International Journal of Software Engineering and Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 5 Issue 1, pp. 36-51, February 2019
©Universiti Malaysia Pahang
https://doi.org/10.15282/ijsecs.5.1.2019.3.0053

BIOMETRIC BASED POINT- OF- SALE AUTHENTICATION SYSTEM

Abikoye O. C [1], Afolabi, G. K [2], Aro, T. O [3]

[1, 2] Department of Computer Science, Faculty of Communication & Information Sciences
University of Ilorin, Ilorin, Nigeria.
Email: kemi_adeoye@yahoo.com

[2] Department of Computer Science, Lens Polytechnic Offa, Offa, Kwara State
Nigeria.
Email: ganiyatunclefatty@yahoo.com

[3] Department of Mathematical & Computing Sciences, Faculty of Pure Applied Sciences
KolaDiasi University, Ibadan, Oyo State, Nigeria
Email: taye.aro@koladaisiuniversity.edu.ng

ABSTRACT

Several problems are encountered by cardholders at the point of sale (POS) terminal, these include; inadequate security of automated teller machine (ATM) card through theft, not remembering personal identity number (PIN) and the problem of identifying cardholder as the owner of the card, these have caused delay process in transactions and also reduce the integrity of the POS machine. The existing POS machine uses PIN-Card as an authentication process in which the security can be easily breached. This paper proffers a solution to reduce the identified problems by applying a biometric system into POS machine. Iris scan was introduced at the authentication level of the existing POS machine. A system prototype was designed to imitate a typical PIN-card based POS system that used iris recognition to improve upon the security of the POS. The developed system demonstrated a two-tier architectural structure for recognition: the identification and verification module. The verification module which focused on the enrolment, normalization, localization, extraction of features and matching of iris images obtained from CASIA database. The experimental results showed that the developed system could significantly minimize cardholder fraud at the POS machine if not totally eradicated.

Keywords: Automated Teller Machine (ATM), Biometric system, Point of Sale (POS), Personal Identity Number (PIN).

INTRODUCTION

A Point of Sales (POS) is an electronic banking outlet that enables customers to complete the basic financial transactions using debit or credit cards without the aid of bank representative or teller (Ahsan, Iqbal, Hussain, & Nadeem, 2016); it is used in describing the technology a customer employed to make payment for exchange of goods and services (Alimi, Rosenberger & Vernois, 2014). This device enables a card owner to have immediate online access to money and information in the customer's bank account through debit or credit cards. In POS operation, merchants give the total amount to be paid to customer, indicate the amount and may make available an invoice and create a directory for payment by the customer. A customer makes a payment to the merchant in exchange for goods or services using POS. The POS is much more complex than the cash registers due to the fact of its capacity to record, process buyer orders using cards.

Today, in developing nations, the POS systems are common due to the fact that they offer quick and suitable means for businesses (Kabir & Han, 2016). These systems have important business activities such as transactions based online process, online business facilities, security, taxes, and various management reports. Hence, with the rise in number of transactions in supermarkets and the competitive environment for business in developing countries, guaranteeing the effective security platform becomes very essential. One of the major problems linked to use of credit and debit cards using POS during transactions is that the people with cards having the PIN code turn into owner of that account, without any other verification means of actual account holder (Bhosale & Sawawant, 2014).

There are several authentication methods of POS like passwords, debit cards, and PINs; these are conventional approaches to POS security verification. These approaches are not generally dependable due to the fact that it can be misplaced, work out or stolen by people (Jafri & Arabnia, 2009). Passwords and PINs are usually very difficult to remember or might be guessed by someone; cards and the like can be reproduced, forgotten or lost. There is need to reduce the security flaws in the conventional authentication methods of POS in order to have smooth transactions in point-of-sales terminal. For the effective and efficient operations of security systems, accurate and automatic recognition of persons is becoming increasingly important. Among the security of information techniques, biometric system has been identified to be one of the robust techniques (Kangra & Kant, 2015).

Biometric involves the identification of an individual using the feature vectors derived from biological or physiological characteristics (Singhal, Gupta, & Garg, 2012). Biometrical technologies include face, iris, hand geometry, fingerprint, palm print, keystroke, gait, hand vein, retina, voice, and signature (Jafri & Arabnia, 2009). Thus, a biometrics which uses either the behavioural or physiological characteristics of an individual to identify such individual is being used to replace such conventional methods of securing POS terminal (Gale & Salankar, 2014).

This paper integrated a biometric system with POS terminal to minimize the challenges aforementioned. Iris scan was introduced together with passwords or PINs to be the authenticating means during transactions. The iris authentication is a physiological method of biometrics that uses recognition of pattern based on high-resolution images of any of the irises of a person eyes. It is a dependable approach to visually recognizing people with the capturing being done at distance not more than 1 meter. This technique of biometric is quite useful in situations where a large database will need to be searched for recognition while still ensuring there are minimal or no false matches (Daugman, 2009; Gale & Salankar, 2014).

RELATED WORK

Tiwari, Verma, Jaiswal and Sarve (2018) applied iris recognition technique to the security of electronic mail due to the fact that Authentication of an individual is important and can be perfectly achieved by any of the available biometric system (fingerprint, face, voice, signature, iris and palm print) The system function by scanning / capturing an image and a matching algorithm (any applicable mathematical functions) are being used to match the input image with stored image. They adopted the use of iris recognition due to the fact that it is the most reliable, unique and stable biometric technique over a period of time.

Tawde and Lakshmi (2017) presented a system for biometric authentication for verification of the account holder at the Point of Sale terminal or while using micro-ATM device for banking services. The study suggested that authentication based on biometrics would help in making the security of the account holder stronger and also reduce the frauds up to large extent. Also if the account holder makes use of registering the nominee for his account then the biometric authentication can be supported by sending One Time Password on registered mobile number of the primary account holder to make the transactions transparent and in benefit of the account holder.

A cardless access to POS transactions was developed (Dileepsai & Sudarvizhi, 2016). The system ensured high-level security and simplicity; the proposed method helped in making POS (Point-of-Sales) transactions safer and card-less operation. The study also discussed the technique of making transactions in the absence of card by a numerical identity matching which was done by using a portable hardware and finger vein biometric authentication at the final stage of the transaction, where the user's mobile number was used as the numerical identity.

Ugoh, Onyeizu, Ugwunna and Uwa (2015) responded to the challenges encountered when using internal banking by introducing biometric systems and smart cards as access control methods, a two-level based authentication was developed and attached to the main banking software to reduce these problems. The system employed identity card of staff for identification and authentication by biometric using fingerprint. The methods of the Object-Oriented Analysis, Design Methodology (OOADM) and the prototyping methodology were adopted for the systematic review.

