines

O. M. Olaniyi[1], I. A. Ameh[2], L. A. Ajao[3], O. R. Lawal[4]
1,2,3,4- Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria.
1- (mikail.olaniyi@futminna.edu.ng)

Received (2019-02-26) Accepted (2019-04-21)

Abstract: *Security is a vital issue in the usage of Automated Teller Machine (ATM) for cash, cashless and many off the counter banking transactions. Weaknesses in the use of ATM machine could not only lead to loss of customer's data confidentiality and integrity but also breach in the verification of user's authentication. Several challenges are associated with the use of ATM smart card such as: card cloning, card skimming, cost of issuance and maintenance. In this paper, we present secure bio-cryptographic authentication system for cardless ATM using enhanced fingerprint biometrics trait and encrypted Personal Identification Number (PIN). Fingerprint biometrics is used to provide automatic identification/verification of a legitimate customer based on unique feature possessed by the customer. Log-Gabor filtering algorithm was used for enhancing low image quality and effect of noise on feature extracted from customer's fingerprint minutiae. Truncated SHA 512/256 hash algorithm was used to secure the integrity and confidentiality of the PIN from sniffers and possible adversary within the channel of remote ATM banking transactions. Performance evaluation was carried out using False Acceptance Rate (FAR), False Rejection Rate (FRR) metrics and Collision Attack was performed on the Truncated SHA-512/256 hashed data (PIN). Results of the system performance shows Genuine Acceptance Rate (1-FRR) of 97.5% to 100%, Equal Error Rate of 0.0015% and Collision Attack carried out on the encrypted PIN message digest gave an unsuccessful attack. Therefore, the results of performance evaluation show the applicability of the developed system for secure cardless ATM transaction.*

Keywords: *Attack; Authentication; Confidentiality; Cardless; Fingerprint; Security.*

How to cite this article:
O. M. Olaniyi, I. A. Ameh, L. A. Ajao, O. R. Lawal. Secure Bio-Cryptographic Authentication System for Cardless Automated Teller Machines. J. ADV COMP ENG TECHNOL, 5(2) Spring : 117-128

I. INTRODUCTION

Money allows separation of related sales and purchase of transaction for successful decentralization to the process of exchange [1]. Banking transactions, generally, establish legal obligations in form of exchanges between two or more parties. In essence, transactions have a great significance in all facets of life and their security is essential. With the rapid growth in the Information Technology, new inventions are entering the market daily and many new varieties of smart and secured Automated Teller Machines (ATM) technologies are evolving in out of the counter financial operations. ATM is an electronic computerized communication device that allows customers to directly use a secure method to access fund in their bank accounts. This convenient innovation of information technology has made it feasible for remote and near bank clients to interact and carry out banking activity with ATM as a form of Electronic banking (E-banking).

E-banking offers other services apart from ATM transactions such as Telephone banking, Short Service Message banking and direct purchase sales through Point-Of-Sale (POS). Banks' more dispositions toward ATMs is as a result of reduction of congestion in banking halls and day by day rising cost of setting up and operating bank branch or extension counters [2]. ATM's have found its rapid popularity not only because of its low cost of transactions but also due to customers' convenience and so it has become a necessary part of our life. The traditional and manual banking system is time-consuming and lacks efficiency in record keeping. In recent time, ATM has served as a device that enhances the cashless policy due to its functionality in fund transfer between one account and other. ATM creates a paperless office, ensures security of customers' accounts and privacy, grants customers twenty-four hours access to their accounts, eliminates cash-induced robbery, reduces cost of operation, and enhances proper and effective record keeping [3].

Currently, one major way to get access to one's account in other to perform withdrawal, deposit, balance enquiry and payment of bills is through the use of ATM smart card. The smart card is encoded with user information on a magnetic strip. The magnetic strip or the chip contains an identification code that is transmitted to the bank's central server. The ATM card is designed to replace the manual banking transactions where bank clients proceed into the banking hall to fill tellers, withdrawal booklets or cheque.

Despite all these benefits of an ATM, there are lot of problems associated with the use of ATM smart card, these include: loss or stolen card, use of ATM card by third party to perform transactions, ATM card skimming, card expiration, charges on issuance of the ATM card and maintenance fee by financial institutions. These have made the use of ATM card a threat to safety of customer funds, and the diverse vulnerabilities to fraud has resulted in a call for more security measures [2].

This paper presents the development of secure bio-cryptographic authentication system for cardless ATM using Log-Gabor filtering algorithm on fingerprint biometrics and truncated SHA512/256 cryptographic hash algorithm to secure PIN as second level of authentication. The remaining section of the paper is organized into four sections, Section 2 provides a review of related baseline works, system hardware and software design considerations are presented in Section 3, results and discussions are presented in Section 4, while Section 5 concludes and provides scope for future works.

II. RELATED WORKS

Many recent studies have focused on using biometric techniques in enhancing the security of the ATM. However, a few studies have also exploited the use of GSM Technology, PIN, one-time password OTP, while some have adopted a combination of all techniques. Ravikumar et al., in [6] proposed an authentication method using finger print recognition in digital image processing using both primary and reference fingerprint to authenticate users instead of the traditional pin. This technique gives privilege to third party (family member) transaction by allowing another reference fingerprint belonging to a nominee or a close family member to be captured. Adoption of third-party fingerprint could lead to a security breach through social engineering, thus compromising the security of the primary account owner.

