International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

Design and Implementation of an Image Steganography technique using X-Box Maapping on FPGA

Aniket kulkarni
M. Tech, Dept. of ECE, TOCE, Bangalore

Mrs. Sheela.c
Asst. Prof, Dept. of ECE, TOCE, Bangalore

***Abstract*-Image steganography is a technique of hiding an information into the cover image.LSB (Least Significant Bit) is the most popular method for this technique. This paper presents a simple technique for performing the stegnography which is based on the LSB using the X-box mapping. Here we have used several different X-Boxes that all have different and unique data The embedding part of this is done by the steganography algorithm where we have used four unique X-Boxes which have sixteen various values. Mapping provides large amount of security to the payload the reason is without knowing the key nobody can identify the information.**

***Keywords*-Steganography, X-Box, Least Significant Bit,**

I. INTRODUCTION

As the internet technologies development increasing, the transmission of the digital data is very convenient these days. But the secret information transmitting on the internet is not a safe task now a days. So because of the above reason transmitting the data on the internet has became an important as well as the risky. So it will be a clever task if an information is hidden into an other information and so that nobody can guess that anything is hidden in the information. Hence the idea gives a result called steganography which is the one of the method of information hiding. The word steganography in the Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing") . The main objective of steganography is to hide the secret information inside no harm cover media in such a way that the secret message is not visible to the observer. Thus the stego image should not diverge much in information from the original cover image. In this generation, steganographiy is most widely used on computers with digital data being the carriers and networks being the high speed delivery channels. Figure.1 shows the simple block diagram of a simple image steganographic system. The complete work is performed on the FPGA and simulation is done to get the results.In this Paper MATLAB is also used to generate output values for the sake of simulation. Encoding and the Decoding alfgorithms have been used for work.

II. BLOCK DIAGRAM

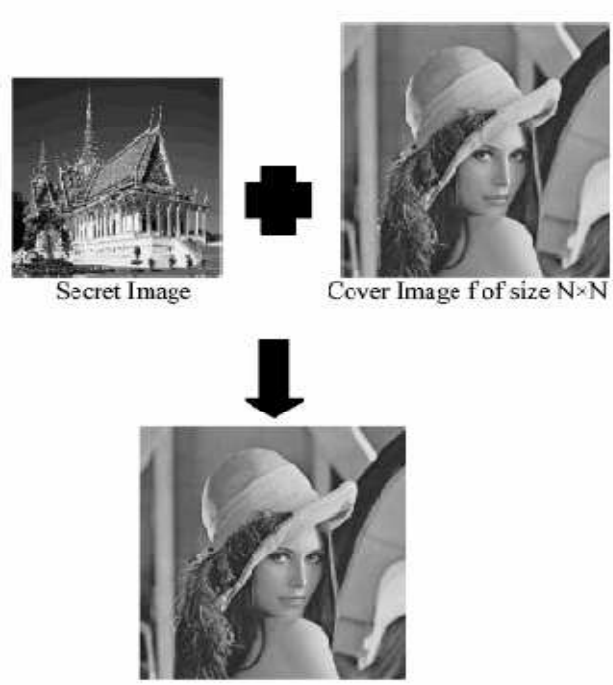


Figure 1. simple block diagram of image steganography

The above block diagram shows simple technique of image steganography. Where the secret image and its data is hided into the cover image where the size of the cover image is 2 times larger than the secret image.The operation is performed on the FPGA.

III. WORKING PROCEDGURE

Least Significant Bit (LSB) Based image steganography is very widely used and well known method for the information hiding technique. This method preserves the quality of the image and doesn't require any difficult operation.

There are three parameters such as Security, Robustness and the Capacity. Capacity explains that the amount of data that can be stored into the cover image. Security relates to the amount of knowledge that information is hiden that can be

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

figured out. Robustness descript the ability to modify or destroying that hidden information

3. IMAGE STEGANOGRAPHY ALGORITHM

The image steganography algorithm is divided into two parts one called encoding and other decoding. where several x-boxes with unique data have been used.

