Steganographic And Visual Cryptographic Approach For Authentication Of Bank Users Using ATM Cards

Rama Moorthy H , CSE Dept., MIT Manipal, India

Krishnaraj Rao N S, CSE Dept, SIT- Mangalore

Prasanna Kumar HR, CSE Dept, NMAMIT Nitte, India.

ABSTRACT

The major issue in banking is the authenticity of the customer and most systems today rely on static passwords to verify the user's identity. However, such passwords come with major security concerns. Users always try to use, easy and guessable passwords, try to use same password for one or more accounts, or some will write down their password, etc. There are more types to steal these passwords by a hacker, they will be using many techniques, such as peeping i.e., shoulder surfing, snooping, sniffing, etc. Also the PIN validation is done at later stages of ATM transaction. The Steganographic and visual Cryptography technique approach on image processing with the help of Mobile Phones is used to authenticate customer. The technique of embedding information of a customer, obtaining a Hash Value, subjecting it to a image, and then generating shares of that particular image is used. When generated shares are created, one is stored in the Bank database and the other is kept by the customer. The customer has to provide the share during all the transactions. This share is stacked with the first share for the process of authentication. The Hash value, of the information stored in image, is considered to decide the authenticity of the customer in the banks, the Hash value of the embedded information and the Current time, of say a transaction in a ATM machine, is considered as input for second round of Hash function, the output obtained is considered as Dynamic Random Key for ATM transactions. So this Method is unique in obtaining a solution for Authentication of a customer for Bank as well as for ATM transactions.

1. INTRODUCTION

General Overview of Steganography: Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word *steganography* is of Greek origin and means "concealed writing" from the Greek words *steganos* meaning "covered or protected", and *graphei* meaning "writing".[14].

There are different techniques involved in Steganography, which can be generally classified into:

Physical: Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include:[14]

- Hidden messages within wax tablets — in ancient Greece, people wrote messages on the wood, then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body — also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
- In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters otherwise. Because of this, a message could be hidden using 2 (or more) different typefaces, such as normal or italic, on a page of type.

Digital : Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems. Development following that was slow, but has since taken off, going by the number of "stego" programs available:

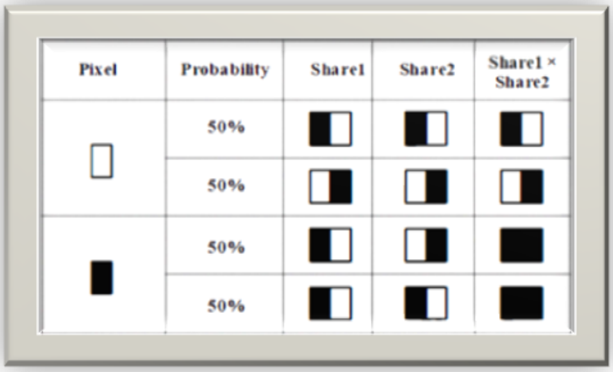
- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data or within random data. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates ciphertext that look perfectly random if one does not have the private key).

- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack.

Thus there are several techniques used in steganography methods out of which these two are generally used more in recent times.

General Overview of Visual Cryptography: The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

The rapid advancement of network technology, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps, space images taken using satellite and commercial identifications are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography scheme [1] eliminates complex computation problem in decryption process. Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are applied. In these situations the human visual system is one of the most convenient and reliable tools to do checking and secret recovery. Visual cryptography (VC), proposed by Naor and Sharnir [1], is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme, which is shown in figure 1.1 below, each secret image is divided into two shares such that no information can be reconstructed from any single share.



Pixel	Probability	Share1	Share2	Share1 × Share2
□	50%	◧	◧	◧
	50%	◨	◨	◨
■	50%	◧	◨	■
	50%	◧	◧	■

Fig 1.1 : A (2,2) Visual Cryptography Scheme

General Overview of Cryptographic Hash Function: A cryptographic hash function is a hash function[12], that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value, which is illustrated in figure 1.2. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

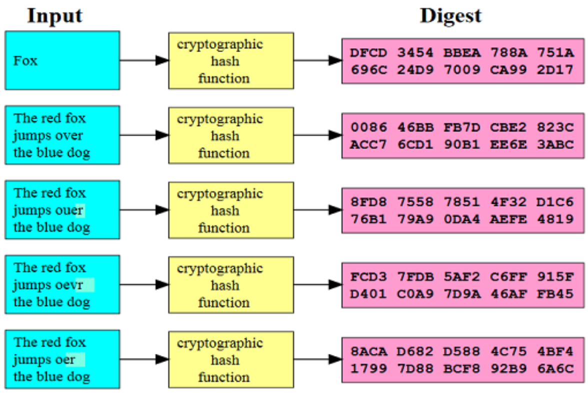

Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Fig 1.2: A cryptographic hash function

In this paper, the Hash value, of the information stored in image, is considered to decide the authenticity of the customer in the banks, the Hash value of the embedded information and the Current time, of say a transaction in a ATM machine, is considered as input for second round of Hash function, the output obtained is considered as Dynamic Random Key for ATM transactions. So this Method is unique in obtaining a solution for Authentication of a customer for Bank as well as for ATM transactions.