Padmariya et al., in [7] proposed a three-way authentication method using a combination of fingerprint biometric, token and GSM technology. The method hardened the security of the system by enabling the use of token and GSM, a third-party fingerprint was incorporated into the architecture of the system. The use of token and GSM are prone to theft, the incorporation of third party could breach the security of the system.

Similar three factor authentication system was proposed by Oruh in [8]. The proposed technique includes: the password, ATM card and fingerprint which improves the security of the ATM system. This makes it almost impossible for hackers and attackers to penetrate into the system proposed, the system limited the Vulnerabilities ATM card to fraud by using fingerprint authentication. Further secure measures were proposed for users' authentication by generating a token number. The proposed work still involves the use of ATM smart card which makes the system vulnerable to third party attack.

A cost effective bi-modal system using

fingerprint and a short-code message to authenticate account holder's transaction was proposed in Awotunde et al., in [9]. The system relied on short messaging platforms. In similar work Alebiosu et al., in [3], proposed a conceptual frame work of design, specification, and model of the cardless automated teller machine system with biometric authentication. The proposed system used alphanumeric PIN and biometric fingerprint to control access to the ATM. The proposed frame work was not implemented and the proposed second-level PIN authentication was vulnerable to attack by an adversary.

Nischarkumar et al., [10] designed a card-less ATM cash withdrawal using One-Time Password (OTP). The use of OTP further enhanced the security of the system for users' authentication. The design emphasizes the use of smart card which is vulnerable to loss or stolen by erring third party, use of ATM card by third party to perform transactions, card skimming, card expiry, and huge maintenance costs. The customer still needs the smart card number before transaction could takes place.

Consequently, an improvement on [3, 10] was carried in the work of Ameh et al., [2], but with different method entirely. Principal Component Analysis (PCA) was used to extract the fingerprint features which compress higher dimensional set to a lower dimension for data analysis. The PCA algorithm functions in spatial domain, covers low computational space of an image, produces low image quality and effect of noise on fingerprint minutiae was not considered. Ameh et al., in [2] recommended the use of Truncated SHA-512/256 to harden the security of PIN which is the second level authentication method to protect the integrity of data and confidentiality of users. Ganesh et al., in [11] proposed cardless ATM authentication system to prevent users attacked by strangers to withdraw from user's account ad More et al., in [15] improved on service of cardless ATM withdrawal by combining fingerprint biometrics with developed be-spoke mobile banking application with QR code.

In this work, we improve upon secure bio-cryptographic techniques for cardless ATM in [2, 3, 10, 11, 15]by the application of Log-Gabor filtering to remove the noise on the feature extracted from customers fingerprint images to achieve good quality image require to harden the security of valid customer in first mode, the authentication and encryption of second level, PIN with Truncated SHA-512/256 cryptographic hash function to address the issue of user's confidentiality and data integrity for secure cardless ATM transactions.

III. MATERIALS AND METHODS

This section describes the hardware design, materials used, software design and some salient considerations for the design and prototyping strategies to achieve the aim of this work.

1. Hardware and Software System Design

The hardware system and software prototype consist of R305 fingerprint module, Arduino Uno development board, the developed account registration and ATM transaction application software system respectively. The R305 fingerprint module was used to obtain fingerprint template and the Arduino Uno development board integrated with Atmega328 microchip further processes requests coming from the application server through the serial communication port. The ATM transaction application software system enables interaction between the customer account and the ATM. The overall system flow process is presented in Fig. 1.

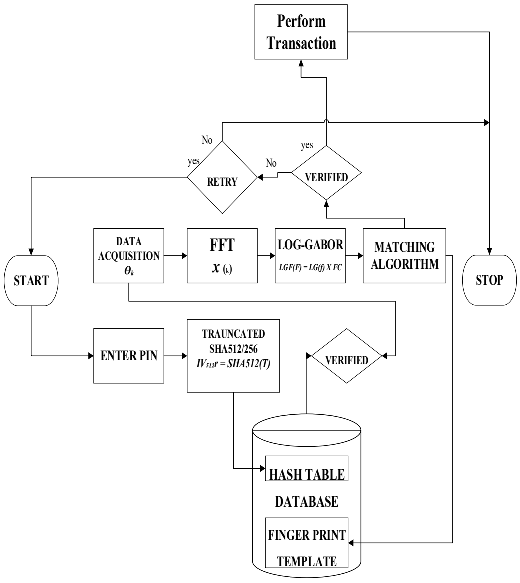


Fig.1. The overall system flow process diagram

2. Hardware System Design Consideration

In this section, a brief description of the hardware components involved in the system development is presented. The system hardware for the skeletal and compact coupling both are illustrated in Fig. 2 and Fig. 3 respectively.

