A New Method In Image Steganography With Improved Image Quality

SANDESH KUMAR[1] LAVALEE SINGH[2]
DR. ZHITM,AGRA

GAURAV KUMAR GUPTA[3] VIVEK KUMAR[4]
MANGALAYATAN UNIVERSITY

ABSTRACT:

The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography. This paper deals with the image steganography as well as with the different security issues, general overview of cryptography, steganography and digital watermarking approaches and about the different steganographic algorithms like Least Significant Bit (LSB) algorithm, JSteg, F5 algorithms. It also compares those algorithms in means of speed, accuracy and security.

This paper gives a brief idea about the new image steganographic approach that make use of Least Significant Bit (LSB) algorithm for embedding the data into the bit map image (.bmp) which is implemented through the Microsoft .NET framework.

1.INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to Transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet.

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and digital watermarking. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

2. LITERATURE REVIEW

2.1 The Scope Of Steganography

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and codingtheory, steganography has gone ‘‘digital’’. In the realm of this digital world, steganography hascreated an atmosphere of corporate vigilance that has spawned various interesting applications,thus its continuing evolution is guaranteed.

Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing stegnography techniques against popular attacks like steganalysis.

2.2 Cryptography

The word cryptography is derived from two Greek words which mean “secret writing”. Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. Cryptography is an effective way to protect the information that is transmitting through the network communication paths.

2.3 Steganography Versus Cryptography

The comparison and contrast between steganography and cryptography is illustrated from the following table 2.1

S.no.	Context	Steganography	Cryptography
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of Attack	Steganalysis: Analysis of a file with a objective of finding whether it is stego file or not.	Cryptanalysis

Table 2.1 Comparison and contrast between Steganography and cryptography

2.4 Types of Attacks

A hacker can disrupt this normal flow by implementing the different types of techniques over the data and network in following ways. They are:

1. Interruption
2. Interception
3. Modification
4. Fabrication

Interruption**:** Interruption is an attack by which the hackers can interrupt the data before reaching the destination. This type of attack shows the effect on availability and usually destroys the system asset and makes the data unavailable or useless.

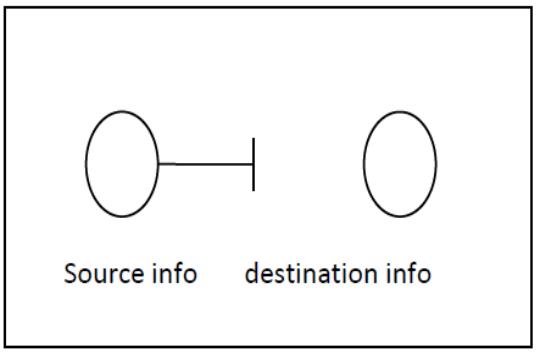


Figure 2.1: Interruption

Interception:

Interception is one of the well known attacks. When the network is shared that is through a local area network is connected to Wireless LAN or Ethernet it can receive a copy of packets intended for other device. On the internet, the determined hacker can gain access to email traffic and other data transfers. This type of attack shows the effect on confidentiality of data.

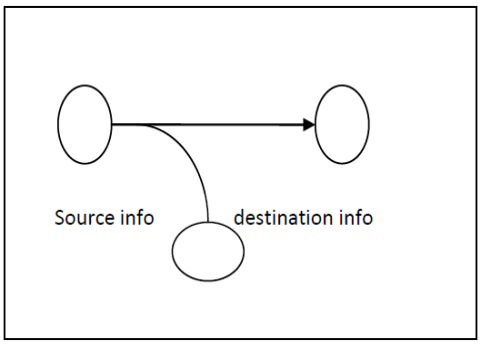


Fig2.2 Interception

Modification:

This refers to altering or replacing of valid data that is needed to send to destination. This type of attacks is done usually by

unauthorized access through tampering the data. It shows effect on the integrity of the data.