A program prototype that imitated an ATM system using a fingerprint authentication as the means of identification was designed by (Awotunde & Adewunmi-Owolabi, 2014) in response to the problem of ATM fraud, forgetting or loss of password that has caused a lot of damage to people and organization. The use of PIN-CARD that is a very weak of security. The system adopted architectural structure centered the identification process on registration, enhancement, extraction of features and fingerprints matching. The system also adopted a backend database system that is the warehouse for all account holders' having ATM card with pre-registered fingerprints. The developed system allowed business activities, which include withdrawals, bill payment, buying through the use of credit cards and balance inquiries. The results confirmed that the system could have a positive impact in the reduction of ATM fraud if not totally eradicate it.

Gupta and Sharma (2013) considered a study that applied an innovative model for biometric ATMs to replaced card system in ATM operations. The system developed an improved security in authentication which also keeps the service user from unauthorized access. The proposed system users are to be verified with biometric system, PIN and choice of bank branch. These ATMs communicate with the farmers in their local dialects as the system is developed for the rural farmers and semi-literate people. The system minimized complexity with authentication as authentication is always with you and of effective security. The system reduced environmental pollution problem cause by excess number of plastic cards. It also saves time, cost, and efforts compared with card-based ATMs and also saves

Aranuwa and Ogunniye (2012) developed an effective biometric system for authentication of e-payment platform that consolidated security as well as fraud prevention in Nigeria. The archetype of the developed system with multi-stage recognition mechanism designed in the study indicated and demonstrated that the enhanced method would aid the elimination of insecurity in online payments with a realistic degree of trust and acceptability for wider patronage of electronic payment solutions in Nigeria.

Umamaheswariph, Sivasubramanian and Kumar (2010) presented an Online Credit Card Transaction Using Fingerprint Recognition. The study proposed a new solution that combined fingerprint biometric recognition with online credit card transactions. The proposed system provided more security than the existing system with fingerprint recognition because of the uniqueness of finger print. The system out rightly removed the stress of remembering of passwords before a transaction can be made, with the fingerprint replacing the password.

METHODOLOGY

The biometric Point-Of-Sale system employed two modules, the identification and authentication of the cardholder. The system designed produced a more secured means of authenticating the cardholder at a every Point Of Sales terminal with the use of iris biometric technique. The system's initial stage required the use of Automate Teller Machine card and Personal Identification Number for the identification of users, at the authentication stage the iris image is considered as input in order to match the user identity, when the input to the iris sensor matches to the template stored in database then the transaction is processed, in case of mismatch, transaction gets declined completely. The system framework is illustrated using block diagram as shown in Figure 1.

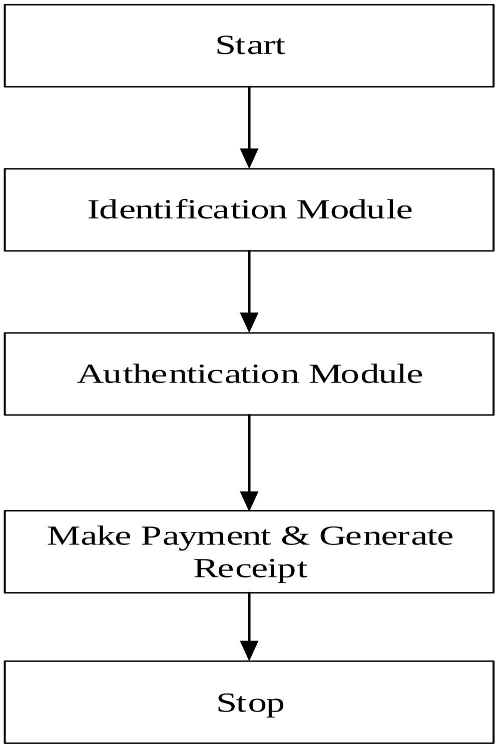


Figure 1: Block Diagram of the Proposed Biometric POS System

From Figure 1, the identification module involves Identification with ATM card number, ATM card verification value (CVV), and customer's PIN The ATM card which could be any of master card, verve, visa and so on whose number must be of sixteen (16) digits, the CVV number which is in three (3) digits, the PIN which is a typical four (4) digits number and any combination of digits 0-9 would be adopted for identification.

IDENTIFICATION MODULE PHASE

The phase shows the identification stage of the developed system as shown in Figure 2.

