

Multimedia Security through LSB Matching

Rupali Bhardwaj

Computer Science and Engineering Department, Thapar University,

Patiala, India

rupali.bhardwaj@thapar.edu

ABSTRACT

Steganography is the art of hidden communications, encoding/embedding hidden information in cover media in such a way so as not to provoke an eavesdropper's suspicion. In this paper, we propose an efficient image steganography technique which provides high embedding capacity as well as imperceptibility of stego image. Using fixed number (i.e. two) as the upper limit criteria for embedding, the target pixel, based on equality between pixel bits and secret data bits is selected for embedding. As an indicator to determine which pixel is used for embedding, least significant bit is reversed. The experimental results showed preserving stego image quality with ability of embedding high data capacity. Results showed that the proposed method gives better results than simple LSB and inverted LSB with higher PSNR and lower MSE.

Keywords

Data Hiding, LSB, LSB Matching, PSNR

1. INTRODUCTION

With rapid advancement in Multimedia technologies during the recent years, communication and information exchange have become much easier and faster but at the same time the issues related to data security and confidentiality have become a major concern of the time. To cater to this need of information security, a number of hidden and secret communication techniques have been developed. Steganography refers to the art of hidden communications[1], encoding/embedding hidden information in cover media in such a way that it is a difficult job for an unauthorized person to see that there is something hidden in the cover media. The output is an image called stego-image that is similar to the cover media. A stego-key is used for embedding/encoding process to restrict decoding or extraction of the embedded data in cover media. The modern age steganography is usually implemented computationally, where multimedia files are used as cover media. A good Steganographic method has three features, good hiding capacity, good imperceptibility and the last is robustness.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org. ICTCS '16, March 04-05, 2016, Udaipur, India © 2016 ACM. ISBN 978-1-4503-3962-9/16/03...\$15.00 DOI: <http://dx.doi.org/10.1145/2905055.2905087>

2. LITERATURE REVIEW

2.1 Basic Least Significant Bit (LSB) Image Steganography

Digital images are categorized into two parts (i) RGB (24 bit image) and (ii) Grey (8 bit image). Three bits of hidden information can be embedded in RGB image; one bit in LSB of each plane while in grey image one bit can be embedded. In basic LSB technique (in other words, eight bit technique), bit of bit plane zero of cover image is replaced by bit of the hidden message.

1: For $m = 1$ to N

2: For $n = 1$ to N

3: If $C(m, n) = \text{even}$ and $M(m, n) = 0$

4: $S(m, n) = C(m, n)$; //no change in LSB of $C(m, n)$

5: End If

6: If $C(m, n) = \text{odd}$ and $M(m, n) = 1$

7: $S(m, n) = C(m, n)$; //no change in LSB of $C(m, n)$

8: End If

9: If $C(m, n) = \text{odd}$ and $M(m, n) = 0$

10: $S(m, n) = C(m, n) - 1$; //Make it Even and Embed

11: End If

12: If $C(m, n) = \text{even}$ and $M(m, n) = 1$

13: $S(m, n) = C(m, n) + 1$; //Make it Odd and Embed

14: End If

15: End

16: End

where $C(m, n)$, $S(m, n)$, means pixel value at position (m, n) in cover image, and stego image respectively. $M(m, n)$ means message bits value at position (m, n) .

2.2 Inverted LSB Image Steganography

In this paper [8], an improvement in the simple LSB based image steganography through bit inversion technique is proposed and implemented.

3. PROPOSED ALGORITHM

In this paper, we propose an efficient image steganography technique which provides high embedding capacity as well as imperceptibility of stego image. Using fixed number (i.e. two) as the upper limit criteria for embedding, the target pixel, based on an equality between pixel bits and secret data bits is selected for embedding. As an indicator to determine which pixel is used for embedding, least significant bit is reversed. If no equality occurs between pixel bits and secret data bits, data is embedded in cover image though simple LSB.

3.1 Embedding Algorithm

INPUT: Cover Image C of size M x N, Secret Data , P of size n .