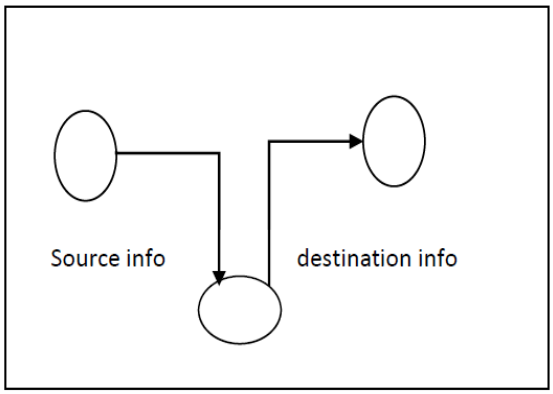


Fig: 2.3 Modification

Fabrication:

In this type, the unauthorized user places data without the interface of source code. The hacker or unauthorized person inserts the unauthorized objects by adding records to the file, insertion of spam messages etc. This type of attack affects on the Authenticity of message**.**

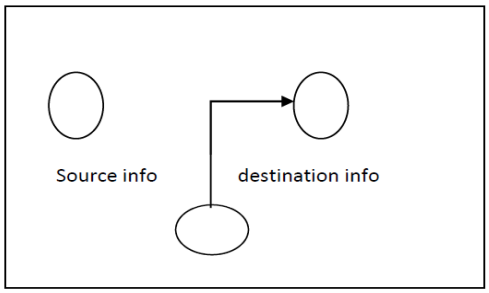


Fig2.4 Fabrication

2.5 Least Significant Bit Substitution

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover.

Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. Figure 2.5 that show a cover image and a stego image (with data is embedded); there is no visible difference between the two images.

Fig:2.5 cover image

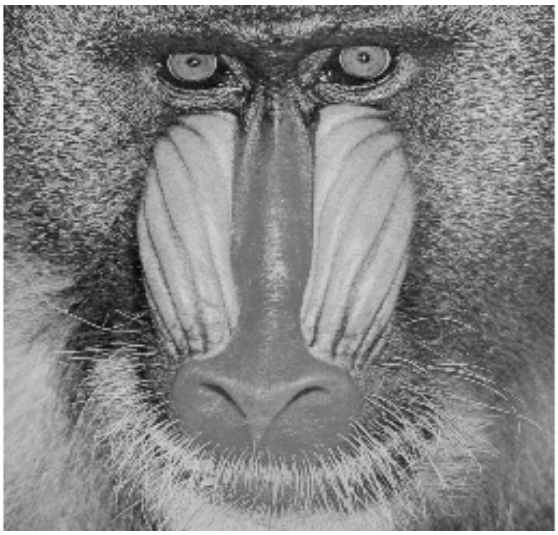


Fig:2.6 Stego Image

Above, replaces the LSBs of data values to match bits of the message. It can equally alter the data value by a small amount ensuring the a legal range of data values is preserved. The difference being that the choice of whether to add or subtract one from the cover image pixel is random**.** This will have the same effect as LSB replacement in terms of not being able to perceive the existence of the hidden message. This steganographic technique is called LSB matching. Both LSB replacement and LSB matching leave the LSB unchanged if the message bit matches the LSB. When the message bit does not match the LSB, LSB replacement replaces the LSB with the message bit; LSB matching randomly increments or decrements the data value by one. LSB matching is also known as ±1 embedding.

In the case of still grayscale images of type Bitmap, every pixel is represented using 8 bits, with 11111111 (=255) representing white and 00000000 (=0) representing black. Thus, there are 256 different grayscale shades between black and white which are used in grayscale bitmap images. In LSB Steganography, the LSB's of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes.

There are three possibilities [3]:

1. Intensity value of any pixel remains unchanged.

2. Even value can change to next higher Odd value Odd Value change to previous lower even value

2.7 DESIGN DETAILS

This section focuses on algorithms of LSB Steganography [10].

Algorithm (1) Least Significant Bit Hiding Algorithm.

Inputs: RGB image, secret message and the password.

Output: Stego image.

Begin

scan the image row by row and encode it in binary.

encode the secret message in binary.

check the size of the image and the size of the secret message.

start sub-iteration 1:

choose one pixel of the image randomly

divide the image into three parts (Red, Green and Blue parts)

hide two by two bits of the secret message in each part of the pixel

in the two least significant bits.

set the image with the new values.

end sub-iteration 1.

set the image with the new values and save it.

End.

2.8 The New method

LSB hiding technique hide the secret message directly in the least two significant bits in the image pixels, hence that affect the image resolution, which reduce the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret message based on searching about the identical values between the secret messages and image pixels, see Figure 3. The proposed

method is used to hide the secret messages by using algorithm 2.

Algorithm (2) The Proposed Hiding Algorithm.

Inputs: RGB image, secret message and the password.

Output: Stego image.