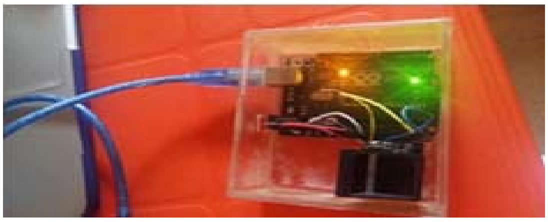


Fig.2. Bimodal authentication system coupling

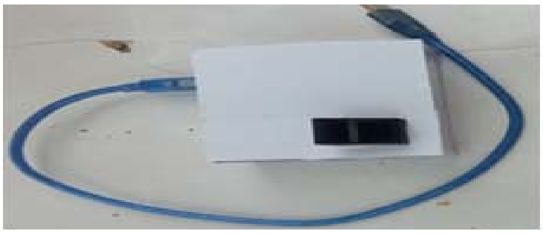


Fig.3.Bio-cryptographic authentication system prototype

3. Fingerprint (R305) Module

The fingerprint (R305) sensor module performs finger pattern enrolment, image processing, and pattern matching, searching and template storage. This device capable of performing 1:1 matching or 1: N matching from the storage template using UART protocol to communicate with the host controller (MCU). The default baud rate is usually 57600bps though the module, and it can support from 9600 to 115200bps. The fingerprint (R305) sensor module uses image buffer and two 512byte character file buffers that contains volatile, and non-volatile flash memory for storing fingerprint templates. The R305 module has four connecting pins; TX, RX, Ground and VCC (+5) as shown in Fig. 4.

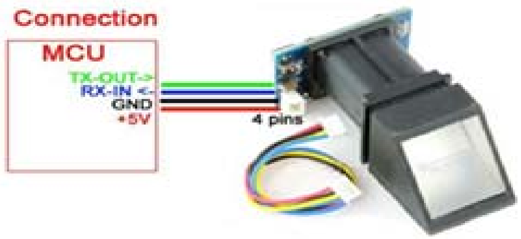


Fig.4. Fingerprint (R305) Architecture

4. Arduino Uno (ATmega 328) Microcontroller

The circuit diagram for the Bimodal Authentication system was designed in the Proteus Virtual Simulation Modelling (PVSM) as illustrated in Fig. 5. It contains an integrated ATmega328 microchip with Arduino Uno board interfacing with fingerprint (R305) module through the logical serial communication channel of transmitter (Tx) and receiver (Rx) of both components.

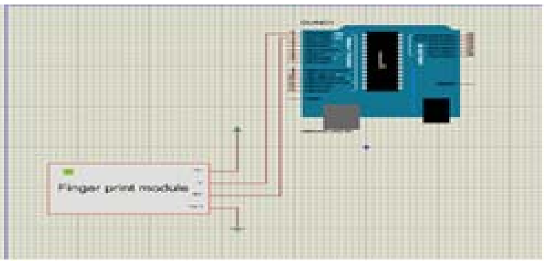


Fig.5. Circuit Diagram for the Bimodal Authentication system

5. Software System Design

The system was developed using the C# language and the .NET framework, which was used to design the interface of the system and implement the SHA 512/256 hashing algorithm; a Windows, Apache, MySQL and PHP (WAMP) server was used to deploy and host the database locally while a MySQL Connector Net was used to ensure that the system connects to and execute MySQL queries made to the database as the application runs. The next subsection discusses how Truncated SHA-512/256 was used to harden the security of PIN.

6. Application of Secure Hash Algorithm (SHA-256/512)

The application of truncated SHA-512 variants, like SHA-512/256 in this paper gives a significant performance advantage over SHA-256 on 64-bit platforms due to the doubled input block size [12]. At the same time, the shorter 256-bit hash values are more economic, compatible with existing applications, and offer the same security level as SHA-512 on PIN for second level authentication. The flow process diagram of the applied hash algorithm is shown in Fig. 6.

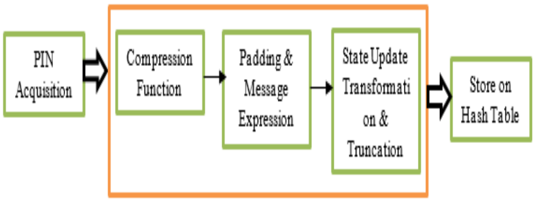

PIN Acquisition
Compression Function
Padding & Message Expression
State Update Transformati on & Truncation
Store on Hash Table

Fig.6. Flow process of the truncated secure hash function

The truncated SHA-512/256 hash algorithm was implemented with C#, using visual studio as a coding environment. The algorithm was implemented as follows.

Step 1: Compression function. The hash value of 512-bit hash value is computed using the compression function f as given in (1) and (2), where hash output is the final 512-bit chaining value ht.

$$h_0 = IV \qquad (1)$$

$$h_{j+1} = f\left(h_j, m_j\right) \quad for\ 0 \le j < t \qquad (2)$$

Step 2: Padding and Message Expansion, The message expansion of SHA-512 separates each 1024-bit message block into 64-bit words Mi where i = 0,…, 15, and then increases these into 80 lengthened message words Wi as given in (3).

$$W_i = \begin{cases} M_i \\ \sigma_1 (W_{i-2}) + W_{i-7} + \sigma_0 (W_{i-15}) + W_{i-16} \end{cases}$$

$$0 \le i < 16,\ 16 \le i < 80 \qquad (3)$$

Step 3: The state update transformation [12], starts from the value hj.