3.1 IMAGE ENCODING

3.1.2 Generation of four different X-Boxes

Here x-boxes means the x-or boxes which are 2x2 matrix of ,where sixteen values resulting from 0 to 15 are stored

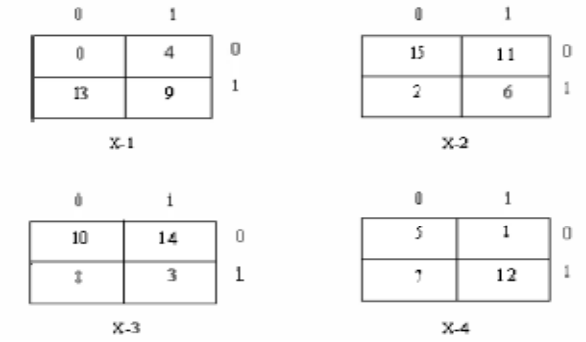


Fig 1.2 X-Mapping boxes

.For inserting the values into these boxes x-or property is used

0 XOR 0=0
0 XOR1 =1
1 XOR1 =0
1 XOR 0=1

Lets consider 13 for example
13=1101=11 XOR 01= 01
Thus 13 position in the above boxes is 2nd row and 1st column.

3.2 BIT DIVISION

Now, we will take the cipher encrypted image
Which having pixel size of 64x64
Now, values to be converted fro m decimal to binary

The first pixel value of the secret image is say 149
Binary Equivalent is $(149)_{10}=(10010101)_2$

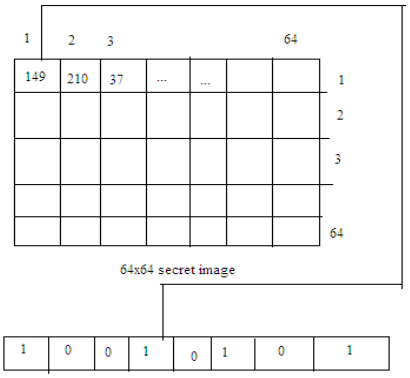


fig 1.3 Bit Division

Now, we will divide the value of * bit into the four parts by taking each as 2 bits.

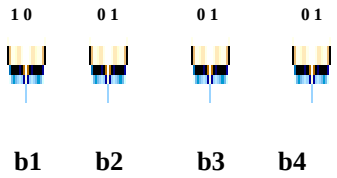
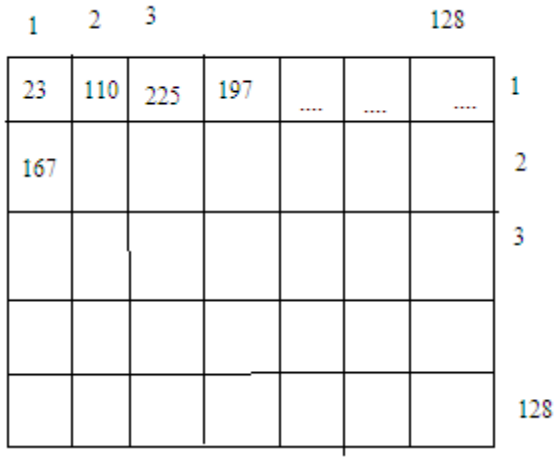


Fig 1.4 x-box mapping

Similarly we map for the other values $\mathbf{b_1}\,\mathbf{b_2}\,\mathbf{b_3}$ and $\mathbf{b_4}$
First we take the value of b_1= 10
Now we search the value of the 1st row and 0th column of the first x-box.
We got 13=(1101) as the value of the b1
Similarly we will apply for all the three remaining b2 b3 and the b4 and we wil get the following values 11,14.1 respectivly.

3.3 Insertion Of The Bits Into Cover Image

After generating the new mapping values we will now insert these values by taking last four bits of these secret image bits into the last four bits of the cover image to generate the new values for the stego image .the last four bits of the cover image are replaced by the 13,11,14,1.



(128x128) cover image
Fig .1.4

$(23)_{10}=(00010111)_2$

$(110)_{10}=(01101110)_2$

$(225)_{10}=(11100001)_2$

$(197)_{10}=(11000101)_2$

The above values are the pixel and binary equivalent of the cover image .now we will insert the lasrt four bits into the cover image values in the following way.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