Begin

scan the image row by row and encode it in binary.

encode the secret message in binary.

check the size of the image and the size of the secret message.

start sub-iteration 1:

choose one pixel of the image randomly

divide the image into three parts (Red, Green and Blue parts)

Hide two by two bits of the secret message in each part of the pixel

By searching about the identical.

If the identical is satisfied then set the image with the new values.

Otherwise hide in the two least significant bits and set the

Image with the new values

Save the location of the hiding bits in binary table.

End sub-iteration 1.

set the image with the new values and save it.

End

2.9 Experiment Results

The LSB and the proposed hiding algorithms have been implemented in the VB6 programming language on duo core 2.0 GHZ in 2013 The two methods are applied to hide the secret message "I will come to see you on the first of June" on two Bmp images, the first with size (24 x 502 x 333) and called "The nature image" which is considered as a darken image see Figure 4a, while the second one with size (24 x 646 x 165) and called "The Jerash image" which is considered as a light image, see Figure 2.6.

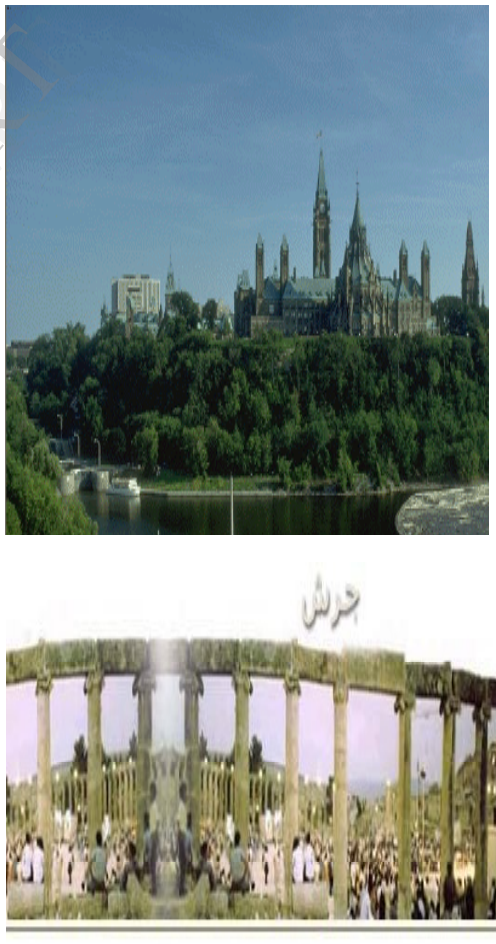


Fig 2.6

2.10 Discussion and Analyses

The proposed method and the LSB hiding methods, hiding every 6 bits of the secret message in one pixel of the image which usually chosen randomly therefore the secret message used in this paper has 43 characters which are 344 bits, to hide those bits 58 pixels are needed. In this paper, the results of the proposed and LSB hiding methods are analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. Figure 5 shows the shows the resultant images and the analysis table which present the ratio success obtained by the proposed hiding method when applied on the 2.7(a) and 2.7(b) images respectively. On the other hand Figure 6 shows the resultant images and the analysis table which present the ratio success obtained by the LSB hiding method when applied on the 2.7(a) and 2.7(b) images respectively.

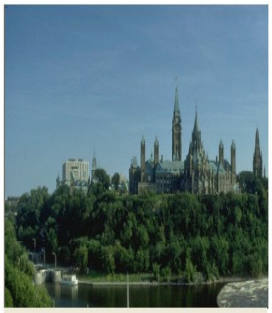
	Identical	No IDT	Ratio IDT	Ratio no ID1	Net Ratio
CLR RED	46	12	79%	20%	99%
CLR GREEN	45	13	77%	22%	99%
CLR BLUE	49	9	84%	15%	99%
SUM	140	34			

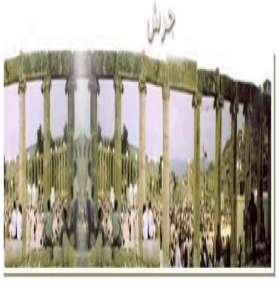
(a)

	Identical	No DT	Ratio IDT	Ratio no ID1	Net Ratio
CLR FED	35	23	60%	39%	99%
CLR GREEN	46	12	79%	20%	99%
CLR BLUE	31	27	53%	46%	99%
SUM	112	62			

(b)

Figure 2.7 The resultant images and the analysis table obtained by the proposed hiding method when applied on the (a) 4a and (b) 4b images.





