International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 07 | July -2020 ISSN: 2582-3930

Securing ATM transaction by using Face Recognition Technique and GSM Module

Priyanka P[1], Yashonidhi Yajaman[2]

Electronics and Communication Engineering, GSSSIETW Mysuru[1],
Electronics and Communication Engineering, GSSSIETW, Mysuru [2]

---***---

Abstract - ***Abstract*— Automated Teller Machine (ATM) systems have become instant cash providers for people around the globe and have increased in vast numbers in the past few years. Now a day's robberies have also increasing day by day. There is an urgent need for improving security in banking region. With the advent of ATM though banking became a lot easier it even became a lot vulnerable. The existing security in these systems is lagging behind in providing fool proof security. ATM systems today use no more than an access card and PIN for identity verification. This situation is unfortunate since tremendous progress has been made in biometric identification techniques, including finger printing, retina scanning, and facial recognition. This technique presents a secure approach in rendering money with the help of combination of Face recognition and Subscriber Identity Module (SIM) technologies. The system recognizes the face of the user with the help of image processing and Global System for Mobile communication (GSM) modem is used to send SIM identity to the server data base. This paper proposes the development of a system that integrates facial recognition technology into the identity verification process used in ATMs. The development of such a system would serve to protect consumers and financial institutions alike from fraud and other breaches of security.**

***Keywords*— ATM; GSM; SIM, CISC, RISC;**

1. INTRODUCTION

The rise of technology in India has brought into force many types of equipment that aim at more customer satisfaction. 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.

An automatic teller machine security model combines 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 LITERATURE REVIEW

For most of the past ten years, the majority of ATMs used worldwide ran under IBM's now-defunct OS/2. However, IBM hasn't issued a major update to the operating system in over six years. Movement in the banking world is now going in two directions: Windows and Linux. NCR, a leading world-wide ATM manufacturer, recently announced an agreement to use Windows XP Embedded in its next generation of personalized ATMs (crmdaily.com.) Windows XP Embedded allows OEMs to pick and choose from the thousands of components that make up Windows XP Professional, including integrated multimedia, networking and database management functionality. This makes the use of off-the-shelf facial recognition code more desirable because it could easily be compiled for the Windows XP environment and the networking and database tools will already be in place.

For less powerful ATMs, KAL, a software development company based in Scotland, provides Kalignite CE, which is a modification of the Windows CE platform. This allows developers that target older machines to more easily develop complex user-interaction systems . Many financial institutions are relying on a third choice, Windows NT, because of its stability and maturity as a platform.

On an alternative front, the largest bank in the south of Brazil, Banrisul, has installed a custom version of Linux in its set of two thousand ATMs, replacing legacy MS-DOS systems. The ATMs send database requests to bank servers which do the bulk of transaction processing (linux.org.) This model would also work well for the proposed system if the ATMs processors were not powerful enough to quickly perform the facial recognition algorithms.

In terms of the improvement of security standards, MasterCard is spearheading an effort to heighten the encryption used at ATMs. For the past few decades, many machines have used the Data Encryption Standard developed by IBM in the mid 1970s that uses a 56-bit key. DES has been shown to be rather easily cracked, however, given proper computing hardware. In recent years, a "Triple DES" scheme has been put forth that uses three such keys, for an effective 168-bit key length. MasterCard now requires new or relocated ATMs to use the Triple DES scheme, and by April, 2005, both Visa and MasterCard will require that any ATM that supports their cards must use Triple DES. ATM manufacturers are now developing newer models that support Triple DES natively; such redesigns may make them more amenable to also including snapshot cameras and facial recognition software, more so than they would be in regards to retrofitting pre-existing machines.

There are hundreds of proposed and actual implementations of facial recognition technology from all manner of vendors for all manner of uses. However, for the model proposed in this paper, we are interested only in the process of facial verification – matching a live image to a predefined image to verify a claim of identity – not in the process of facial evaluation – matching a live image to any image in a database. Further, the environmental conditions under which the verification takes place – the lighting, the imaging system, the image profile, and the processing environment – would all be controlled within certain narrow limits, making hugely robust software unnecessary .One leading facial recognition algorithm class is called image template based. This method attempts to capture global features of facial images into facial templates. Neural networks, among other methods, are often used to construct these templates for later matching use. An alternative method, called geometry-based, is to explicitly examine the individual features of a face and the geometrical relationship between those features (Gross.) What must be taken into account, though, are certain key factors that may change across live images: illumination, expression, and pose (profile.)

