ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
*Vol. 2, Issue 6, June 2013*

# FPGA IMPLEMENTATION OF X-BOX MAPPING FOR AN IMAGE STEGANOGRAPHY TECHNIQUE

**Mr.Jagadeesha.D.H[1], Mrs.Manjula.Y[2], Dr.M.Z.Kurian[3]**

M.Tech[DE], Dept of E & C, SSIT, Tumkur ,India[1]

Assistant Professor, Dept. of E&C, SSIT, Tumkur,India[2]

HOD, Dept. of E & C,SSIT, Tumkur, India[3]

**ABSTRACT**: In this paper I have implemented FPGA based steganography technique based on x-box mapping. Image steganography is a method of hiding the information in a cover image in such a way that only intended recipient can know that there is a hidden message. Least Significant-Bit (LSB) based approach is most popular steganographic techniques in spatial domain due to its simplicity and hiding capacity. This paper presents a new technique based on LSB for Image steganography using X-box mapping where we have used several Xboxes having unique data. The embedding part is done according to the X-boxes and this technique give more security to the secret information without knowing the mapping rules no one can extract the secret data.

**Keywords:** Steganography, X-Box, LSB Technique, Information Hiding.

## I.INTRODUCTION

Image steganography is a method of hiding the information in the cover image  Steganography, the word steganography is coming from the Greek words. stegos, means covered and the graphia  means writing, it is the art and science of hiding the message in such way that only recipient can know the their is a exists of the message . Using this method, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are very closely related. Cryptography hides the content of the  messages so they cannot  understand. Steganography on the other hand, will hide the both content of the message and also the existence of the message. In some situations, sending an encrypted message will arouse suspicion while an “invisible” message will not do so. Both sciences can  combine to produce good protection of the message. when the steganography fails and the message can be detected, it is still of no use and it will be similar to encrypted using cryptography techniques. The principle defined  by Kerckhoffs for cryptography, also holds good for steganography.The quality of a cryptographic technique should only depend on a small part of information, that is secret key. The same is valid for steganographic technique: knowledge of the system that is used in these technique, should not give any information about the existence of secret messages. Finding a message should only be possible with knowledge of knowing the secret key or stego key.

As the development of Internet technologies increases, the transmission of digital media is now-a-days convenient over the networks. But secret message transmissions over the Internet system suffer from serious security overhead. So, protecting of secret messages during transmission becomes an important issue In this generation, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Figure.1 shows the block diagram of a simple image steganographic system.

Fig.1 The block diagram of a simple image steganographic system.

Fig.1 The block diagram of a simple image steganographic system.

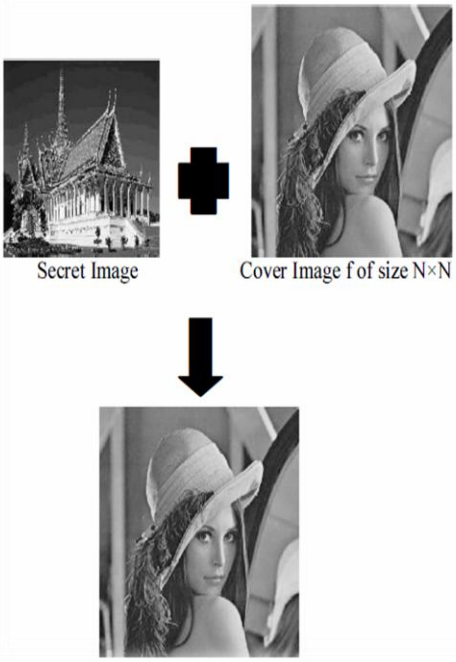


Fig.1 The block diagram of a simple image steganographic system.

## II. RELATED WORKS

Least significant bit (LSB) insertion is a common, simple approach in the image steganography technique. In this method embedding information in a cover image in such a way that The least significant bit (the 8th bit) of some or all of the bytes inside cover image is changed to a bit of the secret message. 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,and it is embedded into the least significant bits of this part of the cover image, the resulting grid is as follows:

(0010110**1** 0001110**1**1101110**0**)

(1010011**0** 1100010**1**0000110**0**)

(1101001**0** 1010110**0**01100011)

Although the number was embedded into the first 8 bytes of the grid, only the three underlined bits needed to be changed according to the secret message. On average, only half of the bits in an image will need to be modified to hide a secret message and it requires maximum cove size. Since there are 256 possible intensities of each primary color, changing the least significant bit of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye ,thus the secret message is successfully hidden. With a well chosen image, even we can hide the message in the least as well as second to least significant bit and still not see the difference. In the example discussed above, consecutive bytes of the image data – from the first byte to the end of the message – areused to embed the information. This approach is very easy to detect the secret message. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. It should an adversary suspect that LSB steganography has been used, no one has way of knowing which pixels to target without the secret key. LSB matching (LSBM),LSBM revised (LSBMR) [2] and Edge Adaptive based LSBMR [3] steganography techniques are popular LSB like steganography methods.

