IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 21-27
www.iosrjournals.org

Data Concealment within Image Files using Visual Cryptography

Yash Mehata[1], Garima Kaushik[2], Jesalkumari Varolia[3]
[1](B.E. Student, Computer Science, Thakur College of Engineering & Technology, India)
[2](B.E. Student, Computer Science, Thakur College of Engineering & Technology, India)
[3](Assistant Professor, Computer Science, Thakur College of Engineering & Technology, India)

Abstract: *Digital Steganography is an science of hiding data in a medium carrier which in this paper is a cover image .On the other hand Visual Cryptography is a technique of dividing an image into a no of indecipherable part which a know as shares. Many algorithms have been proposed is the field of Steganography and Visual Cryptography with goal of improving security, reliability and efficiency in the field Computer Science. This paper discuss the combination of both the methodologies in which a secret message in divided into shares and hidden within cover images using SPIHT compression and LSB method for embedding shares in cover image. Encrypted data tempt hackers and others cyber criminal in decrypting the data where as on the other hand Data hiding helps in transferring confidential data in form innocent file like image without any cyber criminal suspecting .*

Keyword: *Steganography , Visual Cryptography , Digital Halftoning , SPIHT, LSB*

I. Introduction

In Today's modern world as Computer Network and Communications move forward in providing new and better technologies to transfer data across a network, the security of data is becoming the main concern. Many of our confidential information like email account information, credit/debit card ,exam papers may be included in this data . Security measures for these issue are being developed and improving. Cryptography being one of the security measures taken, helps in making data unreadable to the third party , but transmission of encrypted message may easily arouse attacker's attention , and the encrypted message may thus be intercepted, attacked or decrypted violently. In this paper we will be discussing the combination of two methodologies which will help in making data unreadable and hidden from the third party.

Visual Cryptography is a technique in which an image can be encrypted and decrypted without the use of any public or private key. In this methodology an image is divided into 'n' indecipherable images called 'shares'. Each share contains random black and white pixels . This technique does not need any decryption algorithm . Only when all 'n' share images that were generated are stacked together , the secret image can be revealed through Human Visual System (HVS) . This technique was proposed by Moni Naor and Adi Shamir in 1994[1].Visual cryptography uses images on transparencies. The simplest example is 2 out of 2 scheme where a secret information is divided into 2 share .These 2 shares are printed on transparent paper. One share cannot reveal the secret information , both the shares are mandatory for a successful decryption. This example can further be extended to 'k' out of 'n' scheme where the image in divided into 'n' shares . Out of these 'n' shares 'k' shares are required for a successful decryption . If 'k-1' share are presented, the secret information would not be revealed.

On the other hand Steganography is an art and science of hiding information within a medium carrier and transmitting data unsuspected. The word "steganos" means "covered" and "graphical" means "writing".Steganography consists of three terms that is message , cover image and stego-image (or stego-object).

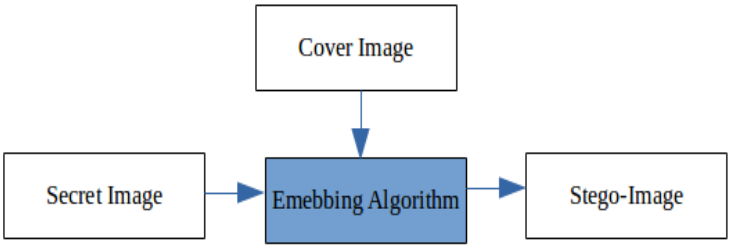

Figure i: Stego-image = Message + Cover image

Steganography was first practiced in 480 BC , that is during the golden age in Greece[2] by melting wax off wax tablets , inscribing the message on the underlying wood and then reapplying the wax to the wood giving it an appearance of an unused tablet. Since then there have new techniques developed in this field . There are mainly two techniques in digital steganography , that are i) Substitution Domain ii) Transform Domain . Traditional steganography generally uses simple techniques to encode binary data into pixels of cover image , but in this paper we will be taking inputs like text, binary, gray and color image to encode into cover images

II. Proposed Work

The proposed work is a framework designed Matlab consisting of two modules i.e. Visual Cryptography and Steganography. The input message to be hidden can be taken in the form of a text or an Image which can be binary, gray or color. The second input is a taken as a set of cover images. The output of this system generates a set of images having a share of the input message embedded within them which in not visible to anyone. The system can later take all the generated images as input and extract the secret message and reveal it to the user. The system is divided into two main functions i.e. Encoding and Decoding

