JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-4 E-ISSN: 2347-2693

Implementation of Secure Bank Authentication using Visual Cryptography and Image Processing

B. Mehta [1*], T. Varshney[2], Y. Mandloi [3], J. Belel[4], V. Deshmukh[5]

[1*]Computer Engineering Dept, NMIMS University,India
[2]Computer Engineering Dept, NMIMS University,India
[3]Computer Engineering Dept, NMIMS University,India
[4]Computer Engineering Dept, NMIMS University,India
[5]Computer Engineering Dept, NMIMS University,India

*Corresponding Author: bhaumikmehta.nmims@gmail.com , Tel.: +91-7768086847

www.ijcseonline.org

Received: 19/Mar/2017, Revised: 04/Apr/2017, Accepted: 20/Apr/2017, Published: 30/Apr/2017

***Abstract*—**With the advent of e-commerce and electronic transactions the need for development of secured systems has grown tremendously. The need for security of information is especially affecting the banking sector. This paper implements an algorithm which proposes an efficient way for decreasing forgery during bank transactions using Visual Cryptography and Image Processing. Visual Cryptography is a generic cryptography technique which takes an image as input for encryption and makes use of human visual system rather than automated computing machines for decryption. Here we use a modified version of Visual Cryptography in which a combination of mechanical process and computation process is used for decryption. Due to the ease of implementation, this technique can be implemented by the people with non-technical background. It encrypts the visual data by dividing it into shares and decrypts the data by stacking some or all shares. Image Processing is used to perform operations on the image. The technique used in this paper works on the signature of the account holder for authentication.

***Keywords*—**Visual Cryptography, Bank Security, Secret image sharing

I. Introduction

Security is ubiquitous. With the advent of e-commerce and electronic transactions the need for development of secured systems has grown tremendously. This has also increased venture of people in hacking sector, internet is becoming an insecure place for sharing valuable information. This is especially affecting the banking sector. It has not only increased the people's mistrust in online banking but has also led to some serious financial losses for both the bank and the client. So, in order to overcome security issues faced during electronic bank transactions we are implementing an efficient algorithm for Secured Bank Authentication by making use of Visual Cryptography and Image Processing only. Our main aim is to hide sensitive and important information from malicious attacks. This can be done by making the information hidden from the outside world in a way that either it is not readable or completely invisible [1-9].

Cryptography is the art of concealing information in order to hide it from unintended users. The word Cryptography means "secret writing". It provides service of privacy and security. Cryptography is used to ensure that the contents of a message are confidentially transmitted; integrity of the message is maintained that is, it is not altered while transmission and that the message is sent and received by authenticated parties only.

Encryption is a process of converting information into a scrambled form so that it is unreadable. The desired message to be encrypted and transmitted over insecure channel is known as plaintext and the resultant message produced after the encryption algorithm is applied to the original message is known cipher text. Cipher text is usually scrambled text, in an incomprehensible form. Encryption is performed using a key which converts the plain text to cipher text. It also helps in decoding the message. This key can either be the same for the sender and the receiver (called Symmetric Key Cryptography) or can be different for both (called Asymmetric Key Cryptography). Decryption is the process of decoding the original message from the encrypted message. The cipher text received is useless until the receiver knows the key.

In today's world, it is necessary to preserve information about nearly all aspect of our daily lives. In other words, Information is an asset whose value can be compared to no other asset and thus it needs utmost security from malicious attacks. This information can be in any format such as text, image, video etc. Thus we need a more sophisticated cryptography technique which can even encrypt information which is not in textual format. To satisfy the requirement of encrypting pictorial information, hence the concept of Visual Cryptography was introduced. It is advancement in the method of encrypting information that is in visual format like images. It accepts an image as input. This image is a secret image which has to be sent over an insecure channel. Encryption of the information is done by dividing the secret image into shares based on some parameter. The decryption of data present in distinct images can be obtained by stacking them, henceforth reducing the use of complex computational process. Image processing is a form of signal processing where the input is an image and the output is a modified image or a set of parameters of the image. It is done to alter the characteristics of the input image to convert it into desirable format on which Visual Cryptography functions can be applied.

This paper studies and implements an algorithm based on the concepts of image processing and improved version of Visual Cryptography to carry out secure bank transactions. The main aim is to authenticate the user before they carry out any transaction. This helps to eliminate forgery at the very first step.

II. Literature Survey

In order to gain full understanding about the concept, we have done a literature review on some relevant papers. The literature review is as follow.