$$h_j = (A_{-1}, \ldots, A_{-4}, E_{-1}, \ldots, E_{-4}) \qquad (4)$$

The previous 512-bit chaining and updates it by applying the step functions 80 times. In each step i = 0, …, 79, Wi (one 64-bit expanded message word) is used to compute the two state variables Ei and Ai as demonstrated in (5).

$$E_i = A_{i-4} + E_{i-4} + \sum\nolimits_1 (E_{i-1}) + IF(E_{i-1}, E_{i-2}, E_{i-3}) + K_i + W_i,$$

$$A_i = E_i - A_{i-4} + \sum\nolimits_0 (A_{i-1}) + MAJ(A_{i-1}, A_{i-2}, A_{i-3}) \qquad (5)$$

Following the last step of the state update transformation, the previous chaining value hj is included to the output of the state update. The output of the feed-forward sum is the chaining value hj + 1 for the subsequent message block mj + 1 (or the final hash value ht):

$$h_{i+1} = (A_{79} + A_{-1}, \ldots, +A_{-4}, E_{79} + E_{-1}, \ldots, E_{76} + E_{-4} \qquad (6)$$

The truncated variant of SHA-512 differs only in its initial values and the final truncation to 256 bits, while the rest of the algorithmic description does not change. By neglecting the output words E79 + E−1, E78 + E−2, E77 + E−3, and E76 + E−4 of the last compression function call, the message digest of SHA-512/256 is obtained. The truncated SHA 512/256 have same security strength as SHA-

512, the only exception is in the resulting output which uses Equation 15 to set the initialization vector.

$$IV_{512t} = SHA512(T) \qquad (7)$$

7. System Implementation

The bio-cryptographic authentication system consists of five basic modules similar to system in [2] but with further enhancements as shown in the next sections: data acquisition module, feature extraction module, database, matching module and decision-making module. The system architecture is presented in Fig. 7.

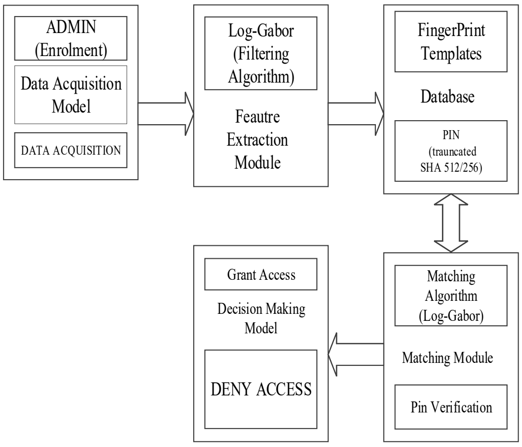


Fig.7. Bio-cryptographic authentication system architecture

8. Pattern Authentication System

The algorithm employed in this work to enhance low image quality and effect of noise on feature extracted from customer's fingerprint minutiae is Log-Gabor filtering algorithm because of the two important characteristics is possesses. It has no DC component and possesses an extended tail at the high frequency domain [4]. Log-Gabor filter promotes the quality and reliability of fingerprint extraction. The flow diagram of the fingerprint authentication system is shown in Fig. 8 and further extended in Fig. 9.

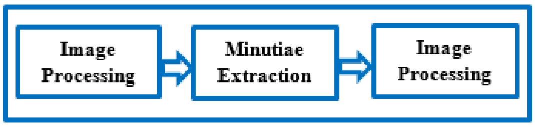


Fig.8. Flow diagram of fingerprint authentication system

The process adopted for this algorithm is the Log-Gabor Orientation with run-length code based for feature extraction approach to enhanced security of the fingerprint as proposed in [4]. The algorithm was implemented as follows [4]:

Step 1: Frequency domain was used to perform image enhancement as expressed in "equation (8)".

$$e^{i2\pi f x}\theta_k \qquad (8)$$

Step 2: Fast Fourier Transformation was used to obtain the frequency values which transforms the image into a frequency image.

$$FFT: X_{(k)} = \sum_{j=1}^{N} X_{(j)}\omega_N^{(j-1)(k-1)} \qquad (9)$$

Step 3: The Log-Gabor filter parameters are well-defined and the Orientations are estimated. At this stage, Log-Gabor features and Local ridge orientations are also computed.

$$LGF(f) = LG(f) \times FC \qquad (10)$$

$$\theta_k = \frac{\pi(k-1)}{n}, k = 1, 2, \dots n \qquad (11)$$

Step4: Binarization process, converting grey-level (0-255) to binary image (0 or 1).

$$I_{new}(p1, p2) = \begin{cases} 1 & if\ I_{old\ (p1,p2 \geq local\ Mean)} \\ 0 & otherwise \end{cases} \qquad (12)$$

