"A Novel Approach Of Secure Banking Application Using Visual Cryptography Against Fake Website Authenticity Theft"

Chandrasekhara.
Department of ISE,
East West Institute of Technology,
Bangalore.

Dr. Roopalakshmi. R
Department of ISE,
East West Institute of Technology,
Bangalore.

Abstract

The bank may provide two sets of services namely core banking and net banking. In a core banking system, there is a chance of encountering forged signature for transaction, and in net banking system, the password of the customer may be hacked and misused. With the advent of internet, various online attacks has been increased and among them the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. A computer that is connected to the Internet can be considered trustworthy secure or not. The question is how to handle the application that requires a high level of security, such as core banking and net banking. In core banking and net banking the major problem is the authenticity of the customer due to unavoidable hacking of the databases on the internet. To overcome this problem of authentication we are discussing with the two topics based on image processing i.e. steganography and visual cryptography.

***Key terms* – phishing, core banking, net banking, steganography, visual cryptography.**

I. Introduction

Web Banking has been popular among young Internet-savvy people for many years, its popularity is expected to grow rapidly as Internet usage grows internationally and people discover the many advantages that it provides. But it may have its own drawbacks. Due to unavoidable hacking of the databases on the internet. In a core banking system there is a chance of encountering forged signature for transaction. In a net banking system password of the customer may be hacked and misused. Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. One definition of phishing is given as "it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication". Here we will use some of the techniques to secure the customer information and to prevent the possible forgery of password hacking. The concept of image processing a steganography and visual cryptography is used. Steganography is the art and science of writing hidden messages in such a way that no one apart from intended recipient knows the existence of the message. Original message is being hidden with a carrier such that the changes so occurred in the carrier are not observable. In steganography digital images can be used as a carrier to hide images. Combining secret image with a carrier image gives the hidden image, the hidden image is difficult to detect without retrieval, and the most of the steganographic technique are either three or four adjacent pixels around a target pixel. Whereas the proposed technique is able to utilize at most of all eight adjacent neighbors so that imperceptibility value grows bigger and the dividing it into an shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created one is stored in the bank database and the other one is kept by the customer. The customer has to present the share during all of his transaction. This share is stacked with the first share to get the original image. Then decoding method is used to take the hidden password on acceptance or rejection of the output and authenticate the customer. The visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image.

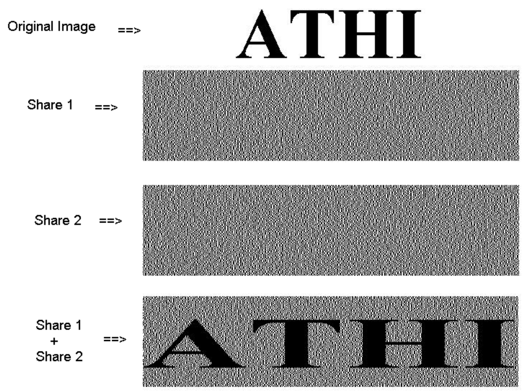


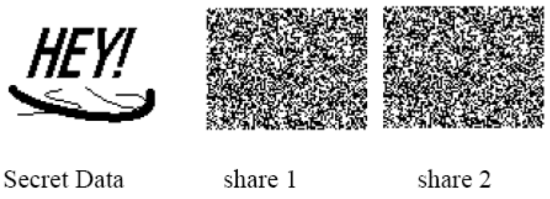
Figure1. Conceal a secret with two innocent-looking shares

The simple visual cryptography is given by the following steps. Secret image consist of a collection of black and white pixels where each pixel is treated independently to encode the secret image we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into n black and white sub pixels. To decode the image a subset s of those n shares are picked and copied on separate transparencies. If **S** is a qualified subset, then stacking all these transparencies will allow visual recovery of the secret.

II. Related Work

Visual cryptography, the most notable features of this approach is that it can be recovery secret image without any computation. It exploits human visual system to read the secret message from some overlapping shares, thus overcoming disadvantage of complex computation required in the cryptography. Naor and Shamir introduced a simple but perfectly secure way that allows secret sharing without any cryptography computation termed as a visual cryptographic scheme. The problem of encrypting written material (printed text, hand written notes, pictures etc) in a perfectly secure way which can be directly by the human visual system. The idea is to convert the written material into an image and encode this image into n shadow images. The decoding requires only selecting some subset of these n images, making transparencies of them and stacking them on top of each other.

1 Level 1 hiding using Visual Cryptography



2 Super Imposing Share1 and Share2 to Form the Original Secret Data

The original motivation was to safeguard cryptographic keys from loss. One of the best known techniques to protect the data is cryptography. it is a art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the messages. Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

1.(2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2.(2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3.(n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4.(k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold,, and n, the number of participants.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

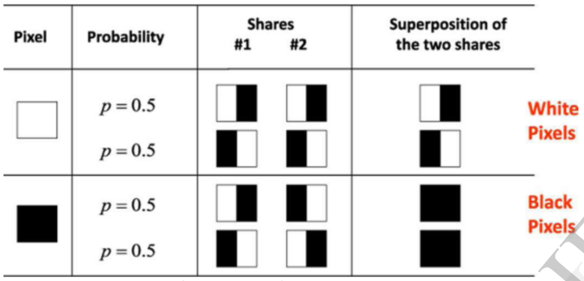


Fig. 1 Illustration of a 2-out-of-2 VCS scheme with 2 subpixel construction.

