Implementation of Steganography Secret Sharing approach (N,1) for Color Digital Images

M.Thaneshwari
PG Student/ECE Dept
National Engineering College
Kovilpatti

N.Arumugam
Associate Prof/ECE Dept
National Engineering College
Kovilpatti

ABSTRACT
Steganography has been considered as the solution for illicit interception and unauthorized copying of digital media. Steganography hides secret data in a host medium and conveys the hidden data. The intended recipient can then extract the secret data from the stego image. The hidden data should make a visually imperceptible change to the stego image when viewed by an unintended recipient. A remedy to achieve the imperceptibility of the stego image has been proposed, and is a concept called secret sharing. In a secret sharing approach, the sending party sends N stego images to one or multiple recipients and allows a receiving party to extract the secret data only when all N stego images are available. The (N,1) is a steganography secret sharing approach that utilises N+1 cover images. Both the sending party as well as the receiving party shares the N cover images through a secure channel. The remaining one cover image is converted to gray coded stego image at the sending party and is to be sent through an unsecure channel. The conversion is performed based on operations through the N+ 1 cover image pixels and secret data.

Keywords
Steganography, Least Significant Bit, Embedding, Extracting

1. INTRODUCTION
With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years.The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in images, video clips ,texts, music and sounds. Nowadays, using a combination of steganography and the other methods, information security has improved considerably. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging.

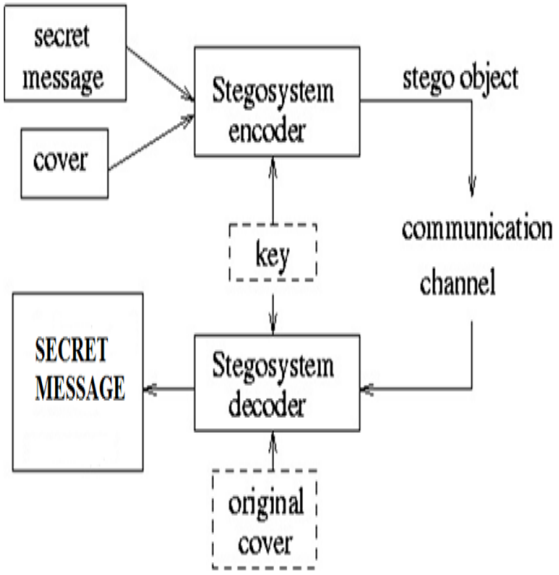

Fig 1: Steganography System Model

Steganography hides secret data in a host medium and conveys the hidden data. More importantly, it conceals the existence of data embedding and in the best case, a third party cannot recognize that both parties are communicating in a secure manner. In an image-based steganography hiding system, the original image in which the secret has to be hidden is called as cover image. The image after embedding the secret into the cover image is called as stego image. Then the intended recipient can extract the secret from the cover image.

1.1.Steganography
The steganography can be performed in four approaches. Steganography in image format, Adaptive steganography ,steganography in frequency domain and steganography in spatial domain. In this paper the spatial domain steganography is chosen. The spatial domain steganography utilizes the least significant bit. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image.The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is `11001000`, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.

1.2.Secret Sharing Approach

In (N,1) secret sharing approach hidden data makes a visually imperceptible change to the stego image when viewed at that image level for any unintended recipient. The requirement of high visual quality of the stego image creates a conflict between two performance objectives. First, the sending party has to apply the least modification to a cover image to provide high embedding efficiency. Conversely, one has to embed the maximum amount of secret data to the cover image to provide high capacity. Therefore, an acceptable compromise between high embedding efficiency and high embedding payload is made by users, depending on their different desires.

The conventional image-based hiding schemes have not been sufficient to achieve the imperceptibility of the stego image. A remedy for this has been proposed, and is a concept called secret sharing. In a secret sharing approach, the sending party sends N stego images to one or multiple recipients and allows a receiving party to extract the secret data only when all N stego images are available.

The (N,1) secret sharing approach utilises N+1 cover images. Among the N+1 cover images, the N cover images are selected and are transmitted from the sending party to the receiving party as such it is without any alteration through a secure channel. The remaining one cover image is converted to a gray coded stego image at the sending party to the receiving party. The gray code conversions are performed based on the pixels in N+1 cover images and the secret data. In this approach N number of images is chosen in which no changes are made and it is known to both the sending and receiving parties. The changes are made only in the image which is additional to that of the N cover images. That is the embedding of the secret data is done on the remaining one cover image which is not known to the receiving party and is known only to the sending party where the sending party embeds the secret data.