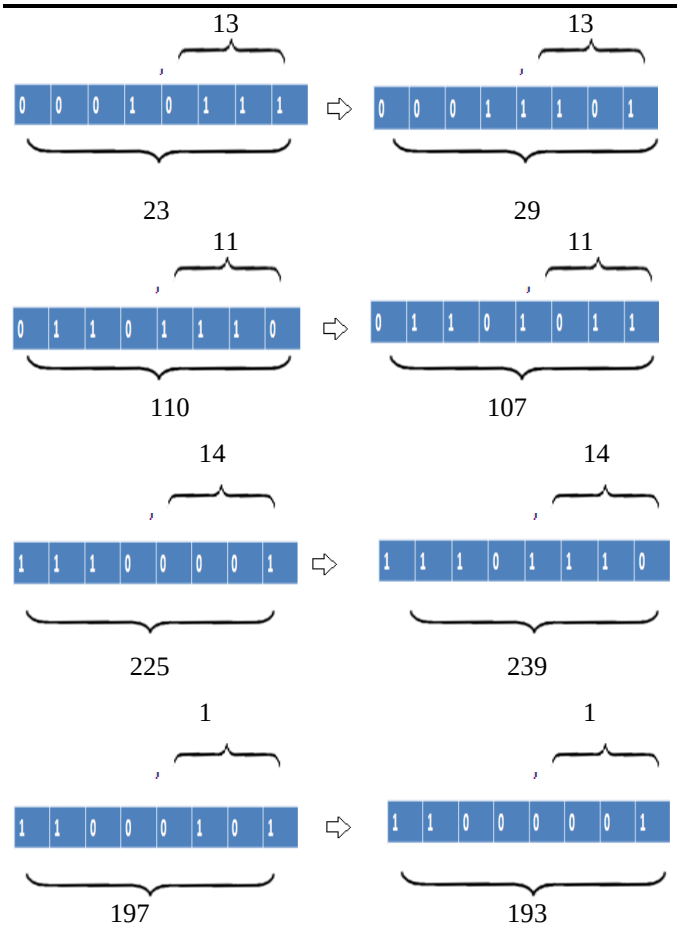
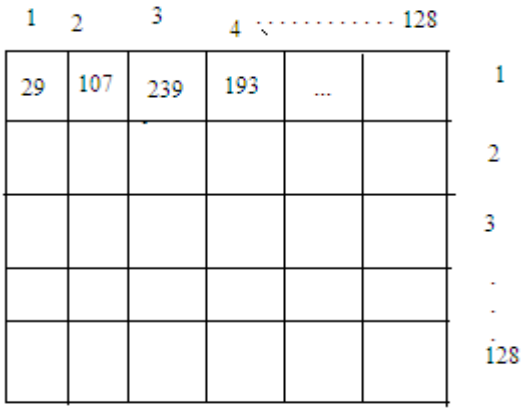


Fig 1.5 insertion of bits into cover image

3.4 Formation Of Stego Image

After generating the new pixel values which are as 29,107,239,193 will be placed into the position of the earlier values this procedure is followed for all the remaining values to get the stego image

The following figure will show the stego image.



(128x128) Stego Image
Fig 1.6

The above stego image consist of the secret image information but nobody can identify that .The changes in the pixel values are varied by the 0 to 15 which is in a small amount hence the data will not change much

Encoding algorithm

Input: a gray secret image.

Output: a cover image of 2 times larger than secret.

Steps

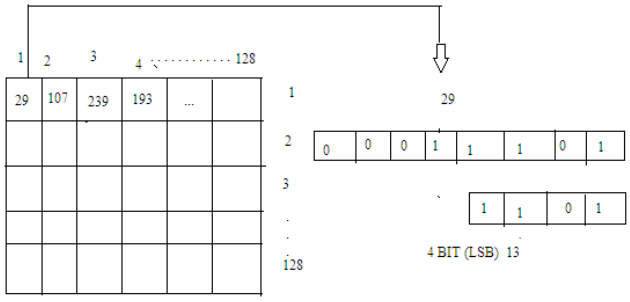
1. Deviding the secret image pixel value into 4 parts of the 2bits each.
2. Generating the new values by mapping the 4 parts into the x-boxes
3. Inserting the values of the last four bits of the cover image.
4. End

IMAGE DECODING

For converting the stego image into the original imagr that is to perform decoding the following steps are used.

3.6 Generating the 4LSB bits from the stego image

The stego image contains the pixel value now we will take these pixel values one after another to get the the by converting it into the binary.



(128X128) Stego image

Fig 1.7 4bit LSB extraction from stego image

Accordingly we will take the similar values for the remaining 29,107,239and 193.

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

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

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

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

LSB1 = 1101; LSB2 = 1011; LSB3 = 1110; LSB4 = 0001;

3.7 RECOLLECTING THE INSERTED BITS OF THE SECRET IMAGE

Here we take the 4 LSB bits of the stego image which are 13,11,14,1 and we will perform the xor operation of the 4 bits by taking the 2 bits and we will perform xor.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

Lsb1 = 1101 = 11 EXOR 01 = 10;

Lsb2 = 1011 = 10 EXOR 11 = 01;

Lsb3 = 1110 = 11 EXOR 10 = 01;

Lsb4 = 0001 = 00 EXOR 01 = 01;

3.8 RESULT OF THE XOR OPERATION

After getting the each 2 bits of the xor operation we will take these 8 bits and then it will form the pixel value of the secret image.and the decimal value is 149 which is pixel value of secret image.

