Global Scientific JOURNALS

GSJ: Volume 7, Issue 10, October 2019, Online: ISSN 2320-9186

www.globalscientificjournal.com

ATM PIN Authentication using Facial Recognition

Aishani Bangia* and Prabu S
School of Computer Science and Engineering
Vellore Institute of Technology, Vellore, Tamil Nadu, In
*Email: aishani.bangia2016@vitstudent.ac.in

***Abstract*— Whenever someone enters their pin while withdrawing money from the ATM machine, they make sure that no one has stuck their eyes to it. People tend to check their pockets and wallets thousand times once they have entered their card in some machine just to check if they have their cards safely with them. They remain very careful, yet people have different ways like - skimming, using fake keyboards, using hidden cameras, card tapping and keystroke logging to hack the pin and use others' card. So, to avoid such practices we plan on designing a machine that along with the pin, also detects the face of the person using the card. If the user's face does not match with the database, he/she will not get access to the further page. The access will be denied and the person using the card will not be able to make any transactions or alter any data. Along with the user, authorized spouse, and children whose information is fed in the database can use the card. So, if the family can manage only one card, there is no problem since, it won't hamper the security of the system anyways. This enables full security as no other person can access and use the card except for the most trusted ones who are registered in the database. Even if someone manages to get the card, he/she cannot use it; as facial recognition runs parallel with the pin entering process, the system remains unbeatable.**

Keywords—Pin authentication, database, security, ATM Machine, Facial Recognition.

I. INTRODUCTION

The main objective of our paper is to make a device that improves the safety of the existing devices by adding an extra element which will run in parallel with the already existing one. We plan on adding the normal ATM machines with a face recognition feature. So, to make a prototype of an ATM machine. We make a device which detects the presence of a card. From the magnetic strip on the card a unique identification code should get extracted.

This identification code should be matched with an identification code in the database, and the pin should be fetched. After this, the device asks for the pin and if the entered pin matches the pin extracted from the database, we move onto the face recognition feature.

To make the facial recognition feature, we detect the face of the person who's accessing the ATM machine. We then try to match the face of the user with the faces saved in the user information extracted by the unique identification code. If the face matches with either one of the faces, the user identification gets confirmed and future transactions are allowed.

A lot of people face security issues after they lose their cards. Only the physical presence of a card and its pin is not enough to protect the finances of any customer. An extra feature of facial recognition will not only protect the money of the customers but also their safety. We aim on providing a device that verifies both the pin and the facial features with the user information extracted from the card so that money can be withdrawn only by the customer and his/her authorized spouse and children. Almost all major transaction services provide a two-factor authentication, but they differ in terms of how they protect user's accounts. Hackers have ample methods for overcoming the weakness in implementations, can be either intercepting codes or even exploiting an ambiguity in accounts or recovery systems. The general Architecture still provides a significant protection, but it has its limits.

There are a number of cases where two-factor authentication is secure and reliable for Credit Card Authentication. However, with that there is also the possibility of multi-factor authentication using SMS service to not always be secure. However, that side of it has more to do with human error which is not your own. That's where things start to get quite risky. In the present age of 2019, just implementing the two-factor authentication is nowhere near satisfactory.

The reasons why two-factor authentication is normally inadequate: The registered cell phone provider breaches methods and measures of security, Lack of a security Pin code that is strong and thus a weak pin is given to cell phone provider, Authentication Pin chosen by the user is simply not strong enough, The passwords that you store are not in secure locations, Your Bank credentials are stolen from your phone or other mobile devices, You don't keep your phone or other mobile devices securely locked, Your computer or laptop is stolen, You fall prey to phishing attacks by email or by phone.

Phishing is the easiest and most direct way to lure victims to a fake Bank login page. When the target gives his credentials, the hacker forwards these values to the real login page separately, thus triggering the proper authentication procedure that leads to the target inputting the numerical code that was texted or mailed to him on his own volition, or in other cases produced by an authenticator app of that respective service. The attacker phishes this code on the self created fake login page the target is still using

and now has completed the authentication procedure. Even though, due to the limitation in usefulness of the generated code, the hacker will have to be fast, but once he does successfully log in, he can freely change and manipulate the phone number or even the email id where the next code will be sent to, in the end being granted the complete access to all the resources provided to the account for himself. Using their Net Banking Account, they can easily bypass 2FA of credit card transactions.

