ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

An Efficient Image Steganography using the Secured Bit Inversion Technique

R. Ruba Mangala[1], P. Eswaran[2]

[1]*M.Phil Research Scholar,*[2]*Assistant Professor,*

Department of Computer Science and Engineering, Alagappa University,

Karaikudi, Tamil Nadu.

[1]rupakrish29.rsau@gmail.com,[2]eswaranperumal@gmail.com

***Abstract*— Steganography is an art of hiding information within other data. Least Significant Bit (LSB) is the most commonly used Spatial Domain Technique to conceal information inside the cover image. This paper provides, an enhancement on the classical LSB based Image Steganography and bit inversion technique is proposed to improve the stego image quality. Two phases of bit inversion techniques are proposed. In these phases the LSB of some pixels is inverted if they appear in a particular pattern. In this method, fewer number of pixels are modified and PSNR of the stego image is enhanced.**

Keywords - Steganography, Least Significant Bit(LSB), Bit inversion, PSNR.

I. Introduction

Steganography is one of the information hiding technique which hides the secret in another medium (Image, Audio, Video). It differs from Cryptography, which encrypts and transmit the data without hiding the existence of data. Stenography system uses multimedia objects as cover media due to several advancements in digital technology and networks so it is very easy to transmit or share the data over the internet. It is very important to secure the secret data. Steganography prevent the privacy of data by changing its properties so that it is not detectable to hackers or attackers. The media with hidden information is known as stego image and without hidden information is known as cover media.

Steganography is derived from the Greek origin, which literally means "covered writing". "Steganos" refers to "covered" and "Graphos" refers to "writing". It is widely used in military, diplomatic, personal and intellectual property applications. Several techniques are used to conceal the secret data such as invisible inks, microdots, digital signature, character marking, pin punctures [10]. In Steganography secret data is hidden in cover media (carrier object) resulting in stego image (contain secret data). It is difficult to recover the information due to the hidden factor without knowing the steganography technique.

An image with the secret data is called the stego image which is sent to the receiver and the receiver receive the stego image by applying the de-steganography method (Figure. 1 and Figure. 2). Least Significant bit (LSB) method is the simple steganographic technique to conceal the secret data in an image and it is commonly used.

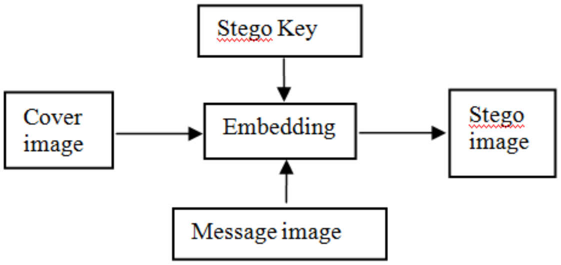

Fig. 1 Steganography at senders side

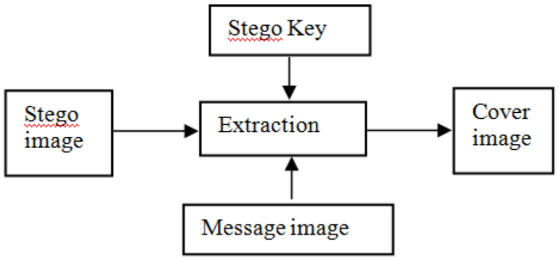

Fig. 2 Steganography at receiver side

This method preserves the quality of the image. It hides the bits of the message image into the LSB of the cover image. The advantage of LSB Steganography is that it is very simple, easy to understand and implement and the resultant image obtained will be almost similar to the cover image. Several steganographic techniques such as LSB Matching (LSBM), LSBM Revised (LSBMR) and Edge Adaptive based LSBMR have been proposed and implemented [1].

A good image steganographic technique aims at three aspects Capacity, Imperceptibility, Robustness [6]. The imperceptibility of the LSB method is good but the capacity of hiding the data is low due to modification of the last significant bit. Since, it is very simple to implement as well as easy to identify that the image contain hidden secret data by retrieving the LSBs. Therefore, Plain LSB is not a robust method.

This paper is organized in such a way that the session II describes the literature survey on various image steganographic technique. Session III describes the proposed work plan and the methodology followed by the conclusion in session IV.

II. Related Work

Nadeem Akhtar *et al.* [2] proposed an Image steganographic technique where a classical LSB algorithm is used to replace the secret message bit with the LSB bit of the cover image. Moreover , this method provided two layer of security by combination of classical LSB algorithm and a bit inversion method.

Mohammed Abdul Majeed *et al.* [3] proposed an Image steganographic method where a standard LSB algorithm is used to create a stego image and in addition it inverts the bits which increases the security and quality of the image.

Suma S *et al.* [11] proposed an bit inversion technique where a the cover image is encrypted in the embedding part. Encryption algorithm along with bit inversion technique provides the multilayer of security thus increasing the quality of the image

Manu Devi *et al.* [12] proposes a enhanced data hiding method based on LSB for embedding the random and non adjacent pixels of the secret message and 1-2-3 LSBs of red, blue, green components of randomly selected pixels.

