International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

FPGA Implementation of Secured Image STEGNOGRAPHY based on VIGENERE CIPHER and X BOX Mapping Techniques

Aniketkulkarni
M.Tech, TOCE
aniketoxc@gmail.com

Sheela .c
Asst.Prof, TOCE

DhirajDeshpande
Asst .prof ,BKIT

Abstract: **Image steganography is a method of concealing information into a cover image to hide it by encrypting the secured image using the vigenere cipher algorithm. Least Significant-Bit (LSB) based approach is most popular steganography techniques in spatial domain due to its simplicity and hiding capacity. This paper presents a novel technique for Image steganography based on LSB using X-box mapping where we have used several Xboxes having unique data. The embedding part is done by this Steganography algorithm where we use four unique X-boxes with sixteen different values (represented by 4-bits) and each value is mapped to the four LSBs of the cover image. This mapping provides sufficient security to the payload because without knowing the mapping rules no one can extract the secret data (payload).the previous methods for image steganographic are designed by using matlab. Here the proposed system is implemented on FPGA.**

INDEX TERMS : Steganography, veginere cipher X-Box, LSB Technique, Information Hiding

I. INTRODUCTION

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. Though cryptography changes the message so that it cannot be understood but this can generates curiosity level of a hacker. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden there or not. This idea results in steganography, which is a branch of information hiding by camouflaging secret information within other information. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing") . The main objective of steganography is to hide a secret message inside harmless cover media in such a way that the secret message is not visible to the observer. Thus the stego image should not diverge much from original cover image .In this generation, steganography is mostly use don computers with digital data being the carriers and networks being the high speed delivery channels. Figure.1shows theblock diagram of a simple image steganographic system.

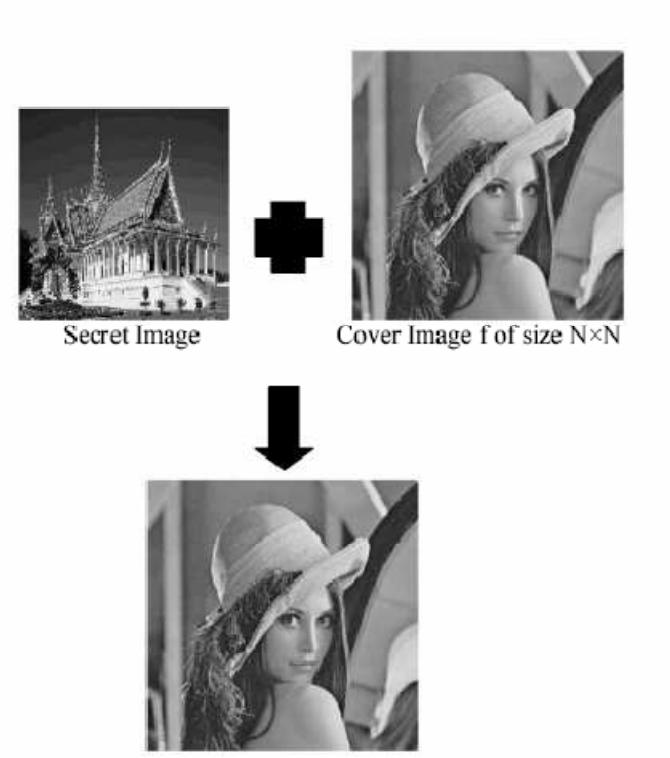


Figure. 1 The block diagram of a simple steganographic system

Least significant bit (LSB)steganography is the common and simple approach to embed information in a cover file. It reserves the image quality and requires no complex operation. It embeds bits of a payload into the LSB plane of a cover image. LSB matching (LSBM), LSBM revised (LSBMR) and Edge Adaptive based LSBMR steganography techniques are popular LSB like steganography methods.