III. Adjustment Technique

Proposed technique considered two consecutive pixels as the one time input in the source image and as a result there shall be four cases in input. These are as follows:

(i) Black and Black, (ii) Black and White, (iii) White and Black, (iv) White and White

To develop a (2, n) visual cryptographic scheme two things are considered as major point of references these are:

(i) Hamming weight of every block in each share should be the same.

(ii) Hamming weight of a black block will be greater than the other blocks in the stacked shares.

Let N is the number of participants (i.e no. of account holders). m=integer part of (n/2), where n= number of total shares. The bank authority has to select the value of n, such that the relation nCm _ min{(N+1)} (where C represents the combination operation) holds.

Hamming weight of each block of each share (H) = Integer part of (nCm)/2; Now Let us consider the four possible cases of input pixels:

(i) Black and Black: In this case arrangement of black pixels in the output block will be different from other blocks. This ensures that after stacking the shares, Hamming weight of the stacked black blocks will become greater than the other blocks.

(ii) Black and White: Here the all the black pixels will be kept together from the first position of the output block.

(iii) White and Black: Where the all the black pixels will be kept together from the last position of the output block.

(iv) White and White: All black pixels will be kept together in the output block.

Now if the number of pixels in the input image is odd then the last pixel will be kept as it is in the shares.

Because the output media of visual cryptography are transparencies, we treat the white pixels of black-and- white images as transparent. Typically, the black-and-white visual cryptography decomposes every pixel in a secret image into 2×2 block in the two transparencies. According to the rules in fig1, when a pixel is white the method chooses one of the two combinations for white pixels in fig1. To form the content of the block in the two transparencies when a pixel is black it chooses one of the other two combinations. Then the characteristics of two stacked pixels are black and black is black, white and black is black, and white and white is white. Therefore , when stacking two transparencies, the blocks corresponding to black pixels in the secret images are full black, and those corresponding to white pixels are half-black and half-white which can be seen as 50% of grace pixels.

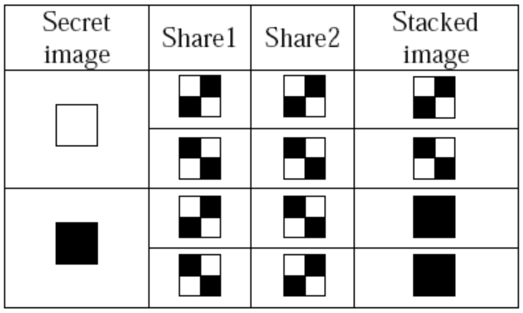


Fig. 1. Sharing and stacking scheme of black and white pixels.

Steganography is the process of hiding a secret message within an ordinary message and extracting it as its destination. Anyone else viewing the message will fail to know it contains hidden /encrypted data. Steganalysis it may identify the existence of the message and deals with the detection of hidden content. Steganalysis is used for identifying the existence of a hidden message, perhaps we can identify the tools used to hide it. If you identify the tool perhaps we can use that tool to extract original message. Steganalysis meets cryptanalysis as stated previously in steganography the goal is to hide message, not to encrypt it. Cryptography provides the means the encrypt the message.

IV.CONCLUSION

The project given the information about existing system steganography and visual cryptography. The project allows the authorized users to work the algorithm developed can be used depending on the situation and application. Undoubtedly visual cryptography provides one of the secure ways to transfer the image on the internet. The advantage of visual cryptography is that it exploits human eyes to decrypt with no computation required. In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution therefore optimum number of shares are required to the secrecy at the same time it also an important issue, hence research in visual cryptography is towards maintaining the contrast at the same time maintaining the security. Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using visual cryptography.

REFERENCES

[1] R. C. Gonzalez and R. E. Woods," Digital Image Processing" Upper Saddle River, NJ: Prentice-Hall, 2006.
[2] S.Premkumar and A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application".
[3] H. Wang and S. Wang, "Cyber warfare Steganography vs. Steganalysis," Commun. ACM, vol. 47, no. 10, pp. 76-82, 2004.
[4] X. Zhang and S. Wang, "Steganography using Multiplebase notational system and human Vision sensitivity," IEEE Signal Processing Letters, vol. 12, pp. 67-70, Jan. 2005.
[5] M. Shirali-Shahreza, "Steganography in MMS," in Multi topic Conference, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4.
[6] Aggelos Kiayias and Yona Raekow, "Efficient Steganography with Provable Security Guarantees"
[7] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An Overview Of Image Steganography"
[8] Chandramathi S, Ramesh Kumar R, Suresh R, and Harish S,"An overview of visual cryptography"
[9] Moni Naor, Adi Shamir," visual cryptography"
[10] Jithesh K , 2dr. A V Senthil Kumar, "Multi Layer Information Hiding -A Blend Of Steganography And Visual Cryptography,"
[11] Young-Chang Hou, "Visual cryptography for color images,"