II. LITERATURE REVIEW

A. Improved Methods on PCA Based Human Face Recognition for Distorted Images.

In this research paper, they examine various techniques and identify the one which works well with principal component analysis for human face recognition. Experimental results show that by applying the technique called Gradient faces at the pre-processing stage which computes the orientation of the image gradients in each pixel of the face images and uses the computed face representation as an illumination invariant version of the input image, it can greatly improve the recognition rates. This focuses on majorly improved the precision if facial recognition in distorted images using Single Scale Retinex and Multi Scale Retinex algorithms and homomorphic filtering. [5]

B. Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN.

In this research paper, facial detection and recognition is studied using principal component analysis and artificial neural network. The proposed methodology is implemented in two stages. The first stage detects the human face in an image using viola Jones algorithm. In the next stage the detected face in the image is recognized using a fusion of Principal Component Analysis and Feed Forward Neural Network. The performance of the proposed method is compared with existing methods. Better accuracy in recognition is realized with the proposed method. The proposed methodology uses Bio-ID Face Database as standard image database. Face recognition plays a crucial role in applications such as security system, credit card verification, identifying criminals in airport, railway stations etc. [6]

C. *Image-based Face Detection and Recognition.*

Face recognition is a popular topic in research for biometrics as they have significant value for security purposes as surveillance is used worldwide. It is widely known that the face recognition has played a crucial role in surveillance system as it doesn't need the object's cooperation. The actual advantages of face-based identification over other biometrics are its uniqueness and acceptance. As human face is a dynamic object having high degree of variability in its appearance, that makes face detection a difficult problem in computer vision. In this field, accuracy and speed of identification is a main issue. The main motive of this paper is to study face recognition and studying the emotions of the subject. [7]

D. A Review paper on face recognition techniques.

This research paper reviews different techniques using different methodologies for each such as Principal Component Analysis, Linear Discriminate Analysis, Independent Component Analysis, Support Vector Machine and Artificial Neural Network. We review these techniques based on certain factors and the advantages they have over each other and in which case will each of them be helpful. [8]

E. Biometric Security Process For Authenticating Identity And Credit Cards, Visas, Passports And Facial Recognition.

Here we have seen the importance of use of biometric security method when it comes to authenticating the credit card holder, identifying the document bearer using his/her facial image, analysis of the facial features of the person, and the finding pattern/features in the database. Basically, this paper talks about the entire process that is used to identify/verify the card holder from capturing his features to checking in the database. [9]

F. Counterfeit Proof ID Card Having a Scrambled Facial Image.

To every credit card a unique descrambling control code is assigned. The facial image of person holding the card is descrambled using the unique code provided to him to enforce the verification of the identity of the card holder. This method prevents the duplication of cards. [10]

G. An ensemble learning approach to lip-based biometric verification, with a dynamic selection of classifiers.

This research paper talks about Lip passed biometric verification using various machine learning and ensemble learning approaches wherein there are various classifiers which are integrated together to give rise to an optimal solution. [1]

H. Automated POS System based on Face Recognition and Password.

This paper talks about the use of Point of Sale system enables credit cards. This credit cards are different from the traditional credit cards as they are contained with bar code readers for their Verification, In modern days use of AI installed POS are also being used with enhanced Security features. [2]

I. Online Signature-Based Biometric Recognition.

In this method the verification of the identity of the card holder is done with the help of physical features like iris and retina scanning or fingerprint scanning or using the features

of facial geometry etc. This additional mode of verification are added to enforce security and make sure that no other person other than the card holder should access former persons card. [3]

J. Face Controlled Liveliness Verification.
This research paper saw using the technique of liveliness verification of the face. The system built here will ask you to look at a set of points on the screen. This is mostly done because a lot of times when someone robs money, to avoid footage in CCTV he may wear a mask then in that case his liveliness verification of the face will fail. [4]

K. A Review of Facial Biometrics Security for Smart Devices
This paper talks about the science behind the trust in facial biometrics as a form of authentication. It explores the security in mobile device applications, both iOS and Android. They also discuss the several tests done on different applications with different methods that they have developed and provide the results.[11]

L. Enhanced security for ATM machine with OTP and Facial recognition features
This paper proposes a new mechanism that can enhance the usability, convenience and experience of a transaction at an ATM. They put forward Features like One-Time Password and face recognition to enhance the privacy of users and security of account. It has been mentioned how facial recognition helps identifying every person uniquely. This system diminishes the possibilities of fraud in ATMs. Pin free system increases the usefulness of the system as there is no need for the user to remember the pin.[12]

