Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 4 (2017) pp. 613-621

http://www.ripublication.com

Confidential Data Transmission Using Encryption Algorithm

Kartik Sau*, Soumi Mondal and Anay Ghosh
Department of Computer Science and Engineering,
University of Engineering and Management,
New Town, Kolkata, West Bengal, India

Abstract

Secret sharing method protects the sensitive data from attackers. These sensitive data may include text, image, audio and video or combination of some or all. Different methods are available in literature for secret sharing having some merits and demerits. To overcome the demerits of some existing methods we are suggesting a new method based on simple graphical schema (SGS). The proposed method is explained in three phases. In the first phase we have critically designed a suitable masking strategy. In the second phase encoding is done by inserting all the pixel values of secret image (SI) to the suitable positions of corresponding pixel in different cover images (CI) based on masking strategy. In third phase decoding is done by taking the corresponding bit values from the quantified set of shares followed by simple ORing operations for all pixels. The proposed method is tested for different images. The experimental result shows the effectiveness of our newly design technique for secret sharing. The quality of the reconstructed image is measured in terms of PSNR values and its value is 100dB for all the cases. The proposed techniques can be used for Confidential Communication, Secret Data Storing and Protection of Data Alteration.

Keywords: Steganography, secret sharing, ANDing, ORing, PSNR.

1. INTRODUCTION

Steganography is a process by which it prevents image from illegal attacks [9]. Some such illegal attacks are stealing, modification and misuse the image etc.

Steganography conceals the confidential information in a cover medium (CM) to ignore spite attempts. The cover medium (CM) could be text, digital image, audio and video. Attackers cannot visualize the presence of secret image (SI) in cover medium. So as a result, they will not estimate the presence of secret image in the apparently innocent covers. Now a day's different procedures are available to prevent the secret image (SI). In most of these procedures, the entire secret image is kept within a cover image. If the cover medium is lost or corrupted then secret data or image cannot be revealed. Such problem can be solved with the help of secret sharing algorithm (SSA). There are different methods are available for the purpose of secret sharing. Most of these methods are well appreciated. In response to the demand, almost every year, the different techniques are introduced by different researchers. Still, it is not sufficient to meet the current requirement. The present paper is organized as follows:
In the section 2 we have discussed the different existing methods along with their pros and cons as a literature survey. In section 3 we have represented the newly designed techniques to overcome the problems as discussed in section 2. The experimental result of our novel proposed methods along with conclusions are presented in section 4 and section 5 respectively.

2. LITERATURE SURVEY

Different techniques are available for secret sharing; some such techniques are mentioned below as a literature survey of this paper. In 1979, Shamir and Blakley individually developed a secret sharing methods based on polynomial interpolation and hyper plane geometry method respectively. The secret sharing method based on polynomial interpolation is described in [1] and hyper plane geometry method described in [2]. In the decoding part of the above two methods, the secret shares are disclosed. It is one of the problems of the above methods of Shamir and Blakley. This problem termed as function sharing problem. There are various function sharing protocols has been proposed by different researcher mostly based on Shamir's secret sharing techniques. In 1992, Kurak and McHugh introduced Image Downgrading and Cover Channels method for secret sharing. It is described vividly in [7]. In this method one gray scale image can be considered as a secret image and also cover image. The stego image can be constructed by replacing the four LSB's of secret image are replaced by the four MSB's of that image. In the decoding part four LSB of stego image is interchanged with four MSB of that image. Hence, in this way the original secrete image can be retrieve. In 2004, Kharrazi, M., Sencar, H. T. and Memon presented the concept of data sharing based on least significant bit substitution method. It is properly presented in [3]. In this approach the LSB's of each pixel of cover image are replaced by each pixel of secret image. As a result the original secret images are hidden uniformly on the single cover image. There are various versions; based on LSB encoding techniques have been proposed by different researchers. In 2015, Bassam Hasan Saghir *et. al* suggested a novel method in spatial domain based on Pseudo Random Permutation Substitution Method using Tree and

Linked List for efficient data transfer. It is vividly described in [4]. In this method the secret images are encoded within the entire cover image in random manner. Here some additive noises are introduced in the cover image and as a result the statistical properties and PSNR values of the cover image are changed. In 2009, Lee and et al proposed filter first method for efficient data transfer in spatial domain. It is elaborately described in [8]. In this approach last 'x' significant bits of each pixel of cover image are exchanged with each pixel of secret image. Remaining (8-x) bits are used for filtering purpose. In 2004, Chan, Chi-Kwong and L. M. Cheng presented hiding data in images by simple LSB substitution method in spatial domain. It is properly presented in [6]. In this approach each pixel of secret image are interchanged with corresponding each pixel of cover image at random positions. In 2009, Mamta Juneja, Parvinder Singh Sandhu presented Robust image steganography technique based on cryptographic concept [5]. In this technique data's of secret image is inserted in the LSB of cover image. The attackers tried to find secret data from stego images by stego analysis. In this paper authors tried to insert secret data to a suitable cover image which is selected from the cover image library. In the cover image library, the images are stored based on their rank. As a result the attacker has less chance to detect and recover secret data using stego analysis from the cover image. Here authors tried to encrypt the secret data by masking method and then insert the encrypted data in the suitable position of the cover image.