The N,1 secret sharing approach provides the following advantages. First, It provides high quality of the stego image since least modification is made on one of the cover images. Secondly, it fully utilises all available stego image pixels to hide the secret data that provides high embedding payload. Finally, extracting or guessing the secret data embedded in the cover image by the intruder is possible only when he knows all N cover images.

2. METHODOLOGY OF (N,1) SECRET SHARING APPROACH

The N,1 secret sharing approach involves the embedding of secret into the cover image at the sending party and the extracting of secret at the receiving party without leaving any clue to the intruder or any unintended receipient. This approach utilises Embedding and Extraction of the secret.

2.1 Embedding secret into a cover image

The embedding of secret into the original image considers N+1 cover images in which some assumptions are made. The first thing is that the N cover images are shared between both the sending and receiving party. The second thing is that both parties agree on N cover images and their before communication starts. Let CI_1, CI_2 .... CI_{N+1} ,be the selected gray images M be the secret message. The one cover image CI_{N+1} which is not known to the receiving party and only known to the sending party is converted to the stego image SI to hide the secret message M. The embedding procedure may be done as follows:

1. Exclusive-OR operation is generated with the size 2^{N+1}.

2. Exclusive-OR equality vector EQU with size 2^{N+1} is generated as follows.

The XOR of a binary value of any decimal is considered and are compared with the XOR value of gray code that matches the binary value. Then the XOR is being calculated for their values to find the EQU value as shown in Table I.

3. The following equation is performed for each image pixel CI(i,j).

XOR(Bin2Dec(LSB(CI_1(i,j))|LSB(CI_2(i,j))|....|
LSB(CI_{N+1}(i,j))))

4.The result is then compared with the secret message M(i,j). The sending party converts the cover image CI_{N+1} to stego image SI depending on the equality of two values. Then the corresponding EQU value is checked.

If(XOR(Bin2Dec(LSB(CI_1(i,j))|LSB(CI_2(i,j))|
...|LSB(CI_{N+1}(i,j))))=M(i,j))
If(EQU(Bin2Dec(LSB(CI_1(i,j))|LSB(CI_2(i,j))|
...|LSB(CI_{N+1}(i,j))))=0)
LSB(SI(i,j)) = LSB(CI_{N+1}(i,j))
else

LSB(SI(i,j))=1scomplement(LSB(CI_{N+1}(i,j)))
else
If(EQU(Bin2Dec(LSB(CI_1(i,j))|LSB(CI_2(i,j))|
...|LSB(CI_{N+1}(i,j))))=0)

LSB(SI(i,j)=1scomplement(LSB(CI_{N+1}(i,j)))
else
LSB(SI(i,j)) = LSB(CI_{N+1}(i,j))

5. Finally the Stego image SI is sent to the receiving party.

Table I Generation of EQU vector

Decimal	Binary	XOR	Gray	EQU
0	0000	0	0000	0
1	0001	1	0001	0
2	0010	1	0011	1
3	0011	0	0010	1
4	0100	1	0110	0
5	0101	0	0111	0
6	0110	0	0101	1
7	0111	1	0100	1
8	1000	1	1100	1
9	1001	0	1101	1
10	1010	0	1111	0
11	1011	1	1110	0
12	1100	0	1010	1
13	1101	1	1011	1
14	1110	1	1001	0
15	1111	0	1000	0

2.2. Extraction of secret from the Cover image

The secret message can then be extracted from the cover image by the receiver. The receiving party knows the N cover images which are identical to those of the sending party. The N cover images are not affected by the equality between the XOR vector values and secure message bits at the sending party. Only the one cover image which is not known to the receiving party is being altered. The extraction may be carried out as follows

1. Exclusive-OR resultant XOR vector is generated with size 2^{N+1}.

2. The gray code to corresponding binary code conversion for each image pixel is calculated by the following equation.
$Gray2Bin(LSB(CI_1(i,j))|LSB(CI_2(i,j))|\ldots|LSB(CI_N(i,j))|LSB(SI(i,j)))\rightarrow B_1(i,j)|B_2(i,j)|...|\ B_N(i,j)|\ B_{N+1}(i,j)$

3. The secret message M is constructed.
$M(i,j)=XOR(B_1(i,j)|B_2(i,j)|...|\ B_N(i,j)|\ B_{N+1}(i,j))$

3. EXPERIMENTAL RESULTS

The Stego object was generated by embedding the text message into cover image using spatial domain technique in MATLAB environment and the performance of the stego image was also calculated. The embedding and the extraction is performed with the help of software and their PSNR value is being calculated.