M. Facial Verification Technology for Use In Atm Transactions.
This paper proposes a system which integrates face recognition in identity verification present in ATMs. It puts forward an ATM machine model that combines a Pin, electronic facial recognition with a physical access card that will increase the security in user identification. [13]

N. A Review Paper on Biometrics: Facial Recognition
This paper discusses why facial recognition is used and various technologies used in it. It talks about different products that have been made to implement this technique and the feedback about it. [14]

O. Face Recognition Technology
This paper discusses the problems associated with password-based controls and its effect on the integrity of systems. It puts forward the advantages associated with facial recognition and how positively it affects the security systems. It talks about the mechanism behind facial recognition, problems attached to it and the verification it provides.[15]

P. BAT for Facial recognition using sensors in ATM
In this research paper, the ATM usage is designed based upon the intelligence system so that ATM can be used without any hesitation. A session is started once the card is inserted by the user. The system starts detecting face using the nearby camera situated close to the ATM which builds a temporary identity database of the user and verification is performed. After checking the validity of the user, if the user is a valid one, it can continue the normal process else a secondary password is given to the system so that the unauthorized user can continue with the transaction.[16]

Q. Random Keypad and Face Recognition Authentication Mechanism
In this research paper, graphical passwords along with text base word passwords are used. The whole process is divided into two parts. The first part being the PIN or the word password. The second part is the graphical password or the face detection. The aim of this system would be to reduce the surfing attacks. This is achieved by two components one being a random keypad and other being the face recognition method. Comparing to the normal keypads, these keypads are more preferable for security concerns.[17]

R. Face Recognition Technology
In this research paper, face recognition is being used to avoid any kind of forgery that can be possible with the possession of identity cards or knowledge of any social security number. Many things can happen when user uses such conventional methods. ID might get lost or it can be forged or even misplaced. Passwords can also be a bit risky since they can be forgotten or compromised. But face can be a full proof solution to these situations as they can neither be borrowed nor be stolen. The face recognition technology can solve all of these problems until and unless the user has an identical twin.[18]

S. Securing Atm By Image Processing –Facial Recognition Authentication
In this research paper, the method proposed is the amalgamation of Face Recognition System in the identity verification of the user in ATMs security system. Certain features of face are taken into mark. More essentially the coordinates of the eyes, nose and mouth is recorded and verified. Certain extra features like facial hair are also taken into concern while performing Face Recognition to prevent any security threat.[19]

T. Atm Security Using Face Recognition
The security of ATM machines is increase by combining access cards, a PIN, and also a face recognition system. The face recognition uses local binary patterns to extract few features if the face. Various other image processing techniques such as histogram equalization has been done for feature distribution. This system prevents robberies and fraudulent activities that can be performed in ATMs while drawing out money.[20]

III. FEASIBILITY

To make a product that will increase the security of ATMs while withdrawing the cash. A facial recognition and pin authentication mechanism is needed.

For that, a good quality camera and a camera holder for facial recognition and a prototype of ATM machine for the card and pin validation is required.