2 EXISTING SYSTEM:

Smart cards can provide identification, authentication, data storage and application processing. Smart cards may provide strong security authentication for single sign-on (SSO) within large organizations. Three universally recognized authentication factors exist today: what you know (e.g. passwords), what you have (e.g. ATM card or tokens), and what you are (e.g. biometrics).

Two factor authentication [15] is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. Withdrawing money from an ATM machine utilizes two factor authentication; the user must possess the ATM card, i.e. what you have, and must know a unique personal identification number (PIN), i.e. what you know.

Figure 2.1: Credit card with smart-card capabilities

The 3-by-5-mm chip embedded in the card is shown in figure 2.1 Smart cards combine low cost and portability with the power to compute cryptographic algorithms.

Banks gives ATM Card as a Token to its user. The ATM card along with the PIN, which is a static one, is said to do the authentication of a user in ATM machines. Considering some simple factors, will see the working of ATM in a brief.

The following components are involved in an ATM transaction:[5], shown as in figure 2.2.

- The ATM machine. This is the machine where you insert your card, punch your pin and take out the cash.
- The ATM server. This is the server that the ATM machine connects to behind the scenes. Your ATM card number and the pin are sent to this server encrypted using a shared secret between the ATM machine and the ATM server. The ATM server verifies the PIN using a separate ATM PIN machine and does the transaction by sending the request to your bank.
- The ATM PIN machine. This is the machine that the ATM server uses to verify your PIN.
- Your bank. Which actually performs the transaction.

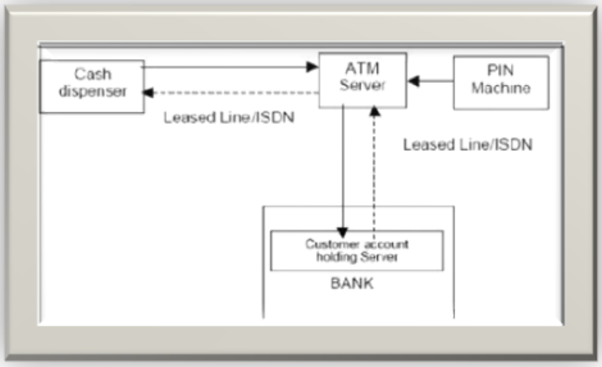


Fig 2.2: Components of ATM PIN Generation and Validation process

PIN generation process: The ATM Pin is never stored in any of the systems. Instead what is stored in the system is an offset of the pin. This is how it is done in very simple form.

First time PIN generation:

- Imagine your card number is 4129123456784321.
- There is a cryptographic function f and a key k so that f(4129123456784321, k) = 9876543212345678
- The function f and key k are known to the ATM PIN machine.
- The ATM PIN machine chooses a random pin, lets say 1234.
- Then the ATM PIN machine takes the first 4 characters of the encrypted number (9876), subtracts your chosen pin (1234), and stores the result (8642) in the ATM server. This is known as the pin offset.
- The ATM PIN machine prints 1234 into your pin mailer using an attached printer

3. RELATED WORK

There are many research and study going on this part of authentication of customers, we have considered two main research works of Chetana et al[3], of authentication using Visual cryptography and the second work of Fadi Aloul et al[4], of Two factor authentication. In which we found these observations, as per work specified.

A) In a core banking, many research work has been done by many researchers. According to research made by Chetana et al [3], A segment-based visual cryptography can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc., the VCS can be applied only for printed text or image. A recursive VC method is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. The proposed method by [3] for authenticating the bank customers scanning a image of the signature of the user from the application form and pre-processing to get a good intensity before it can be divided into shares, and to authenticate the decrypted image, which uses a correlation method. All of them increases the time complexity and also a tedious work to ensure the correctness of the image decrypted, and the signature can be forged if any of share generated is misplaced. Thus the proposed algorithm decreases time complexity as the shares are generated of the Hash value of the information to be hidden in the image of the Customer.

