Image Steganography using Two’s Complement

Sushil Sharma
M.Tech Research Scholar
Department of Computer
Science & Engineering
BBSBEC Fatehgarh Sahib,
Punjab, India

Ishpreet Singh Virk
Assistant Professor
Department of Computer
Science & Engineering
BBSBEC Fatehgarh Sahib,
Punjab, India

ABSTRACT

Nowadays communication is being done through internet so it has become very important to secure the secret information. Steganography is one of the techniques used for secret communication to overcome such threats. This technique hides the secret information behind other information without revealing its existence. This paper presents an Image Steganography Technique using 2’s Complement. In this technique first 2’s complement is performed on the secret pixel and then it is concealed in the LSBs of the cover image.

General Terms

Steganography, LSB (Least Significant Bit).

Keywords

Steganography, Two’s Complement.

1. INTRODUCTION

There has been a tremendous growth in Internet technologies in last few years. It has become very convenient to transmit information over the internet. So there must be some security measures to protect the secret messages sent over the network. There are many cryptographic methods available but these just changes the message in unreadable form which guarantees that something secret is being sent. To solve this Steganographic methods are used. Steganography is a branch of information hiding in which secret message is cleverly embedded in another media in such a way that no one can guess the existence of hidden information [1]. The word steganography in Greek means "covered writing" (Greek words "stegos" meaning "cover" and "grafia" meaning "writing") [1]. 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 stegoimage should not diverge much from original coverimage[1].

2. ASSOCIATED WORKS

Least significant bit (LSB) steganography [2, 3, 4, 5, 6] 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) [4] and Edge Adaptive based LSBMR [5] steganography techniques are popular LSB like steganography methods. X-Box mapping [7] technique is a very efficient and secure LSB substitution technique.

Capacity, security and robustness [5], are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be embedded in the cover medium. Security relates to the ability of an eavesdropper to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

2.1 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 is defmed as:

$$\mathrm{PSNR} = 10\log(255^2 / \mathrm{MSE})$$

$$\text{wherere MSE} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\frac{\big(f(x,y)-g(x,y)\big)^2}{N^2}$$

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 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**.**

3. PROPOSED IMAGESTEGANOGRAPHY ALGORITHM

This algorithm is based on the two’s complement concept. In this algorithm, each secret pixel is first converted into its equivalent two’s complement and after that it is embedded into four pixels of the cover image.

3.1 Encoding Algorithm

Input: A grey-level secret image of size (m x n),

A Grey levels cover Image of size (2m x 2n) at least;

Output: Stego Image of size (2m x 2n);

Steps:

1) Select the secret pixel.

2) Convert the selected pixel into its equivalent two’s complement.

3) Interchange the bit values of the step 2 pixel and divide the pixel into four parts of two bits each.

4) Select the four cover pixels in which to embed these four parts of secret pixel.

5) Replace the two LSB of each selected pixel one by one with the two bits of the secret pixel. Selection of two bits of secret pixel starts from the MSB i.e. bit positions 7 and 6.

3.2 Algorithm in Detail

3.2.1 Selection of Secret Pixel

Select the pixel row wise or column wise from secret image.

83	**89**	**106**			
76	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-
116	-	-	-	-	-

Fig 1.1 128×128 Secret Image

Let the first pixel is selected i.e. 83.

3.2.2 2's Complement of Secret Pixel

Convert the pixel into equivalent 2's Complement.

83=

0	1	0	1	0	0	1	1

Binary

7	6	5	4	3	2	1	0
1	**0**	**1**	**0**	**1**	**1**	**0**	**1**

Fig 1.2 2's Complement

3.2.3 Interchange the bits values

Interchange the bit positions i.e. 1-0, 3-2, 5-4 and 7-6 of complement of secret pixel. Divide pixel into four groups of two bits each.

7	6	5	4	3	2	1	0
0	**1**	**0**	**1**	**1**	**1**	**1**	**0**

Divide into four groups

01 01 11 10

Fig 1.3 Interchange pixel

3.2.4 Formation of Stego Image

Select the four cover pixels in which to embed the complement of secret pixel. Any pattern can be set for selection of pixels depending upon the size of the cover and secret image. Here pixels are selected from the adjacent columns and in each selected column consecutive pixels are selected i.e. in the pattern 1, 2, 3 4 etc... Two LSB of each cover pixel will be replaced with the two bits of above secret pixel.

1	2	3	4	5	-	-	512
156	158	-	-	-	-	-	-
160		-	-	-	-	-	-
158	--	-	-	-	-	-	-
156		-	-	-	-	-	-
157	-	-	-		-	-	-
-	-	-	-		-	-	-

Fig 1.4 512×512 Cover image

Let 156, 160, 158 and 156 intensity pixels are selected. Now place the bits 7 and 6 of step 3 pixel at first two LSB of first pixel. Similarly place 5 and 4, 3 and 2 and, 1 and 0 position bits of secret pixel in the first two LSB of subsequent pixels. This is explained below:

$$\underbrace{(1\,0\,0\,1\,1\,1\,0\,0)_2}_{156} \xrightarrow{01} \underbrace{(1\,0\,0\,1\,1\,1\,0\,1)_2}_{157}$$

$$\underbrace{(1\,0\,1\,0\,0\,0\,0\,0)_2}_{160} \xrightarrow{01} \underbrace{(1\,0\,1\,0\,0\,0\,0\,1)_2}_{161}$$

$$\underbrace{(1\,0\,0\,1\,1\,1\,1\,0)_2}_{158} \xrightarrow{11} \underbrace{(1\,0\,0\,1\,1\,1\,1\,1)_2}_{159}$$

$$\underbrace{(1\,0\,0\,1\,1\,1\,0\,0)_2}_{156} \xrightarrow{10} \underbrace{(1\,0\,0\,1\,1\,1\,1\,0)_2}_{158}$$

Fig 1.5 Bit insertion in pixels

Output Stego image will be as shown in the figure 1.6.