IV. PROPOSED APPROACH

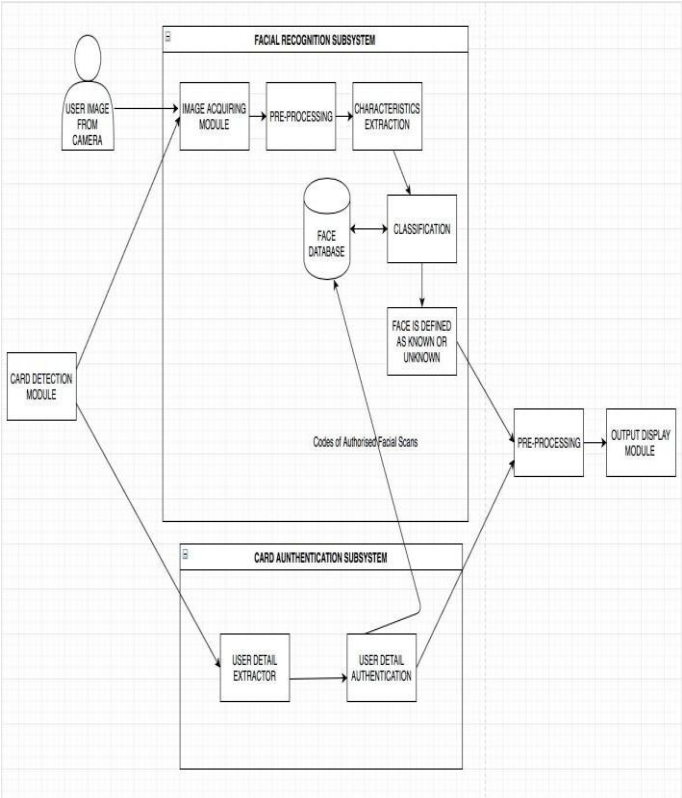
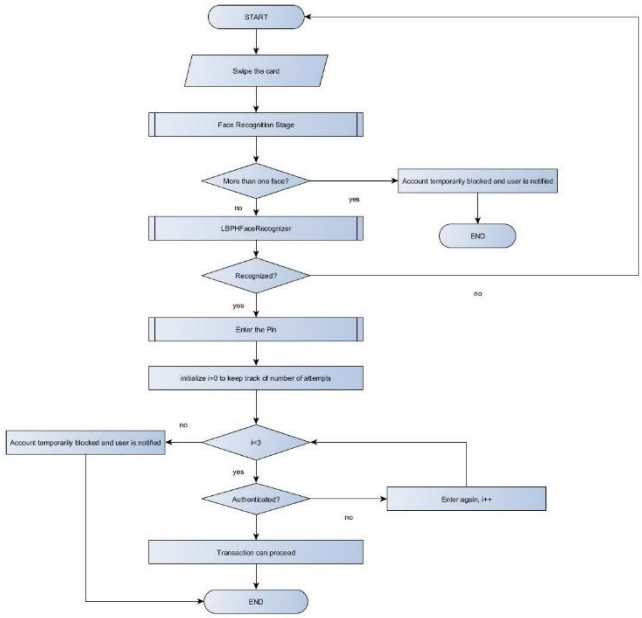


Figure 1.1: Architectural Diagram

V. SYSTEM



- An ATM machine asks for the card and pin in the system to fetch money. In this software that we have created using python, the algorithm operates with the card number and pin to generate a code. This junk code is taken from the bank and then compared to the newly generated code. If these codes match, the money is given. The entered pin is safe in the ATM machine, but the card number goes to the bank server to check the authenticity of the account. The bank has access only to this junk code, not to the passcode. The algorithm gives a true/false output. It gives true if the pin matches which leads to the withdrawal of the requested amount. If it gives false, wrong pin entered is displayed.
  In this case the hash we have taken is the simple conjugation method which is exercised on both the card no and the pin unique to each particular user. This hash is then compared with the database on the platform itself which acts as the server in our demo. At this step the image recognition protocol is called and based on the combined output the final check is assessed.
  The test cases taken considers:
  Card number, pin and image match
  Card number and pin match image does not match
  Card number or pin does not match
  The number of attempts
- For the facial recognition part of the project we are using python3 programming language, the packages we are importing to add functionality to the project is numpy, cv2, pickle and PIL.
  We have two files in this section. One file is use to train the model, we have added to the model as

input few of sample images so that the model can run on them and then it builds a function using which it can be able to decode and understand the other sample images which are getting captured by the webcam.
The technique we are using here to build our model is LBPHFaceRecognizer, there are many other techniques and algorithms available but the best result we were getting using this function only.
The other file that we are using is basically to capture the image from the webcam and them send it to the model built using the earlier file and display the output which it has received. The image is captured using the function of cv2 package called VideoCapture and we are printing the inputted information and the name of the person using the show() function of cv2 package.

VI. CONCLUSION

From the exploration we know the significance of the way toward approving a charge card client's personality or approved client status. Confirming the client is a basic piece of a trader's obligations during the time spent tolerating charge card. As we can see from the review done that the existing security infrastructure is gradually becoming more vulnerable due to increased threat of cyber attacks as more and more banking operations are automated there is a crucial need to increase the security in fund transactions. As reviewed Facial recognition offers far greater accuracy and protection from identity thefts for credit card user. At the same time it is far more convenient to integrate with the existing security infrastructure of credit card authentication as compared to other alternatives. Automated and accurate 24/7 security removes the necessity for security guards to establish surveillance of entry points, perform periodic security checks and use security cameras. At the same time the value of 2 factor authentication in credit cards cannot be ignored and is most suited as the fundamental authentication method. While two-factor confirmation just imply that accounts are progressively impervious to assaults, it makes your records stronger as a programmer needs to split in excess of a straightforward secret key. The feasibility of the proposed prototype gives reasonable probability of it being mass-produced in a few years as the demand rises. From figure 1.1, 2-way authentication operations will run in parallel. Starting with facial recognition, data set acquisition to the preprocessing sub-steps to Attribute extraction to classification and finally pattern recognition will be carried out sequentially with testing and debugging carried out simultaneously. This will then be combined with the result from Card authentication algorithm for linking both records parallel in order to get the result. The hardware will be built with the development of respective modules as per the requirements.