[1] Moni Naor and Adi Shamir paper "Visual Cryptography"

Moni Naor and Adi Shamir in 1994 introduced the idea Visual Cryptography. This proposed encryption technique works on visual data (like pictures, text, etc.) in such a way that it reduces the use of computers to a great extent making it feasible and handy for non-technical personnel.

The main idea presented here is that- the secret image which is to be encrypted is chosen and converted into binary image so as to facilitate further processing of the image. This image is divided into shares. These shares are then distributed among various shareholders (in our case, bank account holders). This way the image is encrypted. To decrypt the image these shares are stacked together. It is possible to decrypt the image using human visual system only.

During the encryption process, the shares are generated in such a way that each image pixel is divided n into sub-pixels (one for each share) and each share has m black and white sub-pixels. This results into a formation of n x m Boolean Matrix S=[Sij] where sij=1 if the jth sub-pixel of the ith transparency is black. In this way, n shares are created in a k-out-of-n scheme[1].

For decryption, we overlap the shares in such a way that any k shares out of n shares are required to decrypt the image. If any k-1 shares are overlapped then the original would not be obtained image.

[2] Secure Bank Authentication using Visual Cryptography and Image Processing

This paper introduces a unique technique which makes use of both Visual Cryptography and Image Processing to perform encryption before a bank transaction is carried out. The main aim is to authenticate the account holder before any transaction is processed. It works on the principle of basic visual cryptography and uses different techniques of image processing to convert the image into a desirable format.

This algorithm commences with taking signature of the account holder as input. Then this image is converted into binary form as it reduces the computation complexity. This stage is called preprocessing. The next stage is of creating shares. The shares are distributed among all the account holders. The number of shares required to decrypt the original image depends upon the visual cryptography scheme used. One share produced is kept with the bank in the bank's database and others are distributed among the 'n' shareholders. Out of which k are needed to decrypt the original image using k out of n scheme. Any k-1 shares cannot decrypt the image. Here we have implemented this algorithm using 3 out of 3 schemes. This means all the 3 shares distributed are required for revealing the original image[2].

After all the shares are distributed, it is assumed that these shares are kept well protected and are not stolen. During any bank transaction, the account holders bring their copy of share. These are stacked together. The overlapping of the shares results in an image; this image is compared with the original image. In order to carry out the transaction, the two input and output image should be same. Using the Karl Pearson's correlation technique, the original image is matched with the resultant image. The correlation factor lies between 0 and 1; a higher correlation factor means that the image is authentic otherwise it is not.

In this way, forgery can be curbed at the very first step. For executing any bank transaction, all the account holders should be present and must hand their shares, this way transaction takes place with the confirmation from all the account holders. This technique is extremely useful in the case when large transactions are carried out.

The implementation of the above explained algorithm is shown in this paper.

[3] Visual Cryptography for Print and Scan Applications

Visual cryptography is not much in use in spite of possessing several advantages. The shares produced by of visual cryptography schemes are printed on transparencies which need to be superimposed in order to decrypt the original image. However, this superimposition is very difficult to achieve due to fine resolution of the image and noise produced during printing. To solve this issue, this paper introduces a method on how to remove alignment discrepancies.

One way to get precise alignment is to make a mark (cross) on the transparency and place it beside each share. This will help to overlap each share on that cross and provide more precise results. However, this mark could be confused with a mark made by the person who is not authorized to access that data and hence there remains vulnerability in the system.

In order to solve this issue, we make use of marks in the frequency domain. Discrete Walsh Transform is considered for this process, as it is useful for pulse signals and is distinct from the discrete Fourier transform(DFT), discrete cosine transform(DCT) and discrete wavelet transform(DWT).The marks are embedded in the high frequency coefficients of the transform[3].

While decrypting the original image, we take the shares and scan the image to extract the marks made during encryption by using Walsh Transformation. This results in an approximate alignment for super imposition of the shares.

[4] Bernd Borchert, "Segment-Based Visual Cryptography" WSI Press, Germany, 2007

This paper proposes a improved version of Visual Cryptography which is not pixel-based but segment-based. The suggested technique on segment-based Visual Cryptography can be used to convert information containing of symbols that can be displayed by a seven segment display. For example, messages comprising of only numbers can be encrypted by this segment-based Visual Cryptography using the seven segment display.

This can be used in banking applications also like when the message is the information describing a money transfer (including account number, bank number and money amount) during an online banking transaction[4]. So such message can be encrypted using this technique.

