EATM: Hybrid Facial Feature Extraction Algorithm for Enhancing ATM Security System

[1]L.William Mary, [2]M.Kannan, [3]K.HemaAishwarya, [4]T.Ajisha

[1,2,3,4]Assistant Professor,
Department of Computer Science and Applications,
St.Peter's Institute of Higher Education and Research (SPIHER), Chennai, India.
DOI: http://doi.one/10.1729/Journal.22231

Abstract : Banking sector and Automated Teller Machine (ATM) system is one of the vital things to do deposit and withdrawal. Simultaneously, in the computerized world, cyber crime was also increasing day by day. This paper mainly focuses to secure the client's account under the help of user's body feature. Feature extraction (FE) is used here to reduce the feature's dimensionality and also which is also used for various curvature processes. Nowadays cyber crime is also one of the main issues, because fraudsters are playing every place like schools, bank, companies, marketing places viz. Now a days security problem is mostly occurring in the ATM mode. The current ATM system is secure, but still it has some small drawback like connection error during generating OTP. This paper, overtake this kind of security problem of the utilization of feature extraction methods to secure our bank account details as much as safely and confidentially from the fraudsters. For this issue, a new hybrid algorithm HFFE (Hybrid Facial Feature Extraction) has proposed.

Index Terms **- Automated Teller Machine (ATM), Credit Card, HFFE algorithm, QR code, OTP, Image Processing.**

I. INTRODUCTION

ATM is an electronic based device used by banking sector that allows bank user's to complete their common transaction functions without the help of others [7] and it is an era of a banking sector. Today everyone has using ATM for various banking and transaction purpose. The current ATM system is using PIN based and OTP based security. This security system helps the user to protect their account information from the unauthorized person. When we are about carried about out the transaction the PIN provides as an input which is encrypted at the client end and the data is decrypted at the server end. When an encryption and decryption [6] is simulated, the transaction is carried out in the form of withdrawal of money. As the technology is getting improved day by day, security is also improved a lot and fraudsters also increased. The input data of ATM security pin would be known by third-party which causes the data can easily hacked and/or retrieved by fraudster's activity. This is the biggest drawback of accessing ATM for doing banking process. Till now many security systems have been followed by the ATM center like biometric, OTP, etc. On the other words, even though, sometimes the third person might be guessing our password or stolen the password, at this terrible situation the user can't do anything. Our main intent is to increase the security for the society peoples against for the fraudsters. This paper proposes a HFFE algorithm for protecting our bank account details from the hackers and/or fraudsters. Generally, ATM is an electronic device [7] the machine doesn't know whether the present cardholder is an original client or a duplicate person. But the ATM systems assume if the card's PIN is correct, then the user is validate user otherwise not. For this confusion HFFE algorithm is proposed to trace the fraudsters and authorized user.

II. LITERATURE REVIEW

Many researchers have focused on to increases a security for the ATM system. Some of them would have done it. Madhuri More [3] et al., has been proposed a biometric security system for protecting the account details. In that system checks the card and cardholder at two ways like one system is the second level authentication in which this is an extracted from the existing level (PIN, OTP, etc.) and another one is, it checks the specified withdrawal amount. It means, the cardholder is an original user then the user will enter the correct amount. Suppose if the cardholder enter the money greater than his account, then the person is a fake, and that unauthorized person will not proceed further. Shrutanjay Kulkarni [8] et al., uses Hidden Markov Models to trace the ATM fraudsters. In this system [8] if the fake person is identified, then the system will automatically send the High Secured Alert Password (HSAP) message to the registered mobile number (Original Client), so the cardholder can change their password within a minute. Srivatsan Sridharan [11] et al., proposes a module to improvise the security for automatic teller machine. The authors [11], introduces the time dependent password key (P_k) to generate the password. Many authors have proposed the security system based on their fingerprint. Like S. Jadhumithran [2] also uses fingerprint procedure to protect the ATM account. Also Mohammed-Bello [9] uses the second level authentication procedure for money withdrawal. Vivek V. Jog and Nilesh R. Pardeshi [10], applied a new and an advanced security model for detecting the fraudsters while ATM transaction. The system first verifies the HSAP, if it is correct, then it will continue the process otherwise card might be blocked. So the fraudulent cannot continue the ATM process. M.Priyadharshini and G.Manisha [5], uses the face recognition method to avoid this issue. They implemented a new process, if the person continuously enters the password trice, then the ATM machine captures the user's full picture and compares the profile document. If the profile is matched, then the user can allow for the further procedure otherwise it blocks the transaction.

