Improved FPGA based X-Box Mapping of an Image using Steganography Technique

Puja Mahajan
BE Student E&TC Dept.
JSPM'S BSIOTR
Wagholi, Pune

Prajakta Nimbalkar
BE Student E&TC Dept.
JSPM'S BSIOTR
Wagholi, Pune

Pratiksha Pawar
BE Student E&TC Dept.
JSPM'S BSIOTR
Wagholi, Pune

ABSTRACT
Image steganography is a method of keeping the data in another image that will be recognized only by the recipient who will be receiving this data. No one is able to treasure the original data, only recipient can. Here, an improved version of X- box mapping for an image using steganography technique is presented[1]. Steganography is the way of keeping data or information in an image which cannot be seen by naked eyes. Only the recipient knows where the data is. Least Significant-Bit (LSB) is most famous technique used in steganography techniques as it is easy and has large covering capacity. X-Box technique is only used for inserting different values. In this mapping method, X-Box will give safety of values and these values will be stored in random manner and that cannot be detected.

Keywords
Steganography technique, X-Box mapping method, Stego image, LSB Technique, Information Hiding.

1. INTRODUCTION
Now a day, it is easy and best method to transmitted any data using digital service, as Internet technology are increasing every day. But these message or information must keep secure and preserved from hacker by using proper security method over Internet[4]. It is very essential to protect message while transmitting them through Internet. Cryptography is method where message content is hiding and one cannot understand it. Whereas Steganography hides both message and its existence in image, audio, video, etc [5].

Here, image steganography is used, to hide message in an image. Steganography is the art and science of invisible communication. Steganography, word came from Greek ("stegos" = cover and "grafia" = writing)[5]. The main objective of Steganography is to hide secret information in cover media (may be image/ audio/ video etc..) in such way that no one can detect its presence in cover media, only receiver can know its existence. The purpose of Steganography is to maintain secret

communication between two parties. Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication. It comes under the assumption that if the feature is visible, the point of attack is evident, thus applications. The basic structure of Steganography is made up of three components: the carrier, the message, and the key. In this generation, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Fig.1.shows block diagram of Steganography technique.

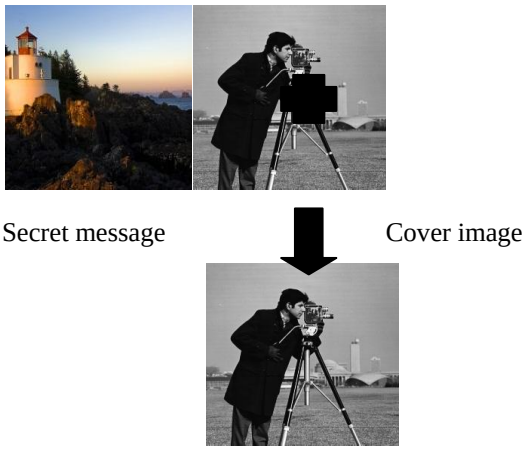

Fig.1.1. Block diagram of Steganography technique

2. RELATED WORK
Least significant bit (LSB) Steganography [2, 3, 4, 5, 6] is the most frequently used and simple method to embed the information in a cover file. It maintains the image quality and requires no complex operations. It embeds bits of the secret message into the LSB plane of the cover image. LSB matching (LSBM), LSBM revised (LSBMR) and Edge adaptive based LSBMR steganography techniques are the popular image Steganography methods.

Capacity, Security, and Robustness are the three main parameters affecting the Steganography. Capacity refers to the amount of the data bits that can be hidden in the cover image. Security is related to the ability of an eavesdropper to figure the hidden message easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

2.1 PSNR (Peak Signal to Noise Ratio)
The measurement of the quality between the cover Image and stego -image g of sizes N x N shown in figure 1 is defined as[2]:

PSNR=10xlog (2552 / MSE)

Where

$$MSE = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}(f(x,y)\ \ g(x,y))^2/N^2$$

Where f(x,y) and g(x,y) are the pixel value at the at position (x, y) in the cover-image and the corresponding Stego image respectively. The PSNR is expressed in dB. The larger PSNR value indicates the higher image quality i.e. There is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR indicates that there is huge distortion between the cover-image and the stego-image.

3. PROPOSED ALGORITHM

The system is based on the different values of X-boxes mapping [4].

