A Review Paper on Secure ATM using Biometric and Color Code

Prof. Shailaja Pede#1, Kalyani Dhotre#2, Chaitrali Dusunge#3, Mrudula Kirve#4, Aarti Sawant#5
[1]Assistant Professor at Pimpri Chinchwad College Of engineering, Pune, India.
[2 3 4 5] Students (UG), Department of Computer Engineering,
Pimpri Chinchwad College of Engineering, Pune, India.

Abstract : **Automated Teller Machine (ATM) is very convenient way to withdraw money from anywhere. As users have been highly dependent on ATM so that Automated Teller Machine is highly in demand. But if someone got our access then they can easily access our bank accounts. To avoid such frauds we studied some more techniques like biometrics and colour code system for recognition of the actual author. under biometrics there are Iris recognition , face recognition , fingerprint recognition. Also one more technique is there which is colour code system. By using these techniques we can easily access our accounts and no one can withdraw our money by illegal way. This paper shows literature survey of each technique like Iris Recognition ,Fingerprint Recognition, Face Recognition and colour code system, etc. This survey shows that the methods which are mentioned above will definately provide proper security to ATM . In this paper we mentioned detail survey of each security technique with their limitations after studying some research papers on each technique. we mentioned comparative study of each technique with their advantages, disadvantages and limitations. As per the information reported to and traced by the Indian Computer Emergency Response Team (CERT-In), upto 1,59,761 cyber security incidents concerning to digital banking were reported in 2018, a total of 2,46,514 incidents in 2019 and 2,90,445 incidents were reported in 2020. These incidents include phishing attacks, network scanning and probing, viruses and website hacking. There has been a 46 percent increment in digital transactions in 2019-20 in comparison to 2018-19.**

Keywords: ***Iris recognition, Face recognition, fingerprint recognition , RFID, Colour code, matlab.***

I) INTRODUCTION

As we know ATM system is used for withdraw or deposit money, check bank balance, print statement of account activities or transactions, etc. And for these actions PIN is required. Now a days, this PIN is not too much safe for security purpose as the MiTM(Man in The Middle) attacks have been increasing in which messages sent by 'ATM Switch' to 'ATM Host' are altered by attackers to withdraw cash fraudulently. As per current situation of cyber attacks, all banks asked to build up their ATM security through end-to-end encryption in the network. So focusing on these points, we studied some research paper related with techniques used in security systems which will enhance the security level of ATM system. In this paper, we surveyed different techniques and methods related to ATM security system. Now a days, generally in ATM machine only PIN is required for money transaction. But to enhance the security of ATM system we studied some different types of techniques which may bring down illegal money transfer or cyber attacks. So, we mostly focused on biometric methods and colour coding methods. These both techniques have their own features which work at their best. In biometric method we added face recognition, iris recognition & fingerprint recognition. And in colour coding method we studied some different techniques. In face recognition technique, we studied totally four papers and each paper is design on different methodologies such as verification, identification, biometric authentication, facial recognition using OTP generation as well as with help of iris recognition. In iris recognition , there are four steps image acquisition, segmentation, normalization and encoding. Iris recognition is done using GSM module, RFID technique and image processing.In colour coding technique, we studied totally five papers. This techniques is new. In colour coding technique, there are so many techniques which are used for security purpose in ATM system. In this paper, in colour coding system, PIN authentication using multi-touch technology, colour pattern, colour code with password, colour wheel PIN technology, and OTP with colour code these techniques are studied.