A study was recently conducted of leading recognition algorithms, notably one developed by two researchers at MIT, Baback Moghaddam and Alex Pentland, and one a commercial product from Identix called FaceIt. The MIT program is based on Principal Feature Analysis, an adaptation of template based recognition. FaceIt's approach uses geometry-based local feature analysis. Both algorithms have to be initialized by providing the locations of the eyes in the database image, from which they can create an internal representation of the normalized face. It is this representation to which future live images will be compared.

In the study, it was found that both programs handled changes in illumination well. This is important because ATM use occurs day and night, with or without artificial illumination. Likewise, the programs allowed general expression changes while maintaining matching success. However, extreme expressions, such as a scream profile, or squinted eyes, dropped the recognition rates significantly. Lastly, matching profile changes worked reasonably well when the initial training image(s) were frontal, which allowed 70-80% success rates for up to 45 degrees of profile change… however, 70-80% success isn't amenable to keeping ATM users content with the system.

The natural conclusion to draw, then, is to take a frontal image for the bank database, and to provide a prompt to the user, verbal or otherwise, to face the camera directly when the ATM verification process is to begin, so as to avoid the need to account for profile changes. With this and other accommodations, recognition rates for verification can rise above 90%. Also worth noting is that Face. It's local feature analysis method handled variations in the test cases slightly better than the PGA system used by the MIT researchers.

Another paper shows more advantages in using local feature analysis systems. For internal representations of faces, LFA stores them topographically; that is, it maintains feature relationships explicitly. Template based systems, such as PGA, do not. The advantages of LFA are that analysis can be done on varying levels of object grouping, and that analysis methods can be independent of the topography. In other words, a system can examine just the eyes, or the eyes nose and mouth, or ears, nose, mouth and eyebrows, and so on, and that as better analysis algorithms are developed, they can fit within the data framework provided by LFA

The conclusion to be drawn for this project, then, is that facial verification software is currently up to the task of providing high match rates for use in ATM transactions. What remains is to find an appropriate open-source local feature analysis facial verification program that can be used on a variety of platforms, including embedded processors, and to determine behavior protocols for the match / non-match cases.

III FACE RECOGNITION SYSTEM

Face Recognition Systems is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source.

One of the ways to do this is by comparing selected facial features from the image and a facial database.

A database of people's faces is maintained by the system that handles face Recognition. Whenever a face needs to be identified, a photograph of the person's face is taken and compared to the faces present in the database to see if a match is found.

There are usually 3 parts to a face recognition system –

1) Face Detector

2) Eye Localiser

3) Face Recogniser

1) The Face Detector:

The face detector detects the face, eliminating any other detail, not related to the face (like the background). It identifies the facial region, leaving out the non-facial region in the photograph of the person to be identified.

2) The Eye-Localiser:

It finds the location of the eyes, so that the position of the face can be identified better.

3) The Face Recogniser:

It then checks the database to find a match.

TECHNIQUES OF FRS

There are three types of techniques employed. They are

1) 2-D,

2) 3-D

3) Surface Texture Analysis.

1) 2-D Technique:

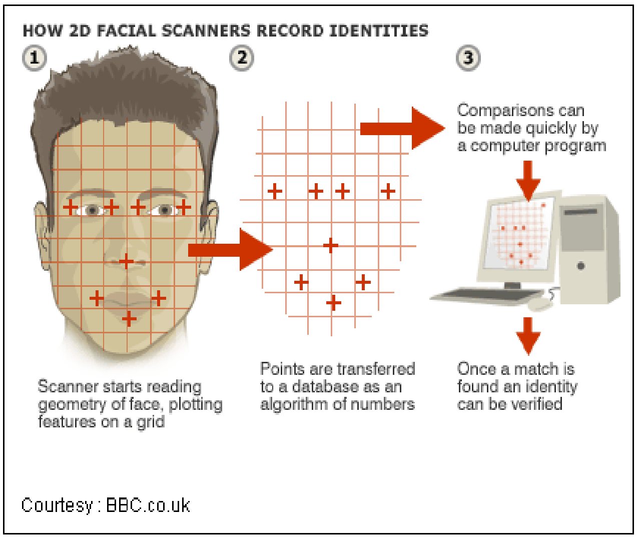
The 2-D recognition technique was one of the earliest techniques used. It maintained details of people's faces as seen 2 dimensionally. Details like width of the eye, width of the nose, jaw line, distance between the eyes, cheek bone shape and the like were used for comparison. This kind of face recognition was not very accurate. Difference in ambient lighting or a face that is not directly looking into the camera, or a change in facial expression did not produce expected results.