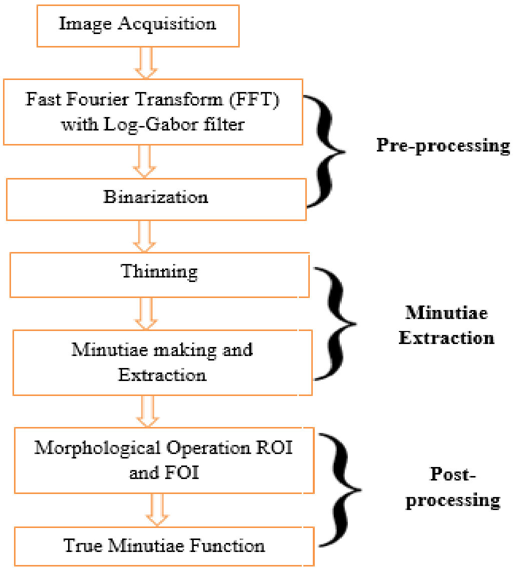


Image Acquisition
Fast Fourier Transform (FFT) with Log-Gabor filter
Binarization
Pre-processing
Thinning
Minutiae making and Extraction
Minutiae Extraction
Morphological Operation ROI and FOI
True Minutiae Function
Post-processing

Fig.9. Flow diagram of Log-Gabor filtering algorithm feature extraction technique [4]

Step 5: Thinning which is the process of transforming the thickness of an image into one-pixel width representation, the thinned and sharp ridges of fingerprint features are derived from the thinning process. The thin operation implemented using the following algorithm as following algorithm [4]:

Level 1: fingerprint image was divided into two distinct subfields in a checkerboard pattern.

Level 2: Pixel P will be deleted from the first subfield if and only if the conditions G1, G2, and G3 are all fulfilled in the first iteration.

Level 3: Pixel P will be deleted from the first subfield if and only if the conditions G1, G2, and G31 are all fulfilled in the second sub-iteration.

Condition G1:

$$X_H(P) = 1 \qquad (13)$$

Where,

$$X_H(P) = \sum_{i=1}^{4} b_i \qquad (14)$$

$$b_i = \begin{cases} 1, if\ x_{2i-1} = 0\ and\ (x_{2i=1}\ or\ x_{2i+1} = 1) \\ 0, \qquad otherwise \end{cases} \qquad (15)$$

X1, X2 …X8 are the values of the eight neighbors of p, starting with the least neighbour and n counter-clockwise order. Table 1 shows the neighbour of p in a checkboard format.

Condition G2:

$$2 \leq \min\{n1\ (p), n2\ (p)\} \leq 3 \qquad (16)$$

Where,

$$n1\ (p) = \sum_{i=1}^{4} x_{2k-1} V x_{2k} \qquad (17)$$

$$n2\ (p) = \sum_{i=1}^{4} x_{2k} V x_{2k+1} \qquad (18)$$

Condition G3: G3 is in the first sub-iteration.

$$G3^1 : (x_6\ v\ x_7\ v x_4)\ \Lambda\ x_5\ = 0 \qquad (19)$$

Step 6: Minutiae marking, Terminations and Bifurcations are used to extract the level 2 features. These features are marked using labeling technique and also Run-length Coding algorithm. The algorithm to find the minutiae is implemented as follows [14];

Level 1: Apply Run-Length Encoding on the input image (RLE).

Level 2: Scan the rounds by assigning preliminary labels on connected components in binary image.

Level 3: The equivalence classes are determined.

Level 4: All relevant classes are concatenated.

Level 5: Re-label the rounds based on the equivalence classes determined (LB).

The label and its properties are described in Table 1, Fig. 8 shows the templates of the Termination and bifurcations.

Step 7: Minutiae Extraction, Minutiae extraction hinge on the labels and properties of the minutiae marked in t

Table 2). Based on the properties, the ridge terminations and bifurcations are extracted from the fingerprint image (see Fig. 8). The red circle refers the ridge endings and the blue square refers the ridge bifurcations [4].

IV. RESULTS AND DISCUSSIONS

The R305 Fingerprint module designed in Section IIIC was used to capture fifty (50) real time unique images captured from users of ATM. The experimental results obtained show the uniqueness while extracting minutia from sixteen (16) filtered real time images captured from fifty (50) real time users. From the first stage fingerprint image is captured and then pre-processing stage is carried out. In the second stage, minutia extraction is accomplished to eliminate the false minutia, while the post-processing is also achieved thirdly; finally, the true minutiae set are obtained while the extracted minutia set is under the post process

The process defined in Figure 7 was used to obtain the result of the fingerprint images displayed in Figure 10, Image (a) is the original fingerprint image acquired (real time unprocessed image). Image (b) and (c) in Figure 11 are in the pre-processing stage where the first level features like the Arch and whorl are being extracted using FFT, Log-Gabor and binarization. Image (d) and (e) in Figure 12 are in the enhancement and minutiae extraction stage where the second level features like line unit and hook are being extracted using thinning and minutiae marking. Image (f) in in Figure 12 is the post-processing stage where the level 3 features are being extracted using ROI and FOI operations to obtain the true minutiae which are the final stage of extraction.