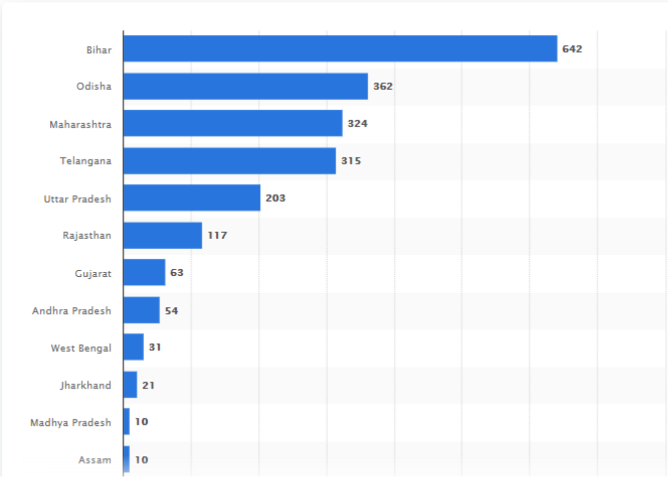

Fig.no.1 ATM frauds in 2020

In fingerprint authentication GSM technology is used for cellular network. In ATM data fingerprints of ATM holder and nominee will be registered for transactions. When ATM holder or nominee will enters the ATM in ATM machine it will asks for fingerprint. When this fingerprint authentication will succeed GSM technology send the OTP code to registered mobile number.

II) LITERATURE REVIEW

We studied five research papers of each technique and a short survey of these techniques is discussed in this literature paper. Also we discussed some limitations of each technique.

1)SECURE ATM USING BIOMETRIC TECHNIQUE

A) Iris recognition
B) Fingerprint recognition
C) Face recognition

A. SECURE ATM USING IRIS RECOGNITION TECHNIQUE:

In [1]In this picture is taken under proper radiance, distance and other elements affecting picture quality are taken into consideration. This step is important because image quality plays an important role in iris determination. Next is Image Segmentation. In this step, the iris region is separated from the given image. The iris subdivision is a dynamic step for overall act of the system. In the feature extraction step, different property from the subdivided iris is taken out to generate an iris template. This template further used for identification . Typically, fourth is Matching. The patterns taken out are mapped onto the patterns already extracted and stored in databank. In [2] When the account holder scans his/her RFID tag then the ATM transaction process starts, then the RFID scanner scan the RFID tag. The account which is connected with unique RFID number will be accessed. Once the scanning of the RFID tag is done the next step is iris scanning ,and then taking the picture of the iris pattern, we will use CMOS camera, it will produce a code for the iris. If the code gets match with the iris pattern kept in the database of the account, then the account will get accessed, then the customer will be allowed to do the withdrawal process. In [3] The withdrawal process begins after taking iris picture of iris and matching iris patterns. The system automatically matches the iris image of client with iris image kept in the databank .if there is no matching found, then the further process will not occur, if the iris images gets match then the password will be required to get verification code, if the password entered by client is not valid then the process will get stop again, if password is correct, then a GSM module which is attached to the Arduino ATmega 328 sends message of a verification code created by the system to the registered mobile number. The client enters verification code to the system, if the verification code is not valid authentication will get stop, if the verification code is valid then the client can withdraw his /her money. In[4] This involves the identification of the iris of the user and allows the client to make transactions. In this method we use matlab software for identifying iris and allows the client for the transaction and send the message automatically to authorized person. It consist of a generating OTP and other banking details. After identification of OTP client can do futher process. For other banking operations the client will receive another OTP. In[5]The whole process consist of two main verification steps to ensure zero security threats. The first step is RFID detection, or radio frequency identification, in which the individual will bring his RFID tag in front of the RFID reader. If the RFID tag will get match to an account in the database, then the further step is iris scanning. If the stored iris pattern matches to the scanned iris image, the transaction will be processed, otherwise, process gets stop.

Fig no.2 iris recognition

Limitations : The simultaneous use of this system may hurt iris because it is continuously scanned with infrared light. Iris scanners are more expensive than the other biometrics. A person has to be steady in front of the scanning device, regardless of their movements. Sometimes it is quite difficult to stay steady till the process gets complete.

