# AN ATM WITH AN EYE


## 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, retina scanning, and facial recognition. 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.


## 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.

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.

## 2. 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 FaceIt'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.

## 3. 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.

## 4. 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.