IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 120-124
www.iosrjournals.org

An Adaptive Bit Flipping Technique In Colour Images

ShaniMol. A
(SN. Higher Secondary School Chithara Madathara, Kollam, India)

ABSTRACT : *In this paper an adaptive steganographic method using bit flipping technique based on some complexity values of the cover image pixels is proposed. Here a bit position in the image for embedding the payload is selected by analysing each pixel whether it is located in smooth or dark area of the image based on the complexity measure calculated using neighboring pixels .Unlike other spatial domain technique this proposed algorithm uses more bit positions other than LSB to embed the message. To increase the perceptibility of the image the proposed algorithm uses only the blue component of the pixels. Before embedding, the image is compressed and the message is encrypted. The proposed method claims a better capacity and a higher security.*

Keywords – *bit flipping ,cryptography, image steganography , image compession ,pixel complexity*

I. INTRODUCTION

Steganography is the process of hiding information (usually secret message) in any media like text, audio, image, video etc. The term steganography came from two Greek words 'stegos' and 'graphia' meaning 'cover' and 'writing' respectively [1]. Steganography can be applied in different areas like defense, banking, software security etc. Image steganography is applicable in defense for conveying their secret codes or messages between similar units. Now a days many users face problems related to the security of m-banking, net banking etc. Users are insecure of their account information and money which can be prevented by applying the steganographic techniques. Steganography can also be applied for the security of software, personal information, digital signature etc.

The process of hiding information has a long history. In ancient Greece, people wrote messages on the wood, and then covered it with wax upon which an innocent covering message was written. Modern steganography evolved in 1985 with the advent of personal computer being applied to classical stenographic problems. Like cryptography, now a number of stenographic programs are also available. Though both the cryptography and steganography have same meaning and are used for the same purposes, they differs each other in a way that cryptography focuses on keeping the content of the message secret but steganography focuses on keeping the existence of a message secret[2]. Both technologies has its own demerits that both alone is not perfect and will not give a strong and complete support for security. Once the presence of hidden message is revealed or even suspected the purpose of image steganography will be defeated[2].

Steganography

Steganography is a technique which hides the message in such a way that no one can identify the existence of hidden message[1]. Steganography is an area in which many studies and intensive research have been carried out. It is very important to have secure transmission of confidential information through network. There are several different methods and algorithms for hiding data in different types of files such as images, audio, video etc. Digital images are a preferred media for hiding information due to their high capacity and availability on internet.

Steganography techniques are mainly divided in to two categories-The spatial domain technique and frequency domain technique. In each of these categories we can have adaptive and dynamic methods. Adaptive methods are image statistics based, where as dynamic methods are message bit dependent. When hiding information inside images usually least significant bit (LSB) substitution method is used. In the LSB substitution method the 8th bit (LSB bit) of every byte of the carrier file is substituted by one bit of the secret information [3]. This can be done in two ways-LSB-F (LSB Flipping)OR LSB-M(LSB Matching).In LSB-F the image bit is replaced with the message bit but in LSB-M the whole pixel value is changed a certain unit.

The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes and hence the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. On the other hand, in frequency-based image steganography, the information is hidden using frequency domain techniques like DCT, DWT etc.. Unfortunately, frequency-based techniques are more complex and require much more computations. Usually BMP and GIF images are used mainly for image domain steganography since they use lossless compression. But JPEG file format is very popular file format for transform domain steganography because of the small size of the images.

Types of Steganography

Almost all digital file formats like text, audio, video etc. can be used for steganography, images are more suitable for steganography because of the high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of the objects are those bits that can be altered without the alteration bing detected easily. The four main categories of file formats that can be used for steganography are

Image steganography

Images are the most popular hiding media for steganography because of its large amount of redundant bits and greater availability of images on the internet.

A digital image is actually an array of light intensity values (numbers) of the different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. The number of bits in a colour scheme, called the bit depth refers to the number of bits used for each pixel. The smallest bit depth in current colour scheme is 8, means that there are 8 bits used to describe the colour of each pixel. Monochrome and grey scale images need only 8 bits for each pixel but colour images need 24 bits , 8 bits for each primary colours (red, green and blue). Thus in one pixel there can be 256 different values of red, green and blue getting more than 16 million colours.

Audio steganography

For hiding information in audio files, similar techniques are used as for image files. One different technique to audio steganography is masking, which exploits the properties of human ear to hide information. A faint but audible sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information [4].

Text steganography

One of the methods used in ancient days was to hide the secret message in every n^{th} letter of every word of a text message. It is only since the beginning of the internet and all the digital file formats that has decreased its importance. Text steganography using digital file s is not used very often since text files have a very small amount of redundant data [4].

Protocol steganography

This refers to the technique of embedding in the network control protocols used in network transmission. In the layers of OSI model there exist covert channels where steganography can be used [4].