## III. PROPOSED IMAGE STEGANOGRAPHY

**Image Encoding:** This technique is based on mapping of different values from x-boxes.

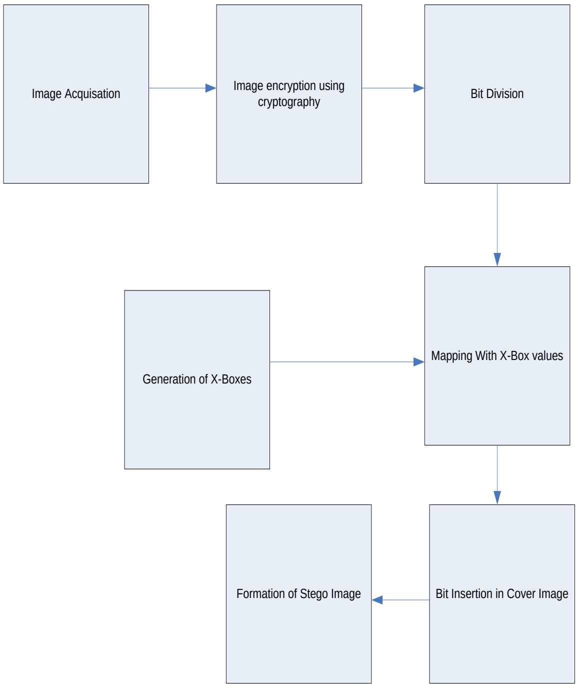
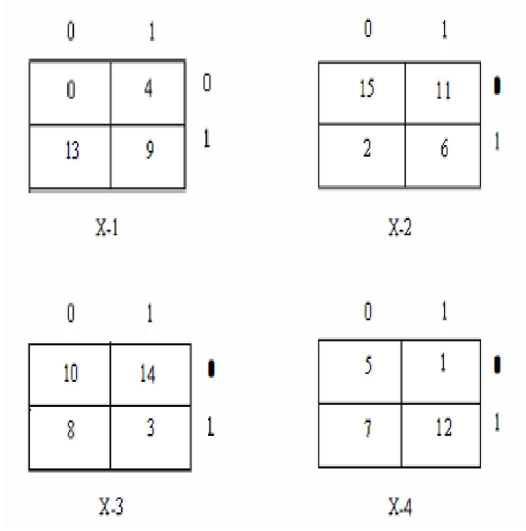


Image Acquisation
Image encryption using cryptography
Bit Division
Generation of X-Boxes
Mapping With X-Box values
Formation of Stego Image
Bit Insertion in Cover Image

Fig1.1Block diagram of Encoding of Steganography.

**Generation of four different X(X-OR)-boxes:** X-Boxes are a 2x2 matrix, where 16 (0 to 15) values are stored as given fig[5].



| 0 | 1 | |
|---|---|---|
| 0 | 4 | 0 |
| 13 | 9 | 1 |

X-1

| 0 | 1 | |
|---|---|---|
| 15 | 11 | ▮ |
| 2 | 6 | 1 |

X-2

| 0 | 1 | |
|---|---|---|
| 10 | 14 | ▮ |
| 8 | 3 | 1 |

X-3

| 0 | 1 | |
|---|---|---|
| 5 | 1 | ▮ |
| 7 | 12 | 1 |

X-4

Figure1.2 X- Boxes

To put values in X-boxes, we use X-OR property: o XOR 0 = 0 , 1 XOR 1 =0 and 0 XOR 1 = 1 , 1 XOR 0= 1.
For example 13 is inserted in any one of the four X-Boxes as follow: 13=1101=11 XOR 01=10 Thus the position of 13 is 2nd row and 1st column.
**Bit Division:**Then, we need to take the cipher encrypted image; say with dimension 64x64. Now, we convert the values from decimal to binary. For example, Thefust pixel value of the encrypted image=149 Then, binary of

