American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-05, pp-188-193
www.ajer.us

Research Paper Open Access

Facial Verification Technology for Use In Atm Transactions

Aru, Okereke Eze, Ihekweaba Gozie
Department of Computer Engineering Michael Okpara University of Agriculture, Umudike, Umuahia, Abia State, Nigeria Opara, F.K.
Department of Electrical/Electronics Engineering Federal University of Technology, Owerri, Imo State, Nigeria

Abstract: There is an urgent need for improving security in banking region. With the birth of the Automatic Teller Machines, banking became a lot easier though with its own troubles of insecurity. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great efforts to rescue the unsafe situation at the ATM. This research looked into the development of a system that integrates facial recognition technology into the identity verification process used in ATMs. An ATM model that is more reliable in providing security by using facial recognition software is proposed .The development of such a system would serve to protect consumers and financial institutions alike from intruders and identity thieves. This paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition that will go as far as withholding the fraudster's card. If this technology becomes widely used, faces would be protected as well as PINs. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts. The combined biometric features approach is to serve the purpose both the identification and authentication that card and PIN do.

Keywords: *ATM, Security, Face, Verification, Fraud, PIN, etc*

I. INTRODUCTION

To use an ATM with facial recognition system, all you need is walk to the atm. its digital camera is on 24hours a day, and its computer will automatically initiate a face recognition procedure, whenever the computer detects a human face in camera obtains a picture of your face, the computer compares the image of your face to the images of registered customers in its database .If your face (as seen by the ATMs camera) matches the picture of the in the data base you are automatically recognized by the machine.

The machine will then play a recording will be heard through a loudspeaker, the recording will say" your face is recognized".

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 a physical 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. The main issues faced in developing such a model are keeping the time elapsed in the verification process to a negligible amount, allowing for an appropriate level of variation in a customer's face when compared to the database image, and that credit cards which can be used at ATMs to withdraw funds are generally issued by institutions that do not have in-person contact with the customer, and hence no opportunity to acquire a photo**.** Because the system would only attempt to match two (and later, a few) discrete images,

searching through a large database of possible matching candidates would be unnecessary. The process would effectively become an exercise in pattern matching, which would not require a great deal of time. With appropriate lighting and robust learning software, slight variations could be accounted for in most cases. 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 (read: significant fraud reduction) achieved by this system might motivate such an overhaul.

The last consideration is that consumers may be wary of the privacy concerns raised by maintaining images of customers in a bank database, encrypted or otherwise, due to possible hacking attempts or employee misuse. 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

.

II. COMBATING AUTOMATED TELLER MACHINE FRAUDS THROUGH FACIAL RECOGNITION ATM TECHNOLOGY

ATMs have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic with its attendant issues. Gone are the days of maintaining long queues in the banking hall which made the work of bankers more difficult thus leading to all forms of errors. Even to customers, having to leave the comfort of their homes for financial transactions before bankers close for the day's business is a major problem solved by Automated Teller Machines. However, as man begins to realize the gains of technology brought about by this machine to supplement human tellers, little did one know that the joy shall be short lived by the various sharp practices leading to financial losses.

As banks are losing, so are the customers. News Media are filled with various forms of complaints on how users are losing money to fraudsters. Some have vowed never to come near usage of various cards – debit, credit or prepaid– local or international. The problem may even go as deep as engaging in legal battle between banks and their customers. The need to find a lasting solution is the main focus of this paper.

2.1 Present Controls

Considering the volume of transactions being processed by several branches of a commercial bank, proper control in form identification and authentication should be in place.Several control measures have been put in place to ensure interests of all concerned parties such as issuers, acquirers, third party processors, switching companies and cardholders are protected. Some of the controls in place include:

About ATM

- Well lit up to discourage shady deeds at night
- Fortified with camera for footage
- Keypad protector against key logger and shoulder surfing
- Dual control of physical access to the machine
- Default password disabled to avoid unauthorized access
- Lines of demarcation between a current user and the next person on the queue to prevent shoulder surfing.
- Timely reconciliation of cash loading with ATM Till account
- Surveillance through physical monitoring and CCTV cameras

B. About Cards

- Strong algorithms are used in generating PANs
- Storage of card details is done on protected systems
- Card details (such as PAN, expiry date) are jealously guarded.
- While communicating, PAN is masked

- Strong Encryption is used when transferring files especially, between TPP and Issuer
- Magnetic stripe type is outlawed in some countries to avoid card cloning.
- Some restrictions are placed on cards in terms of allowable transactions and withdrawal limits

C. About PIN

- Where PIN mailers are used, they are not dispatched at the same time with the cards and usually through a different medium.
- PIN selectable options are used to prevent insider compromise
- PINs are masked during usage against shoulder surfing.