III. EXISTING SYSTEM

Sometimes Automated Teller Machine also called Any Time Money [11]. The main intention of inventing this ATM system is to receive our savings money in the fastest way without any making delay. At first, in the banking sector does not have any ATM system to withdraw the money. If the user wants to withdraw the cash, then the user should visit the respected bank and complete the withdrawal process. Then only he can withdraw the money. But in the computerized world, all the scientific systems have been improved today. Actually, in an existing ATM system, the user can insert or swipe the card in the machine. Then the user or cardholder performs the basic ATM operations. After completing all the processes [2] and [3] the user will receive cash and a receipt from the machine.

IV. PROPOSED SYSTEM

This paper proposes a new algorithm called Hybrid Facial Feature Extraction (HFFE), which is used here for the high security purpose. This algorithm handles the security issues and it verifies the card holder while the user using ATM service. The normal ATM system is which identifies only the QR and Password of the user. But in this HFFE algorithm will detect the features (nose, lips and etc) of the user and it will execute, when the cardholder starts to type or enter the 4-digit password. So for, we protect our account information from the fraudsters. This proposed system of ATM service architecture diagram is discussed in the system architecture section [figure.3].

V. THEORY OF AUTOMATED TELLER MACHINE

An automated teller machine is an electronic telecommunication device, which enables a customer to perform financial transactions of cash withdrawal without a cashier. The first automated banking machine was created by American businessman named Luther Simjian in the year 1960. A Scottish inventor, John Shepherd-Barron, created an ATM that used for paper vouchers printed with radioactive ink so the machine could read them in 1967.

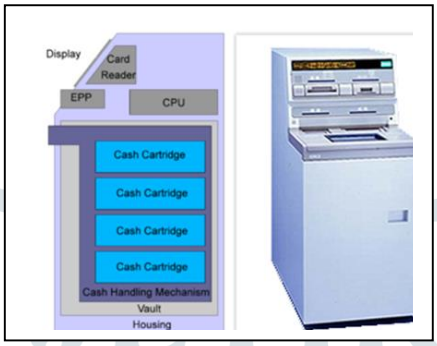

Fig 1: Traditional ATM Systems

Finally, in 1969, Donald Wetzel created the first ATM in the United States that was used plastic cards which was similar to the ones we use today. For withdrawing cash, the customer needs to identify by inserting a plastic ATM card with a magnetic strip or a plastic Smart Card with a chip which has a unique card number which is 16 digit card number, and some security information such as card expiry date, card holder name, ATM card type (master card or visa card), International debit card, Platinum debit card. Using an ATM card, customers can access the bank for deposit, withdrawal, bill payment, and third party fund transfer. There is a limitation on the amount of withdrawal from the ATM. The limit is Rs.25000 being withdrawn at a time which is being counted as one transaction.

5.1. Process of ATM

A general procedure of ATM is on discussed below:

5.1.1 Card reader

At the beginning stage of this cash withdrawal system is, user need to insert his card to the machine. Then card reader will capture the account through the information presented in the magnetic strip on the back of the ATM card.

5.1.2 PIN

In the second stage, the bank requires the cardholders to have a personal identification number (PIN) for validating and making ATM transactions. The four digit security pin can be set by a customer and this PIN can be easily recollected at any point of time as well it can be reset in case of PIN is wrongly setup or forgotten for any reason. PIN needs to be remembered by the card holder and it should not be shared with others.

Fig 2: Card Information

5.1.3 Keypad

The keypad allows the card holder to tell the bank transaction details such as what kind of transaction is required like cash deposit, cash withdrawal, balance inquiry, etc.

5.1.4 Display Screen

The screen will displays the and also leads the way to the transaction instruction to the cardholder. The ATM instruction has been presented in the figure (3).

