Improvement in Image stenography by LSB inversion Method- A case study

Ms .A.S. Bhandare[1], Ms. S.A. Patil[2]
[1,2]*P.V.P.I.T Budhgaon*

***Abstract*- Steganography is the idea of hiding private, confidential, sensitive data or information within a video, audio or a digital picture that appears to be nothing out of the normal. If a person views this object, he or she not gets any idea that secret information is hidden. So we are providing the security to import and dada against an unauthorized user. LSB (least significant bit) insertion is very efficient method to embed the information in cover file. In this paper we study the methods for improvement in traditional method. Here LSB bit inversion technique is used to improve the quality of stego image. In these methods a particular pattern of LSBs of selected bits of pixels are inverted if they occur with particular pattern of some bits of pixels. So only few pixels are modified and so PSNR of stegoimage is improved. At receiver side for correct de-stenography, the bit pattern for which LSBs inverted needs to be store. With this technique though intruder gets idea abbot hiding, he has to face much difficulty to recover the secret message. Hence we provide more security to our secret information**

***Index Terms*- bit inversion, Least significant bit, stegnography, PSNR**

I. INTRODUCTION

An important need of today's life is a communication. A various and many number of devices present today that have an ability to transmit the many forms of information from one place to another through different ways of communication , like different types of wireless networks, public network, or mostly used Internet. Under the rapid development of the Internet and multimedia techniques, digital data such as texts, images, videos, and audios now have been widely used in our daily life. The process of the digital information makes human lives become more convenient. People can transmit huge information via computer networks. But in some situations we need our information to be get secured carefully. However, the security of the computer networks is insufficient, and the transmitted data could be intercepted or grabbed by an illegal user. Therefore, how to ensure the digital data to be securely transmitted via the Internet is an important issue.[1],[2].The methods to overcome these problems are Steganography and cryptography. Steganography and cryptology are similar in the way that they both are used to protect important information. The main goal of steganography is to hide secret information in the other cover media (video, audio or image) so that other persons will not notice the presence of the information. Although steganography is separate and different from cryptography, but they are related in the way that they both are used to protect valuable information. Steganography is the science and art of writing hidden messages, by which third party cannot recognizes that message which is existed. The word "Steganography" comes from the Greek and it means "covered or secret writing."[11] as defined today, it is the technique of embedding information into something else for the sole purpose of hiding that information from the casual spectator. in steganography secret data in the form of text, voice, video, image, etc. . . is hidden into cover object using an embedding process or algorithm and form a stego object.

The basic concept is that it has a cover object that is used to cover the original message image, a host object that is the message or main image which is to be transmitted and the steganography algorithm to carry out the required object. The output is an image called stego-image which has the message image inside it, hidden. This stego image is then sent to the receiver where the receiver retrieves the message image by applying the de-steganography

There are different types of Steganography:

i).Text Steganography: It is not used very often because text files have small amount of redundant data.

ii).Image Steganography: This is used widely for hiding information in the cover image.

iii) Audio/Video steganography: Compared to others this is very complex to use [8]

Steganography is often confused with cryptography because they both are similar in the way that both are used to protect important and secrete information. The difference between the steganography and the cryptography is that steganography involves hiding information so it appears that no information is hidden at all. If a person views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

On the other hand cryptography is a method used for secure communication in the presence of third parties [3]. The various aspects in information security are,

• Confidentiality: The information transmission is only for reading by authorized persons.

• Authentication: The origin of the message is identified correctly with an assurance that the identity is not false.

• Integrity: Only authorized persons can be able to modify transmitted or stored information.

• Non-Repudiation: It requires that neither the sender, nor the receiver of message can be able to deny the transmission.

• Access Control: Requires that access may be controlled by the target system.

• Availability: The computer system assets are available to authorized parties whenever needed.

I. Comparison between Cryptography and Steganography

Sr No.	Cryptography	Steganography
1	Known message passing	Unknown message passing
2	Encryption prevents unauthorized person from discovering the contents of communication	Stenography prevents the discovery of existence of communication
	Cryptography alters the structure of the secret message.	Stenography does not alter the structure of secret message.
4	The goal of cryptography is to make data unreadable by third party.	The goal of Steganography is to hide the data from third party

A good technique of image steganography aims at three aspects. First one is capacity (the maximum data that can be stored inside cover image). Second one is the imperceptibility (the visual quality of stego-image after data hiding) and the last is robustness. The LSB based technique is good at imperceptibility but hidden data capacity is low because only one bit per pixel is used for data hiding [9]

Applications of Steganography

Steganography is very useful in the field of information technology for secure communication [3]. It is applicable to the following areas:

• Secret data storing and efficient confidential communication

• Protection of data alteration

• Media Database Systems

It keeps the integrity of data; this means there will not be modification in the content of the information during communication. Steganography technique is also used for watermarking. Watermarking is the process of hiding information in a carrier in order to protect the ownership of text, music, films and art. [8]

Cover Image Selection

To hide the secret message in cover image the proper cover image should be selected .It is very important to hide the information in digital image using lossless compression algorithm, because there is a chance for losing of information at the time of communication.. It provides chance for selecting the proper cover image that should be suitable for hiding the message [8].