3.1 Encoding Of Image

3.1.1. Generation of X-boxes

2x 2 matrixes are used in which 16 (0 to 15) values are stored as shown below [2]

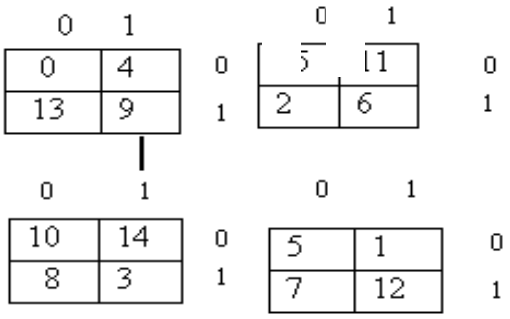

Fig.3.1. Mapping of X-boxes

Here, for mapping of X-boxes , the property of X-OR is used. Properties of X-OR: 0 XOR 0 = 0 , 1 XOR 1 =0 and 0 XOR 1 = 1 , 1 XOR 0= 1.For eg., 5 is placed to one of the X-Boxes as shown:5=0101= 01 XOR 01= 00. Hence, the position of 5 is 1st row and 1st column.

3.1.2. Bit Division

Now, we take cipher image of ant dimension let take 64X64.Now, we convert the values from decimal to binary.

Just map these values of b1, b2, b3, b4 from X-Box.Take b1=10, then we search the value of 1st row and 1st column of X-Box.After mapping, the value (13)10 =(1101)2

Similarly, mapping values of b2, b3, b4 are obtained as 11, 14, 1 resp.

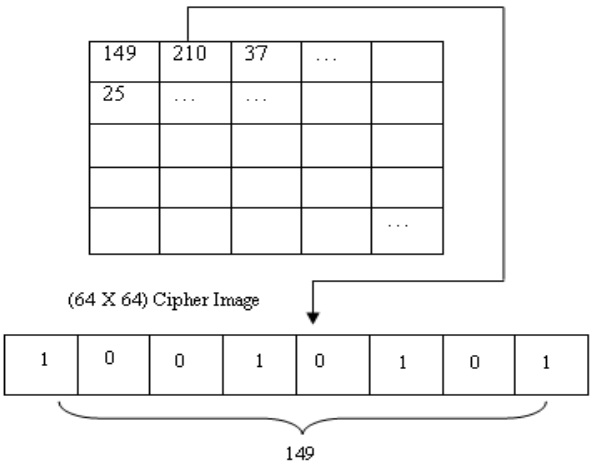

Fig.3.2. Bit Division

Now, divide this 8bit values into 4parts taking 2 bits in each.

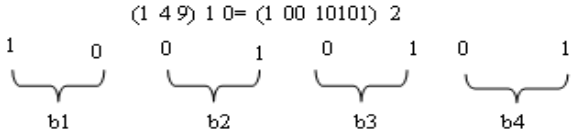

Fig.3.3. X-Box Mapping

3.1.3. Bit insertion into the cover image:

After getting the new mapping values, insert these values into the cover image. Placed these values into the 4 bit LSB of cover image sequentially. First, take the pixels one by one from the cover image. The 4 LSB bits are replaced by 13, 11,14,1 respectively.

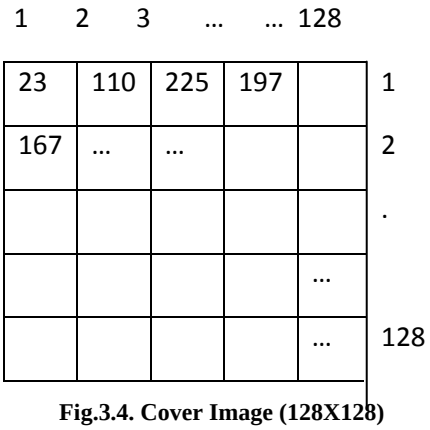

Fig.3.4. Cover Image (128X128)

Here, take the pixels sequentially.

(23)10 = (00010111)2&(110)10 = (01101110) 2

(225)10 = (11100001) 2&(197)10 = (11000101) 2

3.1.4. Formation of Stego image [8]:

After getting the new pixel values, the stego image is formed. The pixel values 29, 107, 239, 193 are placed into the position of the previous values. Similarly, take the pixels one by one and insert the cipher image into them and replaced them. Thus, the Stego-image is created.

