RESEARCH ARTICLE OPEN ACCESS

Optimal Contrast Grayscale Visual Cryptography with Modified Multi-secret Sharing for Secure Application

S.Premkumar*, R.Swathiramya**

*AP/CSE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu.

**AP/CSE, Christ the King Engineering College, Coimbatore, Tamil Nadu.

ABSTRACT

Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hackingof the databases on the internet, it is always quite difficult totrust the information on the internet. To solve this problemof authentication, we are proposing an algorithm based onimage processing, improved steganography and visual cryptography.

This paper proposes a technique of encode the password of a customer by improved Steganography, most of the steganographic techniques use either three or four adjacent pixels around a target pixel whereas the proposed technique is able to utilize at most all eight adjacent neighbors so that imperceptibility value grows bigger.and thendividing it into shares. Total number of shares to be created isdepending on the scheme chosen by the bank. When two sharesare created, one is stored in the Bank database and the otheris kept by the customer. The customer has to present the shareduring all of his transactions. This share is stacked with the firstshare to get the original image. Then decoding method issued to take the hidden password on acceptance or rejection of the output and authenticates the customer.

Keywords: Digital Image steganography, visual cryptography**,** Gray Scale, Secret Sharing

I. INTRODUCTION

Today, most applications are only as secure as theirunderlying system. Since the design and technology of middleware has improved steadily, their detection is a difficultproblem. As a result, it is nearly impossible to be surewhether a computer that is connected to the internet canbe considered trustworthy and secure or not. The questionis how tohandle applications that require a high level ofsecurity, such as core banking and internet banking.

In a core banking system, there is a chance of encounteringforged signature for transaction. And in the net bankingsystem, the password of customer may be hacked and misused.Thus security is still a challenge in these applications. Here, we propose a technique to secure the customer informationand to prevent the possible forgery of password hacking.

The concept of image processing, an improved steganography and visual cryptography is used. Image processing is a technique ofprocessing an input image and to get the output as either improved form of the same image and/or characteristics ofthe input image. Visual Cryptography (VC) is amethod ofencrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Naor and Shamir [1] introduced a simple but perfectlysecure way that allows secret sharing without anycryptographic computation, termed as Visual CryptographyScheme (VCS). Basically, Visual Cryptography Scheme isan encryption method that uses combinatorial techniques toencode secret written materials. The idea is to convert thewritten material into an image and encode this image into *n*shadow images. The decoding requires only selecting somesubset of these *n* images, making transparencies of them, andstacking them on top of each other.The simplest Visual Cryptography Scheme is given bythe following setup. A secret image consists of a collectionof black and white pixels where each pixel is treatedindependently. To encode the secret image, we split theoriginal image into *n* modified versions (referred as shares) such that each pixel in a share now subdivides into *n* blackand white sub-pixels. To decode the image, a subset *S* of those*n* shares are picked and copied on separate transparencies. If*S* are a *qualified* subset, and then stacking all these transparencieswill allows visual recovery of the secret.

Most of the steganographic methods consider human vision sensitivity as an essential factor [4] so that the very existence of the secret bits could not be revealed by any third party. One of the

methods to achieve this is hiding the secret information in the edges rather than the smooth areas of a cover image. A method namely Multiple Base Notational Systems (MBNS) considers the edge areas of a cover image while re-expressing the secret bits in multiple base notational systems [3]. Using this technique MBNS adds more security. Furthermore MBNS proposes a walk path through the cover image which is not a row by row selection of target pixels. MBNS method owns the best values in terms of performance and quality metrics in comparison with bit-plane complexity segmentation method (BPCS) [5] and pixel value differencing (PVD)

This paper is organized as follows: Section II deals withthe related work and Section III presents the architecture andmodel. Section IV is about the problem definition and the implementation of the proposed algorithm and the performance analysis. Section V contains the conclusions.