B) In ATM Transactions, Fadi Aloul et al[4], proposed the two factor authentication and one time password generation, which fetches the input from data base from the server, key is generated and then transmitted to the requested devices. The drawback is that the client machine/host has to request for password generation from server and then a PIN is generated and transmitted back. Eventually there will be delay during transmission and data fetching process from database, When in a busy schedule user may be uncomfortable waiting for the key to be delivered. Second drawback is that the ATM machine, Mobile phones, server etc, has to be in synchronized manner, for all the events to occur simultaneous. Third drawback is that, machine need to verify the key, so it has to again generate the same key or the key per transaction. Which has to be shared between the client, the machine and Server, which again is a tedious task. The proposed technique uses Steganography approach to generate a dynamic random key per transaction in more efficient and fast manner

4. METHODOLOGY

The Modules which is used to serve the Authentication of Bank customer is done in two phases.

1. Data Embedding phase
2. Authentication phase

DATA EMBEDDING PHASE: The "Data Embedding phase" uses career file, which is an image file, in which the information related to customer is embedded for embedding purpose. In the encryption phase the data is embedded into the image using "Least Significant Bit algorithm"(LSB) by which the least significant bits of the secret document are arranged with the bits of carrier file such as image, Such that the message bits will merge with the bits of carrier file. In this procedure LSB algorithm helps for securing the originality of image. The encryption pattern depends on the type of encryption we use. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image . In the proposed design, the following factors are chosen, and embedded:

• **Account Number:** This is a unique number generated by bank to each customers. The Account number constitutes of Type of account, Branch number, then the unique number for each account in that branch.

• **Customer Name:** Name of the customer holding that ATM card.

•**Address:** This field have the address of that particular customer.

• **Username:** Although no longer required because the dynamic key will be generated and used. This field is used as the first authentication level for Internet banking. Where the there are two level of authentication level. Thus this information is been used for the generation of Dynamic key in Internet banking.

• **Password:** This is password for the username of first level authentication. Usually it will be system generated and periodically updated or the user is reminded to change it as and when required.

•**Mobile Number:** The Mobile numbers of the customer is registered, verified and then stored in this field. If this field is altered then the message containing dynamic PIN may be misplaced and sent to other customer, however the later cannot do anything with that PIN as it is only for that particular transaction.

After the embedding process is done the data is subjected to MD5 hashing algorithm, where MD5 [13], Hash value is generated. Figure 4.1, illustrates the above.

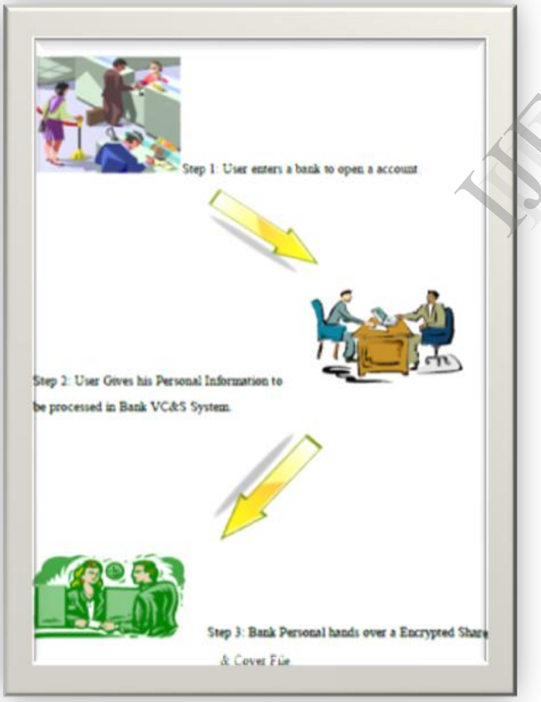

Step 1: User enters a bank to open a account
Step 2: User Gives his Personal Information to be processed in Bank VC&S System
Step 3: Bank Personal hands over a Encrypted Share & Cover File

Fig 4.1: Authentication Phase.

This value is subjected to generation of shares, as part of one time pad algorithm of Visual Cryptography Technique, is taken into account. Here the figure 4.2 is a image of the hash value generated by MD5 algorithm with the customers information as input. Later the One time Image algorithm of Visual cryptography technique is used to generate shares, figure 4.3 and 4.4. [11]. Assuming, the Encrypted Share and a Stego File is Handed over to the user, in a ATM card having a Memory chip.