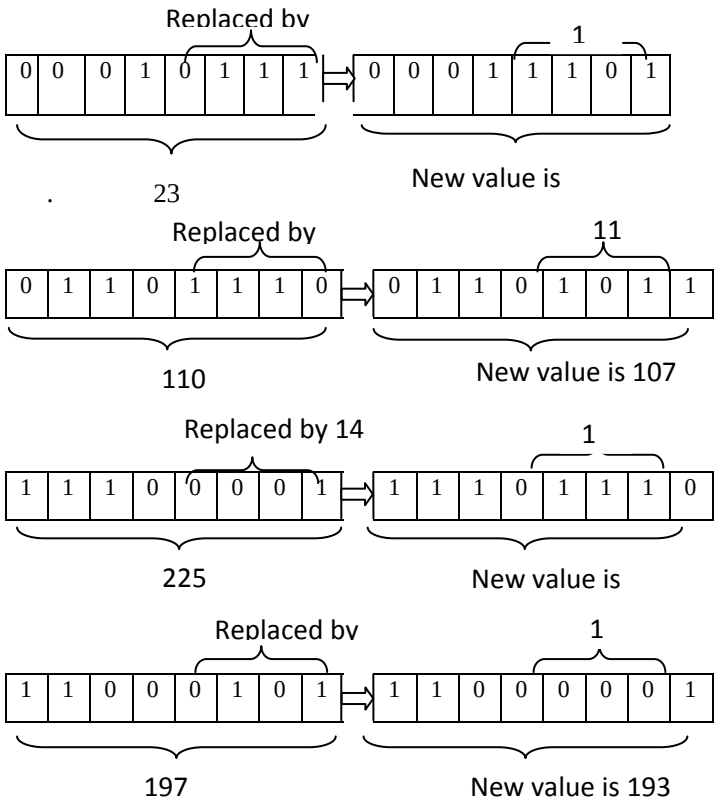

Fig.3.5. Bit insertion to the cover image

These Stego image content the cipher image but can't be recognize the cipher image. The changes of the pixel values will be varied from 0 to 15 which is a negligible amount of pixel value. So the pixel values or colors will not be change in large amount.

3.2 Algorithm of Encoding

Input: A gray level cipher image of size (mxn), a gray level cover image of size (2mx2n).

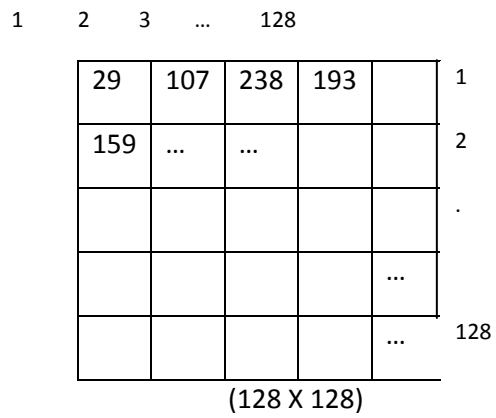

Fig.3.6. Stego image

Output: Stego Image of size (2mx2n)

Steps:

1. Cipher image pixel is divided into 4 parts containing 2 bits.
2. To get new values, these values are mapped into 4 X-Boxes in random manner.
3. These values are inserted into LSB position of cover image.
4. End

3.3 Decoding of Image

For decoding the stego image from cover image at receiver, follow these steps:

3.4 Generation of 4LSB bit from Stego Image

One by one pixel will be taken from the stego image. We will be getting 4LSB bits and convert it to binary values.

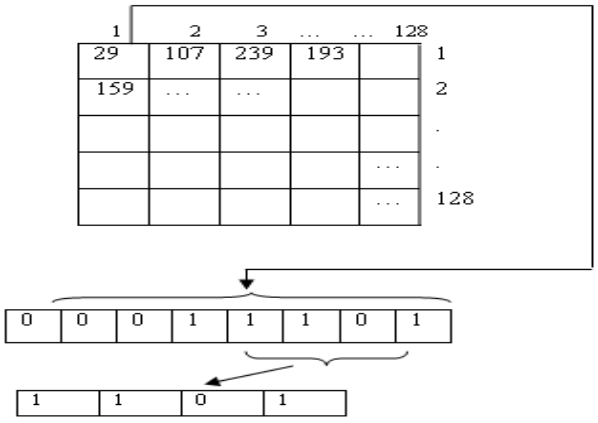

Fig.3.7.Extraction of Stego Image

Also take other three pixels:

$(29)_{10}= (00011101)_2$

$(107)_{10}= (01101011)_2$

$(239)_{10}= (11101110)_2$

$(193)_{10}= (11000001)_2$

LSB1= 1101; LSB2=1011;

LSB3= 1110; LSB4= 0001;

3.5 Retrieve the inserted bits of cipher image

Take 4 LSB bit of the stego image that are 1101, 1011, 1110, 0001; then XOR operation is performed of 4 bits.

First, 2 bits and XOR with other 2 bits

LSB1=1101=11 $\oplus$ 01=10

LSB2=1011=10 $\oplus$ 11=01

LSB3=1110=11 $\oplus$ 10=01

LSB4=0001=00 $\oplus$ 01=01

3.6 XOR Operation Concatenation With Result

Concatenation of 4 results is done and 8 bits are obtained.

These 8 bits are converted to decimal values.