Satwinder Singh *et al.* [13] reviewed the basic image steganography technique and also analysed the performance of each technique. The paper focused on the study of image based steganographic methods

Ratnakirti Roy *et al.* [14] evaluates most commonly recognized algorithms for image steganography in different domains of embedding for high level of security.

Mansi S. Subhendar *et al.* [15] reviewed the fundamental concepts, performance measures, parameters, merits and demerits of embedding secret message in different ways

The proposed method presents an improved LSB based steganographic method which is more secure than the classical LSB method. To analyze the bit patterns in the stego-image steganalysis is performed. Based on this, LSB of those pixels is inverted, which co-occurs with the specific bit pattern. This improves the PSNR of stego-image. The proposed method is based on 24-bit color image to improve the security and quality of stego-image using bit inversion.

III. Proposed Work Plan

A. *Classical LSB Algorithm*

A digital image is a collection of pixels representing the intensity of light at that pixel position. They are stored either in 8-bit per pixel (represents 256 different levels of light intensities) or 24-bit per pixel (represent a large number of color intensities). 24-bit images are called true colors because of the large number of color intensities and they need more space to hide the information. For example, A 24-bit image of dimension 1024 x 768 would have a size that exceeds 2 megabytes. The file size is very large which may attract the attention when transmitted over a network.

8 bit images are used to hide information where each pixel is represented as a single byte like GIF files. Each pixel corresponds to 256 colors which ranges from 0 to 255.

The classical least significant bit implies the use of the LSB plane of the original image by replacing the LSBs of the original image with the bits of the secret data. Since only the LSBs is changed the intensity does not differ between the original image and the stego-image. So the attackers could not identify the difference between the original image and the stego-image which contains the secret data and it cannot be identified by the attackers visually.

An Example shows the plain LSB method

Cover Image pixels :

01000001 01000010 01000011 01000100 01000101
01000110 01000111 01001000

Secret Image pixel : 11100101

Stego-Image pixels :

0100000**1** 0100001**1** 0100001**1** 0100010**0** 0100010**0**
0100011**1** 0100011**0** 0100100**1**

The bits that are bold in the stego-image represent the changed bits. The probability of modification made in the cover image will be 0.5. There are various variations are made by use of LSB approach. More than 1 bit can also be changed which increase the amount of data that can be hidden in the cover image, but depreciate the quality of the cover image [7][8].

The disadvantage of the classical LSB method is that the cover image size for hiding the secret data should be 8 times larger. This increases the bandwidth to send the image. Another drawback is that by collecting the LSB's of the stego image the attacker can easily extract the secret data. For this reason, the classical LSB method is not successful.

B. *LSB based Embedding Algorithm*

Input : A 24-bit RGB cover image (C)

```
        Input Cover image
For k=1 to length  (cover) do
   $S_j$ <- $Cover_j$
   For k=1 to length (p) do
   Compute index $j_k$,
   location to store the $k^{th}$ message bit
   of p
   $S_{jk}$ <- LSB($Cover_{jk}$) = $p_k$
   End
```

Output : Stego image s

C. *LSB based Extracting Algorithm*

Input **:** A 24-bit RGB Stego image (s)

```
Input Stego image s
For k=1 to length (p) do
   Compute index jk location to store
    the kth message bit        of p
    pkj <- LSB(Coverjk)
    End
```

Output : Cover Image (C)

The above LSB based embedded and extraction algorithm is illustrated by Neil F. Johnson *et al.* [5]. In the extraction process without any reference to the cover image in the given stego image the fixed messages can be extracted. Like the embedding process the bits are chosen from the stego image using the similar sequence. The methodology of proposed work is as follows

D. *Bit Inversion Technique*

This technique inverts the last bit of each pixel value in the cover image depending on the secret message. The proposed bit inversion technique is obtained by comparison made on the second and third last bit of the original image with the bits from the stego image obtained from the standard LSB method (Figure. 3). The process of the proposed method :

- Computing three bits of the specified pattern of cover-image. Classify the cover image according to the number of patterns from 3 bits.
- Applying the basic LSB method to get the stego image.
- From the resultant stego image, calculate the pattern occurrences in the last second and third bit of the stego-image.
- Compare the similarity between each pattern from both cover image and the stego-image.
- Invert the least significant bits if the no. of pixels that have been changed is greater than the no. of pixels that are not changed.
- Inverted bits are stored at specific location.

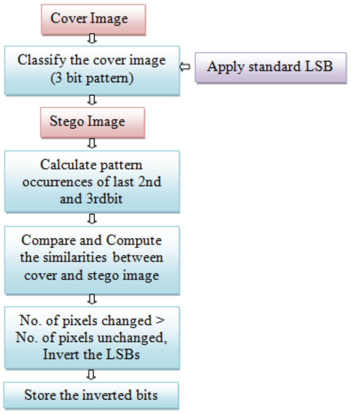
Cover Image
Classify the cover image (3 bit pattern)
Apply standard LSB
Stego Image
Calculate pattern occurrences of last 2nd and 3rdbit
Compare and Compute the similarities between cover and stego image
No. of pixels changed > No. of pixels unchanged, Invert the LSBs
Store the inverted bits

Fig. 3 Steganography at receiver side

An example is considered to show step by step process :

1. Let us consider a Cover image pixels 10001100, 10101100, 10101010 and 10101100
2. Apply standard LSB technique and label the resultant pixels as 1,2,3,4.