5.1.5 QR Code

The QR code is more secure which is used for scanning the ATM machine and verification.

5.1.6 OTP

The OTP (one time password) is required to complete the transactions or to get cash from an ATM. The OTP is a random number for every transaction, which is automatically expired after two to five minutes.

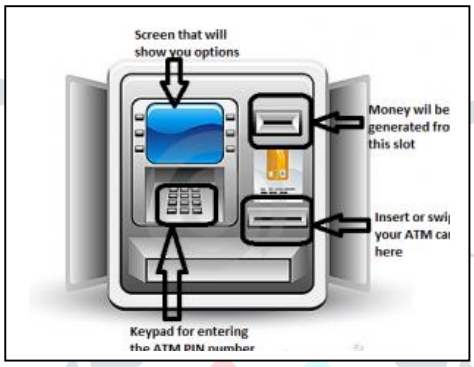

Fig 3: Instruction to use the ATM

5.1.7 Cash and Receipt

Suppose if the withdraw function is selected by the cardholder or by the client, then the cardholder can receive the entered amount and the transaction receipt from the machine with original banking details.

5.1.8 Transaction Message

After completing all the transaction process, then the cardholder or a user receives a receipt and also get the transaction information like date, time, money statement, etc., from the respected bank.

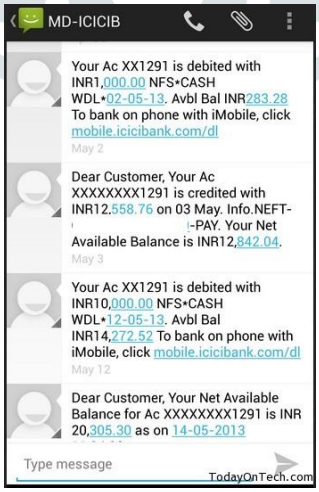

Fig 4: Bank Transaction Message

5.2 Advantages of using an ATM

Some of the main advantages of using ATM are,

- ATM is also referred as Any Time Money. So the customer can withdraw the cash at any time, like day time and morning time.
- Nowadays, ATMs will be placed in multiple locations. So no need to search the centre.
- ATM card is protected by a PIN for safe money.
- It reduces to fill out withdrawal and deposit slips as is required at the bank.

- Fast transaction and reliability.
- It reduces the customer's time.

5.3 Disadvantages of using an ATM

- It is very difficult to withdraw money if the client forgot the password or a PIN.
- People have some minor knowledge to use the ATM.
- Sometimes fraudster's people can also track the system.
- The ATM may be off-line.

VI. Role of Feature Extraction

Feature extraction method and feature detection is one of the most relevant processes of all the computer related works. This concept is most commonly used in image classification and an artificial intelligence [10]. The aim of feature extraction is extracting the feature at step by step from our object. FE is a vital thing to analyze the properties of image features. Some of the extraction techniques are given below.

6.1 Techniques for FE

6.1.1 Gabor filter

This is an image processing tool, applied for feature extraction, and stored the information of the digital images. This technique addressed the new algorithm using a neural network, which is trained by the extracted features of the Gabor filters. The original images are converted into the gray-level images and cropped into 100×100 pixel images.
Due to the various lighting conditions, the images might be a poor contrast; therefore all the images are processed with the same illumination to reach a significant representative. The standard deviation of the illumination will be shown in the equation,

$$C_{rms} = \left[\frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2\right]^{\frac{1}{2}}$$

6.1.2 Canny Edge Detector

A multi-stage algorithm is used to detect a wide range of edges in images. Canny finds gradient where the gray scale intensity changes. The process of canny edge detector consists of five steps. Gaussian filter is applied to smooth the image in order to remove the noise. The intensity gradients of the image are determined. Non-maximum suppression is applied to get rid of response to edge detection. Double threshold is applied to determine the edges. Track edge by hysteresis is applied to finalize the detection of edges that are weak or strong.

6.1.3 Principle Component Analysis

The PCA algorithm identifies patterns in a data, and highlights the similarities and differences. It is mainly used for recognition of face. It finds the vectors which account for distribution of face images within an image space. The advantage of PCA is data compression, carried out by reducing the number of dimensions without loss of information.