Capacity, security and robustness are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the abilityof an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data. Invisibility, Robustness against statistical attacks, Robustness against image manipulation, Independent of file format, unsuspicious files

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Invisibility– The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised

Robustness against statisticalattacks– Statistical stegnoanalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a
mark in the image as be statistically significant.

Robustness against image manipulation– In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image

Independent of file format– With many different image file formats used on the Internet, it mightseem suspicious that only one type of file format is continuously communicated between two parties.The most powerful steganographic algorithms thus possess the ability to embed information in anytype of file. This also solves the problem of not always being able to find a suitable image at the rightmoment, in the right format to use as a cover image.

Unsuspicious files – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

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

PSNR=10xlog(255^2/MSE)

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

Where f(x,y) and g(x,y) means 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 indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego-image.

II. THE VIGENERE CIPHER

To encrypt, a table of alphabets can be used, termed a *tabula recta*, *Vigenère square*, or *Vigenère table*. It consists of the alphabet written out 26 times in different rows, eachalphabet shifted cyclically to the left compared to the previous alphabet, corresponding tothe 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point dependson a repeating keyword.

The key:A sequence of characters. To make brute-force decryption impractical, the key should have at least 15 or 16 characters. Also, it should not be a"special" sequence. such as an English language word. It maybe best if all letters of the key are distinct. *Encryption:* Duplicate the key as many times as necessary, so that thelength of the (duplicated) key matches the length of the plaintext

For i = 0, 1, 2, 3, ...

"Add" letter i of the key to letter the i of the plaintext, toobtain letter i of the ciphertext.(In adding letters, we identify them with integers modulo
26: **a** → 0, **b** → 1, ...,**z**→ 25.)

Example:
key: **wonderland** *(10 characters, not an ideal key)*
plaintext:**alicewasbeginningtogetverytiredof**
key (duplicated): **wonderlandwonderlandwonderlandwon**
ciphertext

WZVFINLSOHCWAQMERTBJAHIHVPEIEHZCS

We obtained letter 5 the ciphertext like this:
w→ 22
+ **r**→ +17
N ← 13 (mod 26)

The 463 character plaintext

```
alicewasbeginningtogetverytiredofsitting
byhersisteronthebankandofhavingnothingto
doonceortwiceshehadpeepedintothebookhers
isterwasreadingbutithadnopicturesorconve
rsationsinitandwhatistheuseofabookthough
talicewithoutpicturesorconversationsoshe
wasconsideringinherownmindaswellasshecou
ldforthehotdaymadeherfeelverysleepyandst
upidwhetherthepleasureofmakingadaisychai
nwouldbeworththetroubleofgettingupandpic
kingthedaisieswhensuddenlyawhiterabbitwi
thpinkeyesranclosebyher
```

encrypts using the key **wonderland** to

```
WZVFINLSOHCWAQMERTBJAHIHVPEIEHZCSVMKEIAJ
XMUHVJTSGHNCAWLVMAANWBQRJYLVVQCBBWLZYGGR
ZCBQGVZRGZEQRVLVSAQSASCHHZYTBWDSORSBSEEV
EGGHVNLSEHWRVQKSFTVWDOQQSGTCGXNSFRVTZNIH
NGNWMFYSVQEHNQHNSAGLOHUHYJPOSDXCBNXYZUTK
POYLGVHIGKKIGSMTEUEHOCEPSEGEEVWHVRRJZSUH
SOFFSEDIQHNWAJMESEERSBZLRULSJHHZNVWYPCBX
HRSRVKSEURPRNBQROEUHNTRHPMPRLVHSRSCRYDFW
QDVGAYPTUHNHUHTCPAFXNSBIQRVIAJWRNLWPNHNL
JKBXPUMEJRNHUWLVERBXXZRRJXPTGLJUHSEEOPVF
GWAJXYPDNLOWRVAYPNFXZRRQPPLWULPSEDFSTTJL
PVCLRBPYRVNOAFPFDEOBDSE
```

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

III. ALGORITHM

Our proposed steganographic technique is based on mapping the different values from X-boxes

Image Encoding

Generation of four different X(X-OR)-boxes

X-Boxes are a 2x2 matrix, where 16 (0 to 15) values are stored as given below.