TABLE I
LABEL PROPERTY OF MINUTIAE [4]

Label (LB	Property
0	Isolation
1	Termination
2	Continuing termination
3	Bifurcation
4	Crossing point

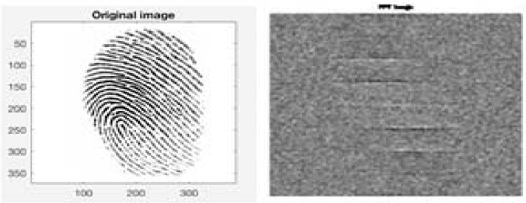


Fig.10. Original image and FFT image

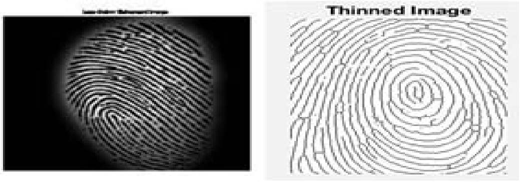


Fig.11. Log-Gabor image and Thinning image

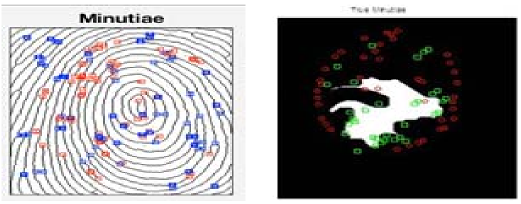


Fig.12. Minutiae image and True minutiae image

1. Accuracy rate of Ridge Minutiae

The result of the accuracy rate applied on the minutiae before and after the pre-processing and post-processing as depicted in Table 2, Table 3 and Table 4 and Figure 13 shows the obtained graph of the accuracy rate. The accuracy rate of the bifurcations and terminations are calculated using [13] definitions for bifurcations and terminations in relations in (20), (21) and (22) respectively.

$$Termination = \frac{T_t}{T_e} \quad (20)$$

$$Bifurcation = \frac{B_t}{B_e} \quad (21)$$

$$Total\ accuracy = \frac{T_t + B_t}{T_e + B_e} \quad (22)$$

where,

= Number of true terminations

=Number of extracted terminations

= Number of true Bifurcations

= Number of extracted Bifurcations

TABLE 2
ACCURACY RATE OF RIDGE MINUTIAE BEFORE PRE-PROCESSING

Images	T_t (%)	B_t (%)	Total Rate (%)
01	2.86	18	3.02
02	1.96	54.71	4
03	24.3	2.6	9.95
04	3.04	16.02	3.5
05	3.69	22.36	4.44
06	5.32	1.94	4.11
07	3.32	22.44	4.21
08	1.64	55.00	2.41
09	16.8	23	6.90
10	6.34	13.34	3.7
11	3.45	64	3.4
12	2.34	8.60	5.3
13	3.33	22	4.56
14	2.09	15	5.26
15	8.76	1.8	2.30
16	2.45	45.3	4.12
Average Rate	5.731	24.13	4.448

The rate of accuracy of both bifurcation and termination of extracted features before the pre-processing stage can be seen in Table 3. It also shows the total rate acquired from each fingerprint, which is the best minutiae point detected during the process of extraction. The result shows the novelty while extracting the minutiae, in which the frequency domain enhancement is followed in order to obtain the frequency values.

Table 4 displays the rate of accuracy of both bifurcation and termination of the level one fingerprint features, which includes; the arch, tented arch, right loop, left double loop and whorl which were extracted after the pre-processing stage. It also displays the best minutiae point detected during the process of extraction, the total rate was calculated using relation (23).

TABLE 3
ACCURACY RATE OF RIDGE MINUTIAE AFTER PRE-PROCESSING

Images	Tt (%)	Bt (%)	Total Rate (%)
01	36.19	36.4	36
02	89.76	47.86	68.75
03	73.32	5.49	26.04
04	43.78	23.24	36.04
05	38.72	28.3	31.45
06	92.2	4.53	20
07	75.27	21.08	43.1
08	90	12.3	45
09	78	46.45	56
10	67	23	25
11	55	5.78	32.78
12	45.89	24	36
13	53	5.38	37.9
14	74.80	34.8	45.8
15	97	25.6	27.67
16	65	46	54
Average Rate	67.183	22.9	38.80

Table 5 shows the bifurcation and termination accuracy rate of level 3 features such as pores and scars, which are extracted after the post-processing. The total rate displayed in the table is the best minutiae point detected during this process.

TABLE 4
ACCURACY OF RIDGE MINUTIAE AFTER POST-PROCESSING

Images	Tt (%)	Bt (%)	Total Rate (%)
01	71.74	45.5	66.85
02	82.64	55.86	74.74
03	94.14	6.46	31.26
04	85	42.44	71.92
05	64.85	40.65	47.42
06	85	5.38	22.09
07	100	75	85
08	80	40	60
09	88.56	55	65
10	76.45	53	56
11	67.45	5.98	75
12	89.29	28.22	54
13	97.32	16.89	34
14	78	52.48	78
15	67	44	61.76
16	98.99	55	36
Average Rate	82.90	38.87	57.44

Table 6 summarizes the average accuracy rate, and shows as they increase gradually from the pre-processing stage up to the post-processing stage. The accuracy rate of ridge minutiae extraction from Table 3 to 5 which demonstrates the stages of fingerprint extraction and the gradual increase as shown in Fig. 13 in the accuracy rate shows that the system is reliable and accurate.