II. RELATED WORK

A brief survey of the related work in the area of visualcryptography and its application in banking sector ispresented in this section. Visual cryptography schemes wereindependently introduced by Shamir [2] and Blakley [3], and their original motivation was to safeguard cryptographic keysfrom loss. These schemes also have been widely employed inthe construction of several types of cryptographic protocols [4] and consequently, they have many applications in differentareas such as access control, opening a bank vault, openinga safety deposit box, or even launching of missiles. Asegment-based visual cryptography suggested by Borchert [5]can be used only to encrypt the messages containing symbols,especially numbers like bank account number, amount etc.,

Cryptography and steganography are cousins in the spy craft family: the former scrambles a message so it cannot be understood; the latter hides the message so it cannot be seen. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, Steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: Steganography fails when the ”enemy” is able to access the content of the cipher message, while cryptography fails when the ”enemy” detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called *cryptanalysis* and *steganalysis.* The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages.

The aim of this paper is to describe a method forintegrating together cryptography and Steganography through image processing. In particular, we present asystem able to perform steganography and cryptographyat the same time. We will show such system is an effective steganographic and is also a theoretically unbreakable cryptography.

Two main issues are considered when using the algorithm. The first issue is imperceptibility which is the visibility of the secret information to the human eyes. The second issue is capacity, i.e., amount of secret information that can be concealed in the cover image.

In this paper the main focus is to present an improvement made in terms of imperceptibility in comparison with MBNS method. The proposed method utilizes the same probability parameter to scatter secret bits as in [9] and considers the maximum number of surrounding pixels to achieve the capacity of every target pixel.

The adjustment technique is discussed in Section III. The proposed algorithm is explained step by step in Section IV. Finally in Section V, the desired conclusion is made based on the results achieved.

III. ADJUSTMENT TECHNIQUE

Once a fraction of secret information is embedded, thetarget pixel value is to be adjusted using a kind of processwhose duty is to find the closest gray-scale value to theoriginal value of the target pixel so that the differencebetween the original and modified value of a target pixelbecomes smaller. Smaller amount of difference makes imagedistortion become smaller as well. In terms of imperceptibility, the value of a famous quality metric calledPeak Signal to Noise Ratio (PSNR) grows larger as imagedistortion gets smaller. A higher PSNR value is regarded asan enhancement in imperceptibility and vice versa. Thereforethe adjustment procedure can improve the quality of the stego-image. The adjustment procedure is as follows:

If a target pixel value is changed after embedding, two other pixel values will be generated by flipping the $(K + 1)^{th}$ bit of the pixel P_i'{ as follows:

$$(P'_- \ , \ P'_+) = \begin{cases} P'_- = P'_i + 2^k \\ P'_+ = P'_i - 2^k \end{cases}$$

where variable P_i' is the modified value of a target pixel i called P_i' P_i is already allowed to carry K bits of secret information in the first K least significant bits (K > 0). In case of finding either a value more than 255 for a negative value for P-', they should be replaced with P_i.

IV. ALGORITHM

The step by step embedding phase is as follows:

1. Input a secret key SK in order to find the desired target pixels in a pseudo random way in the secret area. A cover image consists of two areas such as secret area and embedding area. The secret area comprises of the top-most row and the left-most column of the cover image while the embedding area consists of all the pixels other than the reserved pixels located in the secret area. Secret information will be embedded in embedding area.
2. Input SN as a pseudo random number generator seed number to make a pseudo random selection of the target pixels located in the embedding area. Note that both SK and SN are seed numbers that initialize two pseudo random number generators (PRNG).
3. Let P, PL, M and N be the cover image, secret information size (in bits) and the number of rows and columns of the cover image respectively.
4. Assign the best value to the variable Mb, which is the maximum number of bits allowed to be embedded in a target pixel. The initial value for Mb will be the minimum Mb value.
5. Calculate the probability value and the desired pseudo random numbers as below:

$$\begin{cases} Probability = PL \,/\, MaximumCapacity; \\ Rand('twister', SN); \\ RandMatrix = rand(M, N); \end{cases}$$

6. Choose the desired target pixels located in the embedding area as follows:

$$\begin{cases} If\ \ Randmatrix(i,j) \le probability\ ,\ \ Chosen \\ Else \qquad\qquad\qquad\qquad Not\ chosen \\ where\ i = 1..M\ \ and\ j = 1..N \end{cases}$$

