

STEGANOGRAPHY USING TARGET PIXELS COMBINED WITH PSNR AND VISUAL CRYPTOGRAPHY FOR SECURE APPLICATION

Mr. S. Premkumar

Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Coimbatore, Tamilnadu, India

Mr. V. Krishnakumar

Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Coimbatore, Tamilnadu, India

Mr. R. Vijayakumar

Computer Science and Engineering,
Sri Ramakrishna Engineering College,
Coimbatore, Tamilnadu, India

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 hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this problem of authentication, we are proposing an algorithm based on image processing, improved steganography and visual cryptography. This paper proposes 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 then dividing it into 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 is kept by the customer. The customer has to present the share during all of his transactions. 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 authenticates the customer.

Keywords— Improved Steganography, Visual Cryptography, PSNR.

I. INTRODUCTION

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. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. The question is how to handle applications that require a high level of security, such as core banking and internet banking. In a core banking system, there is a chance of encountering forged signature for transaction. And in the net banking system, 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 information and 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 of processing an input image and to get the output as

either improved form of the same image and/or characteristics of the input image. 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. Naor and Shamir [1] introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, termed as Visual Cryptography Scheme (VCS). Basically, Visual Cryptography Scheme is an encryption method that uses combinatorial techniques to encode secret written materials. 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. The simplest Visual Cryptography Scheme is given by the following setup. A secret image consists 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.

Most of the steganographic methods consider human vision sensitivity as an essential factor [2] [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)

II. RELATED WORK

A brief survey of the related work in the area of visual cryptography and its application in banking sector is presented in this section. Visual cryptography schemes were independently introduced by Shamir [6] and Blakley [7], and their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [8] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles. A segment based visual cryptography suggested by Borchert [9] 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 [11][12] 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 hidden 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[13].

The aim of this paper is to describe a method for integrating together cryptography and Steganography through image processing. In particular, we present a system able to perform steganography and cryptography at 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 [10] 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, the target pixel value is to be adjusted using a kind of process whose duty is to find the closest gray-scale value to the original value of the target pixel so that the difference between the original and modified value of a target pixel becomes smaller. Smaller amount of difference makes image distortion become smaller as well. In terms of imperceptibility, the value of a famous quality metric called Peak Signal to Noise Ratio (PSNR) grows larger as image distortion gets smaller. A higher PSNR value is regarded as an enhancement in imperceptibility and vice versa. Therefore the 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 $(K + 1)^{\text{th}}$ 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

$$\left\{ \begin{array}{l} \text{Probability} = PL / \text{MaximumCapacity}; \\ \text{Rand('twister', SN)}; \\ \text{RandMatrix} = \text{rand}(M, N); \end{array} \right.$$

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

$$\left\{ \begin{array}{l} \text{If Randmatrix}(i, j) \leq \text{probability, Chosen;} \\ \text{Else Not chosen.} \end{array} \right. \text{ where } i = 1..M \text{ and } j = 1..N$$

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

$$\text{Min} \left(\left\lfloor \frac{\log_2 \left(\frac{2 \cdot \sqrt{2 \cdot \sigma \left(\left\{ \text{SPS} \right\} - \left\{ \text{CSP} \right\} \right) \right)}{\text{BestDelta}} \right) \right\rfloor, Mb \right)$$

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. By doing this, the target pixel value will be replaced with the closest candidate and it results in an increase 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 Dynamic Capacity number of a target pixel.
5. Extract the secret information from a target pixel using the corresponding Dynamic Capacity.
6. If the amount of bits extracted equals to PL, the whole secret information is achieved by putting together 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

- [1] 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.

IJAICT