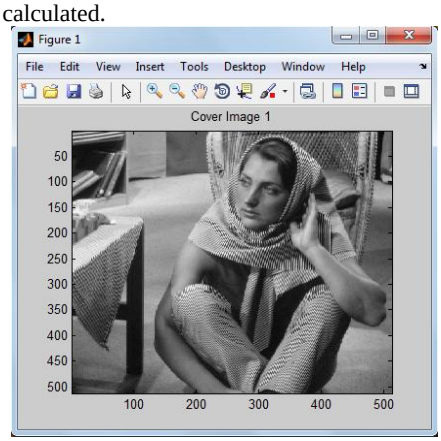

Fig 2 Cover Image 1

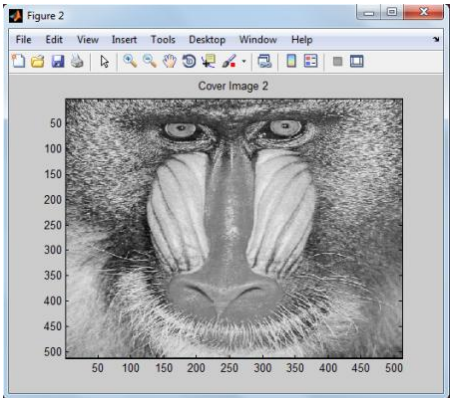

Fig 3 Cover Image 2

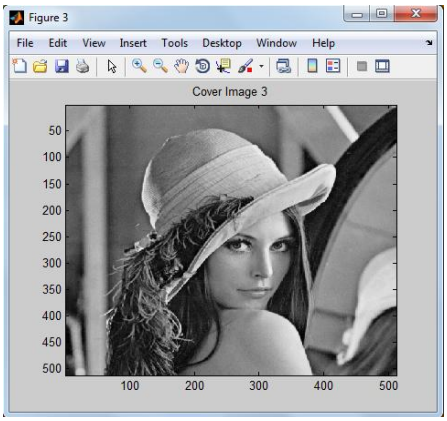

Fig 4 Cover Image 3

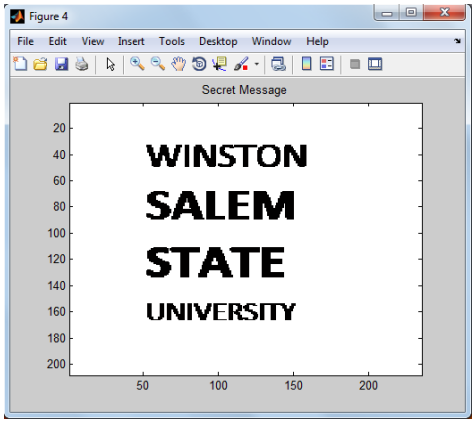

Fig 5 Secret Message

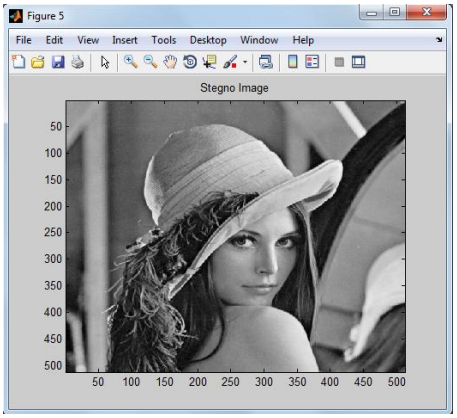

Fig 6 Stego image

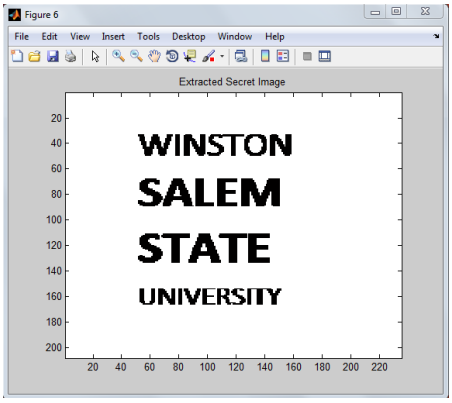

Fig 7 Extracted Secret Message

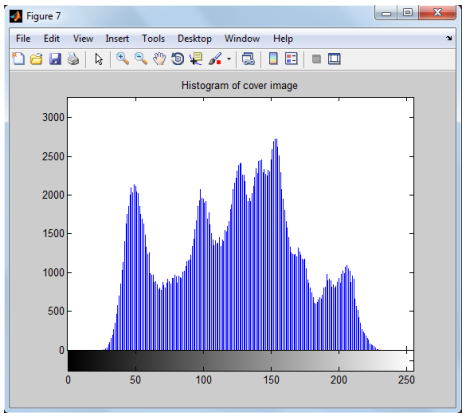

Fig 8 Histogram of cover image

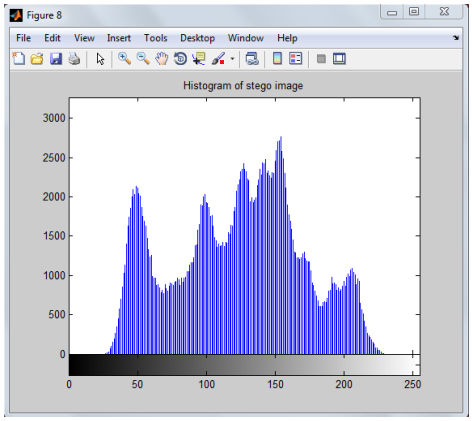

Fig 9 Histogram of stego image

From the result, it is shown that Fig 2 & 3 represents the cover image or the original image which both parties share. Fig 4 is the cover image in which the secret is to be hidden and it is not known to the receiver. Fig 5 is the secret message that is going to be embedded in the cover image shown in Fig 4. Fig 6 shows the stego image that is obtained after embedding the secret message into the cover image shown in Fig 4. Figure 7 Shows the image after extraction from the stego image. Fig 8 shows the histogram of the cover image before embedding and Fig 9 shows the histogram of the stego image after embedding the secret into it. The histograms of both the cover image and the stego image before and after embedding resembles with each other. The PSNR value may be calculated and are shown that

BARBARA IMAGE

PeakSNR =

Inf

Mean2err =

0

BABOON IMAGE

PeakSNR =

Inf

Mean2err =

0

LENA IMAGE

PeakSNR =

58.0004

Mean2err =

0.0936

4. CONCLUSION

So far I have shown the embedding on images using (N,1) sharing approach which involves N number of cover images that remains unchanged and are known to both the parties and one image that is considered to be as the stego image where embedding is being done. The Embedding and Extraction of the secret message is being done and the PSNR value is also calculated for the stego image with the help of MATLAB. The stego image resembles the same as that of the one before embedding. Later the FPGA may be implemented to embed and the extract the secret message into the cover image and their PSNR values are calculated and are compared with that of the software estimation.

