ATM WITH AN EYE

A Seminar Submitted to

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY,

ANANTAPUR

In the partial fulfillment of the Requirements

for the award of the Degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted By

G.Lakshmi

(09G01A0521`)

SRI VENKATESA PERUMAL COLLEGE OF ENGINEERING AND TECHNOLOGY

Approved by A.I.C.T.E., Affiliated to J.N.T.University, Anantapur
(An ISO9001:2000 Certified Institution)
R.V.S.Nagar, K.N Road, PUTTUR-517583, Chittoor(Dt), A.P

ABSTRACT

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 chances of misuse of this much hyped ‘insecure’ baby product (ATM) are manifold due to the exponential growth of ‘intelligent’ criminals day by day. 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, facial recognition, and iris scanning.

This paper proposes the development of a system that integrates **Facial regognition** and **Iris scanning** 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.

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.

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. A system can examine just the eyes, or the eyes nose and mouth, or ears, nose, mouth and eyebrows, and so on.

In this paper , we will also look into an automatic teller machine security model providing the customers a cardless, password-free way to get their money out of an ATM. Just step up to the camera while your eye is scanned. The iris -- the colored part of the eye the camera will be checking -- is unique to every person, more so than fingerprints.

ATM SYSTEMS

Our ATM 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.

HISTORY

The first ATMs were off-line machines, meaning money was not automatically withdrawn from an account. The bank accounts were not (at that time) connected by a computer network to the ATM. Therefore, banks were at first very exclusive about who they gave ATM privileges to. Giving them only to credit card holders (credit cards were used before ATM cards) with good banking records. In modern ATMs, customers authenticate themselves by using a plastic card with a magnetic stripe, which encodes the customer's account number, and by entering a numeric passcode called a PIN (personal identification number), which in some cases may be changed using the machine. Typically, if the number is entered incorrectly several times in a row, most ATMs will retain the card as a security precaution to prevent an unauthorised user from working out the PIN by pure guesswork..

HARDWARE AND SOFTWARE

ATMs contain secure cryptoprocessors, generally within an IBM PC compatible host computer in a secure enclosure. The security of the machine relies mostly on the integrity of the secure cryptoprocessor: the host software often runs on a commodity operating system.In-store ATMs typically connect directly to their ATM Transaction Processor via a modem over a dedicated telephone line, although the move towards Internet connections is under way.

In addition, ATMs are moving away from custom circuit boards (most of which are based on Intel 8086 architecture) and into full-fledged PCs with commodity operating systems such as Windows 2000 and Linux. An example of this is Banrisul, the largest bank in the South of Brazil, which has replaced the MS-DOS operating systems in its automatic teller machines with Linux. Other platforms include RMX 86, OS/2 and Windows 98 bundled with Java. The newest ATMs use Windows XP or Windows XP embedded.

RELIABILITY

ATMs are generally reliable, but if they do go wrong customers will be left without cash until the following morning or whenever they can get to the bank during opening hours. Of course, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures); software (such as operating system; device driver; application); communications; or purely down to operator error.

SECURITY

Early ATM security focused on making the ATMs invulnerable to physical attack; they were effectively safes with dispenser mechanisms. ATMs are placed not only near banks, but also in locations such as malls, grocery stores, and restaurants. The other side of this improvement is the enhancement of the culprit’s probability to get his ‘unauthentic’ share.

ATMs are a quick and convenient way to get cash. They are also public and visible, so it pays to be careful when you're making transactions. Follow these general tips for your personal safety.

Stay alert. If an ATM is housed in an enclosed area, shut the entry door completely behind you. If you drive up to an ATM, keep your car doors locked and an eye on your surroundings. If you feel uneasy or sense something may be wrong while you're at an ATM, particularly at night or when you're alone, leave the area.

Keep you PIN confidential. Memorize your Personal Identification Number (PIN); don't write it on your card or leave it in your wallet or purse. Keep your number to yourself. Never provide your PIN over the telephone, even if a caller identifies himself as a bank employee or police officer. Neither person would call you to obtain your number.

Conduct transactions in private. Stay squarely in front of the ATM when completing your transaction so people waiting behind you won't have an opportunity to see your PIN being entered or to view any account information. Similarly, fill out your deposit/withdrawal slips privately.