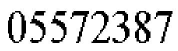


Fig4.2. Image of a hash value

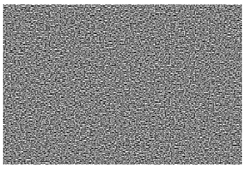


Fig 4.3 Share 1

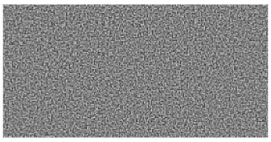


Fig 4.4: Share 2

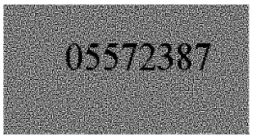


Fig 4.5: Stacked Shares

AUTHENTICATION PHASE: In the Authentication phase, user has to carry two image files along with general information stored.,

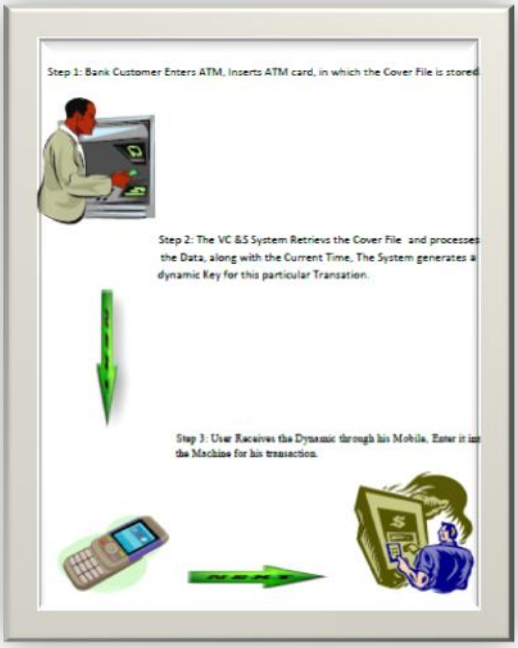
- Any one of the share generated, consider fig 4.4,

- A cover image, which is a image of passport sized photo of Bank customer in which the information stated in Embedding phase is hidden.

In any form, Consider a ATM card having a memory chip, consisting these two image files.

Now when you need the authentication of a customer in a core banking the Share image file stored in the chip of ATM is retrieved and Stacked with the particular share, which is stored in the bank's database. The decrypted Image, figure 4.5, shows the Hash value generated. Authentication is done by comparing the hash value in the image as well as the Hash value Calculated by the information retrieved by the Cover image file.

While authentication of a ATM transaction is considered, when a ATM card is inserted into a ATM machine, the ATM machine retrieves the Stego file stored in the memory chip, in which the Information is hidden, and the hash value is calculated along with current system time. Thus making the Key dynamic and one time per use. The generated Dynamic Key is thus sent to the Users Mobile phone via a text message, for simplicity only the last eight digit of the generated Hash value is considered as Dynamic Key. else it would be long process typing the full length hash value. If the key appropriate for the transaction, the user is allowed to transact further else the transaction is aborted. Figure below, fig 4.6., Illustrates the above explanation.



Step 1: Bank Customer Enters ATM, Inserts ATM card, in which the Cover File is stored

Step 2: The VC &S System Retrievs the Cover File and processes the Data, along with the Current Time, The System generates a dynamic Key for this particular Transation.

Step 3: User Receives the Dynamic through his Mobile, Enter it int the Machine for his transaction.

Fig 4.6: Authentication Process in a ATM Transaction.

Thus the authentication of user in both the Bank, considering Core Banking as well as the Dynamic Key concept to authenticate for ATM transaction.

5. RESULT ANALYSIS

To analyse the result of the current work, first lets go through with the study of previous work, In Chetana et al [3] , the image of signature is scanned from the application(figure 5.1(a)) and later it is given to pre processing(figure 5.1(b)), where the intensity of image is increased, and later that is subjected to generation of shares(figure 5.1(c)). To authenticate, the shares are stacked(figure 5.1(d)). The process is given in figure below.

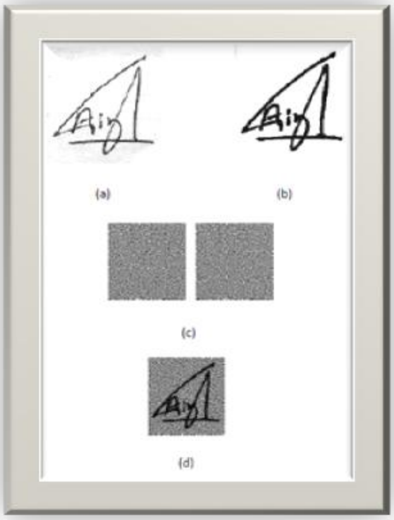


Figure 5.1: Shares Generated from previous work.

Where as in this work, Image is generated instantly after data embedding process, and is subjected to Generation of shares, following figure 5.2, depicts the comparison.