$(149)_{10}=(10010101)_2$

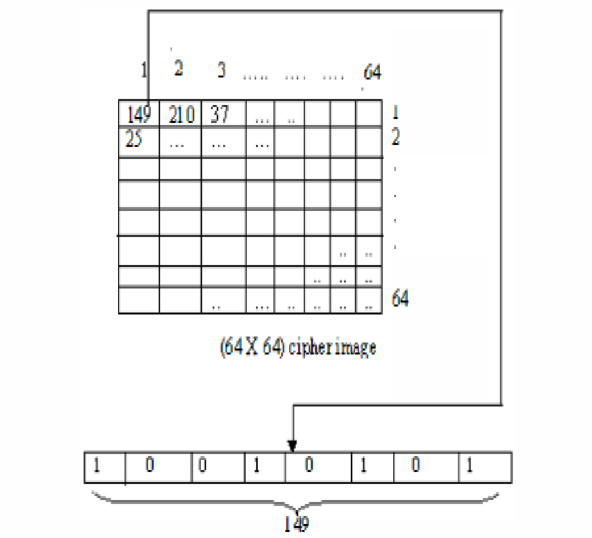
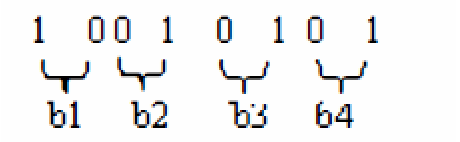


Figure 1.3 bit division.

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

$(149)_{10}=(10010101)_2$



**X-box Mapping:**Now we just map the values of b1 ,b2 , b3 ,b4 from the X-mapping box. First we take b1 =10; Then we search the value of 1st row and O th column of the X-I box; After mapping we get the value $(13)_{10}=(1101)_2$ Similarly we get mapping values for the b2,b3, b4;We get in the same way 11,14,1 sequentially.

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

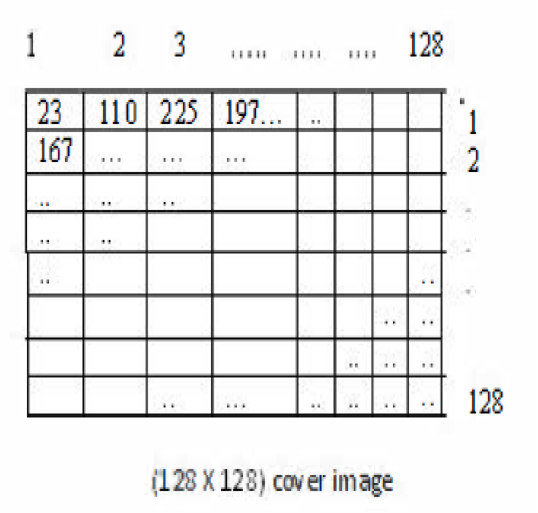


Figure 1.4 cover image.

Here we take the pixels sequentially.

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

$$(110)10 = (01101110)\ 2$$
$$(225)10 = (11100001)\ 2$$
$$(197)10 = (11000101)\ 2$$

**Formation of Stego image:**After getting the new pixel values we form the stego image. The pixel values 29, 107, 239, 193 are placed into the position of the previous values. Similarly we take the pixels one by one and insert the cipher image into them and replaced them. Thus we get the Stego-image

