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

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Secure Steganography Approach using 2 X-Box Mapping Technique

Namrata S. Malge[1], Alaknanda S. Patil[2]

PG Student [VLSI & Embedded System], Dept. of E&TC, PVPIT, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of E&TC, PVPIT, Pune, Maharashtra, India [2]

ABSTRACT: The incredible evolution of Internet technologies & its applications requires high level of security for data over the unsecured communication channel. This paper presents steganography technique using 2 x-box mapping technique. Image steganography is a skill 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 common Steganographic techniques in spatial domain due to its simplicity and robustness, hiding embedding capability. In this paper a new technique is implemented based on LSB for Image steganography using 2 X-box mapping. In an existing method for hiding the secret data in the LSB substitution method four X-boxes are used to hide two secret bits in each pixel of the cover image. In this method using two X-boxes, 4 bits of secret message is hidden. This enhances the security of the secret message, with no movement of the PSNR value of the cover image. .

KEYWORDS: Steganography, 2 X-Boxes, LSB Technique, information Hiding, network security.

I.INTRODUCTION

Due to copyright violation, counterfeiting, forgery, and fraud, transmitting the digital data in open networks such as the Internet is not consistently safe. Thus, for protecting the secret data many approaches are forward for protecting essential digital data [5]. Cryptographic methods are used for transmitting the secret data encrypted by cryptosystems and used for secret communication. The meaningless form of the encrypted data may draw the thought of hackers. This confidential data can be protected by using information hiding techniques such as watermarking and steganography, which hides the secret information into a cover object and create an embedded object. Figure 1 shows a basic steganography model.

Watermarking is used for screen monitoring, copyright defence, tracking transaction and similar activities. In contrast, steganography is used primarily for secret communications. This method invisibly alters a cover object to mask a covert message. Thus, it can hide the very existence of concealed communications. For further protection, a cryptographic technique is used before embedding process [3]. Image steganography techniques are further classified into Image Domain and Transform Domain [6]. In image domain embedding process is done by using its pixel intensity, this manipulates to hide the secret data in more significant areas. Image domain is also known as spatial domain is more robust. Alternately transform domain, uses transformed embedding data to hide in the secret communication and independent the image format and the embedded message. Transform domain is otherwise known as frequency domain is the most secure method [7].

In image steganography LSB substitution method that is the least significant bit (LSB) placing is a common, simple approach for hiding covert information in a cover image. In this method, some or all of the bits in the covert image are changed to a bit of the secret message [5].

10.15662/ijareeie.2015.0403032

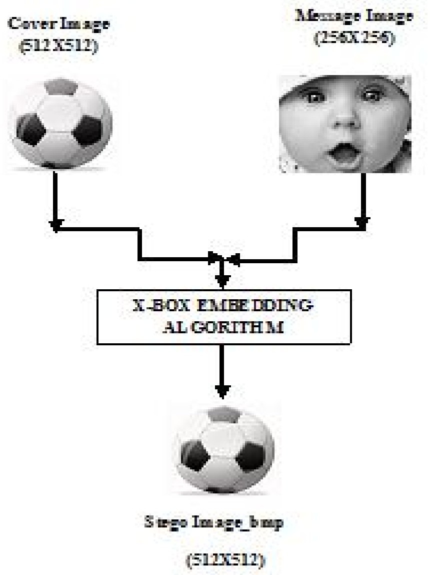

Figure 1. Block Diagram of image steganography on embedding side [11]

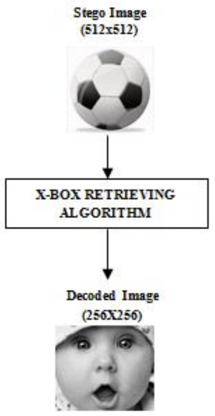

Figure 2. Block Diagram of image steganography on retrieving side [11]

II.RELATEDWORKS

There are large numbers of steganography embedding techniques proposed in the literature. These procedures Modify the cover image with different methods. But the entire embedding techniques share the considerable goal of maximizing the capacity of the stego channel [15]. In other words, the endeavour is to embed at highest possible rate while remaining imperceptible to Steganalysis attack. Special domain embedding technique operates on the principle of correcting the parameter of the cover image like payload or disruption, so that the divergence between cover and stego image is insignificant and undetectable to the human eyes.

Steganography generally exploit human perception because human senses are not skilled to look for file that has hidden information inside them. Therefore steganography disguises information from people trying to hack them. Payload is the amount of data that can be hidden in the cover object. The most widely known image steganography algorithm is based on modifying the least significant bit of pixel value, hence known as LSB technique [1]. They are based on two techniques i.e. LSB replacement and LSB matching.