B. SECURE ATM USING FINGERPRINT RECOGNITION TECHNIQUE:

In [6] ATM security is increased with fingerprint authentication. In this paper, fingerprint recognition is a biometric privacy system is used to identify the owner of specific bank account. In this system, if an ATM card is lost, and unknown person got this ATM card which has known that PIN number. But because of fingerprint system that unknown person cannot make missuse of that ATM card for transaction. In [7], ATM security is increased with fingerprint recognition with PIN also. Always customers used PIN to keep ATM security. For safe transaction Fingerprint authentication is the best option. Firstly customer have to register his/her fingerprint then further process will executed. An ATM machine is designed in such a way that after fingerprint confirmation further options will appear on the screen.

In [8] with PIN fingerprint authentication along with OTP generation also created .This paper combines fingerprint recognition and OTP generation with the help of GSM technology. GSM technology is used to generate OTP and send on registered mobile number. This method is very latest and easy. In [9], ATM with PIN is designed by fingerprint authentication and OTP generation for increasing security of customer’s transaction. SM630 fingerprint module is used to fingerprint authentication . ATmega128 is also used with GSM technology . In [10] **,** For improve ATM security it includes fingerprint recognition and OTP generation. Also for customer’s convenience it also added nominees details . So in the absence of customer’s or in emergency nominee can use this system for transaction .

Limitations : Due to multiple steps or stages it may be time consuming . It requires quality and faster device. Biometric devices are costly.

Island
Bifurcation
Ridge ending
Pore
Scanning
Crossover
The core of fingerprint pattern
Short Break
The delta is where the ridges divide

Fig no.3 Fingerprint recognition

C. SECURE ATM USING FACE RECOGNITION :

In[11] in this paper, face recognition technique is used for verification and that is Basically like system checks that particular person who want to access his /her bank account. Also, In that paper second type of comparison is based on identification. In This, System compares that particular users to all other user in the database. If any person who wearing mask or any thing on face him/her didn’t get any cash .This paper gives the way towards Facial Recognition Based on Local binary pattern which is also known as LBP texture features. In this paper Authors also describe their proposed system in which they present scheme like withdraw rate of ATM is reduced using face recognition method. They also said in this paper that they estimate their proposed system under tricky condition of real ATM usage. This paper also includes comparative study of some quality measures which have been effectively used in different applications and some new techniques which are suggested recently. They done classification based on Kullback discrimination. They mention their input design based on

- Which kind of data should be given as input?
- How the data ordered or sorted?

Their output design based on building block like Preprocessing in which crop image of face is going through histogram equalization which is method for image processing . second is the Feature extraction for that they use Local Binary Pattern(LBP). Also Verification System is used to verify users are valid or invalid by using front image of user which is captured by an camera fixed on ATM. Last building block is Object Detection it is used to detect Can user wear mask or any other object on face or not? After reviewing this paper we can see some advantages like ,By this security model which is designed for ATM it will increases the reliability of ATM transactions. Also best advantages which is mention in this paper itself that, If person wearing any mask or any object that person didn’t get any money or cash. In[12] In this paper , ATM security is done by using Biometric technique which involves the process like when wants to access their account Insert ATM card first after inserting ATM card and enter the PIN no. If that PIN no. is correct then camera which is fixed into ATM that captures the face of that particular user from front angle and if that front angle is correctly match then further process takes place otherwise not (means that model shows result like front face image is not matching shows like not valid and hence reject this card)also if front angle is correct then scan face from left angle 90 degree if this correct them moves further then also check by right angle, in this way they matching from the three angles and all three angles are correct then only user access their account. Best part of this paper that it takes very fast decision in less than 5 sec. In this paper author also shows Use case Diagram for ATM Simulator this they use Biometric Authentication Technique for matching the extracted features which are already stored in database. They also shows that how working of Biometric Authentication takes place when live image of the user is match with sample image which is stored in database then only user is allowed to access their account otherwise sensor shows the signal that user is invalid. After reading this we have understood that Biometric ATM security system is more secure.it is also easy to maintain with lower cost. But it also Difficult in understanding Biometric Authentication Technique. In[13] in this system Security of ATM is done by face recognition and OTP in ATM By using hybrid model which consist of both face recognition and One Time Password . In this method firstly individual or user will swipe their ATM card and then live image of that user is generated and then immediately it will compare with the image stored in database if that correct then only transaction gets proceed otherwise not so, By this method ATM is more Secured by combination of both Face recognition as well as OTP . Their proposed model is based on PCA (Principal Component Analysis) which is fall under holistic texture features. Their motive of using PCA is :

- As PCA technique use or consider only essential part of images so it takes very less time.
- PCA takes input images based on multiple or different expressions of each person.