III. SECURING CUSTOMERS THROUGH FACIAL RECOGNITION AUTHENTICATION

ATM usage usually, works on two-factor authentication requiring something you have and something you know or you are. To use an ATM presently, demands having a card that has to be authenticated by PIN as a second factor authentication. To aid memory, some users write their PINs in diaries or store them on some other unprotected devices.

The moment the card is accessible, PIN is guessed or obtained through other means such as social engineering, shoulder surfing or outright collection under duress. Recently, Biometric ATMs are introduced to be used along with card. This will definitely impact on the amount frauds if fully implemented. Further development has produced biometric authentication in Japan where customers face is used as a means of authentication. Phil (2012),examined the "You are the cash card" roll out in Japan where authentication is just by your face, PIN and the card.

3.1 Secure Atm By Facial Recognition Technology (Image Processing)

To use an ATM with facial recognition system, all you need is walk to the atm. its digital camera is on 24hours a day, and its computer will automatically initiate a face recognition procedure, whenever the computer detects a human face in camera obtains a picture of your face, the computer compares the image of your face to the images of registered customers in its database .If your face (as seen by the ATMs camera) matches the picture of the in the data base you are automatically recognized by the machine.

An Image may be defined as a two dimensional function f (x,y) where x and y are spatial(plane) coordinates x, y is called intensity or gray level of the image at that point. When x, y and the amplitude values of f are all finite, discrete quantities, we call the image a digital image.

Interest in digital image areas: improvement of pictorial information for human interpretation: and representation for autonomous machine perception.

The entire process of Image Processing and starting from the receiving of visual information to the giving out of description of the scene, may be divided into three major stages which are also considered as major sub areas, and are given below

Discretization and representation: Converting visual information into a discrete form

3.2 Methodology

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 compilable 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. 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.

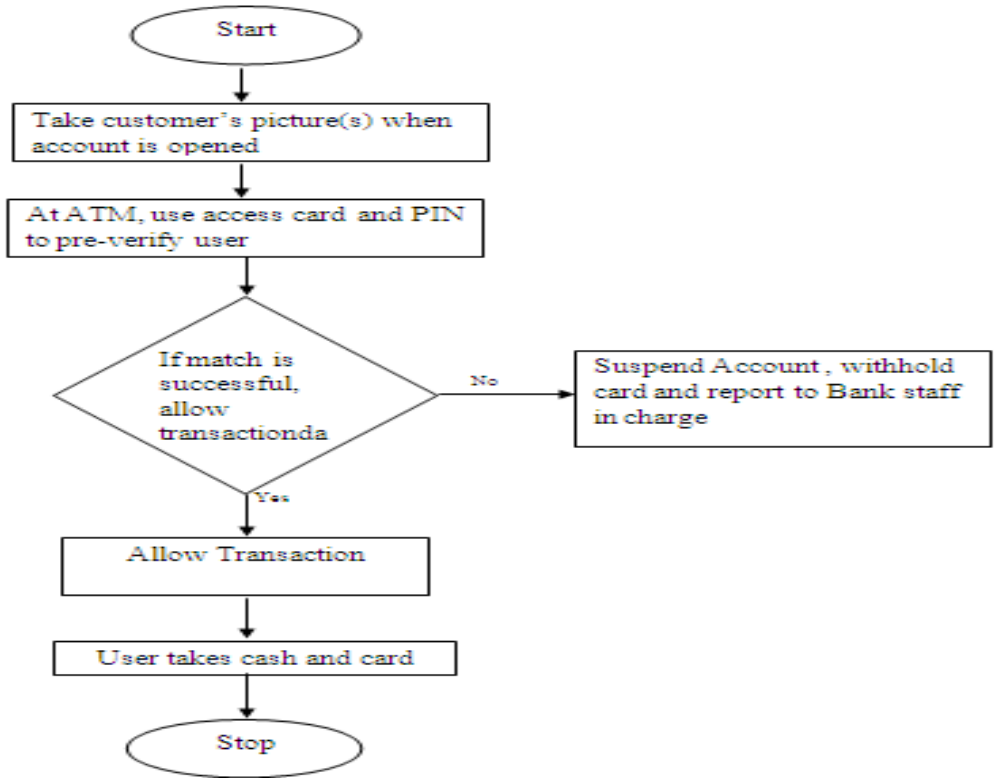
Both pieces of software will be compiled and run on a Windows XP and a Linux system. Once they are both functioning properly, they will be tweaked as much as possible to increase performance (decreasing the time spent matching) and to decrease memory footprint.

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.