157	158	-	-	-	-	-	-
161	-	-	-	-	-	-	-
159	--	-	-	-	-	-	-
158	-	-	-	-	-	-	-
160	-	-	-	-	-	-	-
-	-	-	-		-	-	-

Fig 1.6 512×512 Output cover image

3.3 Decoding Algorithm

Input: A grey-level stego image of size (2m x 2n),

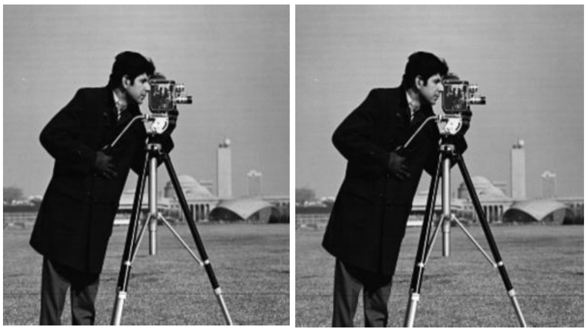
Output: A Secret Image of size (m x n);

To decode the stego image at the receiver side, perform the following steps:

1) Extract the two LSBs from the embedded pixels of the stego image one by one.
2) Concatenate the extracted bits.
3) Rearrange the bits position of recovered pixels according to the encoding algorithm.
4) Convert the pixel into its 2's complement. This will be the original pixel.

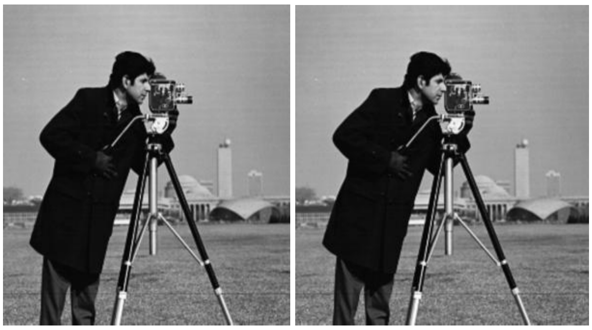
4. EXPERIMENTAL RESULTS

Experiment is carried out on two patterns of selected cover pixels to embed the secret bits. PSNR value is calculated in both cases and results are compared.



(a) (b)

Figure 1.6 (a) cover image and (b) Stego image of cameraman using 2's complement with consecutive cover pixels.



(a) (b)

Figure 1.7 (a) Cover image and (b) Stego image of cameraman using 2's complement with distance of 4 pixels in each row and column.

Since only two bits are replaced there will only be a difference of at maximum three values in the modified pixel which is acceptable and does not produce much distortion in the cover image. As seen in the stego cameraman image, there is negligible distortion. No one can identify the existence of something hidden secret. In this way goal of steganography is achieved. Following two tables shows the PSNR values for different stego images for two different patterns of cover pixels.

Table 1.1 PSNR values with consecutive selection of pixels

Sr. No.	Image Name	Size (Pixels)	Secret image size (Pixels)	PSNR with consecutive pixel in every row and column (in dB)
1	Cameraman.jpg	512×512	128×128	+ 53.4717
2	Baboon.jpg	512×512	128×128	+ 53.5315
3	Lena.jpg	512×512	128×128	+ 53.6227

Table 1.2 PSNR values with distance of four pixels in row and columns

Sr.No.	Image Name	Size (Pixels)	Secret image size (Pixels)	PSNR with distance of four pixels in each row and column (in dB)
1	Camera man.jpg	512×512	64×64	+ 59.5348
2	Baboon. jpg	512×512	64×64	+ 59.6400
3	Lena.jpg	512×512	64×64	+ 59.7031

High values of PSNR in the above two tables means that there is not much distortion in the stego image. Also PSNR value increases if the size of the secret image is reduced from its maximum acceptable size and by maintaining some distance between two selected cover pixels.

5. CONCLUSION AND FUTURE SCOPE

This algorithm is very secure because different levels of security are implemented in this algorithm. First is 2's complement of secret pixel. Secondly bit positions are interchanged before embedding. Third the secret pixel is broken into four parts of two bits each and lastly intruder needs to find out the pattern of cover pixels to fetch the information. There is negligible distortion in the stego image which is the ultimate goal of steganography.

Future research is focussed on improving and extending this algorithm for coloured images.

6. REFERENCES

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

[2] C.-C. Chang, T.D. Kieu, A reversible data hiding scheme using complementary embedding strategy, Inform. Sci. 180 (16) (2010) 3045-3058.

[3] C.-C. Chang, W.-L. Tai, c.-c. Lin, A reversible data hiding scheme based on side match vector quantization, IEEE Trans. Circ. Syst. Video Technol. 16 (10) (2006) 1301-1308.

[4] 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.

[5] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.

[6] Chen, B. and G.W. Wornell, 2001. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. lEEE Trans. Inform. Theory. 47: 1423-1443. DOl: 10.1109118.923725.

[7] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, An image steganography technique using x-box mapping, IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012,709-713.