For OTP generation they make GSM model to send SMS TO users mobile number. And their OTP is 6 digit code. In working of Face recognition technique they used Eigenfaces Initialization and Eigenfaces Recognition.

Their proposed system shows three main steps like Card swiping, Face recognition and OTP. After swiping card face recognition stage get started in that room of ATM more than one face detected account gets temporarily blocked and if not then PCA based face recognition starts. After recognition of image OTP sent to registered mobile number after receiving OTP user have enter that OTP if that OTP is matched then only Transaction can proceed if OTP not matched again Enter OTP this can be done only 3 times if more than 3 attempt of entering OPT then account temporarily blocked and user is notified by same mobile number. After reading paper it seems that Facial recognition technique is more challenging among all other biometric techniques, drawbacks in face recognition technique like problems in detection of face when beard, aging, etc.

In[14] in this Paper, They present two techniques about facial Recognition that is 2 D Technique and 3D Technique . In 2D Technique it stores details like width of nose and eyes ,distance between two eyes as faces seen two dimensionally. This type of technique not too exact certain changes in any type of facial expressions didn’t produce expected results. In 3 D technique it is basically used in facial characteristics like contours of the eye sockets ,chin, nose, peaks and valley. Also , In this paper ATM Security is done by Iris Recognition it provides card less , pass word free service to the user to access their account . The database of the face image is organized by the 3 parts related to face recognition.

- Face detector
- Eye localizer
- Face recognizer

Using 2D and 3D technique for identification, it provides security t By using Software which verifies the facial characteristics. As software required in it so it will be more costly.

Fig no.4 Face recognition

2) SECURE ATM USING COLOUR CODE:

[15]In this paper, PIN authentication which is most important step in any security system is done using color keypad in different devices. The algorithm for this system uses four digits from PIN. Each digit have one block which is separated by combining two colors. So that it prevent hacking by extracting PIN digit after all user's handling is done. In this system, each digit's block from PIN is divided by two colors and that colors is choose by user. But this colours must fulfils user's PIN digit key in every round. Here totally four cycles are carry out for PIN verification. And in this actually four times each digit is verify to build up security. **[16]**In this paper, security system uses VLC based NFC technology using color coded ID tags. The system includes magnetic lock, which access the control of the system using Remote Control Unit(RCU) which is designed for security control and smartphone based color code NFC ID tag. The RCU interface is with combination of central CCTV monitoring and control system to control the user's authentication. This CCTV camera is attach to just upper side of machine. One important step is required to unlock the security system that is, "by scanning smartphone based color coded ID tag by CCTV camera". In this system, authentication is executed on central security management server to give user secured authentication.

Limitations: In this system, hardware and software are needed for security purpose so, it is costlier.

[17]In this, session there are totally two sessions are included. This two sessions include session password and session image & color. Session two is combination of image and color. In session password, password is required which can use by user only once. Every time new password will required for login process. Old passwords are not required in this. Means one password used by user only one time for next time they required new password. Then in session image, at time of registration various images are given to user and user have to select any number of images which he/she want. So that after login time he/she identify the pre-selected images (means images which are choose by user at time of registration) from set of images for proper verification. Then in color session, at registration time, totally eight color grids given to user in order of "RLYOBGIP" and they have to rate that color in range of one -eight in numeric form. And this is important for user to remember the ratings which he/she done at registration time for login process every time.