3.2.1 Flow Chart of The Operation



3.3 FACE RECOGNITION SOFTWARE:

Face recognition technology: Ideal for access control, financial transactions and ATM machines.

3.3.1 The face key recognition technology performs the following tasks:

- Locates a moving object within the camera view
- Determines if the moving object is face
- Compares live faces with samples from database
- Face recognition technology can work with both low resolution USB
- Cameras and low or high resolution CCTV cameras

3.3.2 Face capturing technology: Captured and stored with time and date.

Face finding technology captures all the faces in a cameras view .Then is stores each image in a separate folder for quick reviews-or for use with another face key technology. Each face is saved with a time and date stamp. In addition to faces, facial profiles and images of human bodies can be captured and stored.

Search and match advisory technology:

Search and match advisory technology is available to assist in the identification of facial images extracted from the video stream or from a watch list database. This function operates by comparing a subject's photo to a database of faces and selecting the faces from the database which look the most like the subjects face….your face is your key.

3.4 Atm Fraud Types To Be Prevented By Atm Facial Recognition Technology

- Unauthorised financial operations using lost or stolen cards and pin codes which many inexperienced card owners write down on a card or sore the PIN code together with the card.
- Fraud based on Trust- The card or its duplicate can be used by a fraudster without the permission of the card owner.
- Installation of additional devices that allow the reading of a cards magnetic stripe and save on video numerical combinations typed on cash machine keyboard.

3.5 ATM Security - Importance of ATM Security

Importance of ATM security

Having a solid security to ATMs is very vital for banks to maintain their quality service and reputation. Most leading and established banks do consider this fact as a top priority when you have a reliable security to your ATMs there are many positive outcomes. Mainly you will win the customers' trust and loyalty, reduction of financial losses due to technical and non-technical robberies, and added security will improve the rate of transactions and eventually the banks can profit through it.

3.6 Advantages Of Facial Recognition Technology

Eradicate Fraud costs for the bank

* Deliver a practical and workable solution that addresses the requirements of the regulatory authorities.
* Limit the financial risks given that they were forced to take responsibility for financial loss [rather than being allowed to pass this on to the account-holder]
* Provide a framework that still allowed for high withdrawal limits to cater for the demands of a cash-focused customer base
* Take societal responsibility to reduce rising levels of crime that were associated with cash-card transactions
* Increase customer satisfaction

For the account-holder, the potential advantages are:

* Different charges for transactions given that the transaction takes place in a more secure manner
* Higher withdrawal and transaction limits
* Peace of mind given the higher level of security applied to the account

IV. CONCLUSION

We thus develop 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 we 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. In this paper, we have tried to 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.

REFERENCES

[1]. Adeoti, J. (2011). Automated Teller Machine (ATM) frauds in Nigeria: the way out.
[2]. Adini (2010). Nigerian banks look to biometric ATM machines to reduce fraud.
[3]. http://nairavilla.com/topic/743. accessed October 12,2012.
[4]. Bhargav-Spantzel A., Squicciarini A., Bertino E.Kong X & Zhang W.(2010). Biometrics-Based
[5]. Identifiers for Digital Identity Management.
[6]. Consultative Group for International Agricultural Research, CGIAR (2009). Network user identification and authentication good practice guide.
[7]. Das, S. & Debbarma, J.(2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in India e-Banking system. International Journal of Information and Communication Technology Research vol 1 no 5 p 197-203.
[8]. Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450-2275 issue 21.
[9]. George Webster (2010). Biometric ATM gives cash via facial recognition scan. Http://edition.cnn.com. accessed October 10, 2012.
[10]. Heather Crawford (2011). Applying Usable Security Principles to Authentication.
[11]. Jacobs, B. & Poll, E. (2010) Biometrics and Smart Cards in Identity Management.
[12]. Mohammed, L. (2010). Use of biometrics to tackle ATM fraud.
[13]. Researchers at MIT, Baback Moghaddam and Alex Pentland, and one a commercial product from Identix called FaceIt

Aru, Okereke Eze
is a lecturer in the Department of Computer Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. His research Interests include Computer Hardware design and maintenance, Security system design, , expert systems, Design of Microcontroller and Microprocessor based system, digital systems design using microcontrollers and other computer related subjects.

Dr. Ihekweaba, Gozie
is the Head, Department of Computer Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. Her research interests include Computer Hardware design and maintenance, Security system design, expert systems etc.

Dr. Opara, F.K.
is the Head, Department of Electrical/Electronics Engineering, Federal University of Technology, Owerri, Imo State, Nigeria. His research interests include Computer Hardware design and maintenance, Electronic and Communication Systems, Electronic Security system designs etc.