SECURED ATM CARD VERIFICATION BASED ON FACE RECOGNITION

[1]P.Ramya, [2]M.Sivaranjani, [3]M.Vinoth Kumar, [4]R.Vignesh Kumar, [5]M.Dinesh Kumar, [6] K.Kasthuri
[1234]UG Scholar, [5]Assistant Professor, [6] Software Engineer.
[1,2,3,4,5]Department of Electronics and Communication Engineering
Knowledge Institute of Technology, Kakapalayam, Salem-637504, Tamilnadu, India.
[6]Robert Bosch Engineering andBusiness Solutions Pvt Ltd, Coimbatore
†ramyapkiot@gmail.com, [2]mmsivani@gmail.com, [3]vinoth05031995@gmail.com, [4]vigneshsriram1975@gmail.com,
[5]mdece@kiot.ac.in

ABSTRACT: Facial recognition is a biometric method of identifying a person based on a photograph of their face. Biometric methods use biological traits to identify people. The human eye is naturally able to recognize people by looking at them. However, it recognizes known people much more easily than perfect strangers. Therefore, computerized methods have been developed to perform the facial recognition. Identification of faces is an important for security, surveillance, and in forensics. Basic idea of the paper is to provide wireless mode of transmission using GSM. In this paper GSM has been used because this is an efficient and cheap solution. If unauthorized person is trying to access the account via ATM card, an alert message is send through SMS and email by using GSM module. More than one person can also access an account by storing image in the database. In this work, the design and implementation of a GSM based wireless security system is used which takes a very less power.

KEYWORDS: ATM card, Face recognition, GSM module.

I. INTRODUCTION

ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his „unauthentic□ share. Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure. Our paper proposes an automatic teller machine security model that would combine aphysical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account and the live image and stored image match would a user be considered fully verified.

Further, a positive visual match would cause the live image to be stored in the database so that future transactions would have a broader base from which to compare if the original account image fails to provide a match thereby decreasing false negatives. When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for use in fraudulent transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions.

In the case of credit card use at ATMs, such a verification system would not currently be feasible without creating an overhaul for the entire credit card issuing industry, but it is possible that positive results achieved by this system might motivate such an overhaul. However, one could argue that having the image compromised by a third party would have far less dire consequences than the account information itself. Furthermore, since nearly all ATMs videotape customers engaging in transactions, it is no broad leap to realize that banks already build an archive of their customer images, even if they are not necessarily grouped with account information. With appropriate lighting and robust learning software,slight variations could be accounted for in most cases.

II. FLOW CHART

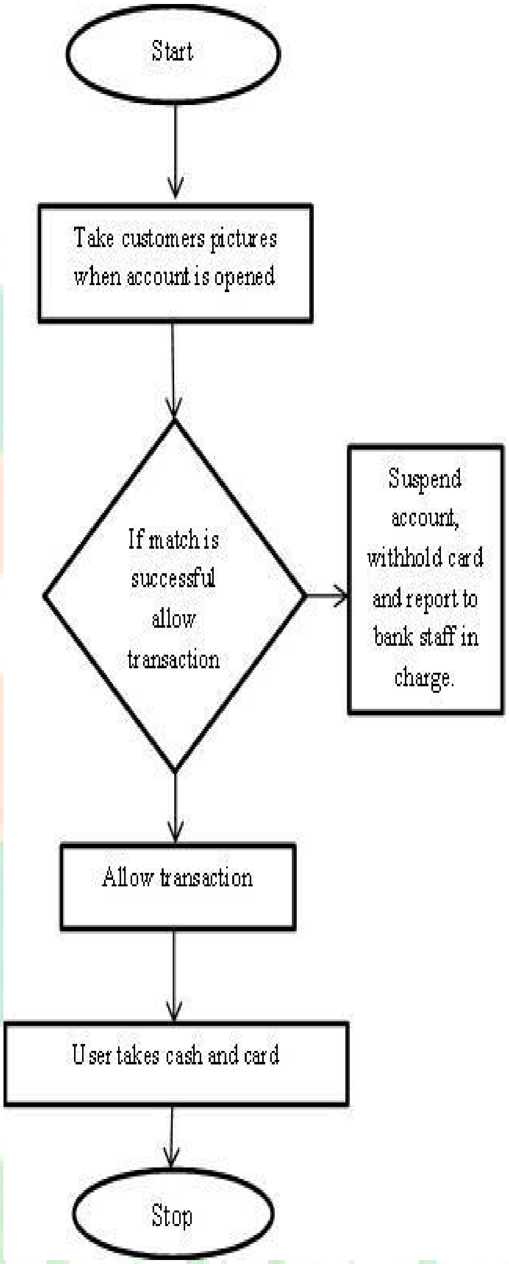

Start
Take customers pictures when account is opened
If match is successful allow transaction
Suspend account, withhold card and report to bank staff in charge.
Allow transaction
User takes cash and card
Stop

Fig.1. Flow chart of ATM authentication process

From fig.1, ATM takes a picture of the user and compare with the database, if, it matches then transaction is allowed. Otherwise, picture of the unknown user is sent to the account owner and bank employee.

