# An ATM with an Eye

**Udit Sunchey[1] Mohit Kumar Singh[2]**
[1,2]MCA-3rd Year Student
[1,2]Institute of Management & Computer Studies Approved by AICTE & Affiliated to Mumbai University C-4, Wagle Industrial Estate, Near Mulund Check Naka, Thane (W)-400604

*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.

***Key words:*** ATM, Facial Recognition Technology

## I. 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.

This Technique 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.

## II. 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 pass code 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 unauthorized user from working out the PIN by 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.

## III. ATM System

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.

## IV. Hardware & software

ATMs contain secure crypto processors, 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 crypto processor 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 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. 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. 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.

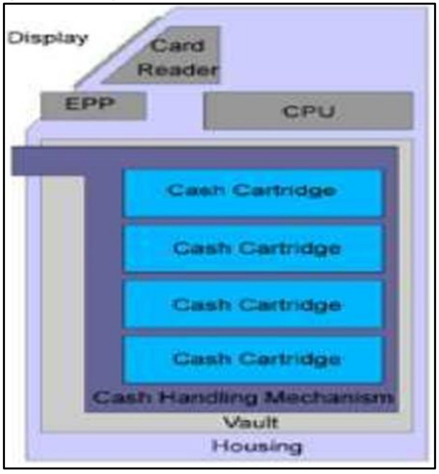

Fig. 1: Block Diagram of ATM

### *A. 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 an 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.

Fig. 2:

The iris -- the colored part of the eye the camera will be checking -- is unique to every person, more so than fingerprints.

Fig. 3:

ATM system would only attempt to match two 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.

## V. Iris Recognition

In spite 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 card less and 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.

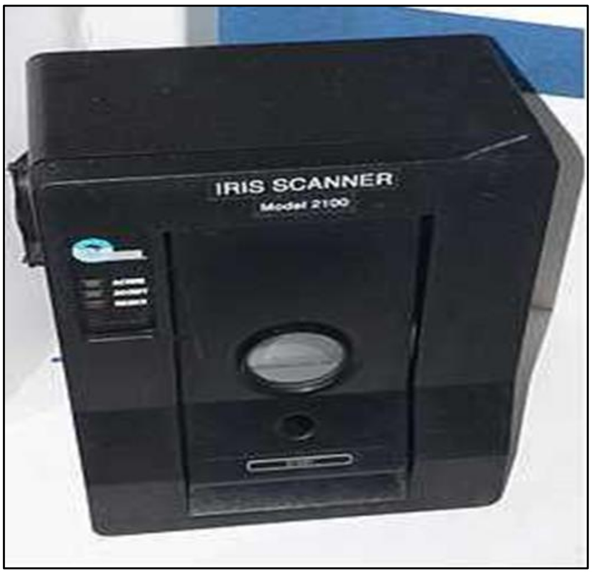

Fig. 4: An IriScan model 2100 iris scanner

Many millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to False Matches, is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

### A. *Deployed Applications*

- Aadhar, India's UID project uses Iris scan along with fingerprints to uniquely identify people and allocate a Unique Identification Number.
- Police forces across America plan to start using BI2 Technologies' mobile MORIS (Mobile Offender
- Recognition and Information System) in 2012. New York City Police Department was the first, installed in Manhattan fall of 2010.
- At Schiphol Airport. Netherlands. Iris recognition has permitted passport-free immigration since 2001.
- Google uses iris scanners to control access to their datacenters.
- On May 10, 2011, Hoyos Group demonstrated a device called EyeLock using iris-recognition as an alternative to passwords to log people in to password-protected Web sites and applications, like Facebook or eBay.

### B. *Advantages*

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

- It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.
- The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.
- The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals have completely independent iris textures.

## VI. Security

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 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 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.

### A. 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.

### B. Keep Your 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.

### C. 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.

### D. 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.

### E. 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.

### F. Immediately Report Any Crime to the Police

Contact the Department Of Public Security or your local police station for more personal safety information.

## VII. 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.

## VIII. Advantages of ATM with an Eye

1) The entire process will takes time less than 2 seconds as 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.
2) 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. Iris scans are much more accurate than other high-tech ID systems available that scan voices, faces and fingerprints.
3) The iris is the best part of the eye to use as an identifier because there are no known diseases of the iris and eye surgery is not performed on the iris.
4) 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.

## IX. Disadvantages of ATM with an Eye

1) Iris scanners are significantly more expensive than some other forms of biometrics, password or proxy card security systems
2) Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera.
3) In Fingerprinting technique there is chances of replacement or injury. Scientists have identified 250 features unique to each person's iris -- compared with about 40 for fingerprints.

## X. 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.

## REFERENCES

[1] ATM With an Eye“Wikipedia”
[2] Report on “ATM with an Eye “.
[3] All, Anne. “Triple DES dare you.” ATM Marketplace.com.
[4] Bone, Mike, Wayman, Dr. James L., and Blackburn, Duane. “Evaluating Facial
[5] Penev, Penio S., and Atick, Joseph J. “Local Feature Analysis: A General Statistical
[6] Theory for Object Representation.” Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477-500,
[7] Wrolstad, Jay. “NCR to Deploy New Microsoft OS in ATMs.” CRMDailyDotCom. 29