6.1.4 Linear Discriminant Analysis

Linear Discriminant Analysis (LDA) and related fisher's linear discriminant is statistical methods used for recognizing patterns and machine learning to find a linear combination of features. This algorithm is mostly used for feature selection in appearance based method. It is more sensitive than the PCA and ICA. LDA has a small size problem when dealing with high dimensional data.

6.1.5 Independent Component Analysis

Independent Component Analysis (ICA) is a computational method for separating a multivariable signal into subcomponents. The ICA is a special case of blind source separation. It considers statistically independent images, these images are sparse and localized in space resembling facial features.

VII. System Architecture

The architecture diagram for proposed ATM security is represented below. This architecture contains feature extraction and/or identifying face vector module during the user start to type the pin number. From this, the account has protected from an unauthorized person.

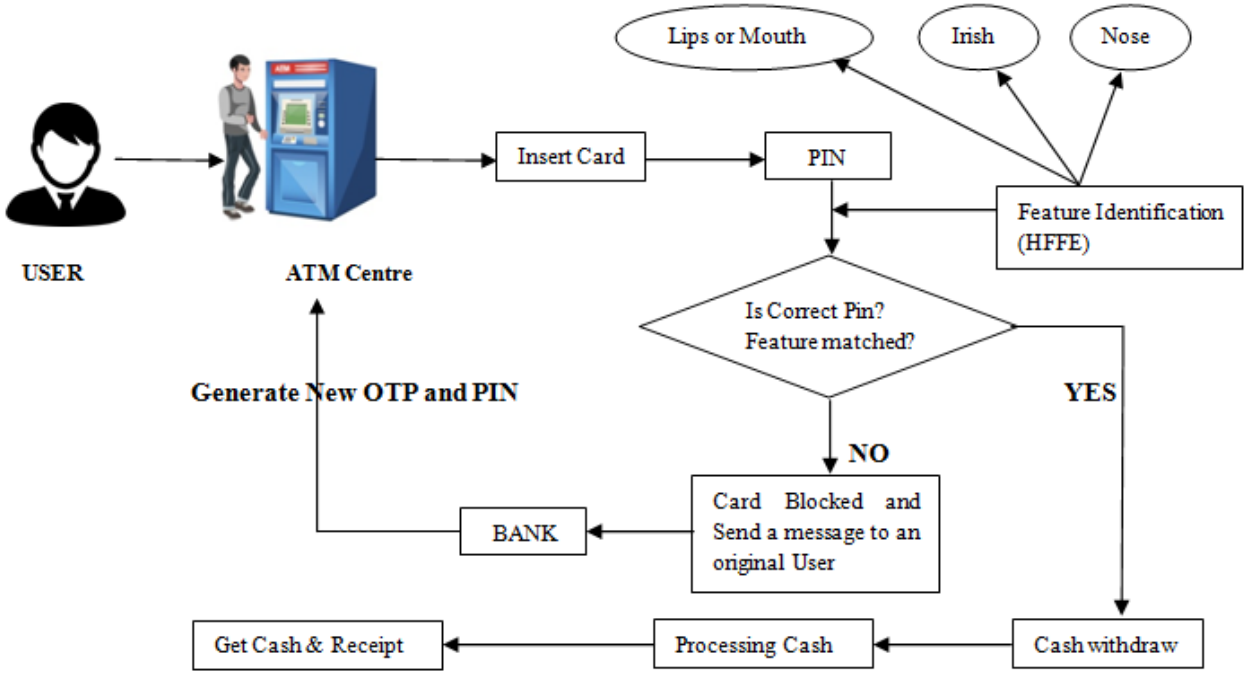

Fig 5: ATM Architecture Diagram Using HFFE

VIII. PROPOSED ALGORITHM – HFFE

Step 1: Start Transaction (Welcome)
Step 2: Insert ATM card
Step 3: Enter 4 digit password and Feature Capturing
While start to enter 4 digit password the system will automatically analyze and detects the user's feature
Step 4: IF both PIN authentication and feature capturing task completed successfully THEN go to step 7
Step 5: ELSE go to step 2 and 3
Step 6: Step 5 will work on a trice, after trice the card will be blocked
Step 7: Select your choices like, OTP generation, Balance Enquiry, Statement enquiry, Withdraw etc
Step 8: Receipt
If you want a receipt for the transaction give YES, Else give NO
Step 9: If select withdraw then, enter your amount
Step 10: After process complete, get your cash and receipt
Step 11: Stop Transaction (Thank you for using an ATM)