A. Encoding

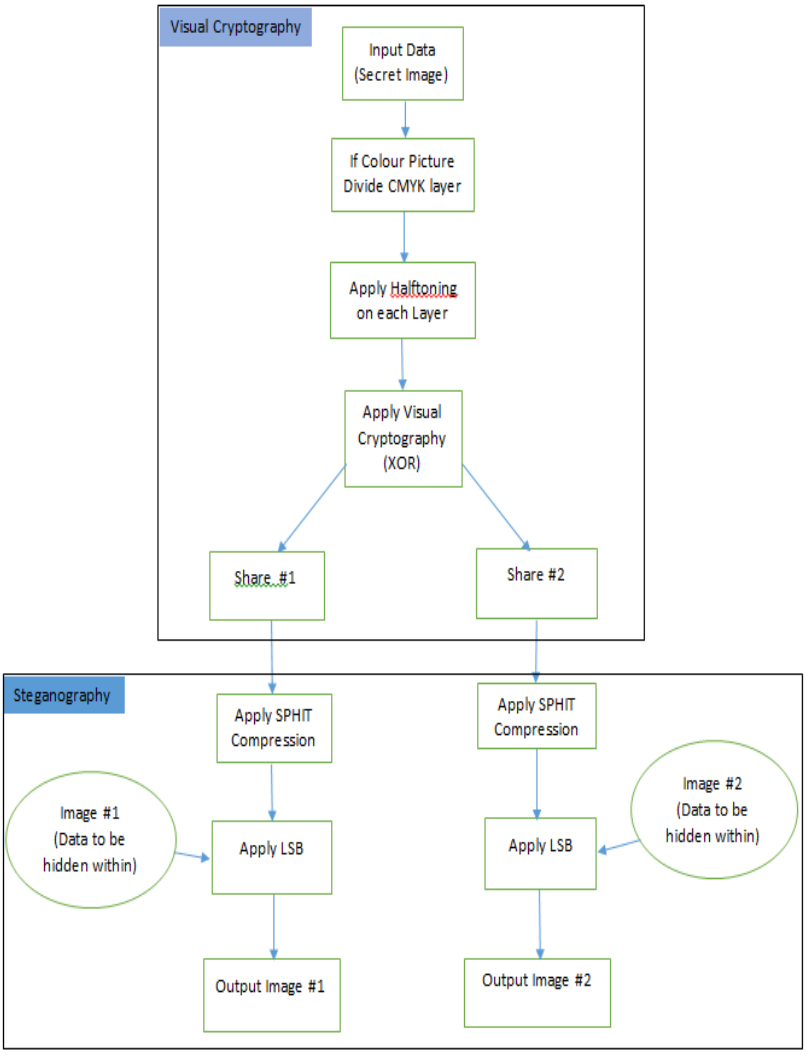

Figure ii: Encoding

The encoding part of the system is responsible for generating a set of image embedded with the secret message taking the cover image as input. The secret message can be a text, binary , gray or color image. Text and binary image is considered to be the same as input . In case of gray and color images , the image has to go through half-toning process to convert the gray images into binary images. This is done so that the binary visual cryptography scheme can be applied on gray images[3].Color image are at first converted into CMY model and

then each layer of the image undergoes half-toning[4] and visual cryptography. Visual Cryptography in the system uses XOR method in which the system will generate shares which can reveal the message only by XORing it . After a set of shares have been generated , each share is embedded within a cover images using SPIHT compression and LSB method . Each share is first compressed using SPIHT algorithm which is a lossless compression method . The algorithm convert the shares into binary files , divides the binary sequence into blocks , change the order of the block sequence using a randomly generated permutation after which it concatenates the permuted blocks which can be changed into a permuted binary sequence[5]. Then LSB approach is utilized to embed permuted binary sequence into the cover image which then generates the output image and also includes a binary header file in top-left corner of the image which consists of stores the number of share generated and the type of input provided.