Here we are proposing a new method based on simple graphical method. The proposed method is explained in three phases. In the first phase we have critically designed a suitable masking strategy. In the second phase encoding is done by inserting all the pixel values of secret image (SI) to the suitable positions of corresponding pixel in different cover images (CI) based on masking strategy. In third phase decoding is done by taking the corresponding bit values from the quantified set of shares followed by simple ORing operations for all pixels.

3. BASIC CONCEPTS

The suggested method is built by keeping the idea of innovative secret sharing technique which is implemented by the simple graphical masking method (GMM), the encoding of data in the proposed method is done by ANDing operation for the purpose of share generation so that it hide actual data within some cover medium and ORing operation is taken out to decrypt the data so that original data can be reconstructed from the selected stego images. For better understanding of the newly proposed technique, we considered original secret data as binary files of several bits. It is generated from different types of secret data. Some such secret data can be text or images or audio or videos. For our experimental purpose here we considered image as secret data. At first the secret image is efficiently distributed into different number of cover images such that the qualities of the modified cover images are not distinguished from the original cover images by human eye. Here the modified cover images are termed as stego image. The stego images are sent to receiver via internet. The original secret data can be reconstructed from k number of shares where $n>k>2$.

Phase 1

In the phase A, we have discussed the masking generation procedure. In the masking generation procedure, let n be the number of cover images (where we want to hide a secret image) and k (< n) is the stego images (from which secret image can be reconstructed). For this purpose, there will be some missing bits in every share and those bits will be available in exactly other (k-1) number of shares. For each component of each share, k-1 number of bits may be missed, and (n-k+1) numbers of bits are available, so the bit which we consider will be present in each and every set of k shares but there is no guarantee of presence in less than k shares. For each bit position there must be ${}^{n}C_{k-1}$ number of combinations. Therefore, the length of each mask will be ${}^{n}C_{k-1}$. The nature of the different shares, which are generated from secret image, depends upon the nature of different masks. To get the secret share every mask is convolute with secret image. After getting the secret share, it is hidden in the cover image. One example of mask for 5 shares and 3 threshold share is given below:

$Share1: 1\,1\,1\,1\,1\,1\,0\,0\,0\,0$
$Share2: 1\,1\,1\,0\,0\,0\,1\,1\,1\,0$
$Share3: 1\,0\,0\,1\,1\,0\,1\,1\,0\,1$
$Share4: 0\,1\,0\,1\,0\,1\,1\,0\,1\,1$
$Share5: 0\,0\,1\,0\,1\,1\,0\,1\,1\,1$

Phase 2

In this section the secret image is embedded in the different cover images, it is termed as encoding strategies. The encoding strategies are described as follows:

1. Construct a matrix (A) of size ${}^{n}C_{k-1} \times n$ such that each row contains (k-1) number of 0's and (n-k+1) number of 1's in different positions. Where 'n' denotes the total number of columns of the matrix A.
2. Compute matrix (B) of size $n \times {}^{n}C_{k-1}$ such that $B = A^{T}$, Where A^{T} indicate the transpose of the matrix A.
3. Each row of B is used as a mask, as there are n numbers of rows so it has n number of mask.
4. For each mask apply the following steps
   a) Now apply the point wise multiplication of secret image with a mask (as defined above), i.e. The values of the secret image corresponding to 1 are kept as it and the values corresponding to 0 is replaced by 0 for a particular mask.
   b) Then the selected pixel of secret image is inserted to the corresponding pixel of cover images at the LSB position. The selected pixel consist of eight bits, first

three bit inserted in the LSB of R , next three bit is inserted in the LSB of G, and last two bit is inserted in the LSB of B value, as we consider the color cover image.

5. Continue until for all masks.
6. Return stego images (STI).

Now the image can be reconstructed from the fewer number of stego images, it is termed as decoding part. The decoding strategy is represented as follows in phase 3.

Phase 3

1. Select any k or more number of stego images (STI) from the set of n stego images, which is generated in the phase 2 as discussed above.
2. To reconstruct each pixel of reconstructed secret image do the following operation.
   a) Extract the share bytes (B_i) (i=1, 2, 3, 4…k) from k stego images.
   b) To extract the share bytes (B_i), Take the last three bit of R component, last three bit of G component and last two bit of B component then concatenate all the bits followed by decimal conversion.
3. To generate the corresponding secret byte(Bs) applies the following operation $Bs= B_1 OR B_2 OR B_3 OR... OR B_K$.
4. Go to step 2.