TABLE 5
AVERAGE RATE OF ACCURACY OF RIDGE MINUTIAE

Images	Tt (%)	Bt (%)	Total Rate (%)
01	5.731	24.13	4.448
02	67.183	22.9	38.80
03	82.90	38.87	57.44

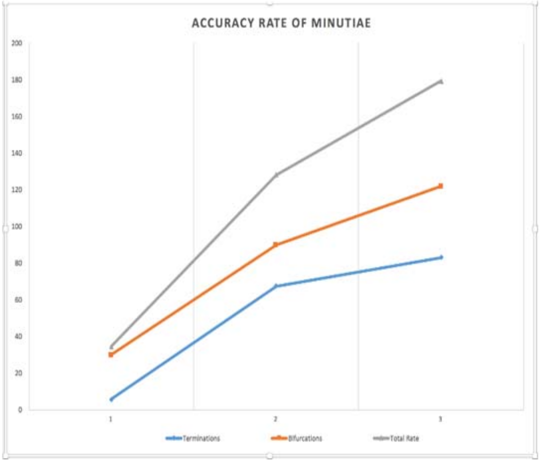


Fig.13. Accuracy rate of minutiae

2. Computation of False Acceptance Rate and False Rejection Rate Evaluation

Performance analyses of system on extracted minutia from sixteen (16) filtered real time images captured from fifty (50) real time images from users of ATM smart card was demonstrated in Table 7, Table 8 and Table 9. Figure 14 shows the Receiver Operating Characteristic (ROC) Curve obtained. The plot of genuine acceptance rate (1-FRR) against false acceptance rate for all possible matching thresholds and measures the overall performance of the system is the ROC curve. Figure 13 is a plot of the FAR and FRR functions against the various thresholds.

TABLE 6
FALSE REJECT RATE ON FINGERPRINT DATA COLLECTED

Threshold (%)	Matching Attempts (N)	False Rejects (nR)	FRR = $\left(\frac{nR}{N}\right)$	$FRR = \left(\frac{nR}{N}\right) \times 100\%$	Genuine Acceptance Rate (1-FRR) x100%
1.0000	160	4	0.025	2.50	97.5
0.77067	160	3	0.019	1.90	98.1
0.68474	160	2	0.013	1.30	98.7
0.24535	160	1	0.006	0.60	99.4
0.19462	160	0	0.000	0.00	100

TABLE 7
ACCURACY RATE OF RIDGE MINUTIAE AFTER PRE-PROCESSING

Threshold (%)	Matching Attempts (N)	False Accept (nA)	FAR = $\left(\frac{nA}{N}\right)$	FAR = $\left(\frac{nA}{N}\right) \times 100\%$
1.0000	160	0	0.000	0.00
0.77067	160	1	0.006	0.60
0.68474	160	2	0.013	0.13
0.24535	160	3	0.019	0.19
0.19462	160	4	0.025	0.25

TABLE 8

ACCURACY RATE OF RIDGE MINUTIAE AFTER PRE-PROCESSING

Genuine Acceptance Rate (1-FRR) x 100%	FAR = $\left(\frac{IM}{N}\right)\times 100\%$
97.5	0.00
98.1	0.60
98.7	0.13
99.4	0.19
100	0.25

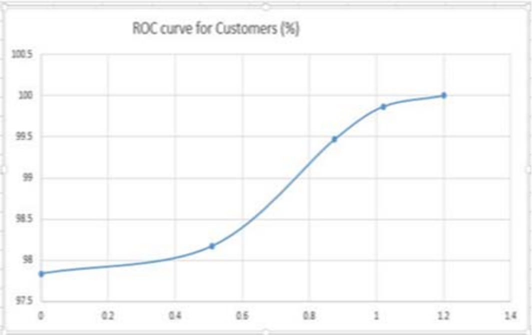


Fig.14. Receiver operating characteristics Curve

TABLE 9
EQUAL ERROR RATE

Error Rate		Threshold
FAR	FRR	Sensitivity
0.000	0.025	1.0000
0.006	0.019	0.77067
0.013	0.013	0.68474
0.019	0.006	0.24535
0.025	0.000	0.19462

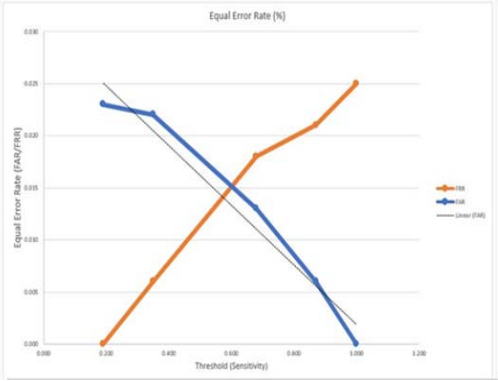
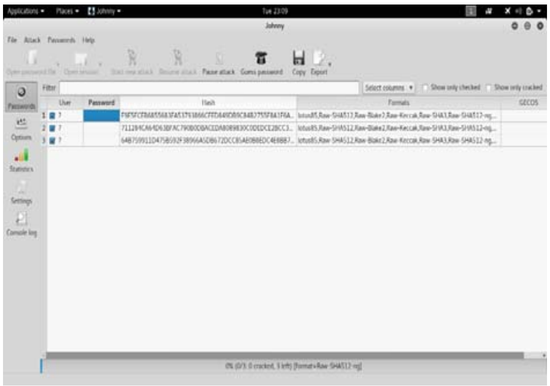


Fig.15. Error rate curve

3. Collision Attack on Hashed PIN Evaluation

The performance of the SHA 512/256 was evaluated using a password cracking tool Johnny to evaluate the security capacity of encrypted PIN. The hashes of encrypted PIN were extracted from the database and loaded into the application. Fig. 16 shows the use of Johnny Password cracking tool on the hash obtained from the hash table, the hash cracking was unsuccessful which implies the integrity of the data is protected.



