Efficient X-box Mapping in Stego-image Using Four-bit Concatenation

Manoharan Shobana

Department of Electronics and Communication Engineering
Karpagam College of Engineering,Coimbatore
(Email: divyashobana.m@gmail.com)

(Received Mar. 20, 2014; revised and accepted Apr. 29, 2014)

Abstract

The approach of hiding the secret information in the covert image is called image steganography. Its goods like strength and defense is broadly used for covert communication, where the secret message is used to hide in the covert image. The least-significant-bit (LSB)-based method is a popular type of steganographic algorithms in the spatial domain. In image steganography the LSB based method is used extensively for hiding the secret data due to its simplicity and high embedding capability. 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-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.

Keywords: Decoding, encoding, image steganography, network security, X-boxes

1 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 [3]. 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.

Figure 1: Basic steganography model

Watermarking is used for screen monitoring, copyright defense, 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 [2].

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 [2].

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 [4, 5].

2 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 bits 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].

3 Proposed Method

Step 1 (procedure for filling values in X-box):
This mapping method used two X-boxes which are capable of holding values from 0 to 15 which is explained in Figure 2.

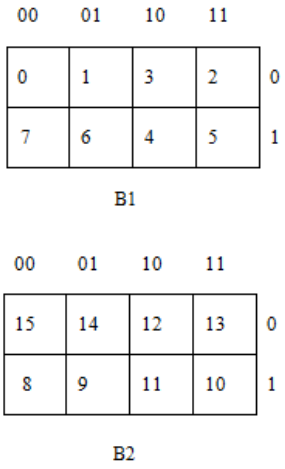


Figure 2: Mapping using X-box

The steps for inserting values in the X-box are described below using an example:

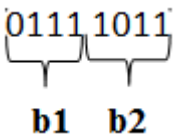
7 => 0111 = 100
0 XOR 1 = 1
1 XOR 1 = 0
1 XOR 1 = 0.

Now take a look at B1 where 7 are placed in the 2nd row and 1st column. This procedure is similar for the X-box B2. Main purpose of using X-box is decoding the pixels of secret image.

Step 2 (Message encoding):
Convert the Secret image into its binary values each of 8-bit length. Split each pixel into two equal parts convert that into 3-bit using XOR operation which is mentioned above. Let us see with an example:

$(123)_{10} = (01111011)_2$

Divide the above values into two equal parts:



Using XOR operation b1 and b2 is converted to 100, 110 respectively.

Step 3 (Mapping):
Now we just map the values of b1, b2 from the X-box. First, we take b1 = 100. Then we search the value of 1st row and 00th column of the X-I box; After mapping we get the value (7)10 = (0111)2; Similarly, we get mapping values for b2 = 11.

Step 4 (Embedding):
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 (See Figure 3). First, we take the pixels one by one from the cover image. The 4 LSB bits are replaced by 7, 11 sequentially Here the message bits get embedded in the sequential manner:

$(200)_{10}$ => $(11001000)_2$
$(215)_{10}$ => $(11010111)_2$

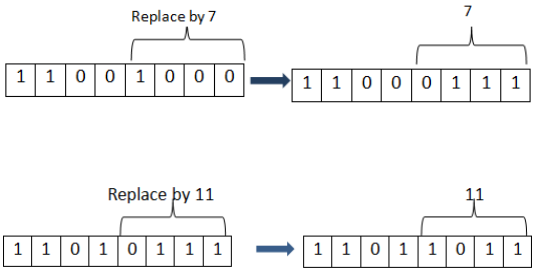


Figure 3: Bits embedding in the cover image

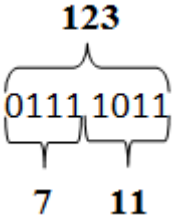
As a result, we get two new stego pixels which are given below:

$(200)_{10}$ => $(196)_{10}$
$(215)_{10}$ => $(219)_{10}$

This process will continue until all secret bits get embedded in the given cover image. The following are encoding procedures:

Input: A grayscale image of 128x128 sizes
Output: A stego-image with secret message of 64x64 sizes
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.

Step 5 (Extraction method):
After getting stego-image its value is converted to a binary value. In that extract all four LSB and perform the consecutive XOR operation to convert that all 4-bit to 3-bit.Then get equivalent values for all 3-bit from both B1 and B2 box alternatively. Convert all the decimal values to binary in the size of 4-bit.Concatenate the successive two 4-bit to form 8-bit. Thus the Stego pixel has been arrived to get the secret image. The concatenation of four bits is given below:



The following are decoding procedures:

Input: A grayscale Stego image of 128x128 sizes

Output: Secret image (64x64)

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.

4 Experimental Results

To evaluate the efficiency of the X-boxes encoding, two parameters are used, that is PSNR and MSE. Here we took 128 x 128 images as cover object (See Figure 4) and 64x64 images as secret data (See Figure 5). After hiding the secret image in the cover image the PSNR and MSE were calculated using the following equations:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right),$$

where R is a maximum disturbance in the resultant image. Table 1 shows performance measures of new stego image.

Table 1: Performance measures of new stego image

Image	PSNR	MSE	Bits per pixel	Maximum embedding capacity
Lena	36.6268	14.1383	4	50%
Gandhi	36.4388	14.7640	4	50%
Temple	36.5729	14.3148	4	50%
Baboon	36.4001	14.3148	4	50%

Figure 4: Original images

Figure 5: Stego images

5 Conclusions

In this approach the number of secret bits in each pixel is raised up to 4 bits, where in previous work only 2 bits are used. Thus the embedding capacity is increased and high value of PSNR value is achieved. This design uses only two Xbox instead of using four Xbox when compared to existing methods. Another advantage is it uses mapping based steganography for security and high image quality, thus without knowledge of the Xbox values the secret image cannot be retrieved correctly. This approach can be further enhanced by using color images instead of using grayscale image.

References

[1] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar,"An Image Steganography Technique using X-Box Mapping," *in the proceedings of the International Conference On Advances In Engineering, Science And Management (ICAESM 2012)*,pp.709-713,Nagapattinam,India,March 2012.

[2] C. Chang, T. D. Kieu,"A reversible data hiding scheme using complementary embedding strategy," *Information Sciences*, vol. 180, no. 16, pp.3045-3058, 2010.

[3] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, vol. 12. no. 6, pp.441-444, 2005.

[4] W. Luo, F. Huang, J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transaction on Information Forensics Security*, vol. 5, no. 2, pp.201-214, 2010.

[5] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp.285-287, 2006.

[6] M. Shobana, R. Manikandan, "Efficient method for hiding data by pixel intensity," *International Journal of Engineering and Technology*, vol. 5, no. 1, pp.75-81, 2013.

M.Shobana is currently working as a Assistant Professor, Karpagam College of Engineering, Coimbatore, India. She obtained B. Tech (Computer and science Engineering) in SASTRA University and then finished M. Tech (VLSI design) in SASTRA university Thanjavur, Tamil Nadu, India. She is interested in the area of Steganography and Network security.