B. Decoding

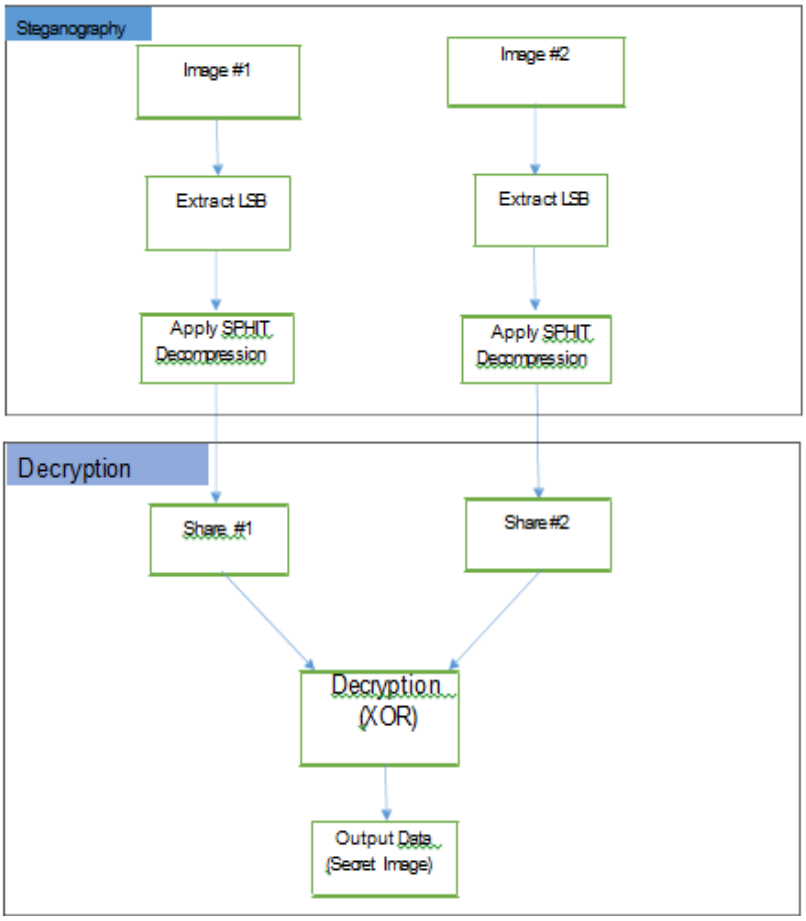

Figure iii: Decoding

The decoding part is the reverse of encoding in which the images generated from encoding are taken as input and the secret message is revealed as output. When the share images are taken as input , the system scans the image for the binary header embedded during encoding to confirm whether the input is a share or not and to get the number of shares required for the message to received . After the number of valid shares has been confirmed , the permuted binary sequence in extracted from them and the shares are then obtained by uncompressing the permuted binary sequence using SPIHT algorithm . Each share obtained is XOR-ed together to revealed the secret message which maybe in the form of binary, gray or color image.

III. Visual Cryptography

Visual Cryptography is a branch of secret sharing. It was first introduced by Naor and Shamir in [1].They produced a basic scheme for sharing secret binary image by using their own coding table. They expanded every pixel in the binary image into 2 or 4 pixel in the share.

Figure iv: (2,2) Visual Cryptography Scheme

Figure iv shows a 2 out of 2 coding table in which when a white pixel was encountered , white and black pixels are put in same positions in both shares whereas when black pixel is encounter white and black pixels are placed opposite positions in both share . This is done so that when both shares are stacked in a right alignment , the message in revealed through HVS which is equivalent to OR-ing the shares. The disadvantage of using traditional VC is that when making shares of the binary image , noise in added in the images which adds distortion when the message is revealed. But when using XOR based VC . distortion in the secret message in very less . When reconstructing image in traditional VC the secret image loses its contrast especially in the background but in XOR-Based scheme contrast is regained [6] . Therefore in this paper we use XOR based VC . In this system as the image goes through half-toning , the image becomes a binary input .

Algorithm:

Encryption
Input: Binary Image
Output: Set of share images
Step 1: Take image as input
Step 2: Create a random binary image of the size equivalent the input image
Step 3: XOR the result of step 2 with the input image
Step *4:* Return the result of step 3 and step 2 as shares

Decryption
Input: Set of share images
Output: Binary Image
Step 1: Take image as input
Step 2: XOR all the images with each other

Result:

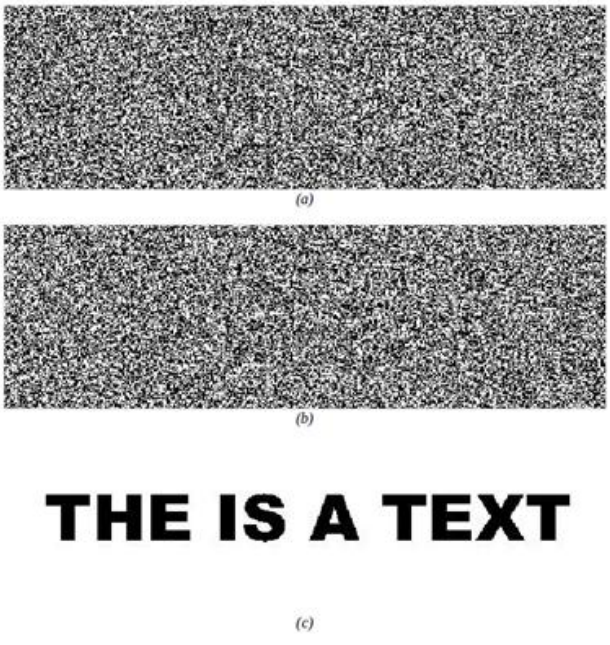

Figure v: (a) Share 1 (b) Share 2 (c) Secret Message

IV. Half Toning

A halftone or a halftoned image is an image consisting of discrete dots rather than a continuous tone. When the image with these dots are viewed from a distance, the dots get blurred and an illusion of a single or a continuous color is obtained.

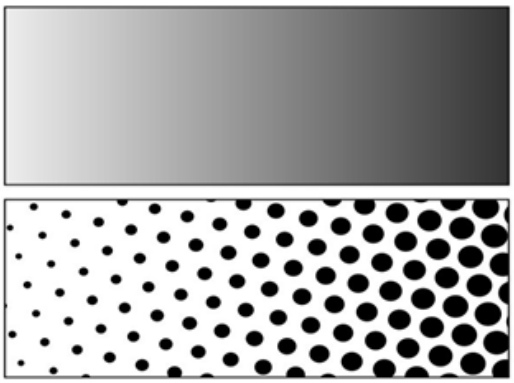

Figure vi: Halftoned image

The image has to be converted into a binary image using half-toning for VC process to work[3].Error diffusion is a type of Half-toning. It is a simple and efficient way to convert gray image to binary image. In this technique, the quantization residual is added to the neighboring pixels which have not been processed for half-toning . Error diffusion algorithm was first proposed by Floyd and Steinberg[7] in which the quantization error is distributed among 4 neighboring pixels . But later P. Stucki improved the error diffusion technique[8] by distributing the quantization error among 12 neighboring pixels. As mentioned in[9] Stucki 's error diffusion algorithm gives better PSNR result . PSNR is most widely used to measure the quality of the reconstructed image. It is defined through Mean Squared error as:

$$|MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}[f(m,n) - f^{'}(m,n)]^2|$$

$$|PSNR = 10\log_{10}\frac{255^2}{MSE}|$$

Therefore in this system, we will be using Stucki 's error diffusion algorithm for half-toning

V. SPIHT Method

SPIHT compression scheme was developed by Said and Pearlman in 1996[10]. SPIHT is a powerful wavelet-based image compression method known as Set Partitioning in Hierarchical Trees. The SPIHT algorithm applies the set portioning rules on the sub-band coefficients. The encoder and the decoder do not need any explicit transmission of ordered information. Both the encoder and decoder maintain and continuously update the following three lists, viz. [10]

- List of insignificant pixels (LIP)
- List of significant pixels (LSP)
- List of insignificant sets (LIS)

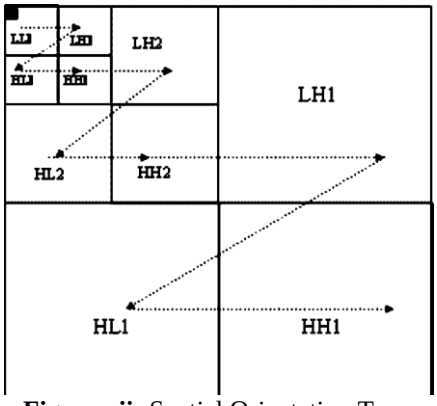

Figure vii: Spatial Orientation Tree

The spatial orientation tree, illustrated in *Figure vii* defines the spatial relationship between the subbands. The subbands are recursively split into four bands. All the nodes of a tree have four offsprings except for the leaves which is the end of the tree. Each node has four filter components, viz. . LL (Low-Low), LH (Low-High), HH (High-High) and HL (High-Low). The algorithm works in majorly two passes i.e., sorting pass which lists are organized and the refinement pass which does the actual progressive coding transmission. The following steps are followed in the execution of SPIHT algorithm.