   Secret message: 1011

   Cover images:

   10001100 10101100 10101010 10101100
   1 2 3 4

   LSB stego-image :

   10001**101** 10101**101** 10101**011** 10101**101**
   1 2 3 4

3. The pattern occurrences in the bit position of stego image. From the above result there are four pixels with the patterns (101, 011). 1,2,4 pixels has the same pattern 101 and C pixel have the pattern 011.
4. For each pattern :

   a. For pattern '101' check the similarity between the pattern from the cover image and stego image, how many pixels are changed or remains unchanged

   b. For pattern '011' we cannot check because there is only one pixel, so comparisons cannot be made.

   c. Inverse the last bit if the number of pixels that have been changed is greater than the number of pixels that has not been changed.

   d. For patterns whose pixels changed the bit inversion operation is performed

   Cover image : 10001100 10101100 10101100

Stego image : 10001101 10101100
10101101

Result : 1000110**0** 1010110**1** 1010110**0**

1 2 4

From the result , stego image and original image look different by only one pixel. Thus the stego image PSNR value is increase as well as improves stego image quality. To extract the secret image from the stego image the patterns of LSB bit, which is inverted must be stored in a specific location. All the possible combinations of the pixels must be checked.

In de-Steganography, the patterns stored leads us to the pixels patterns which are inverted and is first read from the stego image so that it is easy to understand that which pattern is inversed and which pattern is not. Then the re-inverse the bits to recover the secret message bits.

According to existing methods, only 65% of red color are sensitive to the human eye, 33% are sensitive to green and around 2% are sensitive to blue. So based on this research the proposed approach used green and blue color channels from the RGB image. The bit inversion is applied on these color channels to improve the security and the red color act as noise data when an intruder tries to extract the secret message thus it increases the retrieving process more complex.

IV. Conclusion

Steganography is an art of concealing information in another medium where attackers could not identify the existence of secret message. The security has become the most important issue due to the several advancements in technology and networks. The main aim of this paper is to increase the security level of communication with an improved LSB based bit inversion technique. The proposed method meets three aspects high data capacity, imperceptibility and robustness which ensures high level of security and reliability.

References

[1] Amitava Nag, Saswathi Ghosh, Sushanta Biswwas, Debasree Sarkar, Partha Pratim Sarkar, "An Image Steganography Technique using X-Box Mapping", International Conference on Advances in Engineering, Science and Management , pp.709-713, 2012.

[2] Naddem Akhtar, Shahbaaz Khan, Pragati Johri, "An Improved Inverted LSB Image Steganography," Issues and Challenges in Intelligent Computing Techniques (ICICT), pp.749-755, 2014.

[3] Mohammed Abdul Majeed and Rossilawathi Sulaiman,"An Improved LSB Image Steganography Technique using Bit-Inversion in 24 Bit Color Image," Journal of Theoretical and Applied Information Technology, vol. 80, No.2, 2015.

[4] Dagar, S. "Highly randamized image steganography using secret keys," in Recent Advances and Innovations in Engineering (ICRAIE), pp.1-5, 2014.

[5] Neil F. Johnson, S.C. Katzenbeisser, "A survey of steganographic techniques", Proc. Information Hiding, pp. 43-78, 2000.

[6] C.Kessler, "Steganography : Hidding Data within Data. An edited version of this paper with the title "Hiding Data in Data". Windows & .NET Magazine.http://www.garykessler.net/library/steganography.html

[7] CC.Thien, J.C.Lin, "A Simple and high hiding capacity method for hiding digit-by digit data in images based on modulus function", Pattern Recognition 36, pp. 2875-2881, 2003.

[8] Wu, Nan-1., and Min-Shiang Hwang."Data Hiding : Current Status and key issues."IJ Network Security 4.1, 2007.

[9] Wang, c.-m et al., "A high quality steganographic method with pixel-value differencing and modulus function", Journal of systems and software, pp.150-158, 2008.

[10] Rawat D. and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications (0975-8887), 2013.

[11] Suma S. and Dharmambal, "A Novel Image Steganography based on Secured Inversion Technique", International Journal of Innovative Research in Computer and Communication Engineering(2320-9801), Vol 3, Issue 6, 2015.

[12] Manu Devi, Nidhi Sharma, "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images", Proceddings of Recent Advances in Engineering and Computional Sciences pp. 1-5, 2014.

[13] Satwinder Singh, Varinder Kaur Attri, "State-of-the-art Review on Steganographic Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.8, No.7, pp. 161-170, 2015.

[14] Ratnakirti Roy, Suvamoy Changder, Anirban Sarkar, Narayan C Debnath, "Evaluating Image Steganographic Techniques : Future Research Challenges", Computing, Management and Telecommunications, 2013

[15] Mansi S. Subhedar, Vijay H. Mankar, "Current Status and key issues in image steganography : A Survey", Science Direct, Computer Science Review 13-14, pp.95-113, 2014.