A Proposed Framework to Prevent Financial Fraud through ATM Card Cloning

Divya Singh, Pratima Kushwaha, Priyanka Choubey, Abhishek Vaish*, and Utkarsh Goel, **Member, IAENG*

***Abstract*—This paper gives the intersection between the cash cards standards followed in the banks and the financial frauds done by the cash card cloning. It undertakes two primary tasks; namely understanding of the traditional standard cash card provided by the banks and a proposed methodology to make them more secure to reduce the cash card frauds. The methodology uses the watermarking procedure to embed the thumb impression in the magnetic stripe of the cash card which plays a prominent role to authenticate the user. This authentication mechanism is useful while transaction to secure cash card from being cloned via skimming device. This paper provides a generalized solution for financial fraud by the cash card cloning that is being done in the field of E-banking.**

***Index Terms*— Credit card cloning, Digital watermarking, Hash mechanism, Skimming**

I. Introduction

In present scenario Internet is playing very essential role in the online business. The transaction of data is the wheel of internet services. Today E-commerce application is widely used in E-business and various kinds of service industry where all kind of transaction of data is made possible through internet. It is one of the best, cheapest and convenient processes for online business. Privacy and security is the basic concern in this kind of transaction. Privacy is handled by Cryptography but for security we have to apply techniques which are necessary to secure our transaction and the digitized data present in these transactions. Our approach is to enhance information security in the field of E-commerce, E-banking, ATM Security and Credit Card Security through a combined approach of steganography and digital water marking.

Transaction involve among banking institutions offering financial transaction services, Logistics companies offering various kind of transportation services. These transactions contain sensitive information in the form of data so there must be a technique which is applied on these financial transactions. So our basic requirement is to achieve these basic goals of information security:

A. *Privacy*: Information must be kept secret from unauthorized parties.
B. *Integrity*: Assurance that received data not contains any kind of modification, insertion, deletion or replay.
C. *Authentication*: The assurance that the communication entity is the one that is claimed to be.
D. *Non-repudiation*: Sender and receiver prove their identities to each other.
E. *Access control*: This service controls that have access to a resource and under what condition access can occurs.

The frequent use of plastic cash card is the most sensitive and vulnerable part of transaction system. It leads to the violation of all the above security issues and attracts skimmers. But the most important and prominent part is that when the costumer access the ATM machine for transaction.

II. Literature Review

The traditional financial services outlet like automated teller machine, ATM cards, credit card etc becomes a very vulnerable target for exploiting the user ownership and user account as they only rely on the magnetic stripe. Many criminals are operating cash machine frauds in all over the world. One of the most common modes to execute the cash point fraud is a very small tricky device known as skimmers which simply clone the magnetic stripe of the cash card and enable them to get money. As a forensics analyst, one of the prevalence scams in the recent years is placing the card reader in the ATM machine. The idea is simple you put a shell over the ATM card reader so that it looks like a legitimate part of that device. Victims come up and place their credit cards and ATM card into this, enter their code and withdraw money and get their card back but they don't realize that in between their transactions is an illegal device that reads every single piece of data in the card and records it. The skimming device which they fix onto the card reader slot works into two ways-the skimmer is able to read the magnetic stripe the card and the hidden pinhole camera

Manuscript received March 23, 2011; revised April 14, 2011.This work was supported in part by the Indian Institute of Information Technology, Allahabad under Sec .3 of UGC Act, 1956.The paper title is A Proposed Framework to Prevent Financial Fraud through ATM Card Cloning.

Divya Singh is student of Master of Science in Cyber Law & Information Security in Indian Institute of Information Technology, Allahabad, India (phone: 9369155839; e-mail: divi107.singh@gmail.com).

Pratima Kushwaha is student of Master of Science in Cyber Law & Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: kushwaha.pratima@gmail.com).

Priyanka Choubey is student of Master of Science in Cyber Law & Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: priyanka.online85@gmail.com).