7. Determine Dynamic Capacity for P(i,j) that is the number of bits can be embedded in a target pixel using the available surrounding neighbors. Thus the Dynamic Capacity for a target pixel can be calculated as follows:

$$Min\ \left(\left\lfloor \frac{log_2\left(\sqrt[2]{2*|\sigma(\{SPS\}-\{CSP\})|}\right)}{BestDelta} \right\rfloor ,Mb \right)$$

8. Adjust the value of each target pixel using adjustment technique in order to find the closest candidate to the original value of the target pixel. Bydoing this, the target pixel value will be replaced with the closest candidate and it results in anincrease in PSNR value.
9. The embedding process needs SK shared by both the sender and the receiver in order to find the coordinates of the target pixels in the secret area. Simple LSB insertion method is applied for embedding the secret parameters inside the secret area using one LSB of each target pixel selected using SK as in Step 1.

The modified cover-image is called stego image. In order to recover secret information from the stego image, the receiver is expected to know SK so as to extract the rest of secret parameters. Knowing SK, the secret parameters can be extracted easily. The extraction procedure is as follows:

1. Extract secret parameters using SK.
2. Generate random numbers.
3. Choose the desired target pixels.
4. Compute the DynamicCapacity number of a target pixel.
5. Extract the secret information from a target pixelusing the corresponding DynamicCapacity.
6. If the amount of bits extracted equals to PL, thewhole secret information is achieved by puttingtogether all the extracted bits.

V. CONCLUSION

An improved steganography improves imperceptibility in comparison with MBNS method for the main reasons. The reason is that reason is that AMSPU discovers more surrounding pixels rather than utilizing four adjacent neighbors. Fixed neighbors are modified in previous steps so that they cause an increasingly image distortion whereas the rest of unselected neighbors still keep their original gray scale values by the end of embedding process. By using unselected neighbors as well as fixed neighbors, every Dynamic Capacity value can be estimated more precisely and also image distortion will be decreased.

REFERENCES

[I] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding-A survey," Proc. IEEE, vol. 87, pp. 1062-1078,1999.

[2] H. Wang and S. Wang, "Cyber warfare-Steganography vs. Steganalysis," Commun.ACM, vol. 47, no. 10, pp. 76-82, 2004.

[3] 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.

[4] M. Kutter and S. Winkler, "A vision-based masking model for spread- spectrum image watermarking," IEEE Trans. Image Processing, vol. II,pp. 16-25, Jan. 2002.

[5] H. Noda, J. Spaulding, M. N. Shirazi, and E. Kawaguchi, "Application of bit-plane decomposition steganography to JPEG2000 encoded images," IEEE Signal Processing Lett., vol. 9, no. 12, pp. 410-413, Dec. 2002.
[6] D.-C. Wu and W.-H.Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognit.Lett., vol. 24, pp. 1613-1626,2003.
[7] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469--474, Mar. 2004.
[8] O. Kurtuldu and N. Arica, "A new steganography method using image layers," in *Computer and Information Sciences, 2008.ISCIS '08. 23rd International Symposium on*, 2008, pp. 1-4.
[9] J. Mielikainen, "LSB matching revisited," *Signal Processing Letters, IEEE*, vol. 13, pp. 285-287, 2006.
[10] L. Xiangyang, L. Bin, L. Fenlin, "A Dynamic Compensation LSB Steganography Resisting RS Steganalysis," in *SoutheastCon, 2006. Proceedings of the IEEE*, 2006, pp. 244-249.
[11] Provos, N. (2001). Scanning USENET for Steganography.from http://niels.xtdnet.nl/stego/usenet.php
[12] M. Shirali-Shahreza, "Steganography in MMS," in *Multitopic Conference, 2007. INMIC 2007. IEEE International*, 2007, pp. 1-4.
[13] C. Chin-Chen and L. Iuon-Chang, "A new (t, n) threshold image hiding scheme for sharing a secret color image," in *Communication Technology Proceedings, 2003.ICCT 2003. International Conference on*, 2003, pp. 196-202 vol.1.