II. RELATED WORK

For hiding information inside images usually least significant bit (LSB) substitution method is used. LSB embedding can be performed by either LSB flipping (LSB-F) or by LSB matching (LSB-M). In LSB-F technique a data bit replaces the LSB of an image pixel which at most causes a change in the least significant bit of an image. But in the LSB-M method the LSBs are not simply replaced; instead the whole pixel is randomly incremented or decremented if the LSBs differ from data[5]. In the LSB substitution method the 8th bit (LSB bit) of every byte of the carrier file is substituted by one bit of the secret information. For example consider 3 pixels of a 24-bit colour image as follows:

(00101100 00011101 11011100) (10100111 11000100 00001101) (11010011 10101100 01100011) Suppose we are inserting an information 100 and the binary representation of 100 is 01100100.When we insert this information 100 to the cover image pixel , the final image bits will be like this (1010110**0** 0001110**1** 1101110**1**) (1010011**0** 1100010**0** 0000110**1**) (1101001**0** 1010110**0** 01100010)

According to the basic RGB color model, every pixel is represented by the three bytes namely Red, Green, Blue. Red color represents the intensity of red color in the pixel, Green represents the intensity of green color in that pixel and Blue represents the intensity of blue color in that pixel. According to FCA technique the bits of first component (blue component) of pixels of image have been replaced with data bits as visual perception of intensely blue objects is less distinct that the perception of objects of red and green [6]. Since there are 256 possible intensity values for each primary color, changing the least significant bit of a pixel will make only a small changes in the intensity of the colors. These changes cannot be perceived by the human eye, thus the secret message can be successfully hidden. But the above said approach is very easy to detect the secret message. A little better approach for secure communication involves the use of a secret key.

Vajiheh Sabeti et al. tell about another method which embeds data in spatial domain based on the complexity features of an image. Here embedding is only performed for pixels that posses complexity value which is higher than a certain threshold [5].

Shilpa Gupta proposes Enhanced LSB algorithm which works in the spatial domain of colour images. It improves performance of LSB by hiding information in only one of the three colors that is blue color of the carrier image [9].

Mohammad Tanvir Parvez et al. introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: color intensity (values of R-G-B) is used to decide the no of bits to store in each pixel. It is based on the concept that Channels containing lower color values can store higher number of data bits[8].

Adnan Abdul-Aziz Gutub propose a new steganography method using RGB image pixels as its cover media in which information is hidden into two of the RGB pixel channels based on the indication within the third channel[7].

Amanpreet Kaur and Neetu Sardana proposed a technique called NIS that will use four bits of first component to hide the data .Here they Applied XOR on LSB bit of Red component and one bit of secret Key and Computing the result. If result of XOR comes out to be 0, then data is stored in first four bits else data is stored in last four bits of first component (blue) of pixel[6].

Nath et al. proposed another method which substitute the bits of the secret message in to 4-th bit position of every byte of the cover file[10].

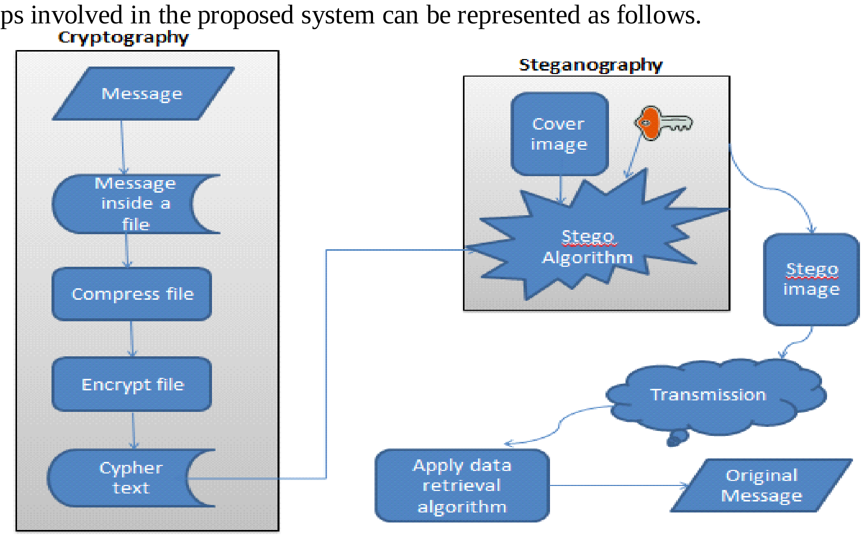
All these above said techniques hide data in fixed pixel locations of the cover image as mentioned in their respective techniques and that can easily be attacked once the attacker happened to know about the technique. This proposed new method is more difficult to attack because here message bits are not inserted in to the fixed position , in most cases Least Significant Bit position ,Here instead of that the data bits are spread across all over the image and hence it is more secure. LSBs are more suspicious, thus embedding in the bits other than LSBs could be helpful to increase the robustness [1].

III. PROPOSED WORK

The work involves a study and implementation of a new algorithm for sending secret message using image steganography with cryptography. The proposed algorithm is using multiple levels of security to maintain the privacy. In the first level cryptography is used which provides a better security and in the next stage, the security is strengthened by a new steganographic algorithm.

For hiding the data, a username and password are required for using the system. The secret message that is extracted from the system is transferred into text file first. Then the text file is compressed into a zip file using a powerful compression technique. Before embedding the secret message in a cover file we encrypt the message using an encryption algorithm and convert the text into cipher text. Then the cipher text file and the cover image files are converted in to binary codes. By applying a new steganographic algorithm, each message bit is embedded in different positions of the pixels in cover image, we get a better steganographic image.

