Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Image Steganography using Efficient Map based LSB Technique (SISEMLT)

Manasi Jana*, Arpita Mazumdar, Kankana Datta
Department of Computer Applications, Haldia Institute of Technology, Haldia,
West Bengal, India

Abstract: ***Steganography is an art of embedding information in a cover image without causing statistically significant variations to the cover image. In this report, we have combined the theme of steganography as well as cryptography to securely send the hidden message to the receiver. Before communication the secret key is securely shared between two parties. The secret message is then embedded mathematically in the cover image with the secret key and stego image is formed using LSB technique. During decoding the secret message is extracted in the reverse process. Here we have used simple, low cost XOR operation. Also applied mapping technique to retrieve cover image from stego image and vice versa.***

Keywords: LSB, mapping, XOR, secret key, PSNR.

I. INTRODUCTION

Steganography [1] is the science of hiding information. The term originates from Greek word "Steganos" means "Covered" and "Graphie" means "Writing"[2]. Here secret message is hidden within an ordinary image in such a manner so that it can't be perceived by normal human vision. Only the message is extracted by the receiver for whom the message is sent. The purpose of steganography is to hide the existence of a message from a third party[3].

1.1 Steganography terms

- **Carrier or cover file** : An original message or a file in which hidden information will be stored.
- **Stego medium** : The medium in which the information is hidden.
- **Embedded or Payload**: The information which is to be hidden or concealed.
- **Steganalysis**: The process of detecting hidden information inside a file

1.2 Types of Steganography

Steganography can be broadly categorised into following groups:

- Text Steganography- uses text as cover media.
- Image Steganography- uses images as the cover media.
- Audio Steganography- uses audio as the cover media.
- Video Steganography- uses video as the cover media.

Among all image steganography is considered to be the most widely used method as it can take the advantage of limited power of human visual system. Also image has large redundant information which can easily hide a secret message.

1.3 Image Steganography techniques

Image steganography techniques can be subdivided into two categories:

- Image domain
- Transform domain

1.3.1 Image or spatial domain

These techniques embed message bits in the intensity of the pixels directly. Image domain techniques involve bit-wise methods. The image formats like BMP,GIF ,8-bit grey scale are most suitable for image domain steganography, as they are lossless and the techniques are greatly dependent on the image format.

Least Significant Bit (LSB) LSB[4] mechanism is a common and simple approach to embed secret message in a cover image. The least significant bit (8th bit) of some or all of the bytes inside an image(cover image) is changed to a bit of the secret message. The resulting stego image appears to be identical as cover image to the human eye.

1.3.2 Transform or frequency domain

These techniques incorporate message bits in the image after they are transformed. It is more robust against various attacks such as cropping, compression etc. There are several transform domain techniques such as DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform),DKT(Discrete Kekre Transform) etc.. Among them DCT is the most commonly used technique[5][6].

II. PROPOSED ALGORITHM

The proposed algorithm is using two folds of security to implement confidentiality and accuracy. In this scheme, a secret key is shared between two communicating parties. The confidentiality of the message remains on the secrecy of the shared secret key. Instead of storing secret message bit directly to the LSB of cover image, XOR operation is performed between the LSB of cover image, secret key and secret message. The resultant bits are embedded in the cover image. A mapping scheme [7] is designed to track the change of corresponding cover image bit and stego image bit. The receiver can only retrieve the secret message if he/she knows secret key as well as the mapping scheme. The cost effective bitwise operation(exclusive-OR) guarantees the accuracy of the system.

2.1 Proposed Algorithm

2.1.1 Algorithm for embedding message

Step 1: Start
Step 2: Read the text message to be hidden and covert it in to the binary form.
Step 3: Read the cover image and convert into the binary form.
Step 4: Find out the LSB of each pixel of the cover image.
Step 5: Consider a secret key 'K' which is known to both the parties before the communication starts.
Step 6: Perform the XOR operation between secret message, cover image and secret key 'K' to get the stego image.
Step 7: A mapping technique is followed to track the change between the cover image bits and corresponding stego image bits.
Step 8: The stego image with mapping information is sent to the receiver.
Step 9: Stop.

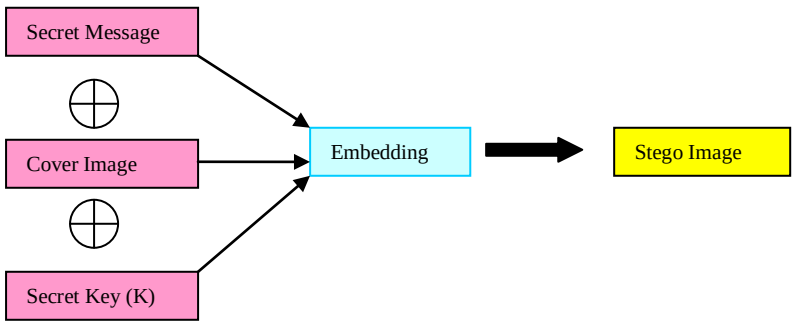

Figure 1: Proposed Embedding Algorithm

2.1.2 Algorithm for extracting message

Step 1: Start
Step 2: Read the stego image
Step 3: Using reverse mapping method cover image can be retrieved from the stego image.
Step 4: Perform XOR operation between stego image, secret key 'K' and cover image to retrieve the actual text message.
Step 5: Stop.