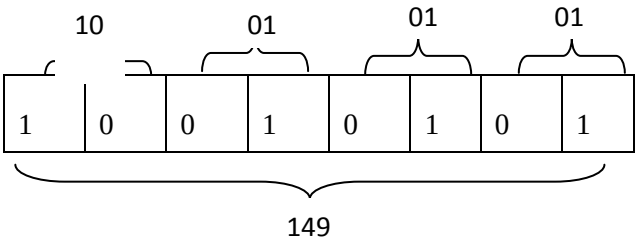

Fig.3.8. XOR operation concatenation with result

3.7 Cipher image Generation:

The generated value is placed into first position. In the same way, take the stego image values and repeat the algorithm steps and will be getting 210, 37 etc.

3.8 Algorithm of Decoding

Input: Stego Image (2mX2n)

Output: Grey –Level Cipher Image of (mxn)

Steps:

1. Select pixel of the Stego-Image and take 4 bits from LSB position.
2. Perform XOR operation and concatenate four result
3. Pixels values of the cipher image are placed
4. End

4. EXPERIMENTAL RESULT AND SECURITY ANALYSIS

4.1 Result

This method increases the embedding capacity of the system by as embedding bits are 2 in cipher image into 4 bit in cover image. Coding these 2 bits by again mapping into another

form. By this no one can find that anything is embedded in that and also mapping will be totally unknown to anyone except the two parties who are communicating. Extraction of image will be difficult**.**

(a) (b)

Fig.4.1.(a)Cover Image and (b) Stego Image of camera man of X-box mapping.

Table.4.1.Predicted Values

Image Name	Size (Pixel)	Capacity (%)	PSNR (in dB)
Camera man.jpg	64	25	+36.17
Lena.jpg	64	25	+34.98
Desert.jpg	64	25	+36.42
Jellyfish.jpg	64	25	+35.29

NOTE: User can also use their own image and the value of PNSR can changed depends upon Quality of Image.

5. CONCLUSION

Earlier, hiding image was done by Steganography technique. Some paper also used same technique but their efficiency and security was low.

Inthis paper, ımproved FPGA based X-BOX mapping for an Image using Steganography technique is presented. Here, main aim is given to improve the security of image and also its quality. Also, to improve the security by embedding the information pixel in cover image in random manner which no one can extract without stego key. This technique can be strongest Steganography technique than normal LSB encoding technique. The user can choose any image for covering purpose.

After comparing this result with earlier method, it gives improved PSNR and also its security. This can be very useful in military applications, net banking and also for commercial purpose where secret communication is necessary.

Here, only the one who have key can able to detect the information from the stego image and one else.

6. ACKNOWLEDGEMENT

We put on record and warmly acknowledge the constant encouragement, Invaluable supervision, timely suggest and inspired guidance offered by our guide Prof. P.R.Shah, Head of Department of Electronics and Telecommunication Engineering, JSPM'S BhivarabaiSawant Institute of Technology and Research this report to a successful Completion.

We are grateful to him for permitting us to make use of the amenities presented in the department to carry out the project successfully. Last but not the least we communicate our sincere thanks to all of our friends who have patiently comprehensive all sorts of help for accomplish this undertaking.

Finally, we extend our gratefulness to Prof. P.R.Shah, and all those who are directly or indirectly involved in the winning completion of this paper work.

7. REFERENCES

[1] Bin Li, Ming Wang, Xiaolong Li, Shunquan Tan, Jiwu Huang "A Strategy of Clustering Modification Directions in Spatial Image Steganography", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 10 (9) (2015) , pp.1905-1917.

[2] EktaDagar, Sunny Dagar, "LSB Based Image Steganography Using X-Box Mapping", International Conference on Advances in Computing, Communications and Informatics (ICACCI), (2014) 351-355.

[3] Mr.Jagdish .D.H, Mrs. Manjula.Y., Dr. M.Z.Kurian, "FPGA Implementation of X-BOX for an Image Steganography Technique", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engg., Vol-2, Issue 6, June 2013.

[4] Amitava Nag, Swati Ghosh, SushantBiswas, DebashreeSarkar, ParhaPratimSarkar, " An Image Steganography Technique using X-Box Mapping", IEEE- International Conference on Advances in Engg., Science and management(2012) 709- 713.

[5] Morland .T., "Steganography and Steganalysis", Leiden Institute of Advanced computing Science, www.liacs.nl/home/tmoerl/private.pdf.

[6] BassamJamilMohd., Saed Abed and Thaier Al-Hayajneh, Sahel Alouneh, "FPGA Hardware of the LSB Steganography Method", 978-1-4673-1550-0/12/$31.00©2012 IEEE.