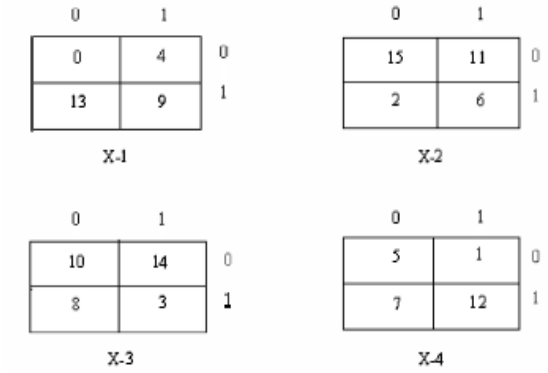


Figure l.l: X-Mapping Boxes

To put values in X-boxes, we use X-OR property:
0 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,
The first pixel value of the encrypted image=149
Then, binary of $(14\ 9)_{10}=(10010101)_2$

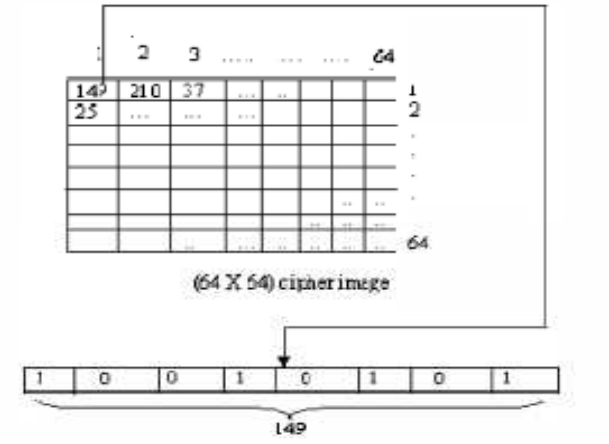


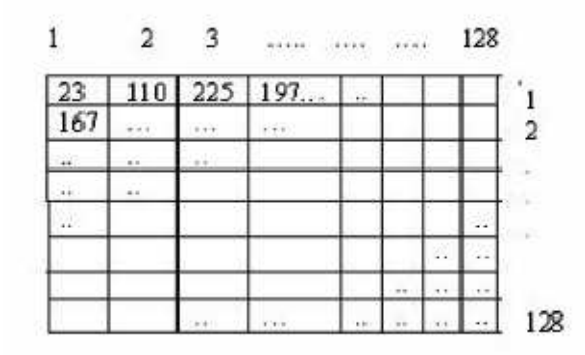
Figure 1.2: Bit Division

Now, we need to divide this 8 bit values into 4 parts taking 2bits in each.
$(14\ 9)_{10}=\{10010101\ )_2$

10 01 0101

b1 b2 b3 b4

Now we just map the values of b1,b2,b3,b4 from the X-mapping box.
First we take $b_1=10$;
Then we search the value of 1st row and 0 the column of the X-I box
After mapping we get the value $(13)_{10}=(1101\ )_2$
Similarly we get mapping values for the b_2 , b_3,b_4
We get in the same way 11,14,1 sequentially