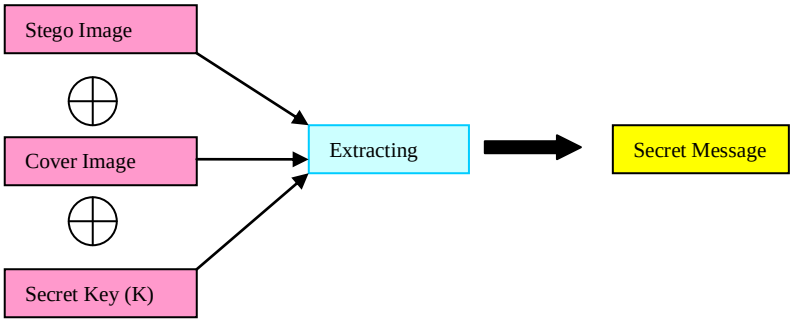

Figure 1: Proposed Extracting Algorithm

2.1.3 Mapping method

Step 1: Start
Step 2: Let two arrays c0 and c1. Where c0 keeps track of the corresponding bits changes from 1 to 0 in cover image and stego image and c1 keeps track of the corresponding bits changes from 0 to 1 in cover image and stego image.
Step 3: Let two variables a and b. where a counts number of changes of bit 1 to 0 and b counts number of changes of bit 0 to 1.
Step 4: Compare each cover image bit and corresponding stego image bit.
i. If the transformation is from 1 to 0 ,increment variable a by 1 and store the value in c0.
ii. If the transformation is from 0 to 1, increment variable b by 1 and store the value in c1.
iii. If no transformation then values of a and b remain same. As a result values of c0 and c1 are unaltered
Step 5: The values of c0 and c1 array contain the mapping information.
Step 4: Stop.

2.1.4 Reverse mapping method

Step 1: Start
Step 2: Compare each corresponding values of c0 and c1.
i. if c0=0 and c1=1 then cover bit=0
ii. if c0=1 and c1=0 then cover bit=1
iii. if values are unchanged from previous position then cover bit=stego bit
iv. if only c0 value is altered from previous value then cover bit=1
v. if only c1 value is altered from previous value then cover bit=0
Step 3: Stop

2.2 Implementation

We have successfully implemented our proposed algorithm(SISEMLT)in MATLAB. Also calculated the Mean Squared Error(MSE)and the Peak Signal-to-Noise Ratio(PSNR)to measure the imperceptibility of the stego message .It has been observed that PSNR[8] value is always satisfactorily high(>50).

2.3 Illustrative Example

Let us consider an example for our proposed algorithm. Let the secret message 'A' and consider 8 bits of secret message. In a 24 bit color image, we have chosen the grid of 3 pixels (RGB components/pixel) comprising (8x3x3) bits.
The following figures explain the embedding process(Figure 3) and extracting process(Figure 4).

Binary equivalent of 'A': 0 1 0 0 0 0 0 1

Three pixels of cover image before mapping
With LSB of each pixel are shown below:-

0 1 1 0 0 1 1 0	1 0 0 1 1 0 0 0	0 1 1 0 0 1 1 1
1 1 0 0 1 0 1 1	0 0 1 1 0 1 0 1	1 1 0 1 0 0 1 1
1 1 1 0 0 1 1 1	0 0 0 1 1 0 0 1	0 1 1 0 0 1 1 1

So, LSB of cover image: 0 1 1 0 1 1 1 1

Cover image bits 0 1 1 0 1 1 1 1

⊕

Key 1 1 0 0 1 1 0 1

⊕

'A' 0 1 0 0 0 0 0 1

Stego image bits 1 1 1 0 0 0 1 1

Figure 3: Example of Proposed Embedding Algorithm

According to the above example after using mapping algorithm the values of c0 and c1 (as mentioned in mapping method) are as follows:
c0=0 0 0 0 1 2 2 2
c1=1 1 1 1 1 1 1 1
To retrieve the cover image bits from stego image bits reverse mapping scheme is followed.

Stego Image bits	1 1 1 0 0 0 1 1
	⊕
Cover Image bits	0 1 1 0 1 1 1 1
	⊕
Key	1 1 0 0 1 1 0 1
	———————
Recovered message 'A'	0 1 0 0 0 0 0 1

Figure 4: Example of Proposed Extracting Algorithm

III. CONCLUSION

In this paper, our proposed scheme provides a cost effective, highly secure and accurate data hiding method. In future we would like to embed the resultant bits(after exclusive OR) in cover image in random LSB positions of cover image based on some random technique.

REFERENCES

[1] Shikha , Vidhu Kiran Dutt , "Steganography: The Art of Hiding Text in Image using Matlab", International Journal of Advanced Research in Computer Science and oftware Engineering, Volume 4, Issue 9, September 2014.

[2] Ganorkar, Sujata Agrawal," Releaving the Hidden Secret with LSB Steganography", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering,Vol. 1, Issue 3, June 2013

[3] Shikha Mohan , Satnam Singh ,"Information hiding with LSB based Image Steganography", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015

[4] Kanika Anand, Er. Rekha Sharma,"Comparison of LSB and MSB Based Image Steganography", International Journal of Advanced Research in Computer Science and oftware Engineering, Volume 4, Issue 8, August 2014

[5] Sandeep Singh, Aman Singh," A Review on the Various Recent Steganography Techniques", International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013

[6] Shikha Mohan, Satnam Singh, "Image Steganography: Classification, Application and Algorithms", International Journal Of Core Engineering & Management (IJCEM) Volume 1, Issue 10, January 2015

[7] Sudhakar Singh, Pankaj Singh , Dr. Rakhi Garg , Dr. P. K. Mishra " Some Observations Of Image Steganography On Implementation Of Least Significant Bit Technique With Mapping Method", International Journal of Advanced Research in IT and Engineering, Vol. 2, No. 2, February 2013

[8] Navjot Kaur, Manpreet Singh," Modified Approach Using Lsb In Image Steganography", International Journal OF Research -Granthaalayah, Vol.3(Iss.5):May,2015