Dr.Abhishek Vaish is Assistant Professor in the Dept. of Master of Science in Cyber Law & Information Security in Indian Institute of Information Technology, Allahabad, India.He is a regular member and reviewer at ISACA,USA and also an active member of IEEE & Springer.His research interests are Information Security Management System,Computer Forensics ,Risk Assessment and Control Implementation.(e-mail: abhishek@iiita.ac.in).

Utkarsh Goel is Lecturer in Indian Institute of Information Technology, Allahabad, India (e-mail: utkarsh@iiita.ac.in).

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

which clearly captures the PIN number related to it. The victim came to use the cash point as they didn't any malfunctioning ensured that the machine is perfectly safe. As they do the transactions, Skimmers reads the card magnetic stripe and the camera captures the PIN. In this way a set of card details pack is ready. Essentially the next step after getting all details of the card from the card reader is downloading all the information into the machine or laptop. All other thing that is needed is cheap magnetic stripe card. The skimmer connected the cheap card reader into their laptops and reading the magnetic stripe card and swipes them once and again and programmed them according to the legitimate card details. Then they went to any ATM card machine, insert that cheap magnetic card in the machine and withdraw cash.

Magnetic stripe card standards [1]-

- Also called as magstripe, is read by physical contact and swapping past a reading head.
- 3 tracks on magnetic stripe-each track is $1/10^{th}$ of an inch.

Table I
TRACK DIVISION IN ATM CARDS

Created by airline industry (IATA)	Created by banking industry (ABA)	Created by thrift saving industry

ISO/IEC standard 7811, used by banks specifies

Table II
SIZE & VALUE OF TRACKS

Track 1	210 bits/inch	79	6-bit+parity bit(read only characters)	Numeric value
Track 2	75 bits/inch	40	4-bit + parity bit characters	Alphanumeric user information
Track 3	210 bits/inch	107	4-bit + parity bit character	VISA

Digital watermarking-The term "Digital watermarking" explains about the procedure of embedding information into a digital stuff in such a manner that it is unrecognizable to a human observer but can be easily detected by an apt computer algorithm as explained in fig 1.

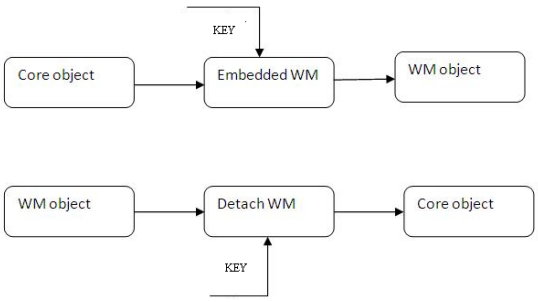

Fig. 1: Digital Watermarking

Application area of digital watermarking [5]

Copyright protection– The digital watermarking is primarily applicable in the area of copyright protection or intellectual property rights protection to prevent the unauthorized copying of the digital media. The digital media may be audio, video or picture. It is the process of embedding information into digital material in such a way that it is unrecognizable in nature.

Annotation Watermarking– Another application of watermarking is Annotation of digital photographs or the images. Using this some extra descriptive data can be added in the digital document. In annotation watermarking embedding of hierarchical data related to objects into user-selected areas on an image can also be done.

Multimedia authentication– There are many use of watermarking but most of them revolve around protecting the multimedia devices so that one can easily prove that given digital file belongs to him. Now a day's basically multimedia authentication is used in three areas of audio, video and still images for differentiating between real and the fake one.

Source Tracing– One of the application of watermarking is source tracing. Mainly it is used for trace the source of distribution. In source tracing, watermark is embedded into a digital signal at every point of distribution. If it is found that the work is copied, then the source of the distribution is finding out by retrieving the watermark from the copied work and can easily detect the source of illegally copied movies or other documents.