The advantage of the segment-based encryption is that it may be easier to overlap the secret images and that such symbols are potentially easier to recognize by the human eye, especially in a transparency-on-screen scenario[4]. Also less random bits are required which makes it simpler to implement. Furthermore, this technique is easier to understand by a non-technical person as well. The only disadvantage is that it cannot encrypt messages containing alphabets and special characters.

III. Concept of visual cryptography

The main idea of Visual Cryptography is to encrypt the information that is in pictorial form. A secret image which is to be encrypted is taken as input. This image is converted into a binary image. Individually they create noise but once stacked together they reveal the actual image. The transparency or the key is shared among n users out of which k users can see the image by stacking their transparencies but any k-1 users cannot.

Various Schemes for Visual Cryptography are explained below:-

(2,n) General Visual Cryptography Scheme

We take an image as an input, containing black and white pixels only. The image to be encrypted is separated into n shares out of which minimum of 2 shares are mandatory to decrypt the image. Each image pixel is divided into non-overlapping sub-pixels. The arrangement of white and black pixel is given by:-

$$\text{White pixel C0=}\begin{bmatrix} 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \end{bmatrix}$$

$$\text{Black pixel C1=}\begin{bmatrix} 1 & 0 & 0 & 0 & \dots\dots\dots & 0 \\ 0 & 1 & 0 & 0 & \dots\dots\dots & 0 \\ 0 & 0 & 1 & 0 & \dots\dots\dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots\dots\dots & 1 \end{bmatrix}$$

Few basic Schemes:

1. (2,2) Visual Cryptography Scheme -

The image is divided into 2 shares and to restore the original image, both of the shares are necessary. Each pixel is divided into 2 sub pixels. The first row describes the case for white pixel and the second row for black pixel. Note that, in case of black pixel the two sub-pixel have complementing values so that when performing the OR operation we get a full black pixel. The number of sub-pixels can also vary from 2 to 4[1].

$$C0=\left\{\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\right\}$$

$$C1=\left\{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$$

2. (2,3) Visual Cryptography Scheme -

Here, we divided the image into 3 shares and any 2 of them are required to decrypt the data. This output can be verified by the human eye itself.

3. (3,3) Visual Cryptography Scheme:

This is more secure when compared to the previous technique. Here, we require all the three shares to restore the original secret image, thus we require both of the account holders to be present at the time of transaction.

4. (k,n) Visual Cryptography Scheme -

The image is divided into n shares and any k of them are required to decrypt the data. Any k-1 shares will not be able to produce the desired results

IV. Methodology

The algorithm discussed as below: -

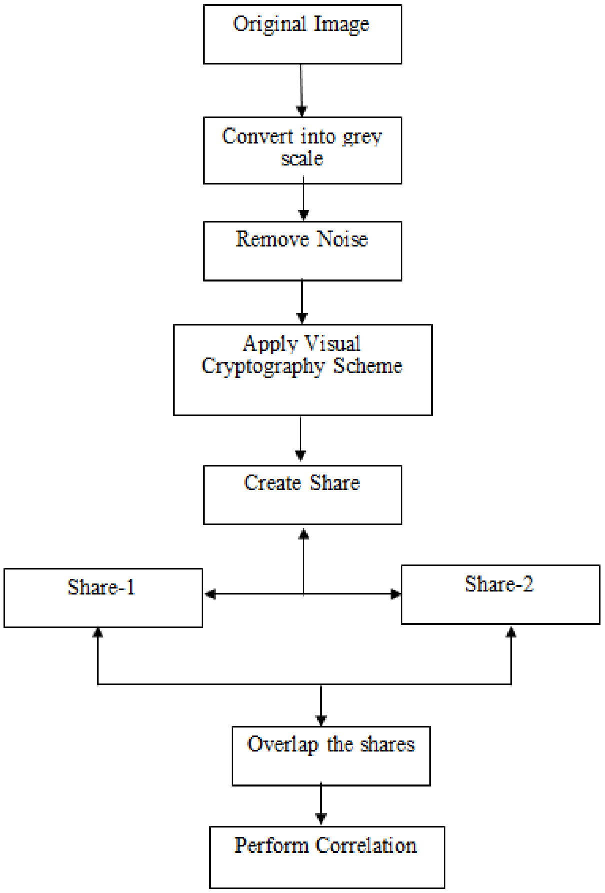

Figure 4.1

Image:

The signature of the account holder is taken as input image as it is one of the most secure way of verifying a person's identity.