Limitations: As every time, password will change so it will not more secure. And sometimes may possible that user will not remember ratings.

[18]In this system, user insert the card in ATM. Then ATM sends card information. After that server generates a random color index arrangements. Corresponding to that ATM generates QR code. Since, user receives color arrangements via Near Field Communication (NFC) or QR code. Then user inputs their PIN and ATM sends user input. After that PIN verification is done and system will unlock for user.

Limitations: As so many process are include in system for higher security so charges and time will required. **[19]**In this paper, different techniques generate a number of OTPs. Generation of OTPs is depend on color grids. User can give any rating to any color but it must be unique, same rating is not allowed for different colors. In this method, color are already given to user and user only have to give ratings. Rating is done using numbers. According to rating, OTP is generated and this OTP is enter by user.

Limitations: It will take time to rate the color grids and after according to rating OTP will generate so it is quite take time. It is not much secure system. As it have totally four cycles so it will take time. Its mechanism is quite hard to understand.

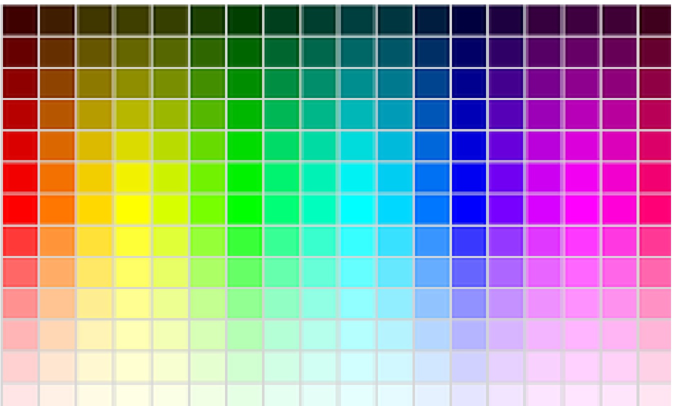

Fig no.5 colour code technique

III) RESULTS

For iris Recognition rate, False Rejection rate was calculated from CASIA-V3 database. They took 20 images for training and 10 images for testing.

In color coding methods, unique and strong security system can be formed. By using these color coding methods, the user can achieve their money transactions with relaxation. These all technologies lead to quality results which indicates the growth of digital India.

III) CONCLUSION

In this paper, we studied security system using biometric methods and colour coding method. Under biometrics, we studied fingerprint recognition, face recognition and iris recognition. In fingerprint recognition, fingerprint scanner is used for security purpose. when user keep his / her finger on fingerprint scanner then scanner take photo of lines and save them and then every time user have to scan their fingerprints for login purpose. In face recognition, the system uses camera and scanner for scanning face. If proper face is match then login is successfully completed. In iris recognition, iris scanning contains up to 240-250 points to match. User does not get access in the system until all points are found or match. In colour coding, different techniques are used. For successful login, in some technique user have to rate the colour grids, in some they have to scan the colour code and in some we have to arrange the colour in specific order which he/she specified at registration time. These both biometric and colour coding techniques are best for security purpose. Aadhar card is used for identify a person. In this Aadhaar card system also biometric methods are used. Biometric methods are used by airport control, in police station, in government offices, in military intelligence, etc. Also colour coding methods are used in different security system such as to unlock the door and any system related with security. These both techniques may bring down the illegal actions & may provide the best security.

IV) FUTURE SCOPE

These security techniques can be used in various technical fields in future. In future we can use QR code for recognition. It is good invention in technical field hence it will support technical industries. Many projects related to security and control can be implemented using this biometric technique. Also, Colour coding is new technology which will very beneficial in security field. Mostly three level ATM security system with colour coding will be strong security system in future. When user id and password will match then on registered email id(user id) user will get a QR colour code which user have to scan on ATM machine. So, because of three level security is attached with ATM system it will more secure and strong. Also we can combine two or more security techniques for high security.