Cases related to credit card fraud-

In March, 2009 Washington D.C. restaurants arrested for supposedly using covert skimming devices to clone customer credit card information. [6]

According to a report from Reuters and authorities in Spain, Police have arrested 178 people in Europe and the United States suspected of cloning credit and debit cards in an international sting worth over 20 million euro. [7]

22-year old computer science student from Mangalore was arrested by crime branch official on March 22, 2010, for using fake credit cards. He made transactions worth Rs 10 lakh in six months. [7]

April 19, 2010, an MBA graduate named Fiyaaz Ahmed was seized in Gurgaon for cloning cards. He had stolen data from 35 cards and did shopping worth Rs 3 crore. [8]

ICICI Bank lost more than Rs 11 crore due to over 8,000 cases of credit card frauds. [9]

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

In Chennai, 4 people has arrested by the Cyber Crime ell for using 160 fake international credit cards and withdrawing money from ATMs. [10]
So, after review of these cases we found that there are some vulnerabilities present in our current E-transaction system which tends to breach of confidentiality and integrity in the financial transaction system. So here our approach is to prevent these basic goals of security through the proposed framework.

III. Methodology

An ATM card contains the information of customer name, 16-digit account number, and the month when card expires in the front of the card. And on the back of the card the magnetic stripe is present which holds the information about card and the signature of a customer. There is also a four-digit number that represents the last four digits of account number and a three-digit number representing Card Security Code.
The magnetic stripe in the ATM card is used to hide the confidential data of the user. By compromising this data any person can easily access the account of the user. The machine will easily identify the account holder status by the ATM card magnetic stripe. When card user swipe the magnetic card in the machine, the machine will decoded by the infrared rays, and some extra security are in the credit card such as signature panel, embossed, verification numbers etc.
Our approach is to add a new feature that will facilitate a detection mechanism for thumb prints. This requires addition of thumb print detection device on the ATM machine. Each customer having their account in the respective branch will have to submit the impression of their thumb while applying for ATM card. The ATM card will now contain new information, i.e. the thumb impression of the customer. Also the ATM machine should have a thumb impression detection mechanism installed in it.
Now the newly facilitated ATM card should be unique for each and every customer. The uniqueness of card will represent the originality of the card. For maintaining the originality, the personal details embedded on the magnetic tape of the card should be hashed via any hash generating algorithm. In this paper, we propose a new ATM card model, by embedding the watermark to prevent it from the cloning frauds. The following steps incorporate the functionality of our approach and explained in fig 2.

1. Firstly the personal details have to be hashed by using a secure hash algorithm. Let this hashed value be X.(fig 2.a)
2. Now the thumb impression of the customer, which is stored in the bank database, has to be hashed by using same hashing algorithm. Let this hashed value be Y. (fig 2.b)
3. Then generate a new hash value by combining both X & Y. Let this recently generated hash value be P. (fig 2.c)
4. This value “P” should be embedded on the magnetic stripe of the ATM card and this “P” is act as a digital watermark for the ATM card.(fig 2.d)

NOTE: [The value Y which is created by hashing the thumb impression is for maintaining the originality of the ATM card and uniqueness of the customer.]

Step1.

Fig. 2.a: Hash value of personal details

Step2.

Fig. 2.b: Hash value of Thumb impression

Step3.

Fig. 2.c: Hash value of combined X & Y

Step4.

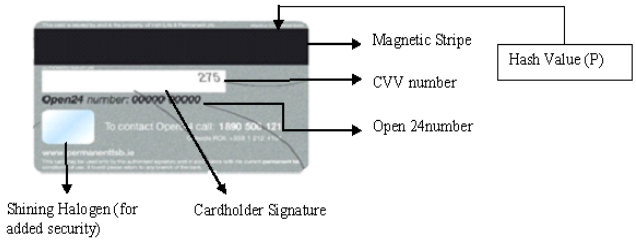

Fig. 2.d: Embedding the Hash Value of combined function (P)

Each time a new ATM card is created, the respective hash value generated for the thumb impression should be unique.
NOTE: [This is because, in case if the details of the card are skimmed and if the thumb impression is somehow replicated, the criminal may embed this stolen details in a new card and can try to use that card as well as the replica of the thumb impression can be applied to the detection device. But, while embedding the “P” value, which is a watermark, the details on the new card will generate a new hash value for “P”. This new value P won`t match with respect to the thumb impression applied.
It is because, for each thumb impression stored in the bank database will have its respective customer details stored in that database. So, when the user attempts to insert card and apply thumb print on the device, both of these information is cross-checked with the database. The flowchart of the proposed methodology is defined in fig 3.