Convert into grey scale:

The scanned image h(a,b) is first converted into grey scale image. It is a pre requisite that image is of high contrast that is, dark colour signature on light coloured background (White paper). To do this, we select a threshold value T, below which all the pixels are black and above which all are considered white.[2].

$$T(a,b) = \begin{cases} 1 & \text{if } h(a,b) \geq T \\ 0 & \text{if } h(a,b) < T \end{cases}$$

Remove Noise:

In order to facilitate further processing, it is important to remove noise. For this we use median filter.

Visual Cryptography scheme:

We have used 3 out of 3 visual cryptography scheme in this algorithm. This means that the shares will be distributed among 2 account holders and one is kept with bank. During decryption all these 3 shares are required to decrypt the original image.

Creating Shares:

The image obtained is a grey scale image which is noise free. Every pixel is divided into m parts, where m is the number of shares to be generated and each share consists of n pixels. This results into a formation of n x m Boolean Matrix S=[Sij] where sij=1 if the jth sub-pixel of the ith transparency is black[2].

Overlap the shares:

It is the process of decoding. To generate the original image, we have to stack or overlap all the generated shares, which are then checked by the bank officials. The number of shares required depends upon the visual cryptography scheme used. The grey level of the resultant image is proportional to the Hamming Weight H (V) of the ORed vector V.

Authentication Testing:

In order to authenticate the user we need to compare the output and the input images, this is done by using a Correlation technique. We use Karl Pearson's correlation technique where correlation coefficient reveals the dependency or independency between the variables[2].

V. RESULT

Input

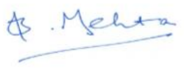

Figure 5.1

Processed Input

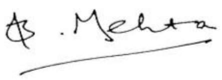

Figure 5.2

Generate_Share()

Step 1: Take image as the input and returns three values, 'share1', 'share2' and 'share3'

Step 2: Calculate the size (row, column) of the image and store in 's'.

Step 3: Declare three matrices, say, 'share1', 'share2' and 'share3' and initialize them with zeroes with the same dimensions as of the original image.

Step 4: Loop through every pixel and perform the steps 4-8.

Step 5: Initialize a random number between 0 to 255.

Step 6: Divide the product of the intensity of current pixel value and 255 by the generated random number and initialize it as the quotient.

Step 7: Floor down the value of quotient and store it in 'share1' for the current coordinates. This serves as the remainder.

Step 8: Calculate the difference between the quotient and the remainder, calculated in the previous steps. Find the product of this difference and the previously generated random number. Store it in 'share2' for the current coordinates.

Step 9: Store the value of the previously generated random number in 'share3' for the current coordinates.

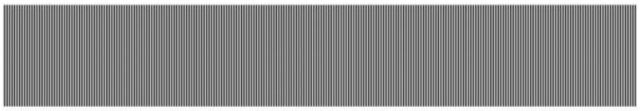

Figure 5.3.1 Share 1

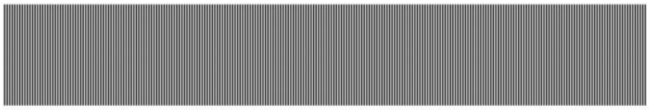

Figure 5.3.2 Share 2

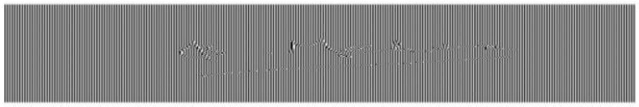

Figure 5.3.3 Share 3

Decrypt()

Step 1: Take share1, share2 and share3 as the inputs, returned by Generate_Share() and returns an image

Step 2: Calculate the size (row, column) of the image and store it in 's'.

Step 3: Declare a matrix 'output' and initialize it with zeroes, having the same dimensions as of the original image.

Step 4: Loop for every value in the matrix, and store the following. Find the product of the values, stored at the current coordinates of 'share3' and 'share1'. Add the product to the corresponding value in 'share2'. Divide this outcome with 255.

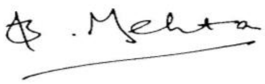

Figure 5.4

VI. CONCLUSION

We have developed an algorithm for the bank for carrying out secure transactions and for authentication of the user using the concept of Visual Cryptography and Image Processing. The main aim of this technique is to reduce the influence of automated machines and provide security of the same level. This technique can be used for reducing forgery in banking application to a great extent. Here, we take signature of the account holders as the identification and distribute the shares among the shareholders. The individual share cannot decrypt the original message. All the shares combined together can only decrypt the message, this way in banking application a transaction will only be carried out with the knowledge of the account holders. The assumption used in this technique is that the share once given to the account holder is not lost or not stolen. Also, that the account holders doesn't share their key with anyone else. There are various other fields also where we can use visual cryptography to maintain secrecy of data. This technique is also known as Secret sharing scheme. Moreover, for verifying that the obtained decrypted image is correct or not we use correlation factor. In some cases, human visual system is also enough for deciding whether the obtained image is right or not.