(128x128) cover image
Figure 1.3

Here we take the pixels sequentially

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

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

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

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

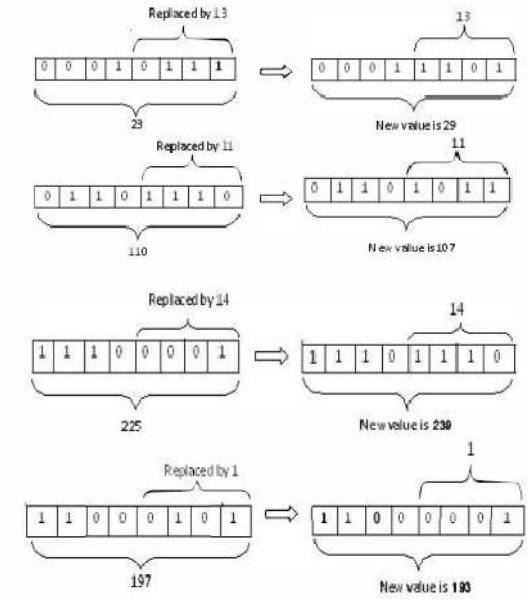
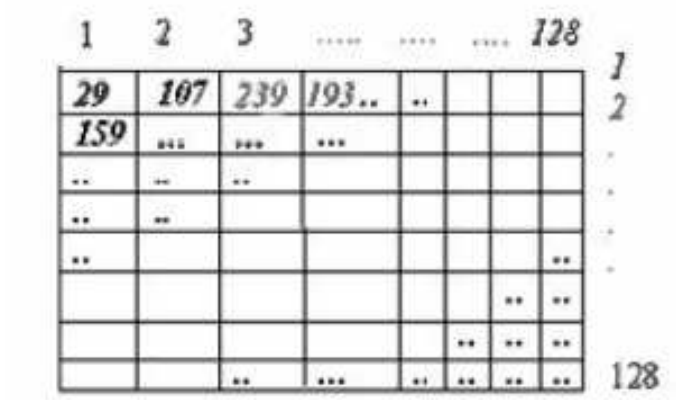


Figure 1.4 Bit Insertion into Cover Image

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

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 themand replaced them. Thus we get the Stego-image.



(128x128) stego image
Figure 1.5

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.

Encoding Algorithm

Input: A grey-level Cipher image of size (m x n), A grey level
Cover Image of size (2m x 2n);
Output: Stego Image of size (2m x 2n);
Steps:
1. Divide the each pixel of the cipher image into 4 parts containing 2 bits.
2. Map these 4 parts into the 4 X-boxes and get the new values for each part.
3. Insert these values into the LSB position of the Cover image one by one.
4. end.

IV. IMAGE DECODING

To decode the stego image in the receiver side we just perform the following steps:

Generate the 4LSB bit s from the Stego image:

We take the pixels one by one from the stego image.Transfer it into the binary values and get the 4 bits (LSB)values from it.

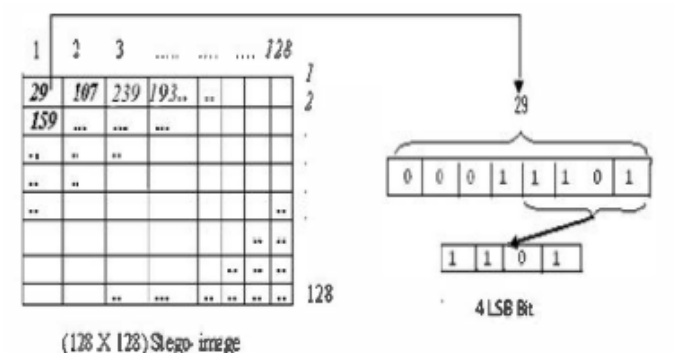


Figure l.6: LSB (4 bits) Extraction of Stego-Image

Similarly we take the other three pixels. That is 107, 110, and 97.

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

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

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

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

LSBI =1101; LSB2=1011; LSB3=111O; LSB4=0001

Retrieve the inserted bits of cipher image:

We take the 4 LSB bit of the stego image that are 11011011, 1110,0001; then we perform the XOR operation ofthe 4 bits. First we the 2 bits, and we do the XOR operation with the other 2 bits.