	Identical	No IDT	Ratio IDT	Ratio no IDT	Net Ratio
CLR RED	18	40	30%	69%	99%
CLR GREEN	12	46	20%	79%	99%
CLR BLUE	16	42	27%	72%	99%
SUM	46	128			

	Identical	No IDT	Ratio IDT	Ratio no IDT	Net Ratio
CLR RED	12	46	21%	78%	99%
CLR GREEN	14	44	25%	74%	99%
CLR BLUE	13	45	23%	76%	99%
SUM	39	135			

Figure 6 The resultant images and the analysis table obtained by the LSB hiding method when applied on the (a) 4a and (b) 4b images

Figure 7 shows the differences between the proposed and the LSB hiding methods in the dark and the light images. Based on that Figure, it is clear that the proposed method is more efficient than LSB method because it search about the identical then start hiding. As well as the change in the bits is quite low and doesn't affect the image resolution

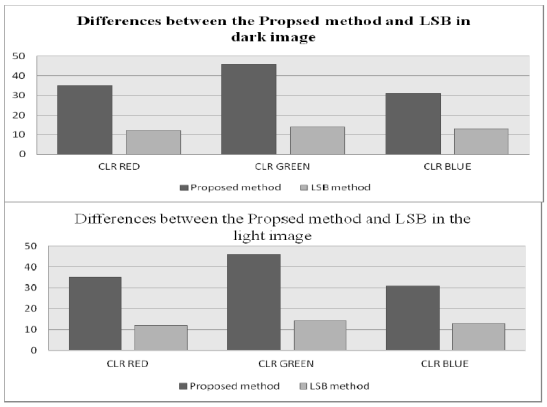


Figure 2.8 the differences between the proposed and the LSB hiding methods in the dark and the light images.

2.11Conclusion

In this paper, a new Steganography technique was presented, implemented and analyzed. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed and the LSB hiding methods were implemented to hide the secret message "I will come to see you on the first of June" on two Bmp images, with size (24 x 502 x 333) and (24 x 646 x 165) respectively.The results of the proposed and LSB hiding methods were discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. This paper conclude that the proposed method is more efficient, simple, appropriate and accurate than LSB method, it search about the identical then start hiding, hence the change in the image resolution is quite low, as well as it makes the secret message more secure. This paper concluded that the LSB

hiding method is the worst case of the proposed method. the result obtained by the proposed method and the LSB hiding method in terms of ratio of accuracy in improving the image quality were 83% and 43% respectively.

References

[1] B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).

[2] C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.

[3] H. Wu, H. Wang, C. Tsai and C. Wang, Reversible image steganographic scheme via predictive coding. 1 (2010), ISSN: 01419382, 35-43.

[4] J, Corporation, Steganography. http://www.webopedia.com/ TERM/S/steganography.html. 2005.

[5] M. D. Swanson, B. Zhu and A. H. Tewfik, Robust Data Hiding for Images, IEEE Digital Signal Processing Workshop, University of Minnesota, September 1996 (37-40).

[6] N Ghoshal, J K Mandal .A steganographic scheme for colour image authentication (SSCIA), Recent Trends in Information Technology ICRTIT 2011 International Conference on (2011), 826-831.

[7] N. Johnson, Survey of Steganography Software, Technical Report, January2002.

[8] N. Johnson, Digital Watermarking and Steganography: Fundamentals and Techniques , The Computer Journal. (2009)

[9] P. Fabien, J. Ross. Anderson, and Markus G. Kuhn. “Information Hiding – A Survey.” Proceedings of the IEEE, 87:7. 1062-1078. 1999.

[10] Spam Mimic. http://www.spammimic.com.

[11] W, Peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarking (second edition). San Francisco: Morgan Kaufmann. 3(1992) 192-213.

Sandesh Kumar received the B. Tech degree in Electronics and Communication Engineering from U.P.T.U in 2009 and M. Tech degree in Electronics and Communication Engineering from Mangalayatan University, in 2013. Currently Working as Assistant Professorf in,R.B Group of Institutions India. Research interests include Image Processing and Wireless Communication.

Lovely Singh received the B. Tech degree in C.S from U.P.T.U in 2007 and M. Tech U.P.T.U in 2011. Currently Working as Assistant Professor in, R.B Group of Institutions India. Research interests include Image Processing and Wireless Communication