2) 3-D Technique:

Advancement in face recognition gave birth to the 3-D recognition technique. This stepped up technique, used features like contours of the eye sockets, nose, chin, peaks and valleys on the face for identification. The database stores such details of faces as well. The advantage of 3-D over 2-D method is that 3-D face detection works well even if the face is turned at 90 degree to the camera. Also, it is independent of lighting environment and facial expressions.

3) Surface Texture Analysis:

A more advanced method is Surface Texture Analysis (STA). This technique does not scan the entire face but a patch of skin on it. This patch is divided into blocks. The skin texture, the pores on the skin and other such characteristics are converted to a code, which is used for comparison.


HOW 2D FACIAL SCANNERS RECORD IDENTITIES
1
2
3
Comparisons can be made quickly by a computer program
Scanner starts reading geometry of face, plotting features on a grid
Points are transferred to a database as an algorithm of numbers
Once a match is found an identity can be verified

Courtesy : BBC.co.uk

Figure: 2D Technique

IV ARM CONTROLLER

The Advanced RISC Machine is a 32-bit RISC processor architecture developed by ARM Limited that is widely used in a number of embedded designs. Because of their power saving features. ARM CPUs are dominant in the mobile electronics market, where low power consumption is a critical design goal.

Today, the ARM family accounts for approximately 75% of all embedded 32-bit RISC CPUs, making it one of the most widely used 32-bit architectures in the world. ARM CPUs are found in all corners of consumer electronics, from portable devices to computer peripherals. The use of RISC processors over CISC processors in embedded systems today is wide spread and seems to be the trend of the future. This is because when it comes to embedded systems, RISC has many advantages over CISC both in hardware and software implementation of these embedded systems.

Some of these benefits of RISC are:

- Simpler assembler coding
- High throughput
- Low power consuming

ARM architecture is developed to utilize the benefits of CISC and RISC by improving the code density and reducing the power consumption. ARM Limited has facial database incorporated a novel mechanism, called the Thumb architecture. The Thumb instruction set is a 16-bit compressed form of the original 32-bit ARM instruction set, and employs dynamic decompression hardware in the instruction pipeline. The ARM architecture is based on Reduced Instruction Set Computer (RISC) principles. The

RISC instruction set and related decode mechanism are much simpler than those of CISC designs.

GSM SIM READER

GSM (Global System for Mobile Communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital Wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compress data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHZ or I 800 MHZ frequency band.

GSM together with other technologies is part of evolution of wireless mobile telecommunication that includes High-Speed circuit-switched Data (HSCSD) , General Packet Ratio System(GPRS) , Enhanced Data rate for GSM Evolution (EDGE), and Universal Mobile Telecommunication Service(UMTS).

GSM networks are most popular and widespread wireless communication media across the world, having a wide customer base in Europe and Asia-Pacific and command more than 50 percent of mobile customers. The advancement of GSM networks increases rapid growth of its users and services. Being an advance technology it becomes favourites for the criminals. These things created worldwide market for the analysis and monitoring of GSM network.

Face recognition technology for ATM

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information. GSM networks are most popular and widespread wireless communication media across the world, having a wide customer base in Europe and Asia-Pacific and command more than 50 percent of mobile customers. The advancement of GSM networks increases rapid growth of its users and services. Being an advance technology it becomes favourites for the criminals. These things created worldwide market for the analysis and monitoring of GSM network.