5. REFERENCES

[1] Chan, C. C. and Hwang, R. J. 1998. Sharing Secret Images using Shadow Codebooks in Information Sciences, 111(1-4): pp 335-345.

[2] Chang C.-C., T. D. Kieu, and Y.-C. Chou 2008, 'A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images', Proc. of the 2008 International Symposium on Electronic Commerce and Security, pp.16-21.

[3] Feng J. B., H. C. Wu, C. S. Tsai, and Y. P. Chu 2005, 'A New MultiSecret Images Sharing Scheme Using Largrange's Interpolation', Journal of Systems and Software,76(3), pp.327- 339.

[4] Kim C., E.-J. Yoon, Y.-S. Hong, and H. 1. Kim 2009, 'Secret Sharing Scheme Using Gray Code based on Steganography' Journal of the Institute of Electronics Engineers of Korea, 46(1), pp.96-102.

[5] Lin C. C., and W. H. Tsai 2004, 'Secret Image Sharing with Steganography and Authentication', Journal of Systems and Software, 73(3), pp.405-414.

[6] Miche Y., P. Bas, A. Lendasse, and C. Jutten 2009, 'Reliable Steganalysis Using a Minimum Set of Samples and Features', EURASIP Journal on Information Security, DOI:IO.1155/2009/901381.

[7] Provos N., and P. Honeyman 2003, 'Hide and Seek: An Introduction to Steganography', IEEE Security and Privacy, 1(3), pp. 32-44.

[8] Sallee P. 2004, 'Model-Based Steganography' LNCS, Vol. 2939, pp. 254-260.

[9] Sharmir A. 1979, 'How to Share a Secret', Communications of the ACM, 22(11), pp.612-613.

[10] Solanki K., A. Sarkar, and B. S. manjunath 2008, 'YASS: Yet Another Steganographic Scheme That Resists Blind Steganalysis', LNCS, Vol. 4567, pp. 16-31.

[11] Thien C. C., and J. C. Lin 2002, 'Secret Image Sharing', Computers and Graphics, 26(1), pp.765-770.

[12] Westfeld A. 2001, 'F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis' LNCS, Vol. 2137, pp. 289-302.

[13] Westfeld A., and A. Pfitzmann 1999, 'Attacks on Steganographic Systems', LNCS, Vol. 1768, pp. 61-76.

[14] Zhang W., S. Wang, and X. Zhang 2007, 'Improving Embedding Efficiency of Covering Codes for Applications in Steganogrphy', IEEE Communications Letters,11(8), pp.680-682.