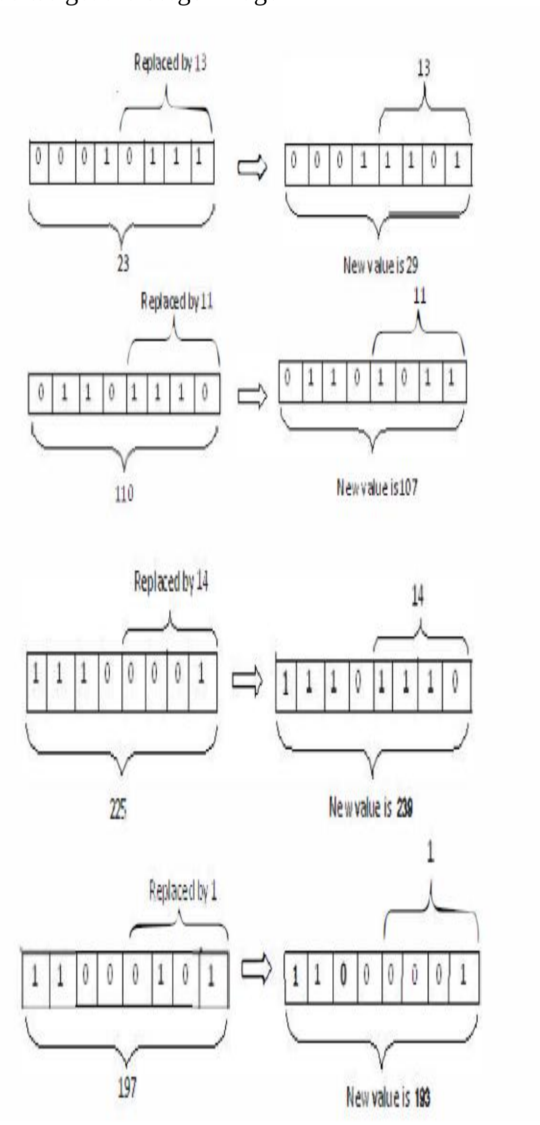


Figure 1.5 Bit insertion to the cover image

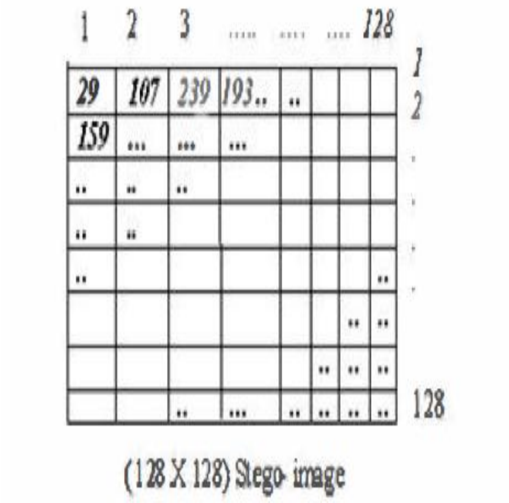


Figure 1.6 Stego image.

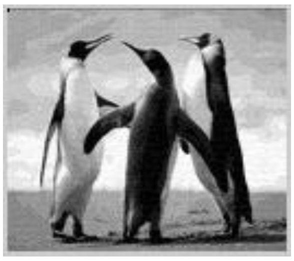
These Stego image content the cipher image but we cannot recognize the cipher image. The changes of the pixel values will be varied from 0 to 15 which is a negligible amount of pixel value. So the pixel values or colors will not be change in large amount.

## IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this we will discuss the experimental results along with the security analysis.This embedding technique is no doubt a strongest Steganography technique than normal LSB encoding technique.Because, we embed each 2 bits of Cipher Image into the 4 bit of Cover Image. Again before insertion we coded these two bits by some mapping box into another form. So if one can understand that something is embedded in it, but the mapping will be totally unknown to him. So to extract the image is really a tough job.

SECRET IMAGE

COVER IMAGE



STEGO IMAGE

The PSNR that I have getting for some images

| image | Capacity | Size(pixel) | PSNR(db) |
|---|---|---|---|
| Lena.jpg | 25% | 64 | 31.11 |
| Cameraman.jpg | 25% | 64 | 31.78 |
| Koala.jpg | 25% | 64 | 31.87 |
| Penguin.jpg | 25% | 64 | 31.80 |

## V. CONCLUSION

In this paper, I have implemented a mapping based steganography process by using FPGA to improve security and image quality compared to the existing algorithms. Our approach is better because without stego key, no one can extract the original information from the stego-image, For purposes of secret communication which is more important.

## REFERENCES

[1] J.R.Krenn.“Steganography and Steganalysis”
[2] S-FChiou “An efficient reversible data hiding scheme based on SMVQ”.
[3] Sivaranjani “Edge adaptive image stegnography based on LSB matching revisited”.
[4] Yan -ping Zhang, Juan Jiang, Chao Xu, Bo Hua “A new scheme for image hiding based on digital images” .
[5] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar“An Image Steganography Technique using X-Box Mapping”

## BIOGRAPHY

**Mr.Jagadeesha DH** currently pursuing his Post graduate degree in digital elecronics from Sri Siddhartha Institute of Technology, he received his Bachelor degree in Electronics and Communication Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, India. His research interests are in the areas of steganography

**Mrs.Y.Manjula G** got her Post Graduate Degree in digital electronics from Visvesvaraya Technological University, Belgaum, Karnataka, India. Currently working as Asst. Professor in the department of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India,Her research interests are in the areas of VLSI Architecture and Implementation for 3-D Neural network based image Compression, Tolaration of Fault in Encoder and Decoder of Nano Memory using EG-LdPC, Edge Detection on HAAR Wavelet, steganography She has published and presented papers in various international journals and several national and international conferences.

**Dr.M.Z.Kurian** received his Bachelor from Bangalore University and Post graduate degree in Industrial Electronics from Mysore University, and Ph.D degree in Software Engineering from Dr.MGR University, Chennai, Tamil Nadu, India. He has more than 30 Years of Teaching in the field of Electronics & Communication Engineering. Published several papers in peer reviewed international journals including IEEE, and several conference papers.