OUTPUT: Stego-image, Key

STEP 1: Embed the message, P to the LSB planes of the cover image C to get the stego-image S. The message embedding procedure is given as below -

```

1:  Initialise flag = 0
2:  While k <= n
3:    For m = 1 to M
4:      For n = 1 to N
5:        If C(m, n) = P(k)
            //match occurs between cover image
            and message
6:          C(m, n) = C(m,n) + 10
7:        Loc(k, 1, 1) = m
            //
            maintain array to get location
8:      Loc(k, 1, 2) = n
9:      k = k + 1
10:     Set flag = 1
11:     Break
12:   Else
13:     Loc(k, 1, 1) = m
            //array element can't be zero
14:     Loc(k, 1, 2) = n
15:   EndIf
16: EndFor
17: If flag = 1
18:   Break
19: EndIf
20: EndFor
21: If flag = 0 // match not found between cover
    image and message
22:   For x = 1 to M
23:     For y = 1 to N
24:       If C(x, y) = (0 || 1)
25:         C(x, y) = P(k)
26:         C(x, y) = C(x, y) + 20
27:         Loc1(k, 1, 1) = x
            //
            maintain array to get location
28:         Loc1(k, 1, 2) = y
29:         k = k + 1
30:         Set flag = 1
31:         Break
32:       EndIf
33:     EndFor
34:   If flag = 1
35:     Break
36:   EndIf
37: EndFor
38: EndIf
39: Set flag = 0
40: EndWhile

```

where C (m, n), S (m, n), means pixel value at position (m ,n) in cover image, and stego image respectively. P (k) means message bits value at position (k) .

3.2 Extraction Algorithm

After receiving of stego-image, the receiver firstly, extracts the hidden message from the stego-image. Extracting the message from the stego-image includes inverse comparison to that used in embedding. The decoding algorithm demands the same key that was used by the sender in the encoding algorithm.

Input: Stego-Image, Key Matrix. **Output:** Secret Data.

The steps of the extraction phase are as follows:

```

1:  For q = 1 to n
2:    If S(Loc(K, 1, 1), Loc(K, 1, 2)) = C(Loc(K,
    1, 1), Loc(K, 1, 2))+1
3:      Set msg(q) = 0
4:      Continue
5:    Elseif S(Loc(K, 1, 1), Loc(K, 1, 2)) = C
    (Loc(K, 1, 1), Loc(K, 1, 2))
6:      Set msg(q)=1
7:      Continue
8:    If S(Loc1(K, 1, 1), Loc1(K, 1, 2)) =
    C(Loc1(K, 1, 1), Loc1(K, 1, 2))+1
9:      Set msg(q)=0
10:     Continue
11:    Elseif S(Loc1(K, 1, 1), Loc1(K, 1, 2)) =
    C(Loc1(K, 1, 1), Loc1(K, 1, 2))
12:      Set msg(q) =1
13:      Continue
14:    EndIf
15:  EndFor

```

Where C(m,n), S(m,n), means pixel value at position (m ,n) in cover image and stego image.

4. RESULT AND ANALYSIS

A set of 8- bit greyscale image and 24- bit RGB image of size 512 × 512 are used as the cover image to hide binary and grey image of size 128 × 128 to form the stego-image. With the experimental study on MATLAB 14, we noticed that the visual differences between the original cover-images and stego images with the LSB matching can be hardly detected with naked eyes.

4.1. PSNR Analysis

MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image.

MSE is the averaged pixel-by-pixel squared difference between the cover-image and the stego-image. Mathematically, MSE is expressed as:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [C(i, j) - S(i, j)]^2$$

where, M and N are the rows and columns of the cover image respectively, and C(i, j) and S(i, j) means the pixel value at position (i, j) in the cover-image and the corresponding stego-image, respectively.

The PSNR is expressed in dB's and can be calculated using MSE as

$$PSNR = 10 \times \log \left(\frac{P^2}{MSE} \right) \text{ where, } P \text{ is the}$$

peak signal value of the cover- image, and

$$P = \max (C(i, j), S(i, j))$$

Table 2 , table 3 give the measured values of MSE and PSNR of different types of cover images of size 512×512 respectively. It is observed that when the payload increases the MSE increases and this affects the PSNR inversely and for all cover-images PSNR is greater than 50, this indicates good performance of the proposed system. Table 4 gives comparative study of proposed method with inverted LSB technique on different message images(fig. 1). It means that the stego-images created with Table 1 gives the measured values of MSE and PSNR of cover images of size 512×512 and hidden message size is 128× 128 respectively. It is observed that PSNR value of proposed method is better than simple LSB.

5. CONCLUSION

Steganography is the art of hidden communications, encoding/embedding hidden information in cover media in such a way so as not to provoke an eavesdropper's suspicion. In this paper, we propose an efficient image steganography technique which provides high embedding capacity as well as imperceptibility of stego image. Using fixed number (i.e. two) as the upper limit criteria for embedding, the target pixel, based on an equality between pixel bits and secret data bits is selected for embedding. As an indicator to determine which pixel is used for embedding, least significant bit is reversed For future work we will generate random number through cellular automata as further securing system and use other type of cover-object for hiding the data.