LSB1=1101=11 ⊕ 01=10

LSB2=1011=10 ⊕ 11=01

LSB3=1110=11 ⊕ 10=01

LSB4=0001=00 ⊕ 01=01

Concatenation of the result of the XOR operation

Now we concatenate the 4 results of the XOR operation. After that we get the 8 bits. Then from them we transfer it into the decimal value .Concatenated value is:

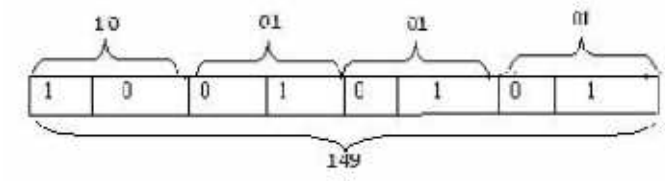
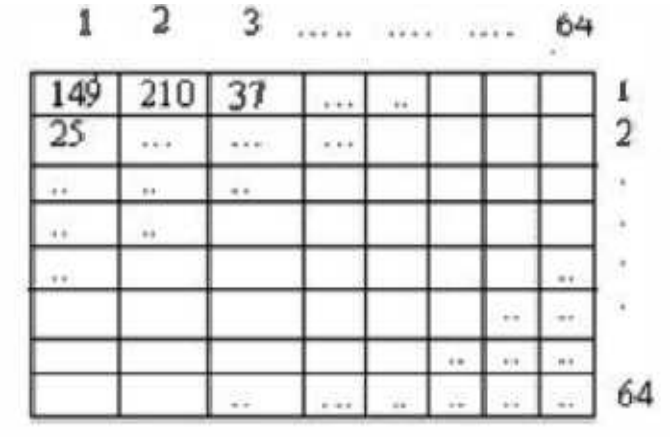


Figure l.7: Concatination the results ofXOR operation

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Generation of cipher image

Now the generated value is placed into the first position .Similarly we take the next value of the stego-image andrepeat the steps 1 to 4. And we get the 210, 37 etc .Ultimately we get the total cipher image



(64x64) cipher image
Figure 1.8: (64 x 64) Cipher Image

These are the total process of the X-box Steganographic. Now let's see the algorithm of that particular method.

Decoding Algorithm

Output: A grey-level Cipher image of size (m x n);
*Input:*Stego Image of size (2m x 2n);

Steps*:*

1) Select each pixel of the Stego-image and take 4 Bits from LSB position.
2) Perform the XOR operation of that 4 bit LSB and concatenate the four results.
3) Ultimately we get the pixel value of the cipher image and place one by one to get a cipher image.
4) end.

V. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

We will discuss the experimental results along with the security analysis.

Experimental Results:

This embedding technique is no doubt astrongestSteganography technique than normal LSB encodingtechnique. Because, we embed each 2 bits of CipherImage into the 4 bit of Cover Image.Again before insertionwe coded these two bits by some mapping boxinto 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 tough job.

Figure 1.9: (a) Cover Image and (b) Stego Image of Lena

of X-mapping box.

Security analysis

As we see here in the Stego Image there is no such abroad distortion. Seeing this image no one can recognizethat some secret image is embedded in it. We can say thatjust seeing its PSNR table given below.

IMAGE NAME	Size (Pixel)	CAPACITY (%)	PSNR in (dB)
Lena.jpg	64	25%	+34.17
Baboon.jpg	64	25%	+33.98
Cameraman.jpg	64	25%	+35.42
Plane.jpg	64	25%	+35.29

Table.10.1Capacity and PSNR of different messages

VI. CONCLUSION

In this paper, we propose a mapping based steganographic process 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]. Cryptography of the Vigenère Cipher, Fall 2006 Chris Christensen MAT/CSC 483
[2]. Steganography based on Adaptive Embedding of Encrypted Payload in Wavelet domainInternational Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012
[3]. Digital Image Steganography: Survey and Analysis of Current Methods]
[4]. http://www.hubblesite.org/sci.d.tech/behind_the_pictures/
[5]. http://heritage.stsci.edu/commonpages/infoindex/ourimages/color_comp.html
[6]. SteganographyAn Art of Hiding Data, ShashikalaChannalli et al /International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141