A 3-Stage secured lossless Encryption Scheme for Image Stegnography

Ms. Poonam Agarkar
Asst. Professor, ETC Department
Rajiv Gandhi College of Engg. & Research,
Nagpur, India
poonamagarkar71@gmail.com

Dr.Pratik Hajare
ETC Department
S. B. Jain Institute of Technology & Research,
Nagpur, India
pratikhajare74@rediffmail.com

Dr. N. G.Narole
Asst. Professor, ETC Department
Rajiv Gandhi College of Engg. & Research,
Nagpur, India
narennarole@gmail.com

Abstract

The paper presents a novel method for Stegnography which embed a secret image with high security in a cover image. The security is maintained by a three level encryption technique. It uses a simple Least Significant bit encoding process on the green plane of color image for lossless decoding followed by robust encryption. In the first stage of encryption two shares are generated after LSB encoding, followed by a secret key encryption and then column permutation performed on a 4x4 block of the shares. Two independent shares are generated based on the odd and even indexed bits of the 8 bit binary value for each pixel. The visual quality of the image after hiding the secret image is preserved. The decryption and the decoding process are able to recover the secret image without any loss of information. The Mean squared error and Peak signal to noise ratio are significant for only the green plane of the cover image.

Keywords – Stegnography, Least Significant bit, encryption, column permutation, mean squared error, peak signal to noise ratio.

Introduction

Stegnography is art of hiding something in some another so that whatever is hidden is indistinguishable and remains secret. Also the secret hidden thing is not visible to naked eye as seen. Text, video, audio or image is used as a cover to hide the secret. There are many approaches used in literature to accomplish the term Stegnography. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text Stegnography over other Stegnography techniques is its smaller memory requirement and simpler communication [1]. There are various techniques involving hybridization of text, audio, image and video where one component is embedded in another. Our work embed an image in image where visual contents of the cover image have no difference after hiding secret image as compared to the original cover image. Also the scheme uses data sharing between two shares where an individual share in unrecognizable.

Visual Cryptography (VC), proposed by Naor et al. in [2], is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret

image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more give the original secret image.

Some of the literature concerning about banking security is listed below which involves security based on Stegnography and visual cryptography. A customer authentication system using visual cryptography is presented in [3] but it is specifically designed for physical banking. A signature based authentication system for core banking is proposed in [4] but it also requires physical presence of the customer presenting the share. [5] proposes a combined image based Stegnography and visual cryptography authentication system for customer authentication in core banking. A message authentication image algorithm is proposed in [6] to protect against e-banking fraud. A biometrics in conjunction with visual cryptography is used as authentication system [7].

The paper consists of proposed system including encoding and three stage encryption, decryption, decoding followed by results and conclusion.

Proposed System

We propose a simple and lossless data hiding scheme using LSB encoding [8] [9] and encryption with secured key. A cover image and the secret image are read and both are resized to same dimension. The size of the cover image was kept as it is and the size of secret image was made similar to the cover image. For better security the green plane of the cover image was selected for hiding the secret image.

LSB Encoding – The secret image chosen was a binary image, if it is color or gray scale image, it is converted to binary image. Each pixel value of the secret image either 0/1 is then inserted in the LSB position of pixel value of cover image after converting the gray value [0 255] in 8 bit binary. A separate function was used to convert each decimal value corresponding to pixel into binary. Since the LSB was replaced by bit from secret image, the green plane cannot be decoded lossless. But the probability of replacing similar bit in cover image with the bit in secret image depends on the features of both the images. Approximately, it can be around 50% more or less. The more the similar bits are encoded, higher the Peak signal to noise ratio (PSNR). The following figure 1 shows the cover image, secret image, green plane image and the LSB encoded cover image.

Cover image

Secret image

Green plane image

Stego Image - Green plane, LSB Encoding

Figure 1 – Cover image, secret image, Green plane image and the encoded image

As seen from the above color images the encoded image is similar to that of the cover image. The actual difference given by Mean squared error (MSE) and the PSNR at this stage after decoding was,

Mean Squared Error (Green Plane Image) = 0.096939

Peak Signal to Noise Ratio with LSB Encoding = 58.2658

Encryption – Encryption involves three stages for better security. In the first stage, the LSB encoded green plane image is divided in two shares. Each pixel value is converted into binary. For share 1 the odd indexed bits are extracted [1 3 5 7] and the remaining bits are assigned a '0' value. Therefore the complete 8 bit binary odd share would be [1 0 3 0 5 0 7]. The odd share will keep the decimal equivalent of this 8 bit binary number. Similar process is adopted for even share, i.e. share 2. Here only the even indexed bits are extracted [0 2 0 4 0 6 0 8].

The following figure 2 shows the process of generating two shares from the encoded green plane component of the cover image.