Algorithm

Input: Set of cover images and set of shares

Output: *Stego-image*

Step1**:** This is the first pass of the algorithm. In this, the pixels are sorted and classified into several clusters. The current threshold is determined, and it is checked if the entry is significant according to the current threshold value. Now here there are two possibilities, either the entry will be significant as per the current threshold or it will not be significant, meaning it will be insignificant. Now if the pixel is significant, then it is removed from the 'List of Insignificant Pixels (LIP). Then there is a standard output for the given input. In this input, the bit is marked as one (1). Also, as we know there is a sign associated with every number. So one more coefficient bit is put up, which is deemed as zero if the current output bit is negative, or else it is one if the current output bit is positive. Alternately, if in the sorting stage we determine that the data bit is insignificant, it stays where it is, and it is displayed by a standard output of zero (0).

Step2**:** In the second step we deal with the entries which are available in the "List of Insignificant Sets (LIS)'. Entries in List of Insignificant Set (LIS) are processed. Now each individual entry in the aforementioned set is analyzed. If it descends directly from a given coefficient, say A, then we need to once again determine if the entry is significant or not. So for this purpose, we use the magnitude test. The direct offspring of this entry have to undergo a magnitude test along with all the other descendants of this entry. Following the convention mentioned in the set above, if the direct offspring is significant it is moved to the set of significant sets, else it is moved towards the insignificant pixels set. Now if a current entry is deemed to be insignificant, it has a cascading effect, this is because we consider the set to be represented by a spatial orientation tree here. That means when the root of the tree, that is the current bit is deemed to be insignificant, the nodes following the root, that is the descendants of the current entry are all considered to be insignificant and there is a halt on further processing of those elements. Now the entire procedure repeats for all of the entries, and then finally it is moved to the end of LIS sets. Now if an entry in the LIS is the type B, then we need to run the significance test on the entry. If the significance test returns a value of true, then the spatial orientation of the given entry is split into four sub-trees, consisting of its direct descendants. Then finally, all those sub-trees, are put in the Type A coefficient and moved to the end of the LIS list. We define the parent-child relationship as a tree, because if makes the task of finding zero trees much easier.

Step3**:** This is the refinement pass where the bits are refined. The output is the nth bit of the List of Significant Bits at the current threshold. As per this algorithm, after every iteration before moving forward, the threshold is halved.

VI. LSB Method

The Least Significant Bit(LSB) is one of the main techniques in spatial domain image steganography. From the byte value of the image pixel, LSB is the lowest significant bit. It is a process of embedding a message into an image. The least significant value of the pixel is altered to insert the hidden message.

VI. Conclusion

A secured visual cryptography for image steganography with compression of message image using SPIHT has been presented in this paper. It proposed a new Steganographic scheme to hide an image into a same sized cover image. Brute-force attack cannot be possible of the steganographic image with visual cryptographic technique. Combining visual cryptography with steganography resulted in a two-level security.

References

[1] M. Naor and A. Shamir, "Visual cryptography" *in Eurocrypt 94*

[2] James .C .Judge "Steganography: Past, Present, Future" *in SANS Institute Reading Room*

[3] Young - Chang Hou, "Visual cryptography for color images," *Pattern Recognition, Vol. 36, No. 7, pp. 1619 - 1629, 200*

[4] Jesalkumari Joshi and R. R Sedamkar "Modified Visual Cryptography Scheme for Colored Secret Image Sharing" *in IJCAT Vol. 2 Issue 3 Pg 350-356*

[5] M. J. Thenzhi and T . Menakadevi "A New Secure Image Steganography Using Lsb And Spiht Based Compression Method*" in IJOER Vol-3 Issue 2 March 2016 Pg 80-85*

[6] Jesalkumari Varolia "Hiding Medical Information of Patient through Image by Recursive Visual Cryptography" *in IJCA Vol 154 -No 9 , Pg 40-43 November 2016*

[7] Robert W. Floyd and Louis Steinberg, "An Adaptive Algorithm For Spatial Grayscale". *Proceedings Of The Society For Information Display 17 (2) 75-77, 1976*

[8] P. Stucki, Mecca - "A Multiple Error Correcting Computation Algorithm For Bi-Level Image Hard Copy Reproduction". *Research Report Rz1060, IBM Research Laboratory, Zurich, Switzerland, 1981.*

[9] Anuprita U. Mande, Manish M.Tibdewal "Parameter Evaluation and Review of Various Error-Diffusion Half-toning algorithms used in Color Visual Cryptography" *in IJEIT Vol 2 Issue 8 February 2013*

[10] Amir Said, William A. Pearlman, "A New, Fast and Efficient Image Code Based on Set Partitioning in Hierarchical Trees". *IEEE Transactions on Circuit and Systems for Video Technology, VOL.6, NO.3, PP.243-250, June 1996.*