RESEARCH ARTICLE OPEN ACCESS

Elimination of Unauthorized and Fraudulent Transactions of ATM Using Image Processing Techniques

R. Swaminathan
Dept of Computer Science, Urumu Dhanalakshmi College, Trichy –19, Tamil Nadu.

Abstract
Chip and Magnetic stripe are the types of technologies embedded on debit, credit and ATM cards in order to store the payment information. This paper mainly deals with the magnetic stripe technology and proposes techniques that can be used to eliminate unauthorized and fraudulent transactions of ATM, Automated Teller Machine. The techniques that this paper proposes such as Attaching a ThumbReader on an ATM to get an impression of the left-thumb from the person who has inserted his card into the slot to access the ATM, Adding the details of the impression of the left-thumb of an ATM card holder to the magnetic strip embedded on the card, and making the ATM capable of comparing the impression of the left-thumb scanned by ThumbReader attached on the ATM, with an impression embedded on the ATM-card using image processing techniques.
Keywords: CardReader,Fraudulent transaction, Magneticstripe, ThumbReader,Unauthorized transaction,

I. Introduction

The smart card [card with a chip] and its usage came into practice in the year 1968. But most banking organizations still rely on magnetic stripe card because of its low-cost production. That is why, this paper deals only with magnetic stripe technology.

Even though the scientific technology has reached a significant development, there is no sufficient tool in order to protect the money placed on the ATM from unauthorized and fraudulent transactions. There is a considerable difference between unauthorized and fraudulent transaction of ATM. Unauthorized access of ATM means that an ATM-card holder may give the card to the third party to withdraw the amount from the cardholder account through ATM. Even though this transaction is done with knowledge of the ATM-card holder, it is treated as an unauthorized transaction. Fraudulent transaction means that the transaction that is carried out without a proper ATM card and a proper permission from the ATM card holder, which means that a person withdraws amount from other's bank account with a duplicate card and without their knowledge. These two types of transaction can be fully removed if the banking organization follows the following proposals suggested by this paper.

- A ThumbReader needs to be attached on an ATM to get an impression of the left-thumb from the person who has inserted his card into the slot to access the ATM.
- The details of the impression of the left-thumb of an ATM card holder need to be added to the magnetic stripe embedded on the card.
- The ATM needs to be made capable of comparing the impression of the left-thumb scanned by the ThumbReader attached on the ATM, with an impression embedded on the ATM-card using image processing techniques.

II. Parts of an existing ATM-card [Debit card and Credit Card]

2.1 Magnetic stripe

The information printed on the front side of the card [Debit, Credit and ATM Cards] is human-readable.

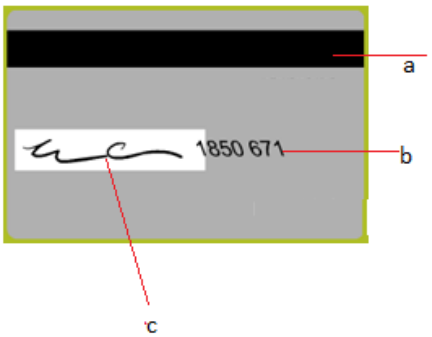

Fig 1: Back portion of the card
a) Magnetic Stripe b) Card Verification Value c) Signature Bar

On the other hand, the back side of the card contains both human-readable and machine-readable information. The information that is non-readable by human stored on a magnetic stripe. The magnetic stripe comprises three tracks in it. The storage limit of the first, second and the third track is 210 BPI density [Bytes per Inch], 75 BPI density and 210 BPI

density respectively. The general structure of a magnetic stripe is as follow

|----------|
Track 1 210 BPI density
|----------|
Track 2 75 BPI density
|----------|
Track 3 10 BPI density
|----------|

Only Track 1 and Track 2 are used by the payment industry. Track data is defined by international standards and is the same for all types of card

Track 1

|----------|
1 2 3 4
< = 19Digits ^ 2-26 characters ^ YYMM ^ 3 Digits
|----------|

- The first column represents the primary account number, known as the card number, which plays an important element in identifying a customer.
- The second column represents the name of the card holder. Like the card number, it is also embedded on the front as well as on the back side of the card.
- The third column represents the expiration date of the card and it is stored in the form of YYMM.
- The fourth column represents the service code.