The steps involved in the proposed system can be represented as follows.



Steganography algorithm

In this section, the steps involved in the proposed steganographic method are discussed.

Finding the pixel location

This step determines whether the pixel to be replaced in the image is located in a smooth or dark region. Here the complexity value of each pixel is calculated by using the values of neighbors of the pixel. If the complexity is larger ,then the pixel will be in dark area and if the complexity is smaller, the pixel will be in the smooth area. We can calculate the complexity in different ways. Here, this proposed algorithm uses 24 neighbours to get a vast area. Taking the difference of the pixel with the neighbouring pixel and summing up the differences[5]. Then we get the complexity value of that pixel. Depending on whether the pixel is in smooth area or dark area different steganographic algorithms are used for embedding the message bits in the image.

Embbedding procedure

Human eyes are more sensitive to changes in the smooth area than dark area. Dark regions are more suitable for embedding data than smooth area[5]. So we can use different bit positions other than LSB for embedding the payload in dark area. The proposed algorithm select up to 4 bit positions for embedding the message from the LSB positions. Thus it provides high security.

For embedding , the following steps are used.
For smooth regions
Replace the LSB of the first pixel
Replace the 7th bit of next pixel
After the 2nd pixel again start replacing the LSB of the next pixel.

For dark regions
Replace the LSB of the first pixel
Replace the 7th bit of next pixel
Replace the 6th of the next pixel
Replace the 5th bit of next pixel
After the 4th pixel again start replacing the LSB of the next pixel.

For example, the binary form of cypher text should embed in the pixels of cover image in the following pattern. one bit of the blue component of every pixel in the cover image(8th ,7th ,6th ,5th) positions of blue component) is replaced with 4 consecutive bits of cipher text. This process is repeated until all the cipher bits are finished. Suppose we are inserting a binary data 01100101 . Following is the binary representation of the target pixels

(10101100 00011101 11011100)
(10100110 11000100 10001101)
(11010010 10101100 01100111)
(10010110 10011100 11100101)

After embedding, the cover image pixels will transform to

(10101100 00011101 1101110**0**)
(10100110 11000100 100011**1**1)
(11010010 10101100 01100**1**11)
(10010110 10011100 1110**0**101)

System Implementation

An application will be developed to input the secret message. Cover image can be browsed locally or remotely. A process button click will process all steps including cryptography and steganography. Entire process is validated against a randomly generated alphanumeric key. The same key will be verified when extracting secret message from the stego-image. The reverse process (exraction process)will include file decompression , data decryption, bit extraction from stego-image and original message extraction.

IV. CONCLUSION

Most of the image steganographic algorithms have their own weak and strong points. Here proposes a simple image domain steganographic algorithm which will be better than available steganographic algorithms based on spatial domain techniques for the following reasons.

Since we use every pixels of an image to hide the message, a large amount of data can be hidden. ie. 600X800 images can store about 60000 characters at a time.

Here, the algorithm compares each pixel with its surroundings and thus selecting the apt positions to replace the bit.

We are using only blue components to hide the data as visual perception of intensely blue objects is less distinct that the perception of objects of red and green [6] .

Unlike LSB algorithms this technique uses different pixel positions to hide the message so that the attackers cannot attack easily and thus provides high security.

REFERENCES

[1] Saeed Ahmed Sohag, Dr. Md. Kabirul Islam, Md. Baharul Islam A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key [American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-09, pp-118-126 www.ajer.org]

[2] Prof. Akhil Khare, Meenu Kumari, J Pallavi Khare , Efficient Algorithm For Digital Images Steganography

[3] Gandharba Swain Saroj Kumar Lenka ,Steganography using two sided, three sided, and four sided side match methods Received: 13 May 2012 / Accepted: 17 April 2013 / Published online: 7 May 2013

[4] Mehdi Hussain and Mureed Hussain , Survey of Image Steganography Techniques *Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, (SZABIST), Islamabad, Pakistan.*

[5] Vajiheh Sabeti & Shadrokh Samavi & Shahram Shirani , An adaptive LSB matching steganography based on octonary complexity measure , Published online: 12 January 2012

[6] Amanpreet Kaur1 , Neetu Sardana2 , A Novel Image Steganography (NIS) Technique , International Journal Of Engineering And Computer Science ISSN:2319- 7242 Volume2 Issue 8 August, 2013 Page No. 2533-2535

[7] Adnan Abdul-Aziz Gutub , Pixel Indicator Technique for RGB Image Steganography

[8] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub , *College of Computer Sciences & Engineering , King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia,* RGB Intensity Based Variable-Bits Image Steganography

[9] Shilpa Gupta1, Geeta Gujral2 and Neha Aggarwal , IJCEM International Journal of Computational Engineering & Management, Enhanced Least Significant Bit algorithm For Image Steganography , Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893 www.IJCEM.org IJCEM www.ijcem.org

[10] A.Nath, S.Ghosh, M.A.Mallik Symmetric key cryptography using random key generator , Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239- 244