	User	Password	Hash	Formats	GECOS
1	?		[illegible]	lotus85,Raw-SHA512,Raw-Blake2,Raw-Keccak,Raw-SHA3,Raw-SHA512-ng...	
2	?		[illegible]	lotus85,Raw-SHA512,Raw-Blake2,Raw-Keccak,Raw-SHA3,Raw-SHA512-ng...	
3	?		[illegible]	lotus85,Raw-SHA512,Raw-Blake2,Raw-Keccak,Raw-SHA3,Raw-SHA512-ng...	

0% (0/3: 0 cracked, 3 left) [format=Raw-SHA512-ng]

Fig.15. Collison attack on Encrypted PIN

V. CONCLUSION

This work has successfully presented an application of biometrics fingerprint trait and encrypted personal identification number for authenticating legitimate customers in a cardless ATM. The Secure bio-cryptographic authentication system for a cardless ATM was successfully designed and prototype model was implemented. Evaluation of the system performance was carried out to validate the suitability of the model to replace the existing card-based ATM system. The proposed bio-cryptographic technique was implemented in order to achieve dual purpose tasks of enhancing minutiae feature extraction through [4]'s Log-Gabor orientation and RLC method. Accuracy rates of minutiae and average error rates were used as the performance evaluation metrics of this method. System performance shows Genuine Acceptance Rate (1-FRR) of 97.5% to 100%, Equal Error Rate of 0.0015% and Collision Attack carried out on the encrypted PIN (message digest) gave an unsuccessful attack. The development of enhanced cardless bio-cryptographic authentication system incorporated with hardened second level authentication, will address the problem of user verification and data integrity in off-the-counter ATM transactions.

REFERENCES

1. Rajendran, K. A., Jacob, E. and Narvekar, C., 2015. ATM security using fingerprint authentication and OTP, International Journal of Current Engineering and Technology, 5(2), pp. 1157–1159.

2. Ameh, A. I., Olaniyi, O. M. and Adewale, O. S., 2016. Securing cardless automated teller machine transactions using bimodal authentication system, Journal of Applied Security Research, 11(4), pp. 469-488.

3. Alebiosu, M. I., Yekini, N. N., Adebari, F. A. and Oloyede, A. O., 2015. Card-less electronic automated teller machine (EATM) with biometric authentication, International Journal of Engineering Trends and Technology, 30(1), pp. 99–105.

4. Kanagalakshmi, K. and Chandra, E., 2014. Log-gabor orientation with run-length code-based fingerprint feature extraction approach. Global Journal of Computer Science and Technology Graphics & Vision, 14(4), pp. 975-4172.

5. Jain, A., Prabhakar, S. and Hong, L., 1999. A multichannel approach to fingerprint classification, IEEE Transactions on Patt. Anal. Mach. Intel, 21(4), pp. 348-359.

6. Ravikumar, S., Vaidyanathan, S., Thamotharan, S. and Ramakrishan, S., 2013. A new business model for ATM transaction security using fingerprint recognition, International Journal of Engineering and Technology (IJET), 5(3), pp. 2041-2047.

7. Padmapriya, V. and Prakasam, S., 2013. Enhancing ATM security using fingerprint and GSM technology, International Journal of Computer Applications, 80(16), pp. 43-46.

8. Oruh, J. N., 2014. Three-factor authentication for automated teller machine system, International Journal of Computer Science and Information Technology & Security (IJCSITS), 4(6), pp. 160–166.

9. Awotunde, J. B., Jimoh, R. G. and Matiluko, O. E., 2015. Secure automated teller machine using fingerprint authentication and short-code message in a cashless society. Proceedings of the 12th International Conference of Nigeria Computer Society, pp. 99–110.

10. Nischarkumar, H. and Sharath, K. R., 2016. Card less ATM cash withdrawal: a simple and alternate approach, International Journal of Computer Science and Information Technologies (IJCSIT), 7(1), pp. 126–128.

11. Ganesh, K. S. and Bulamurugan, C. R., 2018. Enhancement of smartness and security in atm by global system for mobile communications, Journal of Engineering Science and Technology, 13(7), pp. 2065-2083.

12. Dobraunig. C., Eichlseder M., and Mendel, F., Analysis of SHA-512/224 and SHA-512/256, 2015. In Iwata T., Cheon J. (eds) Advances in Cryptology – ASIACRYPT 2015, Lecture Notes in Computer Science, 9453. Springer, Berlin, Heidelberg.

13. Feng, Z. and Xiaoou, T. Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction, Pattern Recognition Letters, 40, pp. 1270-1281.

14. Haralick, R. M. and Linda, S.G., 1992, Computer and robot vision, Addison- Wesley, pp. 28-48.1

15. More, M., Kankal, S.,Kharat, A. &Adhau R (2018). Cardless Automatic Teller Machines (ATM) Biometric System Design with Human Fingerprints. International Journal Advance Engineering and Research Development 5(5) pp. 392-399.