ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# An ATM with Biometrics

**Murari Shyam B. Yadav**[1]
MCA
Mumbai University
Mumbai, India

**RameshKumar R. Tiwari**[2]
MCA
Mumbai University
Mumbai, India

***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.***

***Keywords: Biometrics; Overcoming Security issue of an ATM.***

## 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. IRIS DETECTION

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.


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.

## V. Facial Detection

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.)

## VI. Application

- 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 Eye Lock using iris-recognition as an alternative to passwords to log people in to password- protected Web sites and applications, like Facebook or eBay.

## VII. Advantages

- 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.
- 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.
- 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.
- 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.

## VIII. Disadvantages

- Iris scanners are significantly more expensive than some other forms of biometrics, password or proxy card security systems

 

- 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.

## IX. CONCLUSION

We thus develop an ATM model that is more reliable in providing security by using facial and eye 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. Merriam-Webster Dictionary Automatic Teller Machine.
2. www.ieee.org
3. "ATM:ad First For Comic Relief". creativematch. 2005- 03-10. Retrieved 2011-02-11.
4. "ATM bombings up 3000%".
5. Triton Systems | ATM manufacturer".
6. "NRT Technology Corporation - Gaming and casino solutions: QuickJack"
7. "The No. 1 ATM security concern"

## AUTHOR(S) PROFILE

**Murari Shyam B. Yadav,** Studding Master in Computer Application from Institute of Management and Computer Studies (IMCOST) Affiliated to Mumbai University in the period year 2012-15.

**Rameshkumar Rajmani Tiwari,** Studding Master in Computer Application from Institute of Management and Computer Studies (IMCOST) Affiliated to Mumbai University in the period year 2012-15.

 