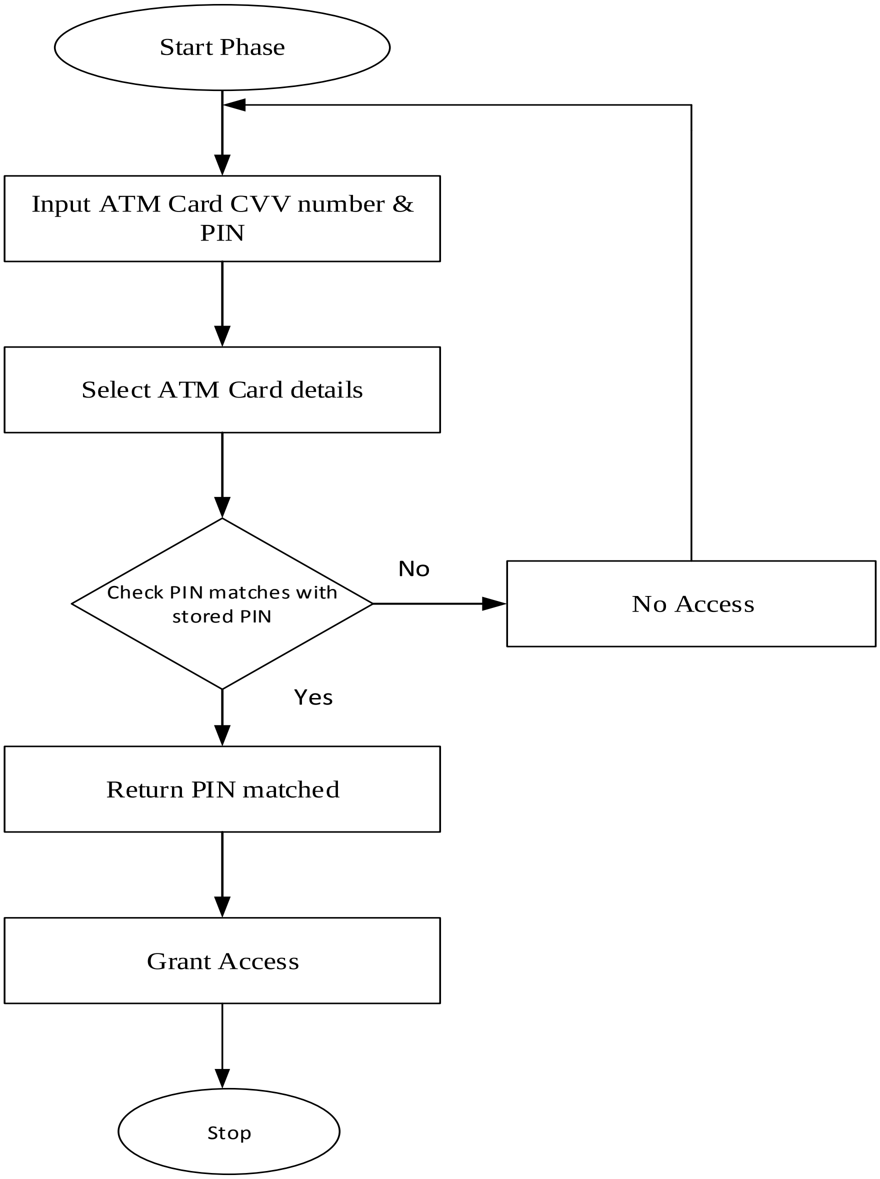


Figure 2: Identification Phase of developed Biometric POS System

AUTHENTICATION MODULE PHASE

The phase displays the authentication section of the Biometric POS system as shown in Figure 3.

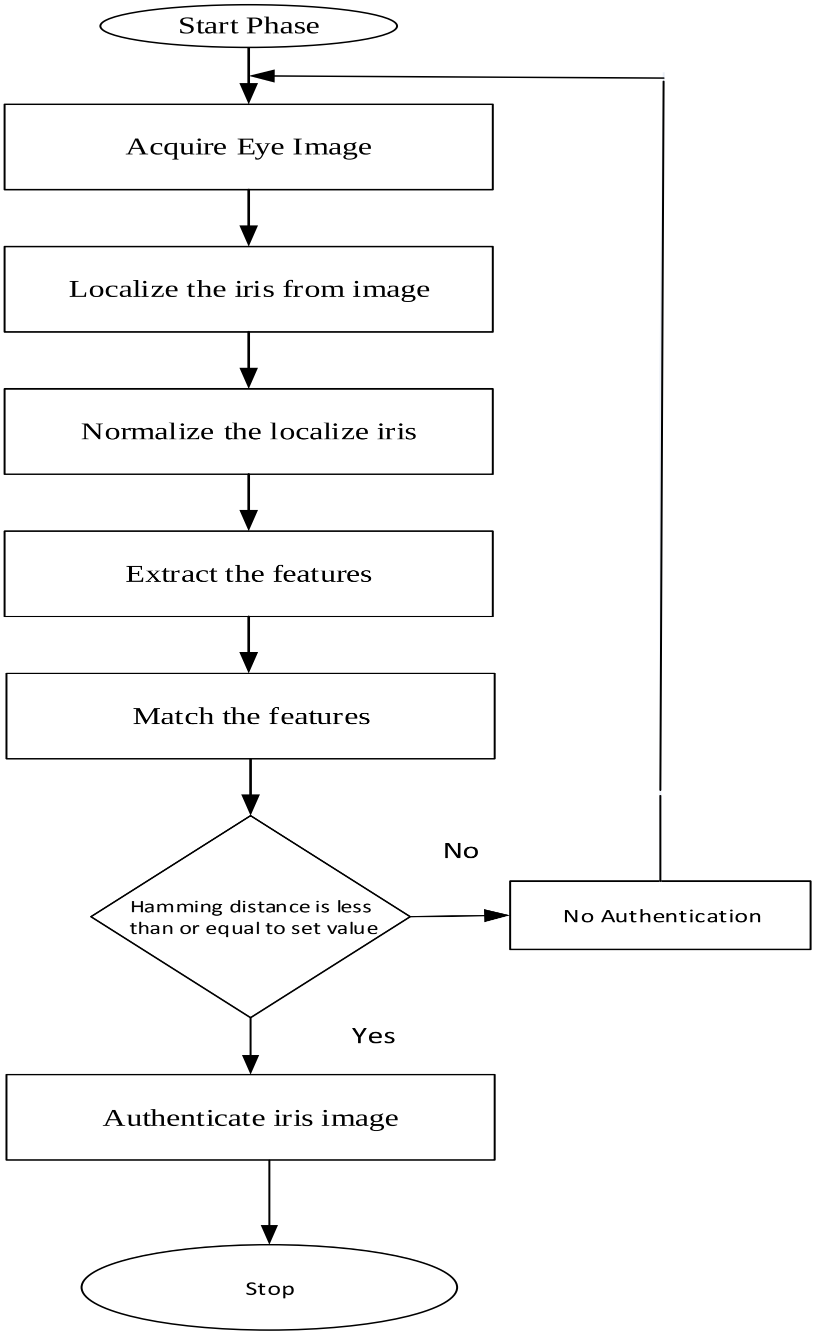


Figure 3: Authentication Module Phase

DATABASE DESCRIPTION

The iris images used in this study were obtained from publicly available database of Chinese Academy of Sciences- Institute of Automation (CASIA). The database is an open source which comprises of 756 eye images gray-scaled with 108 distinct eyes or classes and 7 unlike images of each distinct eye. Images from each class were taken from two sessions with one-month intermission between sessions. The capturing of images was achieved especially on iris recognition research using customized digital optics developed by the National Laboratory of pattern recognition, China. The eye images are mainly from persons of Asian descent, whose eyes are characterized by irises that are densely pigmented, and with dark eyelashes. Due to specialize imaging conditions using near infra-red light, features in the iris region are highly visible and there is good contrast between pupil, iris and sclera regions.

Iris Image Segmentation

The segmentation of the iris image is done using a method developed by (Abikoye, et. al., 2014) and the algorithm used is as stated in the following steps:

Step 1: Start

Step 2: Generate Object1, Object2 (Objects are combined data types that stores the parameters representing the geometry for the boundaries of the iris, the parameters include x, y, r1, r2 where x, y are coordinates of the center of the eye image, and radius1, radius2 respectively).

Step 3: The coordinate of the center of the image of the eye is captured.

Step 4: The coordinates of 2 points on the inner boundaries of the iris (one of the 2 points is vertically above the center of the eye and the other is horizontally eastward of the center of the eye that is pX, pY respectively) is taken

Step 5: Calculate: radius1 (r1) as the distance between the center of the eye image and the a vertical point coordinates as in Equation (1).

$$\text{r1} = \sqrt{\sqrt{x1^2 + y1^2}} \qquad (1)$$

where x1 = pX.x1 – pcentre.x1,   1 = pY.y1- pcentre.y1

radius2 (r2) as space between the center of the eye image and the horizontal eastward co-ordinates as in Equation (2).

$$\text{r2} = \sqrt{\sqrt{x2^2 + y2^2}} \qquad (2)$$

where x2 = pX.x2 – pcentre.x2,   y2 = pY.y2- pcentre.y2

Step 6: Construct an eclipse using the co-ordinates of the center of the eye, radius1 and radius2 (r1 and r2).