There are two types of methods in digital images for hiding the message in cover image.

1. LSB (Least Significant Bit): This is method for embedding data into cover image. The least significant bit of each pixel of an image is altered to a bit of a message that is to be hidden [4].

2. MSB (Most Significant Bit): This method considers the value of the MSB of the pixels of the image for data hiding. The MSB bits of each pixels of an image are changed to a bit of a secret message that is to be hidden. [8]

II. RELATED WORK

Cryptographic is one of the traditional techniques to hide the secret data and protect it from unauthorized user. This may often achieved by scrambles secret data (say, plain texts) into some meaningless binary sequences, which are called cipher texts, using a predetermined key called as private or public key. At receiver side for decryption, the original data can be achieved back by using decryption algorithm and with the same key used for encryption. Though the secrecy of the encryption key promises the security of the important messages, any authorized user may decrypt the data and so pain text may not get well protected.

Usually encryptions manipulate the plain texts by permutations, substitutions, or mathematical operations with a single key [10]

In the past few years, the essential properties of image hiding techniques are summarized as follows: image quality and hiding capacity. The peak signal to noise rate (PSNR) is usually used to evaluate the image quality. Hiding capacity is referred to the hiding bit rate of a stego-image [5]. Information hiding schemes can be classified into two broad categories: spatial domain and frequency domain techniques [6]. The simplest image hiding technique hides the secret message directly into the spatial domain by modulating the least significant bits (LSB) plane of the cover-image [7]. The advantages of spatial domain techniques are high perceptual transparency, efficiency, and easily achieving of high hiding capacity. In frequency domain techniques, a cover-image are first transformed into the frequency coefficients such as discrete cosine transform (DCT)[14] and discrete wavelet transform (DWT)[14]. Then the secret messages are embedded by modulating the magnitude of these coefficients

LSB Stenography

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object. [12]

The below example shows a simple LSB method.

Consider A cover image contains

00111111	10001001	00101000
00111011	11100000	101010001
11111100	00100001	

Message image:

10101010

Steno graphed Image:

0011111**1**	1000100**0**	0010100**1**
0010100**0**	1110000**1**	10101000**0**
1111110**1**	0010000**0**	

This stegnographed images shows the changes tales place in cover image. Only last bit of cover image gets changed. Here only one bit i.e. LSB is changed, only one level of intensity which is indicated by pixel value differs between original and modified pixel. Hence human eyes cannot detect it. Hence an unauthorized person cannot get the idea that some message is hidden in the image. It also not causes a perceptible difference in image quality.

The disadvantages of LSB approach is the size of cover image required for a particular message image that is for a certain capacity of message cover image required is 8 times thus increasing the bandwidth to send the image [1 3]. Another disadvantage is that if an attacker suspects that some information is hidden behind the cover image, He can easily extract information by just collecting LSBs of stego image. For these criteria, this method is not successful.

III. LSB INVERSION METHODS

First Method:

In this paper we are going to study one novel LSB inversion method which is useful for improving the quality of image with very less changes in stego image.

Let's start with one example:

Let's consider the message that has to hide is 1011

Consider the four pixels of cover image as

01001100 01011101 01011011 10101101

After LSB insertion, Stego image pixels will come as
01001101 01011100 01011011 10101101

By observing this stego image pixels we can conclude that, out of four pixels, two pixels, first and second of cover image are changed

If we consider the two bit, we have four possible combinations for two bits i.e 00,01,10,11. For all these combination we are going to analyze stego image too find the number pixels whose LSB has changed and whose has not changed. If the number of pixels changed is greater than the number of pixel not changed, then we are going to invert the LSB of Changed pixels. Due to this less number of pixels of cover image will get changed. The total pixel benefit would be equal to the difference between no of changed and unchanged LSBs.

For above case, two pixels i.e. first and second of the cover image have changed. Now we are looking for second and third LSB. It shows that third pixels of cover image have 0 and 1 as their second and third LSB. Out of these three, for two pixels LSB has changed and one unchanged. So we are going to invert the LSB of these three pixels. So final stego image pixels will be
01001100 01011101 01011010 10101100

Now if we observe this final stego image we can conclude that only one pixel of stego image is different from cover image. This will help to improve the PSNR and hence improving the quality of image. At a receiver side for de-stenography, we need to store the fact that we have inverted LSBs for those pixels that have their second and third LSB as 0 and 1 respectively.