Existing Method

In previous method mapping based image-image steganography is developed. Only grayscale image is used here for both secret message and covert image. The gray scale secret image is converted to binary where each pixel has 8-bit value. Mapping method is nothing but assigning encoded value for the pixels in the secret image using four kinds of X-boxes such as b1, b2, b3, b4.The 8-bit value is further divided into four equal parts of two bits. Each two bit will get equivalent value from X – box in the sequence of the first part from b1, second part from b2 and so on. Then the new values get embedded in the pixels of cover image. As a result only two bits of message gets embed in each pixel of cover image [1].

III. PROPOSED IMAGE STEGANOGRAPHY:

This method is implemented using only 2 x-boxes which are capable of holding values from 0 to15.
This method is using two X-box, 4 bits of secret message is hidden. This enhances the security of the secret message, with no movement of the PSNR value of the cover image.

Embedding capacity and robustness has enhanced in this method.
On average, only half of the bits in an image will need to be modified to hide a secret message and it requires maximum cover 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–are used 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) [19] and Edge Adaptive based LSBMR steganography techniques are popular LSB [1] like steganography methods.

Block diagram of proposed model of image steganography

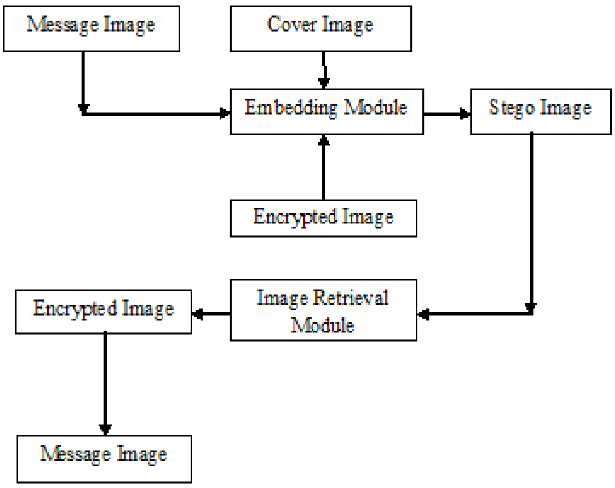

Figure 3. Block diagram of the Image Steganography [14]

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

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Block diagram explanation:

Cover Image: It is the given space for embedding message image. The important property of the cover image is that its statistical properties cannot be significantly altered by embedding the message image information (pixels) into the cover image frames of 2Mx2N is considered for embedding process.

Message Image: It is the secret information in the form of pixels in which each frame consists of MxN pixels is to be hidden in the cover image frame. The size of the message image frame is half of cover image frame.

Stego Image: In this image message image is hidden under cover image. It is the secret information in the form of pixels in which each frame consists of 2Mx2N pixels. The size of the stego image frame is as same as cover image frame.
X-BOX mapping: Here 1 pixel of message image frame is mapped onto 4 pixels of cover image frame based on the XOR operation on the bits of pixel used in message frame.

Algorithm for 2 X-Box technique:

1. Divide the cover image and message image into 50 frames.
2. Set the format of cover image and message image to BMP format respectively. Set the sampling ratio to 4: 2: 0.

Embedding Algorithm:
Input: A Message Image frame of size (m x n), A Cover image frame of size (2m x 2n);
Output: Stego image frame of size (2m x 2n)
Steps:
1. Convert the image into binary format.
2. Divide each pixel of cover image into 2 parts each of length 4-bit.
3. Reduce the each resultant 4-bit into 3-bit using XOR operation.
For example: 1001 => (1 XOR 1 = 0, 0 XOR 0 = 0, 0 XOR 1 = 1) = 001.
4. Retrieve the corresponding value for these two 3-bit of the X-box.
5. Insert each new value into its corresponding pixel's LSB position.
6. Thus the Stego image has been obtained.

Retrieval Algorithm:
Input: Stego image frame of size (2m x 2n);
Output: A Message image frame of size (m x n);
Steps:
1. Convert the Stego image into binary format.
2. Extract LSB of 4-bit from the pixels.
3. Convert all the 4-bit into 3-bit using XOR operation.
4. Get all the equivalent 4 –bit values from two X-boxes.
5. Concatenate 4-bit values to 8 (Stego pixel).
6. Arrange all stego pixels to get the full secret image.

Implementation of 2 X-Box technique:
1. Generation of 2 x-boxes each of 4x2 matrix[14]

00	01	10	11	
0	1	3	2	0
7	6	4	5	1
00	01	10	11	

15	14	12	13	0
8	9	11	10	1

Consider 4 bit binary values from 0 to 15 and represent them as shown above.
Now XOR within first second bits , then XOR within second third bit, then XOR third fourth bits and obtain the 3 bit result.
In the obtained 3 bit result, the first bit represents the row and the second and third bit represents the column.
Now assign the equivalent decimal values to the corresponding rows and column of first XBOX ie x1 box.
Similarly repeat the same steps for all the 15 equivalent numbers and assign it to 2 x boxes cyclically [14].
2. Matching of message pixels with x-box values
Consider a message image frame of size Mxn
It can be represented as Eg:-256x256

123	23	96	…		
56	33				
78	65				
: : :					
89					
87					

It consists of 256pixels in one row and 256 pixels in one column of different intensity with each frame
Consider the intensity of first pixel. The pixel intensity of the above frame is taken and represented as 149.
Convert it into binary
123-------→01111011
Divide the above values into two equal parts [4]:
0111=b1 ; 1011=b2
Using XOR operation b1 and b2 is converted to 100, 111 respectively. Now just map values of b1,b2 from the X-box. First take b1= 100 --→ 1st row 00th column --→ 7; b2= 11.