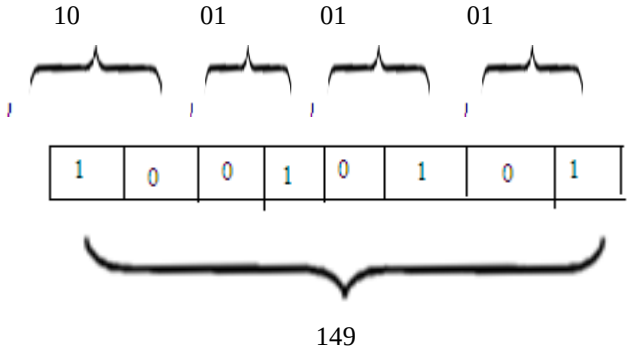
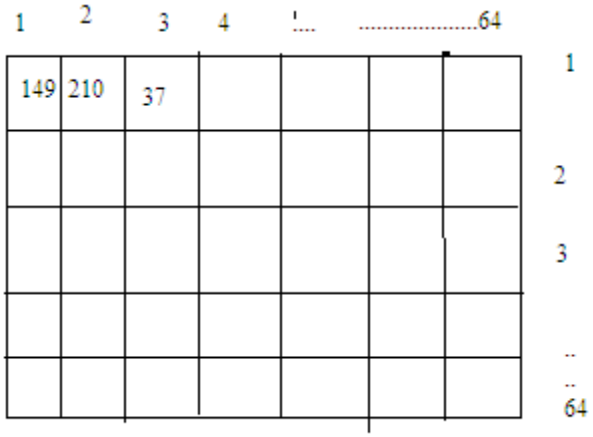


Fig 1.8 Result of the X-or operation

3.9 GENERATION OF THE SECRET IMAGE

After getting the xor operation result we will place these values in the 1st position. S ame work will be carried out for all the remaining values to get the secret image.



(64x64) secret image

Fig .1.9

The above process is called steganography by using x-boxes.

IMAGE DECODING ALGORITHM

Input: stego image of 128x128
Output: generating secret image
Steps:
1 Take 4 bit of the pixel value of the stego image
2 performing X-or operation to get the two bit values to generate the secret image pixel value
3 Finally we will get the pixel value of secret image.
4 End

VI. EXPERIMENTAL RESULT

The technique of embedding the secret imsge into the cover image is no doubt a strongest steganogarphy technique because one can understand that something is hidden but the key and technique will be completely unknown to him The results are obtained for the encoding and decoding part by simulating. The total design is designed in VHDL and simulated by XILINX

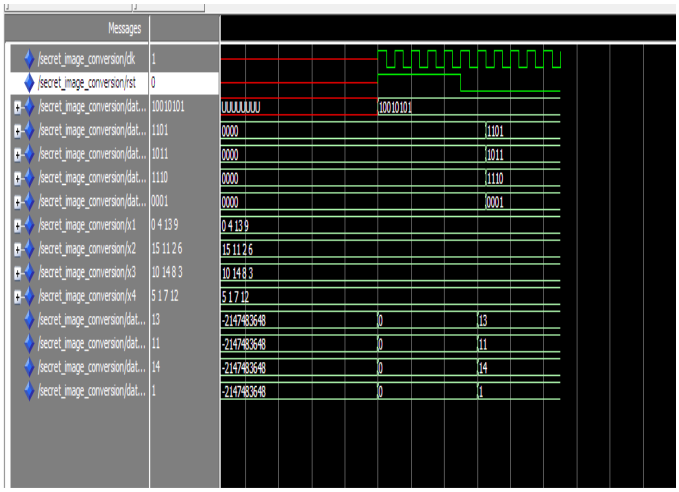


Fig 1.10 simulation of the secret image

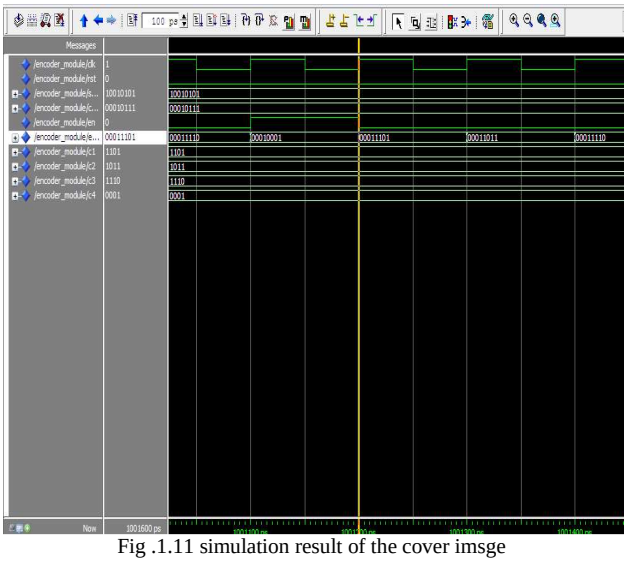


Fig .1.11 simulation result of the cover imsge

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 5, May2014)