Pixel value of 185 of the green plane encoded image

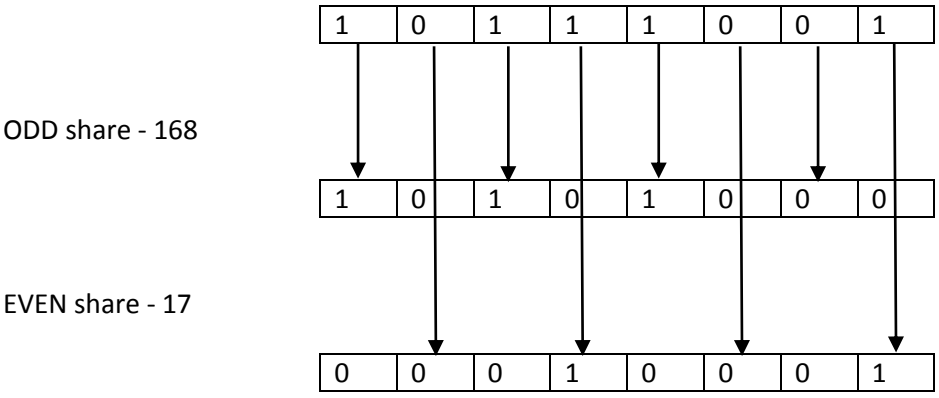

Figure 2 – Generation of Odd and Even shares

In the second stage of encryption the generated shares are secured by generating a private key. Random integer numbers are generated equal to the size of the shares using a seed value. These generated shares are then subtracted from the generated key. Hence at time of decryption, this key should be known, otherwise decryption is not possible. In this way security is increased. The figure 3 below shows the output of the above share generation scheme.

Share 1- Odd index bits

Share 2 - Even index bits

Figure 3 – Two shares generated using the above scheme

The third stage encryption involves permutation [10] process in order to maintain high security. More robust permutation process can be adopted, but we have used only column permutation since the generated shares in the above step have greatly affected the quality of the shares with respect to the green plane encoded image. And as far as visual perception is concerned, it is difficult for any other person to guess the hiding process. The column permutation adopted in this paper is shown below in figure 4a & 4b. Consider a 4x4 matrix block from the generated share. The matrix will have pixel values in general, but to understand for simplicity, the pixel values can be considered as index values as per MATLAB index sequence.

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

Figure 4a – Original matrix of the generated share

4	7	10	13
1	8	11	14
2	5	12	15
3	6	9	16

Figure 4b – Permutated sequence

The first column is shifted vertically be one element, second by two elements and so on. The last column remains same. To increase higher security, row permutation can also be performed and further the matrix can be broken into four equal parts to interchange the elements diagonally. For complexity

reduction, we adopted only the first part. The following figure 5 shows the results of third stage encryption process.

Figure 5 – Shares after third stage encryption

At this stage, these two shares can be part of authentication and kept for example one with a bank and another with the customer. Unless these two shares along with the secret key are available, the secret image (password) cannot be decoded.

Decryption and Decoding – It is now simple to encrypt the share by performing the reverse permutation and then subtracting from the secret key. The reverse permutation index will be as shown below.

2	7	9	13
3	8	10	14
4	5	11	15
1	6	12	16

Figure 6 – Reverse permutation for recover

The next stage involves extracting ODD and EVEN numbered bits from both the shares respectively and then combing them to get the decimal equivalent no representing the gray scale value. Lastly the LSB bit is extracted to get the secret image as shown in figure 7 and 8 respectively.

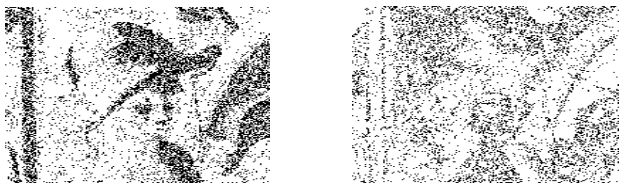

Figure 7 – Decrypted shares

Decoded Cover Image (Green Plane)

Decoded Cover Image

Decoded Secret Image

Figure 8 – Decoded cover green plane image, color image and the secret image

It is seen that the decoded green plane image is somehow different from the original green plane image actually taken to hide the secret image. This is the result of loss of information when LSB decoding was done. Since we cannot recover the lost LSB bit while we put the bit of the secret image. But the final extracted secret image is same as that of the original secret image. Hence the MSE is 0 for the secret image.

Results & Conclusion

The main advantage of the proposed scheme is data security to high extent. No matter LSB encoding scheme is well known and a common approach to hide secret image, further share generation, encryption using secret key and permutation have increased level of security. Secret images involving more complicated texts, features, digital signatures, patterns can be used for more robust security. For data hiding only green plane of the image is used in this paper, other planes of the cover image, red and the blue can be used to combine to have greater depth in security. The main feature of the proposed algorithm is that the secret information can be extracted without a loss.

References

[1] J.C. Judge, “Stegnography: Past, Present, Future,” SANS Institute, November 30, 2001.
[2] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptography: EUROCRYPT’94, LNCS, vol. 950, pp. 1–12, 1995.
[3] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, “Novel Authentication System Using Visual Cryptography,” Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
[4] Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L M Patnaik, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,” Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008.
[5] S. Premkumar, A. E. Narayanan, “New Visual Stegnography Scheme for Secure Banking Application,” Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

[6] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm," Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.
[7] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system, "Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.
[8] K. Thangadurai, G. Sudha Devi, "An analysis of LSB based image Stegnography techniques ", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.
[9] Anu Binny, Maddulety Koilakuntla, "Hiding Secret Information Using LSB Based Audio Stegnography ", 2014 International Conference on Soft Computing & Machine Intelligence, 26-27 September, Pages – 56-59, 2014.
[10] Jiantao Zhou, Member, IEEE, Xianming Liu, Member, IEEE, Oscar C. Au, Fellow, IEEE, and Yuan Yan Tang, Fellow, IEEE, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE transactions on information forensics and security, vol. 9, no. 1, pages- 39-50, January 2014.