8.1 Comparative Analysis

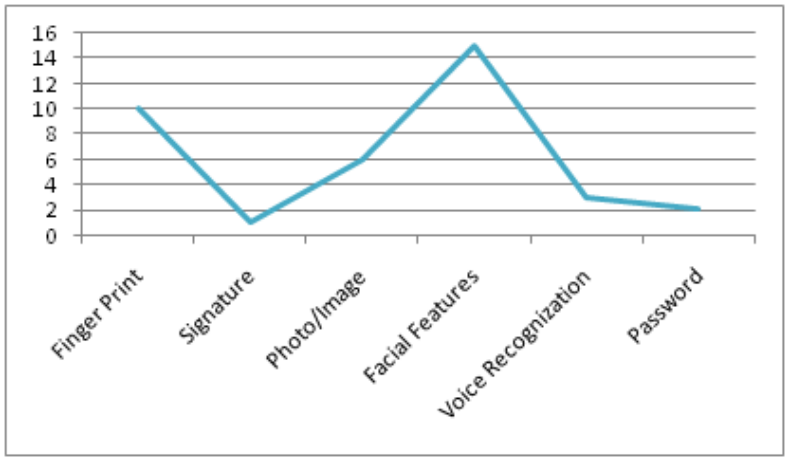

Fig 6: Comparative analysis of feature extraction with another security technique

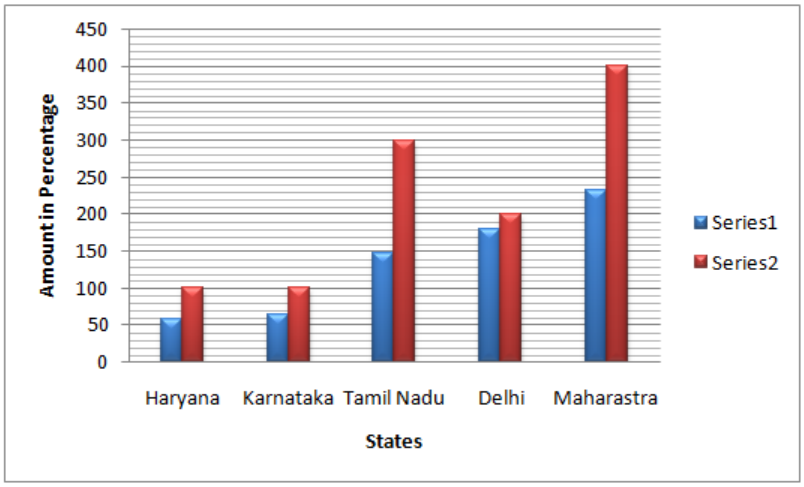

Fig 7: ATM Frauds Result – 2019 Survey

IX. CONCLUSION

Feature extraction is an efficient technique which is most commonly used in the concept image tracking and extracting system also used to find the original client. This paper proposed a new algorithm for ATM service for security. This paper discussed about the feature extraction techniques and their importance. Nowadays, technology has improved to reduce the human's workload and also providing protection. The proposed hybrid algorithm is also another efficient way to protect the user's details from the unknown persons. Because, hacking is one of the recent technology, this provides many advantages, even though has lots of disadvantages which is against for the internet users. The 4-digit password might be stolen by the utilization of various hacking methods. But in this facial detection algorithm never allows to enter the unauthorized user. In the few decades ago, various algorithms and applications are developed and invented. But in the computer knowledge world has overtaken this protection application. In the future, we need to analyze further security techniques/methods, and implement the efficient security algorithm in the recent computer application like a block chain to overcome this type of security problem.