Step7: Reiterate step 3 to step 5 for the outer boundary

Step 8: Store the co-ordinates of the center of the eye image and the 2 calculated radius for the inner boundary into Object1 &Store the co-ordinates of the center of the eye image and the 2 computed radius for the outer boundary into Object2.

Step 9: Stop.

IRIS REGION TRANSFORMATION

After segmentation of iris image, the region of eye needs to be transformed just to have fixed dimensions. This facilitates the extraction of features and compensate for the removal of dimensional inconsistencies such as dilation of the pupil from changing the level of illumination, rotation of camera, head tilt, eye rotation within the eye socket. The Daugman's rubber sheet model is applied for normalizing the iris annular region to a rectangular region. This model remaps each point within the iris region to polar coordinates (r, θ) where r is on the interval [0, 1] and θ is angle [0, 2π] from the Cartesian coordinates. The remapping of the iris region from *(x, y)* Cartesian coordinates to the normalized non-concentric polar representation is modeled as in Equation (3)

$$I(x(r,\theta),y(r,\theta))\rightarrow I(r,\theta) \qquad (3)$$

$$\text{with } x(r,\Theta) =(1- r)x_P(\Theta) +rx_1(\Theta)$$
$$y(r,\Theta) =(1- r)y_P(\Theta) +ry_1(\Theta)$$

The extraction of features is the most significant phase of biometric recognition through iris, which is accomplished by converting image pixel into bits codes. This study used Fast Wavelet Transform for the feature extraction phase since it has been proven to provide easier, simpler, faster and limited / no computational error. The resulted extracted features are later passed as templates for matching. The 2048 bits data was extracted in the following format after the transformation;
For value of pixel greater than 0.5 adopt 11
For value of value greater than 0 but less than 0.5 adopt 10
For value of value greater than -0.5 but less than 0 adopt 01
For value of value less than -0.5 adopt 00.

ALGORITHM OF FAST WAVELET TRANSFORM (FWT)

```
Step 1:  Input normalized image of gray-scale image for size 480 × 160 pixels.
Step 2: Store pixel value into a linear array a(n) where n = width * height
Step 3: Conduct encoding for FWT
        (a) Take each pixel row in the linear array a(n) and store as vector Vec1d
        (b) Transform each vector Vec1d using FWT algorithm
        (c) Store transformed vector(s) back in the linear array a(n)
        (d) Take each pixel column in the linear array a(n) and store as vector vec1d
        (e) Transform each vector using FWT algorithm
        (f) Store transform vector back into the linear array a(n)g) Extract 2048 bit FWT values
            from the array and store in a new array as a template
Step 4: Reiterate steps 1 to step 3 for second normalized gray-scale image
Step 5:  Stop
```

MATCHING OF IRIS IMAGE

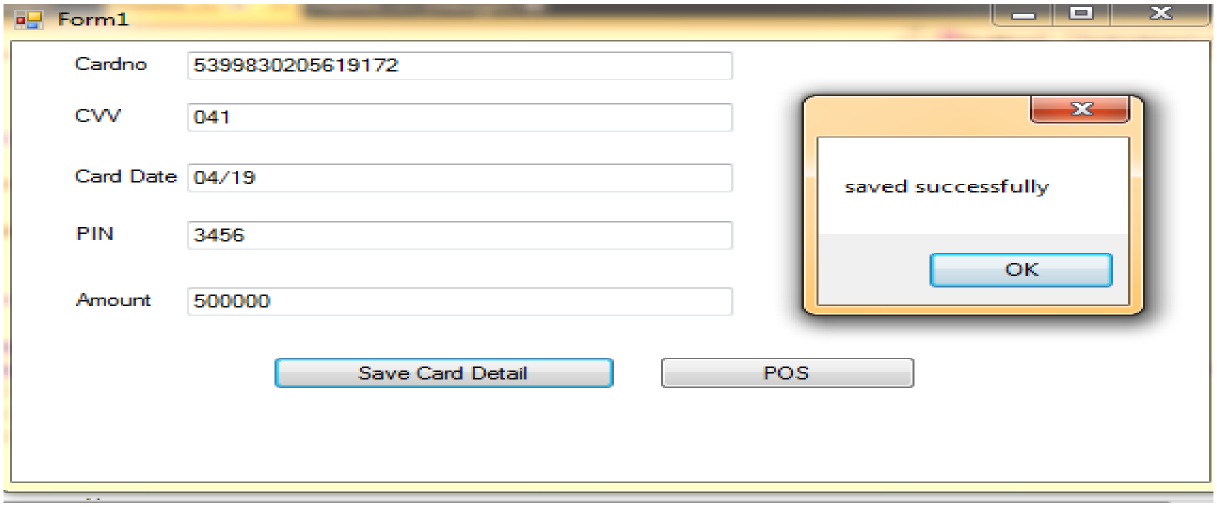
The template of iris is compared with that of database for recognition task, it gives the authentication result. Several algorithms could be used for matching of iris images but for the scope of this study Hamming distance was employed due to its fastness and simplicity features it demonstrated, the algorithm of Hamming distance incorporates noise masking so that only important bits are used in calculating the Hamming distance between two iris templates. When considering the Hamming distance, only those bits in the iris pattern that corresponds to ‘0’ bits in noise masks of both iris patterns were used in the computation. The Hamming distance between the new preprocessed iris image and the stored iris image were calculated. Authentication was allowed for hamming distance of less than or equals to threshold of 0.3, in which the user was authenticated to complete the transaction by making payment with the POS else the user will be denied payment.

RESULTS AND DISCUSSION

The result is presented in two different modules; the identification module of POS and the authentication module using iris.

RESULT OF POS REGISTRATION MODULE

Every cardholder must have an account with the issuer’s banks where the card details have been saved, this page enables the admin to register users using banks simulation methods & this is accomplished by collating the total cost for the purchased product & thus prompting the admin to input the card number, the ATM CVV number, the ATM expired date and the corresponding PIN as shown in Figure 4. After inputting every detail the button ‘Save Card Detail’ is selected to enter all user’s ATM details into the database, then a dialog box is displayed to inform the user that the details have been saved having met with the corresponding fields requirements.