V) REFERENCES

[1] Shetiya, P., Mascarenhas, M., & Deshmukh, M. ATM Security System using Iris Recognition by Image Processing.

[2] harine, m., padmavathi, k., & kumar, m. l. v. (2020). fingerprint and iris biometric controlled smart banking machine embedded with gsm technology for otp.

[3] mahesh, k., brahmal, h. h., & ramaiah, d. g. k. (2015). ATM Based Recognition Technique on IRIS Technology with GSM Module. International Journal of Scientific Engineering and Technology Research, ISSN, 2319, 8885.

[4] Rao, K. L. N., Kulkarni, V., & Reddy, C. K. (2012). Recognition Technique for ATM based on IRIS Technology. International Journal of Engineering Research and Development, 3(11), 39-45.

[5] Bhagat, S., Singh, V., Khajuria, N., & Student, B. (2017). Atm security using iris recognition technology and RFID. International Journal of Engineering Science and Computing, 7(5), 11486-11488.

[6] Onyesolu, M. O., & Ezeani, I. M. (2012). ATM security using fingerprint biometric identifer: An investigative study. International Journal of Advanced Computer science and applications, 3(4), 68-72.

[7] Padmapriya, V., & Prakasam, S. (2013). Enhancing ATM security using fingerprint and GSM technology. International Journal of Computer Applications, 80(16).

[8] Dutta, M., Psyche, K. K., & Yasmin, S. (2017). ATM transaction security using fingerprint recognition. Am J Eng Res (AJER), 6(8), 2320-0847.

[9] Okokpujie, K. O., Olajide, F., John, S. N., & Kennedy, C. G. (2016). Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128 with GSM Feedback Mechanism.

[10] Jaiswal, A. M., & Bartere, M. (2014). Enhancing ATM security using Fingerprint and GSM technology. International Journal of Computer Science and Mobile Computing (IJCSMC), 3(4), 28-32.

[11] Peter, K. J., Glory, G. G. S., Arguman, S., Nagarajan, G., Devi, V. S., & Kannan, K. S. (2011, April). Improving ATM security via face recognition. In 2011 3rd International Conference on Electronics Computer Technology (Vol. 6, pp. 373-376). IEEE.

[12] Malviya, D. (2014). Face recognition technique: Enhanced safety approach for ATM. International Journal of Scientific and Research Publications, 4(12), 1-6.

[13] Karovaliya, M., Karedia, S., Oza, S., & Kalbande, D. R. (2015). Enhanced security for ATM machine with OTP and facial recognition features. Procedia Computer Science, 45, 390-396.

[14] Marathe, K., & Mande, H. ATM Security Using Eye and Facial Recognisation.

[15] Abinaya, K., Pavithra, T., & Divya, P. (2017). Color Code PIN Authentication System Using multi-touch technology.

[16] Han, Sukyoung & Lee, Minwoo & Mariappan, Vinayagam & Lee, Junghoon & Lee, Seungyoun & Lee, Juyoung & Kim, Jintae & Cha, Jaesang. (2016). Smartphone Color-Code based Gate Security Control. International journal of advanced smart convergence. 5. 66-71. 10.7236/IJASC.2016.5.3.66.

[17] Sreelatha, Moturi & Shashi, M. & Anirudh, M & Ahamer, Sultan & Kumar, V. (2011). Authentication Schemes for Session Passwords Using Color and Images. International Journal of Network Security & Its Applications (IJNSA). 3. 10.5121/ijnsa.2011.3308.

[18] Guerar, M., Benmohammed, M., & Alimi, V. (2016). Color wheel pin: Usable and resilient ATM authentication. Journal of High Speed Networks, 22(3), 231-240.

[19] Mallaiah, Shivamurthaiah & Sinha, Sitesh & R, Praveen. (2017). An Authentication for digital transaction with OTP using Color Code Systems (CCS). International Journal of Computer Sciences and Engineering. 5. 285-287. 10.26438/ijcse/v5i10.285287.