REFERENCES

[1] Ram Sundar G, Joe Franklin J et al., "survey on credit card security system for bank transaction using Naive Bayesian and random forest" in International Research Journal of Engineering and Technology (IRJET), Volume 06, Issue: 02, Feb 2019, pp. 487-492.

[2] S.Jadhumithran et al., "Enhancing ATM security using Fingerprint" in ICTACT JOURNAL ON MICROELECTRONICS, JULY 2018, Volume: 04, Issue: 02, ISSN: 2395-1680, pp. 570-575.

[3] Madhuri More et al., "Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using Human Fingerprints", in International Journal of Advance Engineering and Research Development Volume 5, Issue 05, May -2018, pp. 392-399.

[4] M. Sathyapriya and Dr. V. Thiagarasu, "Big Data Analytics Techniques for Credit Card Fraud Detection: A Review", in International Journal of Science and Research (IJSR), Volume 6 Issue 5, May 2017, pp. 206-211.

[5] M.Priyadharshini and G.Manisha "Quick Response Code for Secure ATM Transaction Using Face Recognition" in International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Special Issue 8, October 2015, pp. 176-181.

[6] M.Kannan, Dr.C.Priya and S.Vaishnavisree, "A Comparative Analysis of DES, AES and RSA Crypt Algorithms for Network Security In Cloud Computing" in JETIR, Volume 6, Issue 3, March 2019, pp. 574-578. DOI: http://doi.one/10.1729/Journal.19997

[7] https://www.investopedia.com/terms/a/atm.asp

[8] Shrutanjay Kulkarni et al., "ATM Fraud Detection Using Hidden Markov Model", International Journal of Advanced Research in Education and Technology (IJARET), Vol.4, Issue 1, Jan-Mar 2017, ISSN: 2394-2975, pp. 36-37.

[9] Muhammed Bello B.L et al., "An Enhanced ATM Security System Using Second-level Authentication", International Journal of Computer Applications (0975-8887), Volume 111, - No 5, February 2015, pp. 8-15.

[10] Seyyid Ahmed Medjahed, "A Comparative Study of Feature Extraction Methods in Images Classification", in I.J. Image, Graphics and Signal Processing, 2015, 3, pp. 16-23.

[11] Vivek V.Jog and Nilesh R.Pardeshi, "Advanced Security Model for Detecting Frauds in ATM Transaction", International Journal of Computer Applications (0975-8887), Volume 95, - No 15, June 2014, pp. 47-50.

[12] Dhanush J.Nair and Sunny Nahar, "ATM Transaction: A New Time Based Approach Research Paper", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015, pp. 2254-2256.

[13] Srivatsan sridharan et al., "Improvising Authenticity and Security of Automated Teller Machine Services", in International Journal of Mobile Computing (IJCSMC), volume 3, Issue 2, February 2014, ISSN 2320-088X, pp. 666-674.

[14] https://timesofindia.indiatimes.com/india/maharashtra-tops-in-atm-frauds-delhi-second/articleshow/70322347.cms

[15] Dr.C.Priya and M.Kannan, "A Survey on Fault Detection Enabled Optimal Load Balancing Technique by the utilization of VM in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-7C2, pp.404-407, May 2019.

[16] M.Kannan and Dr.C.Priya, "Fault Detection Enabled Optimal Of Vehicle Alert And Routing Problem Using Hybrid KP-OACO Algorithm For Balancing Load In Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, pp. 903-909, June 2019.

[17] Krishnalitha K.C,Dr.C.Priya, "A Literature Survey on Hybrid Intrusion Detection System for Wireless Sensor Networks" in Journal of Advanced Research in Dynamical and Control Systems (JARDCS), Volume 13, Issue 8, pp 2590-98, 2018, ISSN 1943-023X, SNIP 0.294.

[18] Vidhyalakshmi.A, Dr.C.Priya, "A Study on Supervised Learning in Medical Image Grading using IoT" in International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 5C, pp 274-79, ISSN 2277-3878, February 2019.

[19] C.Priya, N.Prabakaran, "Security Management in Inter-Cloud" in International Journal of Emerging Trends and Technology in Computer Science, volume 1, issue 3, 233-235,ISSN 2278-6856(Online), Sep-Oct 2012. Impact Factor: 4.413.