Track 2

|----------|
1 2 3
< = 19Digits ^ YYMM ^ 3Digits
|----------|

It may be for the purpose of avoiding the creation of counterfeit card and fraudulent transactions, the information stored on column 1, column 3 and column 4 of track 1 are repeated in the column 1 and column 2 and column 3 of track 2.

Track 3

|----------|

|----------|

- The track 3 of the existing magnetic stripe does not have any data within it.

2.2 Card verification value

This is a unique number, which is to be used whenever the card needs to be used to make purchases over the Internet.

2.3 Signature bar

A customer has to sign on the bar as soon as the card is received to protect it against fraud.

III. Magnetic stripe of the proposed card

In addition to the information of the existing magnetic stripe, the proposed magnetic stripe contains the impression of the left thumb of the card-holder, which means that the proposed card contains three tracks of which the first two tracks follow the methodology used by the existing card and the third track follows the structure given below.

Track 3

|----------|
1 2 3
|----------|

The track 3 of magnetic stripe of the proposed card contains three columns all of which comprise the details of the left thumb of the card holder. In order to avoid fraudulent transactions these three columns contain the same details.

IV. Parts of the proposed ATM

Fig : ATM with a ThumbReader

4.1 CardReader

The following steps to be followed by the CardReader

- Read the information stored on the magnetic stripe embedded on the ATM card.
- Pass the details stored on the track 3 to the ThumbReader to compare the thumb impression.
- Get the information from the ThumbReader.
- Disallow the user to do the further transaction if the information passed by the ThumbReader contains ‘invalid’.
- Allow the user to do the further transaction if the information passed by the ThumbReader contains ‘valid’.

4.2 ThumbReader

The Thumb Reader performs three operations which include the following

- Gets an impression of the left-thumb of the ATM user.
- Determines whether the pattern of ridges and valleys of the impression obtained by itself matches the pattern of ridges and valley in the image captured by the CardReader.
- Passes 'valid' to the CardReader if there is no contradiction between the image captured by CardReader and the image captured by ThumbReader.
- Passes 'invalid' to the CardReader if there is any contradiction between the image captured by CardReader and the image captured by ThumbReader.

Every fingerprint has some unique characteristics, which need to be filtered and converted into an encrypted biometric or a mathematical representation.

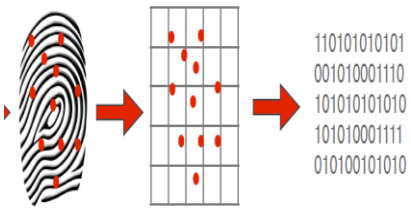

Fig: Mathematical representation of a thumb finger

V. Operations of the proposed ATM

Pseudo-code

Input Card and left-thumb finger
Process
If Expiration date of the card<= current date
and
left-thumb finger = Details of left-thumb finger stored on the magnetic stripe **then**
Allow to enter 'pin-number'
if pin-number = 'valid' **then**
Allow *'transactions'*
Else
Not allow *' transactions'*
End if
Else
Not accept 'pin-number'
End if

VI. Conclusion

Banking Organizations follow magnetic stripe technology rather than Chip based card.
Nowadays a lot of fraudulent ATM transactions take place because it is easy to duplicate a magnetic stripe card. There are two ways to eliminate such type of transactions. The one way is to switch over to smart card. The other way is to make some advancement on the existing magnetic stripe card. The paper describes an advancement that can be implemented on the existing magnetic stripe card. This advancement would be very useful not only in reducing but also in eliminating the unauthorized and fraudulent transactions of ATM.

References

[1] Identifying the quality of tomatoes in images processing using matlab, R.Kalaivani, Dr.S. Muruganand, Dr.Azha.Periasamy, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 8, August 2013.

[2] Image mining of textual images using low-level image features, prof. Mrs. Sushma andgaonkar, Mr. Rahul Jagtap, Mr. Pramod Anarase, Mr. Balaji Khadake, Mr. Akshay Betale, IEEE,2010.

[3] Efficient Image Mining using feature content based image retrieval system, Rajshree Dubey, Rajnish Choubey, Sanjeev Dubey, International journal of Advanced computer engineering and architecture, vol 1, no1, june 2011.

[4] Image clustering and retrieval using image mining techniques, A. Kannan, Dr.V.Mohan, Dr. N. Anbazhagan, IEEE,2010.

[5] An efficient technique using text & content base image mining technique for image retrieval, Mahip M. Bartere, Dr. Prashant, R.Deshmukh, IJERA, 2012.