Cardno 5399830205619172

CVV 041

Card Date 04/19

PIN 3456

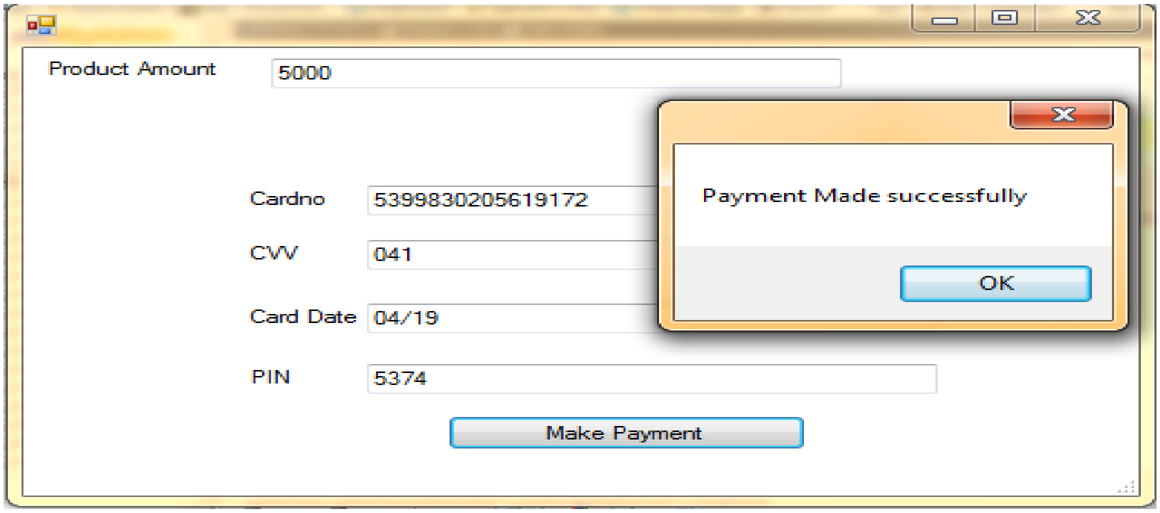
Amount 500000

saved successfully

Figure 4: POS Registration Page

RESULT OF POS PAYMENT PAGE

The payment page allowed the admin to process the customer payment using the ATM card given at the point of purchase by entering the details on the card & confirming it with the saved database details, if true, the amount on the customer’s bill is compared with the amount in the database to check if the bill can be deducted from the customer's account and if true, the amount is deducted as shown in Figure 5.



Product Amount: 5000

Cardno: 5399830205619172

CVV: 041

Card Date: 04/19

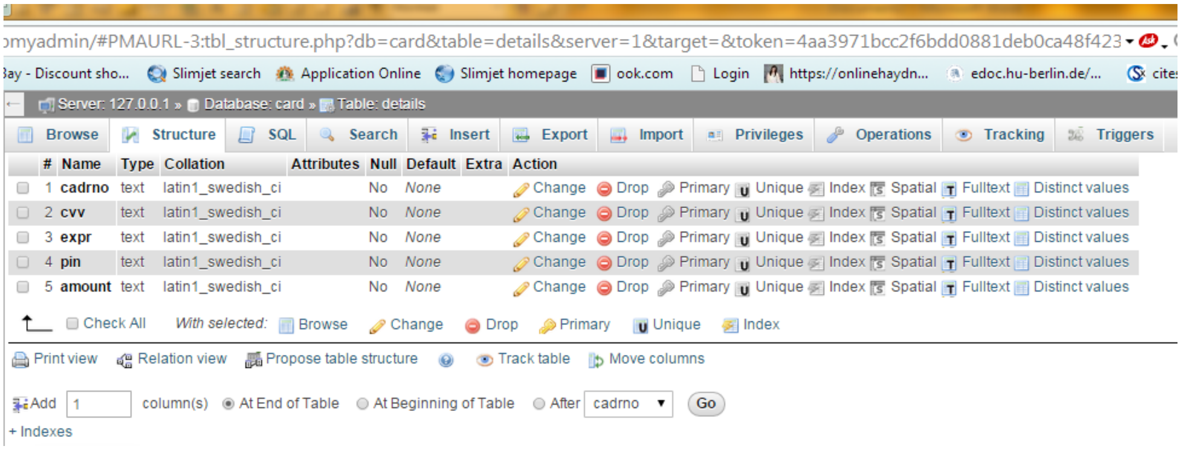
PIN: 5374

Payment Made successfully

Figure 5: POS Payment Page

RESULT OF POS TABLE STRUCTURE

The database was created using the SQL, a query language and using XAMPP server as the webserver; the database is named 'card'; it contains registration table named 'details' where the user card's information are registered. The table fields are CARDNO, CVV, EXPR, PIN & AMOUNT whereby each is of type 'text'as depicted in Figure 6. The POS Entry Details is shown in Figure 7.



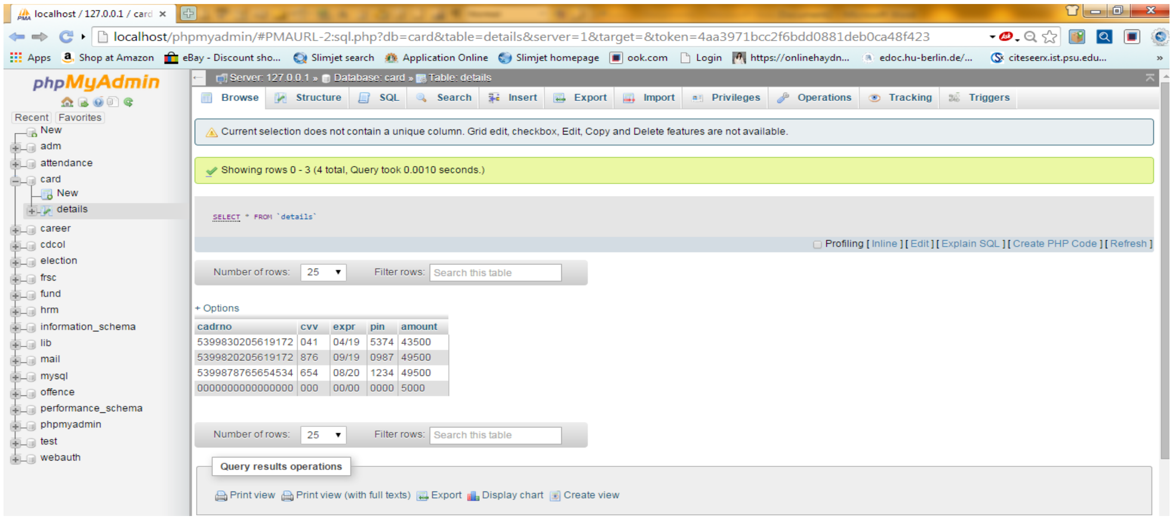
omyadmin/#PMAURL-3:tbl_structure.php?db=card&table=details&server=1&target=&token=4aa3971bcc2f6bdd0881deb0ca48f423

Server: 127.0.0.1 » Database: card » Table: details

#	Name	Type	Collation	Attributes	Null	Default	Extra	Action
1	cadrno	text	latin1_swedish_ci		No	None		Change Drop Primary Unique Index Spatial Fulltext Distinct values
2	cvv	text	latin1_swedish_ci		No	None		Change Drop Primary Unique Index Spatial Fulltext Distinct values
3	expr	text	latin1_swedish_ci		No	None		Change Drop Primary Unique Index Spatial Fulltext Distinct values
4	pin	text	latin1_swedish_ci		No	None		Change Drop Primary Unique Index Spatial Fulltext Distinct values
5	amount	text	latin1_swedish_ci		No	None		Change Drop Primary Unique Index Spatial Fulltext Distinct values

Add 1 column(s), After: cadrno

Figure 6: POS Table Detail Structure



Current selection does not contain a unique column. Grid edit, checkbox, Edit, Copy and Delete features are not available.