Second Method:

For the second approach we are concentrating on receiver side. So we have to consider that stego image is transferred and available at receiver side. With this assumption, stego-image quality can be further improved using bit-inversion technique. Here we are going to consider the LSB of cover image in addition to second and third LSB. For each possible combination (00, 01,10,11) of second and third LSB, we find four different types of pixels. First, the number of pixels in which LSB of cover image is 0 and it hasn't changed. Second, the number of pixels in which LSB is originally 1 and it remain unchanged. Third, the number of pixels in which LSB changed from 0 to 1. And fourth, the number of pixels in which LSB has changed from 1 to 0.let denote these pixels as A, B, C, D.

Now if A is less than C, then we are going to invert LSB in all those pixels which have the particular pattern of second and third LSB and also that LSB which have 0 in the cover image. On other hand if B is less than D, we have to invert the LSB of all those that have the particular pattern of second and third LSB and also that LSB which have 1 in the cover image.

By this scheme very less number of cover image pixels would changed. The total pixel benefit achieved with this scheme would be Min(C, A) + Min (D, B). At receiver side for destegnography, we need to store those pattern for which corresponding LSB bit has been inverted.

In this way, less number of cover image pixels would be modified. Here, pixel benefit would be equal to min(A,B)+min(C,D).As we have consider all possible combinations(00,01,10,11)for second and third pixels and LSB(0,1) for cover image, totally we need to store maximum of 8 patterns.

At receiver side to recover the cover image from stego image we need to analyze first, second, third LSB. Though the second and third LSB pattern of stego image remains same, LSB has changed. So authorized receiver must have the original cover image for correct de-stenography. As in this scheme we have checked total eight patterns compare to four patterns in first scheme, here total pixel benefit is more that first scheme.

V. CONCLUSION

Here we have studied the two methods of LSB inversion which are helpful for stego image enhancement. For the given message, if we select proper cover image then PSNR may get improved largely. If we consider that an unauthorized user determined that the message is embedded in the cover image, he has to face difficulty to recover it as some of the LSBs are inverted and some are not. This will misguide the staganalysis process and so the message recovery gets difficult. This LSB bit inversion method makes the stenography process much better by improving its security and also the image quality.

REFERENCES

[1] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques", Proceedings of the International Conference on Image Processing, IEEE Computer Society, Washington DC., USA., pp: 1019-1022, 7-10,October, 2001.

[2] B. B Zaidan, A. A Zaidan, Fazidah Othman, "Quality of Image vs. Quantity of Data Hidden inthe Image", International Conference Image Processing, Computer Vision and Pattern Recognition, pp. 343-347, 2009.

[3] Prashanti .G, Sandhya Rani.K, Deepthi.S " LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 8, August 2013, pp.788-799.

[4] Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography, Global Journal of Computer Science and Technology", Vol.10, Issue 1, April 2010, pp.4-8.

[5] Li, Xiaoxia, and Jianjun Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm", Information Sciences, Volume 177, No. 15, pp. 3099-3109, 2007

[6] A. F. Mohammed Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science Volume 5, No. 1, Science publications, pp. 33-38, 2009.

[7] S. Venkatraman, A. Abraham, M. Paprzycki,"Significance of Steganography on Data Security", IEEE International Conference on Information Technology: Coding and Computing (ITCC'04),Vol. 2, Las Vegas, pp. 347-351, April 2004.

[8] K.Thangadurai and G.Sudha Devi,"An analysis of LSB Based Image SteganographyTechniques", 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA

[9] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri "An Improved Inverted LSB Image Steganography", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT) 978-1-4799-2900-9/14

[10] Stallings, William, "Network Security Essentials Applications and Standards (For VTU)", Pearson Education India, 1982.

[11] Harish Kumar, Anuradha,"Enhanced LSB technique for Audio Steganography", ICCCNT'12 26th_28th July 2012, Coimbatore, India

[12] Shahzad Alam, S M Zakariya, and M Q Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images" 2013 5th International Conference on Computational Intelligence and Communication Networks DOI 10.1109/CICN.2013.66

[13] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, "Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography", The 18th International Conference on Pattern Recognition (ICPR'06) 0-7695-2521-0/06

[14] O. Deforges,R. L. Tataru, D. Battikh, S. El Assad, H. Noura , "Enhanced Adaptive Data Hiding in Spatial LSB Domain by using Chaotic Sequences", 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 978-0-7695-4712-1/12 $26.00 © 2012 IEEE DOI 10.1109