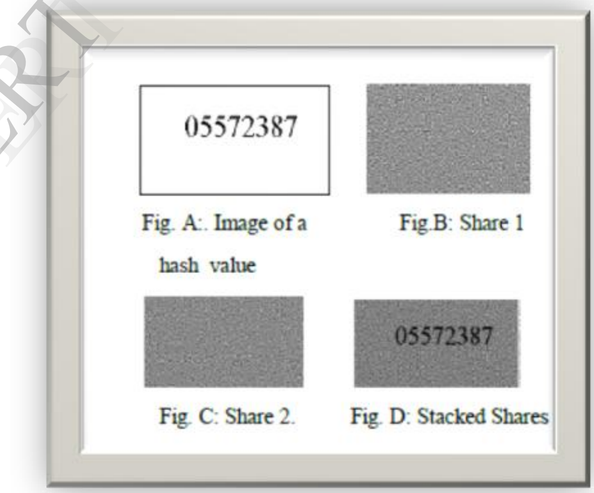


Fig. A:. Image of a hash value

Fig B: Share 1

Fig. C: Share 2.

Fig. D: Stacked Shares

Figure 5.2: Output for Comparison of Result.

In ATM Transactions, Fadi Aloul et al[4], proposed the two factor authentication and one time password generation, which fetches the input from data base from the server, key is generated and then transmitted to the requested devices. The Kay generated, is validated again in the server. So the key must be sent back to server for verification, and it is not said to have instant verification. In the later stages of transaction, the user is verified. Thus in this work, the key is said to be generated in that device, where the transaction is taking place, and only the Key is sent to the Mobile via SMS, to that particular registered number of the user, who is making transaction. Thus authentication is done at entry stage, in a more fast and efficient manner.

6. CONCLUSIONS & FUTURE SCOPE

Simple algorithms are considered for embedding, hashing, Visual Cryptography scheme, etc., as we want faster and efficient services. The image considered for the generation of shares is auto generated while the information is embedded into the Cover file. No need of scanning a particular image or something of that sort which was a tedious work in previous method. Generated Shares if revealed also to any third party, through hacking of database or stealing of the card, does not reveal any information regarding the customer has only a hash value is stored, particular system is considered to authenticate a user only in a bank. The PIN generated with the help of a image and the data hidden, will be sent to the registered Mobile Number of that particular customer as a message only. As to this method, the PIN generated is from ATM machine itself, therefore no need to wait to ATM server to validate the PIN entered. Thus we can achieve Dynamic Key and validation is done at entry level rather than later stages of the ATM transaction.

The process might also be considered for the Net banking facility to provide two level of authentication of the user. As of now the authentication is done by two level usernames and passwords.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography: EUROCRYFT'94, LNCS, vol. 950, pp. 1-12,1995.

[2] John Blesswin, Rema, Jenifer Josel " Recovering Secret Image in Visual Cryptography", Karunya University.

[3] Chetana Hegde, Manu S, P Deepa Shenoy , Venugopal K R , L M Patnaik " Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", *Defence Institute of Advanced Technology, Deemed University, Pune, India.*

[4] Fadi Aloul, Syed Zahidi, Wassim El-Hajj , " Two Factor Authentication Using Mobile Phones ", 2009.

[5] ATM operations. Available at: ´http://sidekick.windforwings.com/ 2008/02/how-are-atm-pins-validated.html"

[6] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik "*Authentication of Secret Information in Image Steganography".*

[7] A. Herzberg, "Payments and Banking with Mobile Personal Devices,"*Communications of the ACM*, 46(5), 53-58, May 2003.

[8] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth-Factor Authentication: Somebody You Know," *ACM CCS*, 168-78.2006.

[9] NBD Online Token. Available at *http://www.nbd.com/NBD/NBD_CDA/CDA_Web_pages/Internet_Banking/nbdonline_topbanner*

[10] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services,"*Communications of the ACM*, 47(8), 42-46, May 2004.

[11] Jeyamala C, GopiGanesh S, Raman G S, "An Image Encryption Scheme based on One Time Pads- A Chaotic Approach. ", 2010 Second International conference on Computing, Communication and network Technologies.

[12] Cryptographic Hash Function, Available at: https://en.wikipedia.org/wiki/Cryptographic_hash_function

[13] MD5 algorithm Available at http://en.wikipedia.org/wiki/MD5

[14] Steganography Available at http://en.wikipedia.org/wiki/Steganography

[15] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in *Inside Risks 178*, *Communications of the ACM*, 48(4)**,** April 2005.