Showing rows 0 - 3 (4 total, Query took 0.0010 seconds.)

```
SELECT * FROM `details`
```

cadrno	cvv	expr	pin	amount
5399830205619172	041	04/19	5374	43500
5399820205619172	876	09/19	0987	49500
5399878765654534	654	08/20	1234	49500
0000000000000000	000	00/00	0000	5000

Figure 7: POS Entry Details

Figure 7 depicts the registered user's information on table 'details', the customer's sixteen digits card number, the three digit cvv at the back of customer's ATM, the ATM card expriy date in month/year, the customer's Personal Identification Number and available balance saved as amount.

RESULT OF IMAGE ACQUISITION

The first phase of iris authentication method is to collect a large database consisting of several iris images from various individuals, and CASIA eye image database is selected for the implementation which has specular reflections. Figure 8 shows the collection of acquired eye images from CASIA database that was used for customer 1, customer 2, customer 3, customer 4, customer 5 and customer 6.

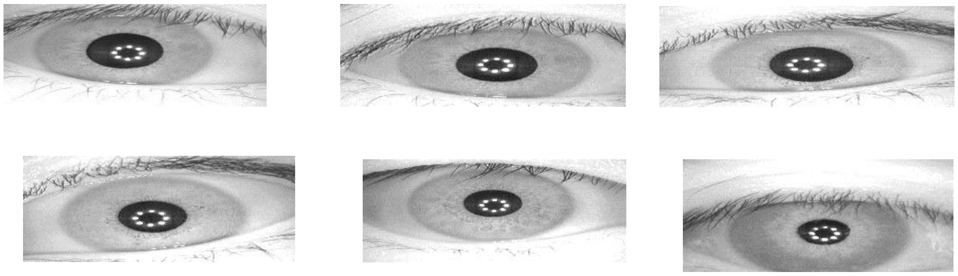


Figure 8: Eye Images from CASIA Database

RESULT OF IRIS LOCALIZATION

The iris localization done using Abikoye et al (2014) model prove successful, Figures 9 shows the representation of the localized customers' iris.

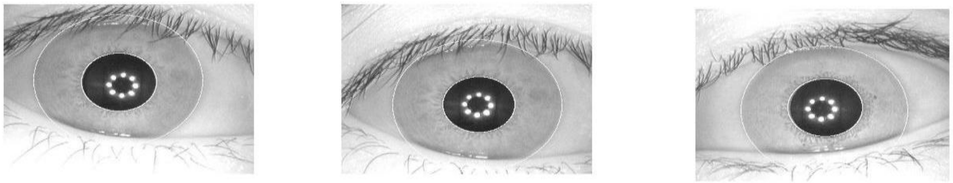


Figure 9: Localized Customer's Irises

RESULT OF IRIS NORMALIZATION

The process of normalization produced irises and some results are shown in Figure 10. To generate 2048 bits the normalized iris was converted to 480 by 160 pixels.

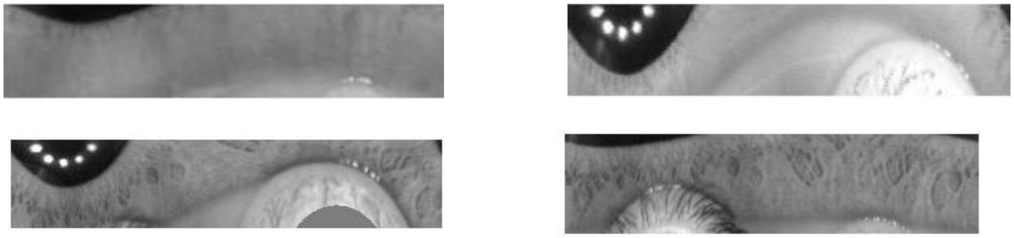


Figure 10: Normalized Customers' Irises

RESULT OF IRIS FEATURE EXTRACTION

The features of the iris were encoded. For value of pixel greater than 0.5, 11 bits is extracted, for pixel value greater than 0 but less than 0.5, 10 is extracted, for pixel value greater than -0.5 but less than 0, 01 is extracted and when pixel value is less than - 0.5, 00 is extracted to generate the 2048 bit iris codes. Figure 11 is a representation of the extracted features for customer 3.

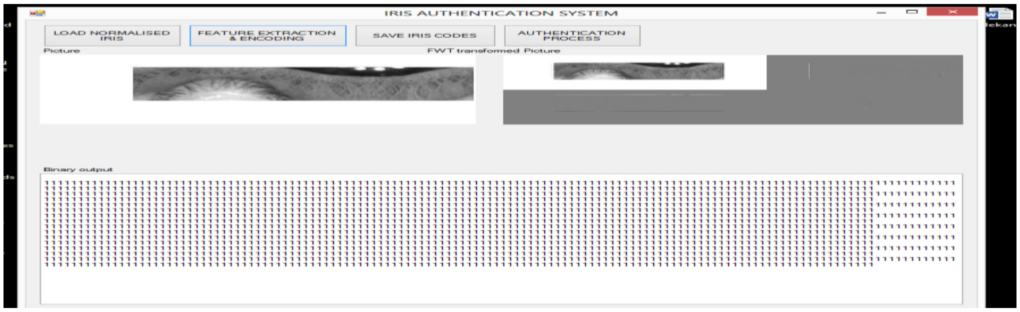
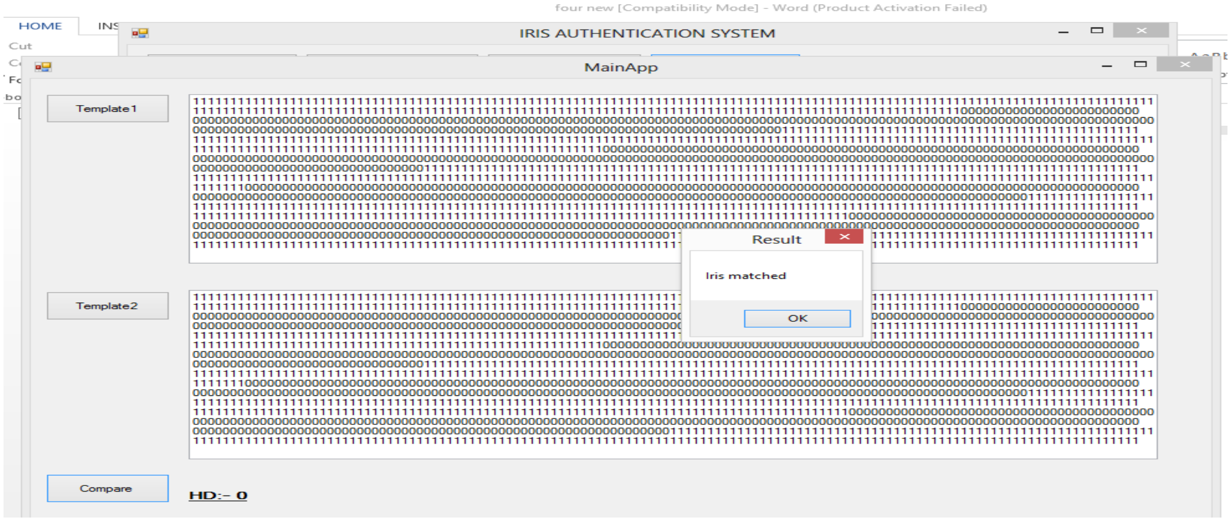