Example; Consider a secret image and five cover images as shown in the figure 1 in the form of matrix. After encoding operation, we get five stego images as shown in the figure 2. The encrypted stego images are transferred to the destination. At the time of transfer of stego images some of them may be lost. Suppose that here, stego 4 and stego 5 are lost. Now we reconstruct the secret image by decoding using rest of the three stego images as shown figure 3. Here all the figures are shown as a annexure I.

4. EXPERIMENTAL RESULT

The proposed method is tested for some standard 8-bit secret images of size 512×512 along with some standard 24-bit cover images of same size as secret image. The experimental result of our newly designed method for data transfer gives the satisfactory result in terms of PSNR and as well as MSE [10] for all the images. The MSE and PSNR can be defined as follows-

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f(i,j)-g(i,j)\right)^2 \qquad (1)$$

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \qquad (2)$$

Where f(i,j) and g(i,j) are the input and output images respectively of the proposed method. The image can be reconstructed from any three stego images out of five stego images. The size of the secret image may different for different cases but there should be relationship with cover images. The experimental result of suggested method is displayed in the figure 5 for the image as shown in figure 4. Here we observed that the PSNR values are 100 dB for all the cases. Therefore, it indicates that the recommended technique for data transfer is highly encouraging. The proposed method can also be applicable for 24-bit image by extending this algorithm. In that cases the size of the cover images should be three times in breath. Here the proposed method is tested for images, though it can be applicable to text, audio and videos also. The proposed technique is applicable for Confidential Communication, secret data storing and some industrial applications also.

Fig. 4: secret image

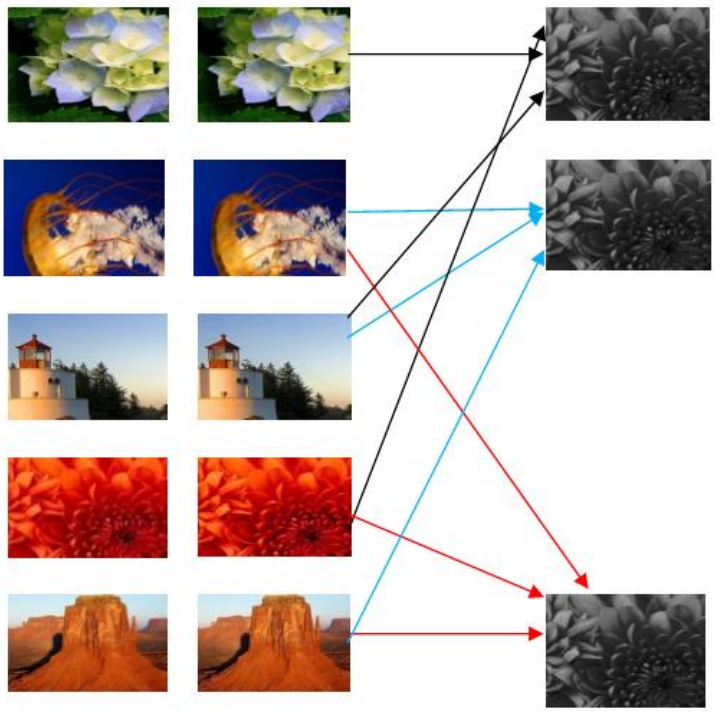

Figure 5: Reconstruction of image decoding phase

5. CONCLUSIONS

In this paper, we propose a novel method for secret data transfer. We implemented this novel technique in three phases. In phase-1, we have implemented the masking strategy based on simple graphical schema. In phase-2, encoding is done by inserting all the pixel values of secret image to the suitable positions of corresponding pixel of different cover images based on masking strategy. In phase-3, decoding is done by taking the corresponding bit value from the quantified set of shares followed by simple ORing operations of the selected shares for all pixels based on masking strategy. Here the experiment is tested for images, it gives the satisfactory result. We can extend this proposal to text, audio and videos as a secret data transfer. It can be applicable for Confidential Communication and Secret Data Storing, Protection of Data Alteration and some industrial applications. Some concluding observations from the investigation are given below.

- The size of the secret image may be anything but there should be some relationship with cover images.
- The secret image is embedded in the different cover images in such a way the quality of the modified cover images are not distinguished from the original cover images by human eye.
- The secret image is reconstructed by fewer number of stego images, if some stego images are lost.
- The quality of reconstructed image is good enough. The PSNR values of reconstructed images are 100 dB for each case.
- The attacker has less chance to detect and recover secret data as the cover images are different in different cases for a particular secret image.
- It can be applicable for Confidential Communication, secret data storing and some industrial applications also.