3. Embedding the mapped values into cover image
Consider the size of cover image frame as 2Mx2N ie 512x512.It is represented as [14]

200	215	… .	…..	…..	
120	140				
: :	: :				
:					
56	78				

The above obtained cover image frame has 512 pixels in rows and 512 pixels in column.
Consider the 2x2 array of pixels 200,215,120 and 140.
Consider 200, converting it to binary we obtain 0001 0111.
Replace the four LSB's first pixel of cover image frame by message's mapped value of b1 i.e. 1000 is replaced by 0111 of b1from above mapped value.

Before replacing After replacement by 0111
11001000-------->200 1100 0111-------->196 in decimal.
In the similar way second pixel of cover image frame is replaced by the value of b2=1011.
Before replacing After replacement by 1011 11010111-------->215 1101 1011-------->219 in decimal.
Now the second pixel of message image is embedded into next 2x2array of pixels of cover image frame in the same procedure as indicated in the above steps.
In these way 256x256 pixel values of message image first frame is embedded onto 512x512 pixel values of cover image first frame.
Thus stego image first frame of 256x256 is obtained. Thus stego image is formed.

4. Retrieving the message image frame from stego image frame
Consider the first frame of stego image.

196	219	….	…..	…..	
126	139				
: :	: :				
:					
56	78				

Consider array of 2x2 pixels.
Consider first pixel of array and convert it to binary
196-------->11000111.
Extract 4 LSB bits ie 0111.
Similarly consider 2nd pixel of the array and obtain b2.
219----------→1101 1011
Extract 4 LSB bits ie 1011
Combine or cascade b1,b2 to obtain first pixel of message as shown below
0111 1011----→ 123
Thus 1st pixel of message is obtained.
Similarly repeat the above steps to obtain all 176x144 pixels of message first frame.
Repeat the above steps to obtain stego image.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

To evaluate the efficiency of the X-boxes encoding, three parameters are used, that is PSNR and MSE. Here we took 512 x 512 images as cover object and 256x256 images as secret data. After hiding the secret image in the cover image the PSNR, Capacity, MSE and Robustness were calculate using the following equations. [5]

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N}$$

$$\text{PSNR} = 10\log 10\,(R^2/MSE)$$

$$\text{Capacity} = \frac{P_{ij}}{C_{ij}}$$

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

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Results of 2 X-Box Technique :

Image	Capacity	Size	PSNR(db)
Cover.bmp	50%	512X512	36.62
Message.bmp	50%	256X256	36.43
Stego.bmp	50%	512X512	36.57
Decoded.bmp	50%	256X256	36.40

V. CONCLUSION

In this paper, we have implemented a 2 x-box mapping based steganography process to improve security and image quality compared to the existing algorithms. Our approach is better because use of only 2 x-boxes.without stego key, no one can extract the original information from the stego-image, for purposes of secret communication which is more important.

VI. FUTURE SCOPE

The Stego image is highly imperceptibly to the attacker. The algorithm offer reasonable capacity of message. In future the algorithm can be improved by improving the capacity and PSNR.
Also using different operating systems like LINUX versions UBUNTU through open CV, we can obtain message image and cover image in real time.

REFERNCES

[1] Liang Zhang, Haili Wang, Renbiao Wu, "A High-Capacity Steganoghraphy Scheme for JPEG2000 Baseline System, 2009".

[2] Weiqi Luo, Fangjun Huang, and Jiwu Huang," Edge Adaptive Image Steganography Based on LSB Matching Revisited, 2010".

[3] Mr.Jagadeesha.D.H, Mrs.Manjula.Y, Dr.M.Z.Kurian,"FPGA Implementation Of X-Box Mapping For An Image Steganography Technique".

[4] Manoharan Shobana "Efficient X-box Mapping in Stego-image Using Four-bit Concatenation. 2014".

[5] Daniel Socek ,HariKalva , Spyros S. Magliveras ,Oge Marques ,DubravkoCulibrk ,BorkoFurht,"New approaches to encryption and steganography for digital videos,2011."

[6] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, Monika Sharma," Image Steganography : Self Extraction Mechanism,2013."

[7] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography, 2011."

[8] M.Shobana, R.Manikandan, "Efficient Method for Hiding Data by Pixel Intensity. 2013".