Figure 11: FWT Feature encoding for normalized iris 3

IRIS FEATURE MATCHING

After encoding the iris, the bits codes generated were saved as template and can be referred for comparison. Figure 12 is a representation of feature matching template whereby the newly generated templates is compared with the existing template.



four new [Compatibility Mode] - Word (Product Activation Failed)

IRIS AUTHENTICATION SYSTEM

MainApp

Result

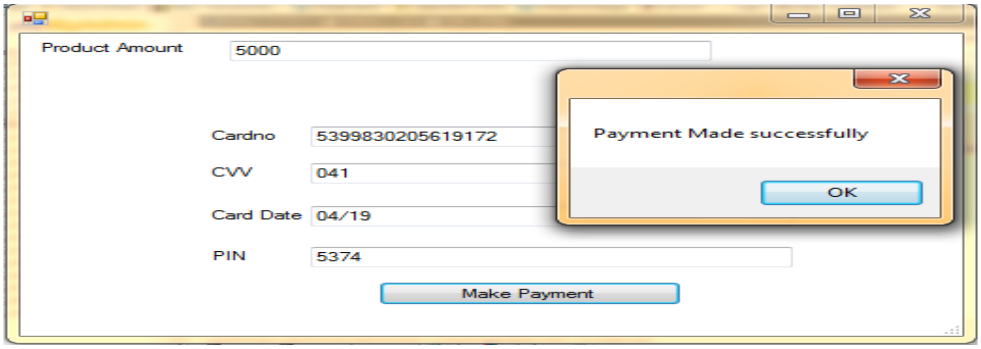
Iris matched

HD:- 0

Figure 12: Feature Matching for Template 3

RESULT OF AUTHENTICATION OF AUTHORIZED CUSTOMER

The system for authorized customers is described as follows:
Stages involves for customers with valid PIN and Iris. Save the customer ATM details as demonstrated, If the details are saved successfully then make payment (and match PIN) as in shown in Figure 13. If the PIN matched, the system waits for five (5) seconds before it acquires the eye image, localize and normalize the iris as in Figure 14. After normalization the feature extraction and matching is done using FWT. If the two iris Templates matches then payment can be made



Product Amount 5000

Cardno 5399830205619172

CVV 041

Card Date 04/19

PIN 5374

Payment Made successfully

Figure 13: Localization of Iris from the Acquired Eye Image

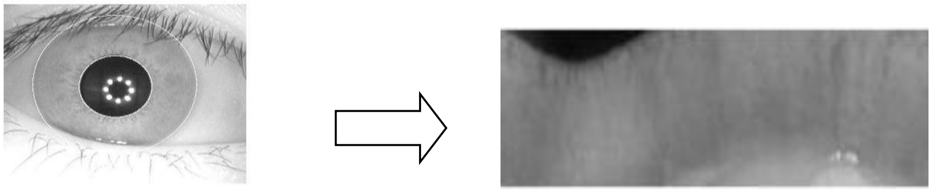
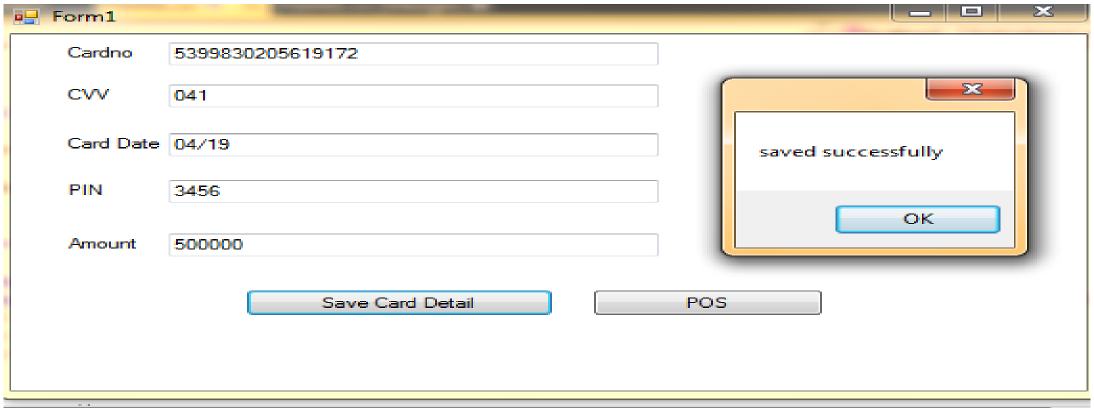


Figure 14: Normalization of the Localized Iris

RESULT OF UNAUTHORIZED CUSTOMER (MIS-MATCHED PIN)

Customers with incorrect PINs were disallowed to use the system. The process followed stepwise approach. Save the customer ATM details as shown in Figure 15.



Form1

Cardno 5399830205619172

CVV 041

Card Date 04/19

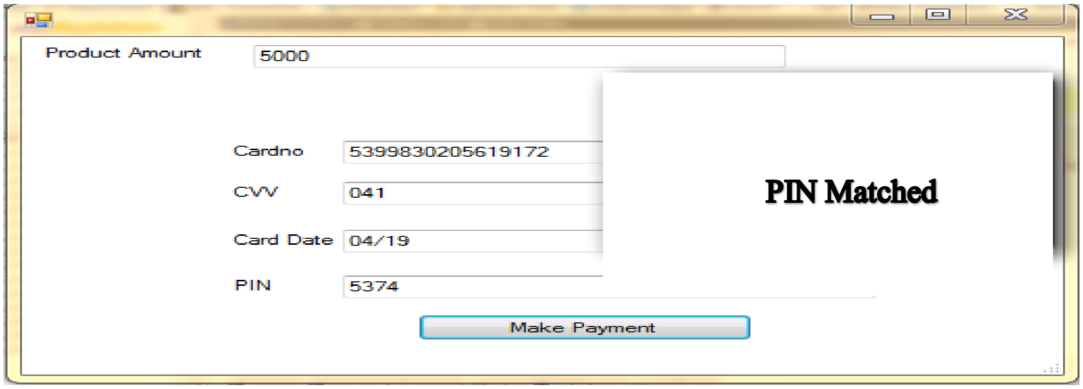
PIN 3456

Amount 500000

saved successfully

Figure 15: Saving Customer Card Details

If the details are saved successfully then make payment (and match PIN) as in shown in Figure 16.