REFERENCES

[1] A.Shamir, “How to share a secret?”, Comm ACM,22(11):612-613,1979.

[2] G.Blakley, “Safeguarding cryptographic keys”, *Proc. of AFIPS National Computer Conference*,1979.

[3] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), “Image Steganography: Concepts and Practice”,*WSPC/Lecture Notes Series: 9in x 6in,* pp.1-31.

[4] Bassam Hasan Saghir et all,”A Spatial Domain Image Steganography Technique Based on Pseudorandom Permutation Substitution Method using Tree and Linked List”, *International Journal of Engineering Trends and Technology (IJETT),*vol.-23,2015.

[5] Mamta Juneja Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption",*International Conference on Advances in Recent Technologies in Communication and Computing,*2009.

[6] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution",*THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY,*2004.

[7] Kurak, McHugh, "A Cautionary Note On Image Downgrading", *IEEE Computer Security Applications Conference 1992*,Proceedings, IEEE press,1992,pp. 153-159.

[8] Lee, Y-K. ; Bell, G., Huang, S-Y., Wang, R-Z. and Shyu, S-J. (2009), "An Advanced Least Significant-Bit Embedding Scheme for Steganographic Encoding", PSIVT 2009, LNCS 5414, Springer, pp. 349–360.

[9] Gregory-Kipper, "Investigator's Guide to Steganography", *Auerbach Publications*, 2003.

[10] Rafael C Gonzalez,"Digital Image Processing",*Pearson Prentice Hall*, edition-3rd, 2008.

ANNEXURE I

Secret image

$$\begin{bmatrix} 72 & 5 & 29 \\ 36 & 140 & 17 \\ 64 & 11 & 198 \end{bmatrix}$$

Figure. 1: Dataset of Secret Image

Cover Image 1

$$\begin{bmatrix} (72,33,121) & (20,214,166) & (50,5,17) \\ (12,10,98) & (14,233,57) & (78,6,210) \\ (229,212,7) & (43,77,18) & (0,211,0) \end{bmatrix}$$

Cover Image 2

$$\begin{bmatrix} (16,33,145) & (160,1,29) & (0,51,77) \\ (20,10,119) & (71,2,185) & (34,29,75) \\ (10,0,77) & (0,5,1) & (134,44,0) \end{bmatrix}$$

Cover image 3

$$\begin{bmatrix} (0,56,37) & (39,84,100) & (129,101,4) \\ (20,4,211) & (14,70,23) & (5,0,79) \\ (11,2,49) & (16,7,88) & (206,4,20) \end{bmatrix}$$

Cover image 4

Cover image 5

$$\begin{bmatrix} (0,5,77) & (11,59,241) & (7,27,87) \\ (9,20,17) & (212,204,31) & (37,55,90) \\ (0,0,0) & (101,127,17) & (18,99,31) \end{bmatrix} \quad \begin{bmatrix} (2,19,72) & (43,215,14) & (51,205,61) \\ (127,57,2) & (26,0,217) & (12,0,222) \\ (118,65,29) & (17,20,25) & (202,13,5) \end{bmatrix}$$

Figure. 2: Dataset of five Cover Images

Stego image 1

$$\begin{bmatrix} (74,34,120) & (16,209,165) & (48,7,17) \\ (9,9,96) & (12,235,56) & (72,4,209) \\ (224,208,7) & (40,72,16) & (0,208,0) \end{bmatrix}$$

Stego image 2

$$\begin{bmatrix} (18,34,144) & (160,1,29) & (0,55,77) \\ (16,8,116) & (64,0,184) & (32,24,72) \\ (10,0,76) & (0,2,3) & (134,41,2) \end{bmatrix}$$

Stego image 3

$$\begin{bmatrix} (2,58,36) & (32,80,100) & (128,96,4) \\ (17,1,208) & (12,67,20) & (0,0,76) \\ (10,0,48) & (16,2,91) & (200,4,20) \end{bmatrix}$$

Stego image 4

$$\begin{bmatrix} (0,0,76) & (8,57,241) & (0,24,84) \\ (9,17,16) & (208,200,28) & (32,52,89) \\ (2,0,0) & (96,120,16) & (22,97,30) \end{bmatrix}$$

Stego image 5

$$\begin{bmatrix} (0,16,72) & (40,208,12) & (48,207,61) \\ (120,56,0) & (124,3,216) & (8,4,221) \\ (112,64,28) & (16,18,27) & (206,9,6) \end{bmatrix}$$

Figure. 3: Dataset of five Stego Images

$$\begin{bmatrix} 72 & 5 & 29 \\ 36 & 140 & 17 \\ 64 & 11 & 198 \end{bmatrix}$$

Figure. 4: Reconstructed Image