VII. FUTURE SCOPE

The above-mentioned algorithm works on black and white image only. This algorithm can be advanced by extending its coverage to coloured images.

ACKNOWLEDGMENT

We would like to take this opportunity to show my gratitude towards my mentor Mr. Varun Deshmukh whose constant motivation, patience and expertise has helped us to work enthusiastically throughout the course of our project. We would also like to show our sincere thanks and deepest gratitude towards Dr. N.S. Choubey, Head of Computer Engineering Department and and Dr. Aaquil Bunglowala, Associate Dean of MPSTME, Shirpur for providing all the necessary facilities and true encouraging environment to bring out the best of our endeavours.

REFERENCES

[1] M. Naor, A. Shamir, "*Visual Cryptography*", Advances in Cryptography-Eurocrypt, Springer, US, pp.1-12,1994.

[2] B. Srikanth, G. Padmaja, S. Khasim, P.V.S. Lakshmi, A. Haritha, "*Secured Bank Authentication using Image Processing and Visual Cryptography*", IJCSIT, Vol. 5, Issue.2, pp.1-6, 2014.

[3] W-Q. Yan, D. Jin, M. S. Kanakanahalli, "*Visual Cryptography for Print and Scan Applications*", ISCAS04, Canada, pp.572-575, 2004.

[4] Bernd Borchert, *"Segment-Based Visual Cryptography"* WSI Press, Germany, pp.1-320, 2007.

[5] C-C. Lin, W-H. Tsai, *"Visual cryptography for graylevel images by dithering techniques"*, Science Direct, Vol.24, Issue.3, pp.340-358, 2003.

[6] D. Chaudhary, R. Welekar, "*Secure Authentication Using Visual Cryptography"*, International Journal Of Computer Science and Applications, Vol. 8, No. 1, pp. 1-4, 2015.

[7] N. Anusha, P. SubbaRao, *"Visual Cryptography Schemes for Secret Image",* IJERT Vol. 1 Issue 5, pp. 1-9, 2012.

[8] H. Yan, Z. Gan and K. Chen, *"A Cheater Detectable Visual Cryptography Scheme",* Journal of Shanghai University, vol. 38, no.1, pp.107-110, 2004.

[9] Md. A. Mushtaque, "*Comparative Analysis on Different parameters of Encryption Algorithms for Information Security"* , International Journal of Computer Sciences and Engineering, Vol. 2, Issue. 4, pp.76-82, 2014.

Authors Profile

Mr. Bhaumik Mehta is currently pursuing the last year of his undergraduate degree in Bachelor of Technology in Computer Engineering from NMIMS University, India. He will complete his degree by May 2017. As a part of his B.Tech project he and his group mates have implemented this paper. He has also published a review paper on Visual Cryptography . His area of interest lie in area of Cryptography, Artificial Intelligene, Machine Learning, Data Science and Databases.

Ms. Tanyya Varshney is currently pursuing the last year of her undergraduate degree in Bachelor of Technology in Computer Engineering from NMIMS University, India. She will complete her degree by May 2017. As a part of her B.Tech project she and her group mates have implemented this paper. She has also published a review paper on Visual Cryptography. Her main area of interests are in Cryptography, Data Science, Data Mining and Databases.Mining.

Mr. Yash Mandloi is currently pursuing the last year of his undergraduate degree in Bachelor of Technology in Computer Engineering from NMIMS University, India. He will complete his degree by May 2017. As a part of his B.Tech project he and his group mates have implemented this paper. His main interests are in area of Cryptography, Networking and Data Structure and Algorithms.

Mr. Jagannath Belel is currently pursuing the last year of his undergraduate degree in Bachelor of Technology in Computer Engineering from NMIMS University, India. He will complete his degree by May 2017. As a part of his B.Tech project he and his group mates have implemented this paper. His main interests lie in field of Cryptography, Networking and System Security.

Mr. Varun Deshmukh is working as an assistant professor in Computer Engineering Department from NMIMS University, India. He has also published a review paper on Visual Cryptography. He has guided his fellow students to implement this paper. His main area of interests are in area of Computer network, Cryptography, application programming.