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

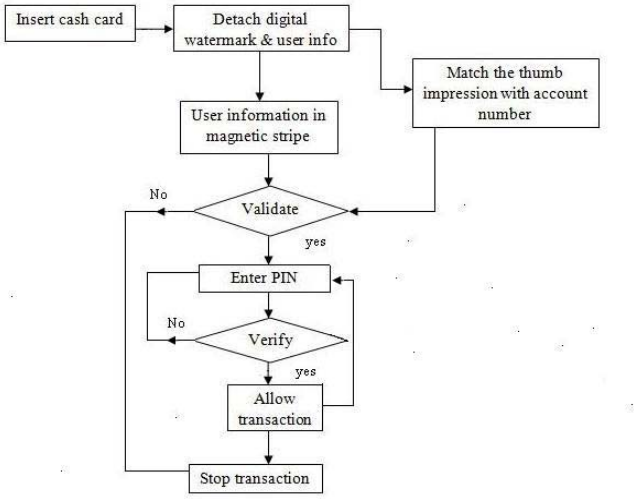

Fig. 3: Flowchart of Proposed methodology

IV. Conclusion

This paper proposed an ATM card identification system using digital watermarking technique and steganography in which watermark is generated by using a hash function of the thumb impression and the credentials of the customer. This watermark is embedded into the magnetic stripe of the ATM card keeping the watermark unperceivable. Ownership is proved by matching the hash code of each corresponding entry of thumb impression taken at the time of transaction with that of hash code embedded on the ATM card. This proposed system is suitable for several practical applications which are used in financial transactions for authentication of user identity and prevention from ATM card fraud.

Acknowledgment

We would like to thank our guide for motivating us to accomplish this paper. Without his help and support we can't complete our research work successfully. This work is also supported by the Indian Institute of Information Technology-Allahabad (A university Established under Sec.3 of UGC Act) and the Key Laboratory of Information Security and Computer Forensics.

References

[1] Hong Guo,Bo jin, *Forensics analysis of skimming device for credit fraud detection.*
[2] Yun Yang, Jia Me, *ATM terminal design is based on fingerprint recognition*
[3] William Stalling, *Cryptography and Networks Security.*
[4] Ingemar J. Cox, Mathew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton kalker, *Digital Watermarking and Steganography.*
[5] *DigitalWatermarking*, [Online] Available: http://en.wikipedia.org/wiki/Digital_watermarking
[6] *Credit card cloning*, [Online] Available: http://www.wired.com/threatlevel/2009/03/washington
[7] *Kerberos Security*, [Online] Available: http://krebsonsecurity.com/2010/06/police-arrest-178-in-u-s-europe- raid-on-credit-cards-cloning-labs/
[8] *Credit Card Theft*, [Online] Available: http://creditcardsnewsindia.blogspot.com/2010/05/money-stolen-by-cloning-credit-cards.html
[9] *Credit Card Fraud*, [Online] Available: http://www.business-standard.com/india/news/icici-bank-faces-most-credit-card-fraud-cases/349344/
[10] *Monetary transaction*, [Online] Available: http://www.moneycontrol.com/news/business/one-swipe-is-all-it-takes_215327.html
[11] Efren Bollain-y-Goytia, Mariko Nakano-Miyatake and Hector Perez Meana, *Authentication of identification card using watermarking.*
[12] Yanqun Zhang, China University of mining & technology, Digital Watermarking Technology:A Review
[13] Mukesh Chandra ,Shikha Pandey ,Rama Chaudhary ,Digital Watermarking Technique for Protecting Digital Images