VI. REFERENCES

[1] Porwik, Piotr, Rafal Doroz, and Krzysztof Wrobel. "An ensemble learning approach to lip-based biometric verification, with a dynamic selection of classifiers." Expert Systems with Applications 115 (2019): 673-683.

[2] J. V. Gorabal, Manjaiah D. H., “Texture Analysis for Face Recognition”, International Journal of Graphics And Multimedia (IJGM), ISSN 0976 - 6448 (Print), Vol. 4, Issue 2, December 2013, pp. 20-30

[3] Tanwar, Sudeep, et al. "Online Signature-Based Biometric Recognition." Biometric-Based Physical and Cybersecurity Systems. Springer, Cham, 2019. 255-285.

[4] Kollreider, Klaus, Hartwig Fronthaler, and Josef Bigun. "Verifying liveness by multiple experts in face biometrics." 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. Ieee, 2008.

[5] Poon, Bruce, M. Ashraful Amin, and Hong Yan. "Improved methods on PCA based human face recognition for distorted images." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. 2016.

[6] Deshpande, Narayan T., and S. Ravishankar. "Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN." Advances in Computational Sciences and Technology 10.5 (2017): 1173-1189.

[7] Ahmad, Faizan, Aaima Najam, and Zeeshan Ahmed. "Image-based face detection and recognition:" state of the art"." arXiv preprint arXiv:1302.6379 (2013).

[8] Bhele, Sujata G., and V. H. Mankar. "A review paper on face recognition techniques." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1.8 (2012): 339-346.

[9] Schroeder, Carlos Cobian. "Biometric security process for authenticating identity and credit cards, visas, passports and facial recognition." U.S. Patent No. 5,787,186. 28 Jul. 1998.

[10] Nathans, Robert L. "Counterfeit proof ID card having a scrambled facial image." U.S. Patent No. 4,972,476. 20 Nov. 1990.

[11] Mary Grace Galterio, Simi Angelic Shavit and Thaier Hayajneh “A Review of Facial Biometrics Security for Smart Devices” Computers 2018, 7, 37; doi:10.3390/computers7030037

[12] Mohsin Karovaliya, Saifali Karedia, Sharad Oza and Dr. D. R. Kalbande "Enhanced security for ATM machine with OTP and Facial recognition features" International Conference on Advanced Computing Technologies and Applications (ICACTA2015)

[13] Aru, Okereke Eze and Ihekweaba Gozie "Facial Verification Technology for Use In Atm Transactions" American Journal of Engineering Research (AJER) e-ISSN:2320-0847 p-ISSN : 2320-0936

[14] Sakshi Goel, Akhil Kaushik and Kirtika Goel "A Review Paper on Biometrics: Facial Recognition" International Journal of Scientific Research Engineering & Technology (IJSRET)

[15] Ms. Swati S. Bobde and Mr. Sumit V. Deshmukh "Face Recognition Technology" IJCSMC, Vol. 3, Issue. 10, October 2014, pg.192 – 202.

[16] Jaganiga M, Vaitheswari S, Rasitra R and Dr.S.Lakshmi "BAT for Facial recognition using sensors in ATM"

[17] Shivani Shukla, Anjali Helonde, Sonam Raut, Shubhkirti Salode and Jitesh Zade "Random Keypad And Face Recognition Authentication Mechanism "

[18] Ms. Swati S. Bobde and Mr. Sumit V. Deshmukh "Face Recognition Technology"

[19] T. Suganya, T. Nithya, C. Sunitha And B. Meena Preethi "Securing Atm By Image Processing – Facial Recognition Authentication"

[20] Arunkumar V, Vasanth kumar V, naveenly king K and Aravindan T "Atm Security Using Face Recognition"