III. METHODOLOGY

Identification (RFID) technology is used for user data sense can be wirelessly interrogated when operating the money transaction. And face identification is to identify the particular person or user identification. As shown in the Fig.2, this paper have used this principle to model, optimize and design a radiometric mode 915-MHz RF identification-based biosensor which uses relative received signal strength indicator (RSSI) to measure and detect different concentration levels of target analyses. Integrating protection of transaction capabilities with face detection and passive RFID tags ensures that the sensors are low-cost and because these sensor-tags operate without batteries, their shelf-life is comparable to the products being monitored.

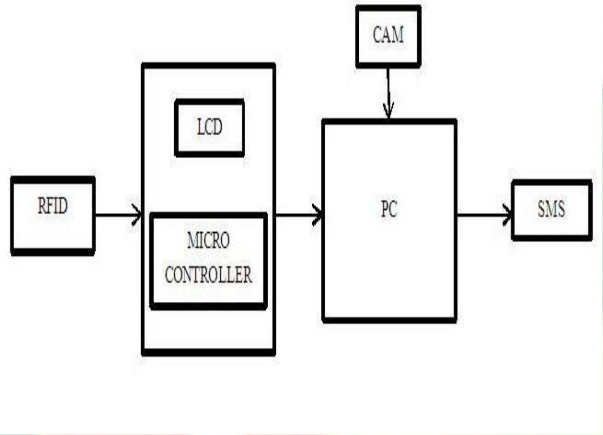


Fig.2. Block diagram of ATM card verification andface recognition system

The first and most important step of this project will be to locate a powerful open-source facial recognition program that uses local feature analysis and that is targeted at facial verification. This program should be compliable on multiple systems, including Linux and Windows variants, and should be customizable to the extent of allowing for variations in processing power of the machines onto which it would be deployed. We will then need to familiarize ourselves with the internal workings of the program so that we can learn its strengths and limitations. Simple testing of this program will also need to occur so that we could evaluate its effectiveness.

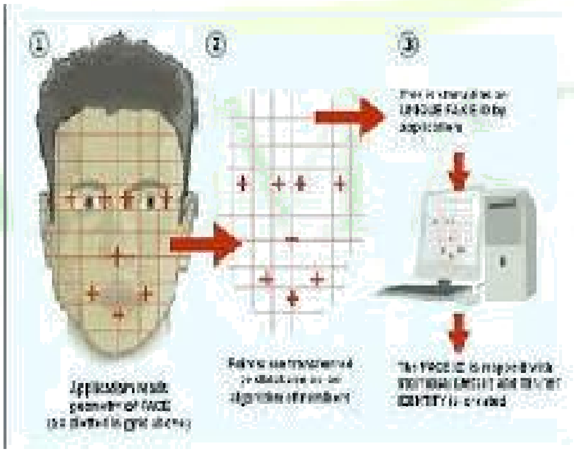


Fig.3. Face Recognition System

As shown in the Fig.3, Several sample images will be taken of several individuals to be used as test cases one each for “account” images, and several each for “live” images, each of which would vary pose, lighting conditions, and expressions. Once a final program is chosen, we will develop a simple ATM black box program. This program will serve as the theoretical ATM with which the facial recognition software will interact. It will take in a name and password, and then look in a folder for an image that is associated with that name. It will then take in an image from a separate folder of “live” images and use the facial recognition program to generate a match level between the two. Finally it will use the match level to decide whether or not to allow “access”, at which point it will terminate. All of this will be necessary, of course, because we will not have access to an actual ATM or its software. Both pieces of software will be compiled and run on a Windows XP and a Linux system. Once they are both functioning properly, they will be tweaked as much as possible to increase performance and to decrease memory footprint.

Following that, the black boxes will be broken into two components a server and a client to be used in a two-machine network. The client code will act as a user interface, passing all input data to the server code, which will handle the calls to the facial recognition software, further reducing the memory footprint and processor load required on the client end. In this sense, the thin client architecture of many ATMs will be emulated. We will then investigate the process of using the black box program to control a USB camera attached to the computer to avoid the use of the folder of “live” images. Lastly, it may be possible to add some sort of DES encryption to the client end to encrypt the input data and decrypt the output data from the server knowing that this will increase the processor load, but better allowing us to gauge the time it takes to process.

IV. BIOMETRIC FACIAL RECOGNITION

The image may not always be verified or identified in facial recognition alone. Identic has created a new product to help with precision. The development of Face It Argus uses skin biometrics, the uniqueness of skin texture, to yield even more accurate results. The process, called Surface Texture Analysis, works much the same way facial recognition does. A picture is taken of a patch of skin, called a skin print. That patch is then broken up into smaller blocks.