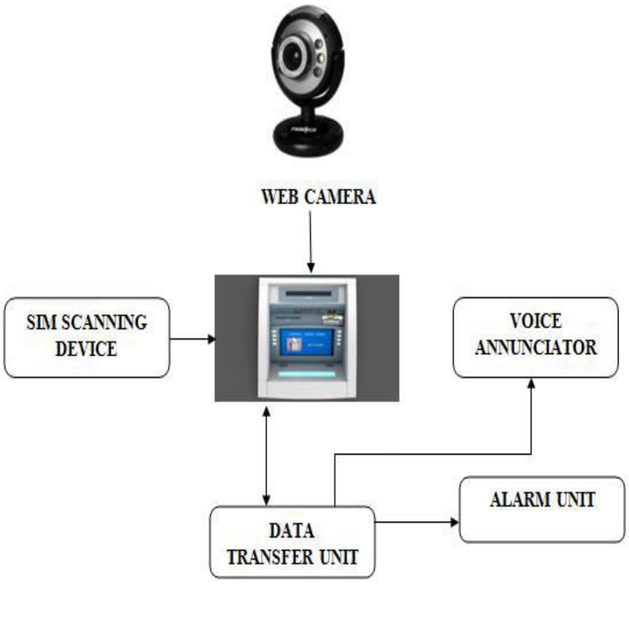


Figure: Block Diagram

1) SIM Scanning Device

Scanning device consist of GSM MODEM which acts like a scanner for tracking the SIM ID. This ID consists of user information from which controller verifies the originality of the user.

2) Web camera

Camera is used for Capturing the face image of the user hence by using suitable algorithm the match of images is performed by ARM controller.

3) Voice Annunciator

The voice annunciator produces the voice which enhances the user to make the transaction effortless.

4) Alarm unit

If the face which given as an input to the controller is mismatched with the data base images then unauthenticated mode is activated and ARM controller activated the alarm signal for alarm unit.

5) Data Transfer unit (DTU)

Data transfer unit transfer the user information from external world to the ARM controller. The information's are stored temporarily in this unit and it acts like mediator for effective function of all units such as providing input for voice annunciator and alarm unit.

Whenever the person or user enters the ATM room for rendering money, the SIM Identity belonging to that customer is inserted in to the SIM scanning device(which here used is a GSM module).The scanning device then tracks the SIM information of the corresponding user. Then the Data Transfer Unit transfers the data to the ARM controller and controller searches for the desired customer Information on the database. If the information provided by the customer matches with the information present in the database then facial recognition process starts with the help of a Web Camera, if the facial image also matches with any one of the database stored images the customer is allowed for the money transaction with the help of voice annunciator. If the facial image does not match with any one of the customer stored images an automatic message regarding ATM access will be forwarded to the actual customer whether to permit the transaction or not. If the customer responds as 'Yes' then transaction continues with the help of voice annunciation unit, if the customer responds as 'No' then the user is treated as unauthorized and Alarm Unit continuously beeps. If the information provided by the customer from SIM ID is mismatched with database then data transfer unit signal the alarm unit to beep continuously and money transaction is banned.

V CONCLUSION

Face recognition techniques are used in the banking sector and also private offices like companies verify the originality of the user identify and only particular user is allowed to use the SIM ID based automatic teller machine**.**

Mainly face recognition technology helps to 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.

REFERENCES

[1] [1] Schultz. Zac. "Facial Recognition Technology Helps DMV Present Identity Theft. WMTVNew. Gary Television. Retrieved 2007-09- 17." Madison: The

[2] Department of Motor Vehicles is using... facial Recognition Technology (to prevent ID theft]"

[3] (2) Crawford, Mask. Facial Recognition progress report". SPIE Newsroom. Retrieved

[4] (3) Discussion with Proof Andreas dangle, DFKI

[5] (4) Willing. Richard (2003-09-02) Airport anti-terror systems flub tests face Recognition technology fails to flag suspects

[6] (5) House, David "Facial Recognition at DMV" Oregon Department of Transportation. Retrieved 2007-09-17. Oregon Department of going to start using "Facial Recognition" software, a new tool in the prevention of fraud, required by a new state law. The law is designed to prevent someone from obtaining a driver license or ID card under a false name"

[7] (6)Bone, Mike, Way man, Dr. James L., and Blackburn, Duane. "Evaluating Facial

[8] Recognition Technology for Drug Control Applications." ONDCP International

[9] Counterdrug Technology Symposium: Facial Recognition Vendor Test. Department of Defence Counterdrug Technology Development Program Office, June 2001.

[10] All, Anne. "Triple DES dare you." ATM Marketplace.com. 19 Apr. 2002.

[11] Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. "Evaluating Facial

[12] Recognition Technology for Drug Control Applications." ONDCP International Counterdrug Technology Symposium: Facial Recognition Vendor Test. Department of Defense Counterdrug Technology Development Program Office, June 2001.

[13] Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. "Quo vadis Face Recognition." Third

[14] Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001.

[15] Penev, Penio S., and Atick, Joseph J. "Local Feature Analysis: A General Statistical

[16] Theory for Object Representation." Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500, 1996.

[17] Wrolstad, Jay. "NCR To Deploy New Microsoft OS in ATMs." CRMDailyDotCom. 29 Nov. 2001