REFERENCES

- [1]A. Menezes, P. Oorschot, S. Vanstone, and A. J. Menezes, "*Handbook of Applied Cryptography*", CRC Press, Boca Raton, FL,1997.
- [2] http://en.wikipedia.org/wiki/Arnold%27s_cat_map
- [3] V. I. Arnold, A. Avez ,"*Ergodic Problems in Classical Mechanics*", New York: Benjamin,1968.
- [4]D.X. Qi, "*Matrix transformation and its applications to Image Hiding*", Journal of China University of Technology, 11(1):24-28,1999.
- [5] F. A. Petitcolas, R.Anderson, M.Kuhn, "*Information hiding: A Survey*", Proceedings of the IEEE, vol. 87, pp. 1062—1078, July 1999.
- [6] G. C. Langelaar, I. Setyawan, and R. I. Lagendijk, "*Watermarking Digital Image and Video Data*" in IEEE Signal Processing

Magazine, pp. 20- 46, September 2000.

[7] B Li, J He, J Huang and YQ Shi., "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, 2011.

[8] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan ,"*Enhancing the Security and Quality of LSB based Image Steganography*", 5th International Conference on Computational Intelligence and Communication Networks, 978-0-7695-5069-5/13 © 2013 IEEE

TABLE 1:MSE AND PSNR VALUE OF HIDDEN MESSAGE (128x128)

















COVER IMAGE (512x512)	HIDDEN IMAGE (128x128)	STEGO IMAGE (512x512)	EXTARCTED HIDDEN IMAGE (128x128)	MSE		PSNR	
				LSB	PROPOSED METHOD	LSB	PROPOSED METHOD
				0.0314	0.0258	62.8116	63.6731
				0.0934	0.0773	58.4292	59.2494
				0.2501	0.1479	53.8020	56.0844
				0.7521	0.4436	49.3681	51.6607

TABLE 2: IMAGE STEGANOGRAPHY THROUGH SIMPLE LSB

SENDER	SIMPLE LSB									
GREY SCALE COVER IMAGE (512 x 512)	MSG1 4,225 BITS		MSG2 16,384 BITS		MSG3 24,964 BITS		MSG4 38,416 BITS		MSG5 48,841BITS	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Goldhill.bmp	0.0076	68.6008	0.0304	62.5911	0.0469	60.7112	0.0725	58.8160	0.0925	57.7620
Peppers.bmp	0.0076	68.4045	0.0313	62.2344	0.0473	60.4458	0.0727	58.5809	0.0932	57.5036

Lena.bmp	0.0083	68.5722	0.0314	62.8116	0.0482	60.9547	0.0736	59.1154	0.0931
Baboon.bmp	0.0076	68.4467	0.0309	62.3287	0.0474	60.4777	0.0734	58.5766	0.0930

TABLE 3: IMAGE STEGANOGRAPHY THROUGH PROPOSED METHOD

SENDER	PROPOSED METHOD									
COVER IMAGE (512×512)	MSG1 4,225 BITS		MSG2 16,384 BITS		MSG3 24,964 BITS		MSG4 38,416 BITS		MSG5 48,896 BITS	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Goldhill.bmp	0.0068	69.0807	0.0258	63.311	0.0389	61.5250	0.0594	59.6864	0.0753	58.5766
Peppers.bmp	0.0068	68.8560	0.0258	63.0865	0.0389	61.3004	0.0594	59.4617	0.0753	58.5766
Lena.bmp	0.0068	69.4426	0.0258	63.6731	0.0389	61.8870	0.0594	60.0483	0.0753	58.5766
Baboon.bmp	0.0068	68.8939	0.0258	63.1243	0.0389	61.3882	0.0594	59.4996	0.0753	58.5766

TABLE 3: COMPARATIVE STUDY BETWEEN INVERTED LSB AND PROPOSED METHOD

MESSAGE IMAGES	COVER IMAGE: BABOON		
	PSNR		
	SIMPLE LSB	INVERTED LSB	PROPOSED METHOD
Laser	54.34	54.80	55.3498
3things	54.11	54.25	56.7877
Crods	54.47	55.25	56.0055
Mandrill	54.20	54.32	56.2722
Fishingboat	54.30	54.62	55.8206
TestPat	53.68	56.05	60.8495