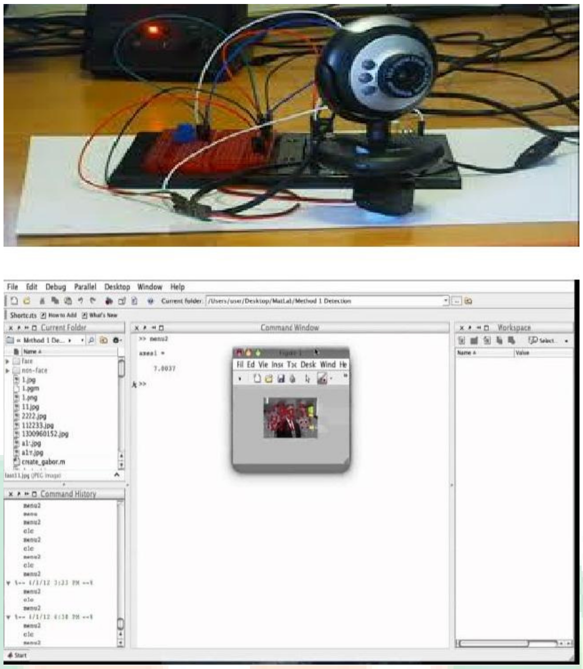
Using algorithms to turn the patch into a mathematical, measurable space, the system will then distinguish any lines, pores and the actual skin texture. It can identify differences between identical twins, which is not yet Possible using facial recognition software alone. According to Identic, by combining facial recognition with surface texture analysis, accurate identification can increase by 20 to 25 percent.

Face it currently uses three different templates to confirm or identify the subject: vector, local feature analysis and surface texture analysis. The vector template is very small and is used for rapid searching over the entire database primarily for one to many searching. The Local Feature Analysis template performs secondary search of ordered matches following the vector template. It performs a final pass after the templates search, relying on the skin features in the image, which contains the most detailed information. It is relatively insensitive to changes in expression, including blinking, frowning or smiling and has the ability to compensate for mustache or beard growth and the appearance of eyeglasses.

V. RESULTS AND DISCUSSION

This paper presented a approach for designing RFID based and face detecting method for money transaction. The change in reflection properties can be detected and measured using a RFID reader. In this paper, we have also proposed a face detection approach for high protection

.



```
>> menu2

area1 =

    7.0037

>>
```

```
menu2
menu
menu2
clc
menu2
clc
menu2
clc
menu2
%-- 4/1/12 3:23 PM --%
menu2
clc
menu2
%-- 4/1/12 4:18 PM --%
menu2
clc
menu2
```

Fig.4.a) Webcam used for face recognition **b)** MATLAB program

VI. CONCLUSION

This paper develops an ATM model that is more reliable in providing security by using facial recognition software. By keeping the time elapsed in the verification process to a negligible amount it even try to maintain the efficiency of this ATM system to a greater degree. Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. This paper provides a proffer a solution to the much dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics that can be made possible only when the account holder is physically present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level.

VI. REFERENCES

[1]Ayo, N.;"Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction", International Conference on Education Technology and Computer, 2009. ICETC '09, Page(s):201 – 204

[2]Chia-Tea Chou; Sheng-Wen Shih; Wen-Shiung Chen; Cheng, V.W.; Duan-Chen;"Non - Orthogonal View Face Recognition System" , IEEE Transactions on Circuits and Systems for Video Technology, Volume: 20 , Issue: 3.

[3].Changbo Hu; Hares, J.; Aggarwal, J.K.;"Patch based Face Recognition from Video", 16th IEEEInternational Conference on Image Processing (ICIP) , Page(s): 3321 – 3324.

[4]Jain, A., Hong, L., &Pankanti, S." BiometricIdentification", Communications of the ACM, Vol no 43, p. 91-98. Issue 4.

[5]Matai, Arturo, Kastner, "Design andImplementation of an FPGA-based Real-Time FaceRecognition System", IEEE International Symposium on Field-Programmable Custom Computing Machines, United States, pp97-100.

[6].Nathan, B.T.; Meenakumari, R.; Usha, S.;"Formation of Elliptic Curve Using Finger Print for Network Security", Process Automation, Control and Computing (PACC), Page 1-5.issue 4.

[7]Nathan, B.T.; Meenakumari, R.; Usha, S.;"Formation of Elliptic Curve Using Finger Print for Network Security", Process Automation, Control and Computing (PACC). Page 1-5.

[8] Ozturk, N.; Unozkan, U.; "Microprocessor based voice recognition system realization", 4th International Conference on Application of information and Communication Technologies (AICT), 2010, Page(s): 1 – 3.