Don’t flash your cash. If you must count your money, do it at the ATM, and place your cash into your wallet or purse before stepping away. Avoid making excessively large withdrawals. If you think you're being followed as you leave the ATM, go to a public area near other people and, if necessary, ask for help.

Save receipt. Your ATM receipts provide a record of your transactions that you can later reconcile with your monthly bank statement. If you notice any discrepancies on your statement, contact your bank as soon as possible. Leaving receipts at an ATM can also let others know how much money you've withdrawn and how much you have in your account.

Guard your card. Don't lend your card or provide your PIN to others, or discuss your bank account with friendly strangers. If your card is lost or stolen, contact your bank immediately.

Immediately report any crime to the police. Contact the Department Of Public Security or your local police station for more personal safety information.

FACIAL RECOGNITION

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.

SOFTWARE SPECIFICATION

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.

Many financial institutions are relying on Windows NT, because of its stability and maturity as a platform.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.

SECURITY

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. 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 .

FACIAL RECOGNITION TECHNIQUE:

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. What must be taken into account, though, are certain key factors that may change across live images: illumination, expression, and pose (profile.)

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%. A system can examine just the eyes, or the eyes nose and mouth, or ears, nose, mouth and eyebrows, and so on

.

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.

OUR 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 server 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.

IRIS RECOGNITION:

Inspite of all these security features, a new technology has been developed. Bank United of Texas became the first in the United States to offer iris recognition technology at automatic teller machines, providing the customers a cardless, password-free way to get their money out of an ATM. There's no card to show, there's no fingers to ink, no customer inconvenience or discomfort. It's just a photograph of a Bank United customer's eyes. Just step up to the camera while your eye is scanned. The iris -- the colored part of the eye the camera will be checking -- is unique to every person, more so than fingerprints. And, for the customers who can't remember their personal identification number or password and scratch it on the back of their cards or somewhere that a potential thief can find, no more fear of having an account cleaned out if the card is lost or stolen.

HOW THE SYSTEM WORKS.

When a customer puts in a bankcard, a stereo camera locates the face, finds the eye and takes a digital image of the iris at a distance of up to three feet. The resulting computerized "iris code" is compared with one the customer will initially provide the bank. The ATM won't work if the two codes don't match. The entire process takes less than two seconds.

The system works equally well with customers wearing glasses or contact lenses and at night. No special lighting is needed. The camera also does not use any kind of beam. Instead, a special lens has been developed that will not only blow up the image of the iris, but provide more detail when it does. Iris scans are much more accurate than other high-tech ID systems available that scan voices, faces and fingerprints.

Scientists have identified 250 features unique to each person's iris -- compared with about 40 for fingerprints -- and it remains constant through a person's life, unlike a voice or a face. Fingerprint and hand patterns can be changed through alteration or injury. The iris is the best part of the eye to use as a identifier because there are no known diseases of the iris and eye surgery is not performed on the iris. Iris identification is the most secure, robust and stable form of identification known to man. It is far safer, faster, more secure and accurate than DNA testing. Even identical twins do not have identical irises. The iris remains the same from 18 months after birth until five minutes after death.

When the system is fully operational, a bank customer will have an iris record made for comparison when an account is opened. The bank will have the option of identifying either the left or right eye or both. It requires no intervention by the customer. They will simply get a letter telling them they no longer have to use the PIN number. And, scam artists beware, a picture of the card holder won't pass muster. The first thing the camera will check is whether the eye is pulsating. If we don't see blood flowing through your eye, you're either dead or it's a picture.

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. 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.

BIBILOGRAPHY:

All, Anne. “Triple DES dare you.” ATM Marketplace.com. 19 Apr. 2002.

Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. “Evaluating Facial 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.

Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F. “Quo vadis Face Recognition.” Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai: December 2001.

Penev, Penio S., and Atick, Joseph J. “Local Feature Analysis: A General Statistical Theory for Object Representation.” Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500, 1996.

Wrolstad, Jay. “NCR To Deploy New Microsoft OS in ATMs.” CRMDailyDotCom. 29 Nov. 2001