Product Amount 5000

Cardno 5399830205619172

CVV 041

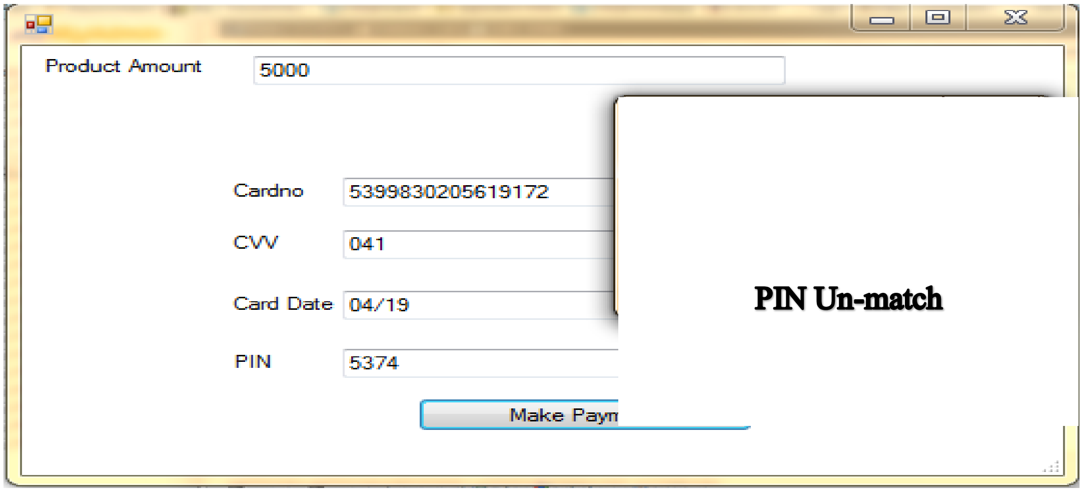
Card Date 04/19

PIN 5374

PIN Matched

Figure 16: Payment with Matched PIN

If the PINs doesn’t match, the system waits for five (5) seconds before it allows the user to enter another PIN or terminate the process as demonstrated in shown in Figure 17



Product Amount 5000

Cardno 5399830205619172

CVV 041

Card Date 04/19

PIN 5374

PIN Un-match

Figure 17: Payment for Mismatched PIN

CONCLUSION

The point of sale is an electronic device used in completing financial transaction using credit/debit cards needs to be protected from all forms of security flaws which can be as a result of misappropriation of debit cards. The paper developed a system to make financial transactions easier and convenient to all POS stakeholder by the introduction of iris scan at the authentication level of POS transaction to produce a highly secured POS compared to the existing POS. The adopted Fast Wavelet Transform used in this study for feature extraction has been identified by several researchers to be easy, fast and simple in carrying out the matching of individual irises.

REFERENES

Ahsan, K., Iqbal, S., Hussain, M. A., & Nadeem, A. (2016). A mobile payment model using biometric technology 1. *International Journal of Advances in Sciences Engineering and Technology*, *4*(4), 17–20.

Aranuwa, F O & Ogunniye, G. B. (2012). Enhanced Biometric Authentication System for Efficient and Reliable e-Payment System in Nigeria. *International Journal of Applied Information Systems*, *4*(2), 56–61.

Awotunde, J. B., & Adewunmi-Owolabi, F. T. (2014). Fingerprint Authentication System: Toward Enhancing ATM Security. *International Journal of Applied Information Systems*, *7*(7), 27–32.

Bhosale, S. T, & Sawawant, B. S. (2014). Secuirty in E-Banking Via Cardless Biometric. *International Journal of Advanced Technology & Engineering Research (IJATER)*, *2*(4), 9–12.

Daugman, J. (2009). How Iris Recognition Works. *The Essential Guide to Image Processing*, *14*(1), 715–739. http://doi.org/10.1016/B978-0-12-374457-9.00025-1

Dileepsai, Y., & Sudarvizhi, S. (2016). Card Less Access to POS Transactions. *Internatioanl Journal of Applied Engineering Research*, *11*(7), 5231–5236.

Gale, A. G., & Salankar, S. S. (2014). A Review On Advance Methods Of Feature Extraction In Iris Recognition System. *"IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)," 3*(1), 65–70. http://doi.org/10.5897/IJCER11.046

Gupta, N., & Sharma, A. (2013). Review of Biometric Technologies used for Biometric system. *Internaltional Journal of Engineering and Innovative Technology*, *3*(2), 460–465.

Jafri, R., & Arabnia, H. R. (2009). A Survey of Face Recognition Techniques. *Journal of Information Processing Systems*, *5*(2), 41–68.

Kabir, A., & Han, B. (2016). An Improved Usability Evaluation Model for Point-of-Sale Systems An Improved Usability Evaluation Model for Point-of-Sale Systems. *International Journal of Smart Home*, *10*(7), 269–282. http://doi.org/10.14257/ijsh.2016.10.7.27

Kangra, M., & Kant, C. (2015). Biometric System and Its Challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(6), 710–716.

Singhal, Z., Gupta, P., & Garg, K. (2012). Biometric Recognition : Personal Identification Technique. *International Journal of Computational Engineering & Management*, *15*(3), 6–10.

Tawde, P., & Lakshmi, G. P. (2017). Enhancing Micro-ATMs and POS Terminals Authentication System Using AdvancedBiometric Techniques. *IOSR Journal of Computer Engineering*, *19*(4), 74–77. http://doi.org/10.9790/0661-1904017477

Tiwari, S., Verma, P., Jaiswal, S., & Sarve, M. (2018). Biometric Authentication using Iris for Email Access, *8*(4), 17008–17010.

Ugoh, D., Onyeizu, M. N., Ugwunna, C., & Uwa, C. O. (2015). Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(6), 529–532. http://doi.org/10.17148/IJARCCE.2015.46114

Umamaheswariph, M ., Sivasubramanian, S & Kumar, B. H. (2010). Online Credit Card Transaction Using Finger Print Recognition, *2*(5), 320–322.