Simulation result for the decoding

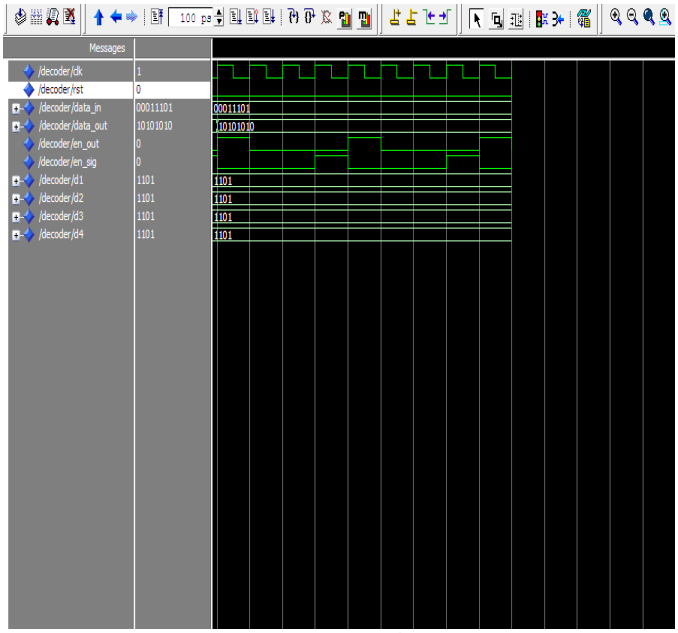


Fig .1.12 simulation result of the decoding

MATLAB RESULTS

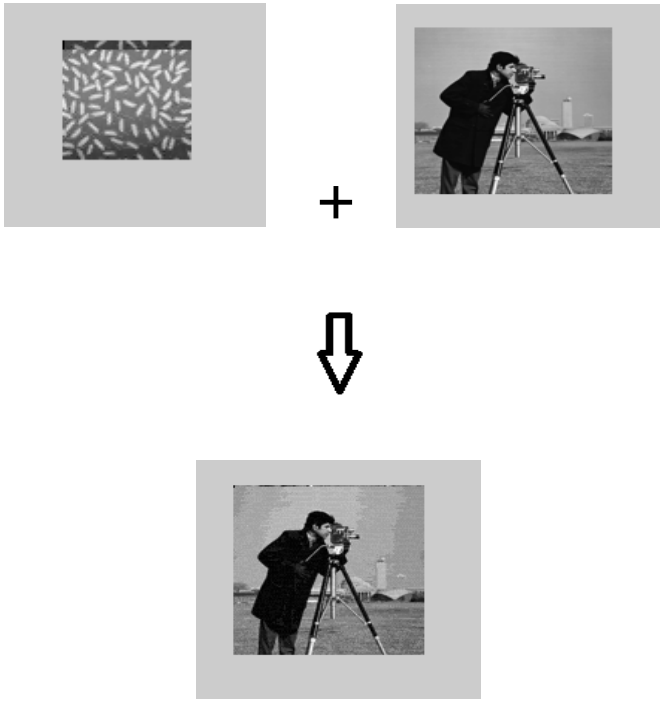


Fig1.13 Matlab result of the secret image and cover image and stego image

VII. CONCLUSION

In this paper, we present the method of steganography which is based on the mapping .This technique gives a secure way of transmitting the data o n the internet. This method is better because in this method nobody can recognize that something is embedded, even if one can fin out that something is embedded without stego key nobody can extract the information.

REFERENCES

[1] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on Isb matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010) 201-214.

[2] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM*, 47:10, October 2004

[3] Moerland, T, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ trnoerl/privtech.pdf.

[4] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", *Signal Processing : Image Communication 20, 2005, pp. 624–642*

[5] Mohammad Shirali-Shahreza , “A new method for real time steganography”, *ICSP 2006 Proceedings of IEEE* .

[6] Hide & Seek: An Introduction to Steganography: Niels Provos and Peter Honeyman, IEEE Security & Privacy Magazine, May/June 2003. http://niels.xtdnet.nl/papers/practical.pdf.

[7] Introduction to steganography, Brigitte Si Athabasca University, COMP607 Project, July, 2004 http://io.acad.athabascau.ca/~grizzlie/Comp607/menu.htm