IMAGE STEGANOGRAPHY USING ENHANCED LSB TECHNIQUE

Nidhi
Kurukshetra University,Kurukshetra, Haryana, 136118, India
Email: nidhik.kashyap@gmail.com

Abstract- The art of information hiding has received much attention in the recent years as security of information has become a big concern in this internet era. Steganography – the art and science of hiding information has gained much attention. Image Steganography is one such field(Image acts as cover media for hiding secret message) with vast applications and opportunities. Image steganeganography is a method of hiding secret messages into a image (cover-media) such that an unintended observer will not be aware of the existence of the hidden messages. This paper is an attempt to analyse the various techniques of image steganography on the basis of parameters like PSNR ratio, MSE, efficiency, robustness and embedding capacity.

Keywords*:*- Data hiding , Image Steganography , Carrier-Image, Stego-Key, Stego-Image

1. INTRODUCTION

This paper's focus is on a relatively new field of study in Information Technology known as Steganography. This paper will take an in-depth look at this technologySteganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” [1]defining it as “covered writing”. In image steganography the information is hidden exclusively in image.

Image Definition

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image . This numeric representation forms a grid and the individual points are referred to as pixels.

Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its colour. These pixels are displayed horizontally row by row.

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 schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour are represented by 8 bits. Thus inone given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours. Not surprisingly the larger amount of colours that can be displayed, the larger the file size 15

2. LITERATURE SURVEY

R. Chandramouli [1] IEEE, in October 2001, analysed some specific image based steganography techniques and show that an observer can indeed distinguish between images carrying a hidden message and images which do not carry a message.

They derive a closed form expression of the probability of detection and false alarm in terms of the number of bits that are hidden. This leads them to the notion of steganographic capacity i.e. bits that can be hide in a message without causing statistically significant modifications. The author defines capacity in terms of detectability. The author provide results to provide an upper bound on this capacity.

Atallah M. Al-Shatnawi [2]in March 2012, discussed that "Steganography" is a Greek origin word which means "hidden writing". The word steganography is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing". In this paper, a new Steganography technique is presented, implemented and analysed. The proposed method hide the secret message based on searching about the identical bits between the image pixels values and secret messages. The proposed method was compared with the LSB benchmarking method. It was 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 LSB hiding method and proposed method were discussed and analysed based on the ratio between the number of the identical and the non-identical bits between the pixel colour values and the secret message values. The proposed method was efficient, simple and fast. It is robust to attack and improved the image quality, hence the method obtained an accuracy ratio of 83%.

ChiKwong Chan, L.M. Cheng Elsevier Publication Journal[3], 11 August 2003 in their paper described Spatial Domain Steganography technique LSB (Least Significant Bit) . Author further proposed LSB with Optimal Pixel Adjustment Process (OPAP).Bits are further divided into intervals & error rate is minimized. The outcomes are Good PSNR Ratio and Low computational Complexity.

AnindyaSarkar, UpamanyuMadhowand B. S. Manjunath,IEEE Transactions[4] , 2010 In their proposed a new steganography technique i.e. combination of matrix embedding & repeat accumulate code (ME-RA Scheme).Here ME is combined with RA technique for powerful error correction codes. The outcomes are High Embedding Capacity and Robust.

WeiqiLuo,Fangjun Huang and Jiwu Huang, IEEE Transactions [5], 2010proposed an Edge Adaptive technique in combination with LSB matching technique.Edge adaptive technique is used for region selection and then LSB is used for substitution. The method has very high quality steganography parameter.

3. COMPARATIVE ANALYSIS

ROBUSTNESS - Message ability to persist despite compression or other modifications.

PSNR Ratio - Approximation to human perception of reconstruction quality.

EMBEDDING CAPACITY - How much stego data can be embedded.

COMPUTATIONAL COMPLEXITY- Tells the complexity of steganographic algorithm.

MSE -Mean Square Error arising due to steganography.

Comparative Analysis

Technique	PSNR	MSE	Robustness	Embedding Capacity	Computational complexity
OLSB [1]	48.2	0.013	Average robust	Average	Low
ME-RA [2]	35	0.0854	Robust	Average	High
Edge	5	0.0	Less	High	High

Adaptive [3]	4.1	523	Robust		
Bit Combination LSB [3]	58	0.0253	Robust	Average	Low

4. Model/Algorithm

LSB Substitution

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.

For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

Region Selection

The other major part of the model concluded from the review done above is region selection. In all the papers there is one substitution technique used for embedding the stego-message & other technique is used for region selection so that there would be no compromise with the quality of the stego image like in paper [3] OPAP is used and in paper [5] edge adaptive method is used.

5. CONCLUSION

So based on the study done, the most appropriate technique to follow is spatial-domain technique i.e. LSB technique (Having High PSNR , Low MSE , Good Embedding Capacity) in combination with some randomization substitution technique(For Security , Robustness).

For better results we are first looking for encrypting the image using appropriate encryption algorithm.

6. PROPOSED WORK

In classical LSB method the data was embedded in last bit of the RGB components of every pixel. Thus every pixel can only store 3 bits of data. This amount of data is very small if we storing large files in an image. Hence, we have modified this concept and decide the number of bits to store in the RGB component based on first set bit of RGB component of current pixel.

Let the RGB components of the pixels (Pi) be:

RED (Pi) = (134)10 = (10000110)2

BLUE (Pi) = (14)10 = (00001110)2

GREEN (Pi) = (108)10 = (01101100)2For the pixel Pi's red component, first set bit is at position 8. If 15 is added to this pixel it would not change image significantly. The minimum 8 bit number is 128 if we add 15 to this number the number become 143.In colour this pixel is not much significant to human eyes. Here is the preview of the red pixel:

Fig. 1 Fig. 2

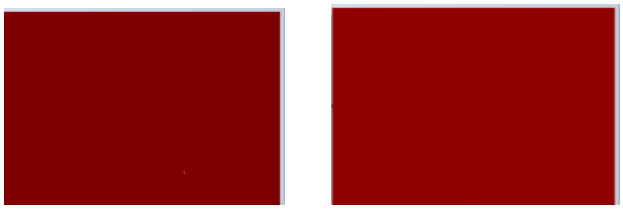


Fig. 1: Image with RED (pi) =128

Fig. 2: Image with RED (pi) =143

The basis for selection of number of bits to replace is shown below:

Bit number(first set bit)	Replace number of the bits
7-8	4
5-6	3
3-4	2
2-1	1

For example:

Data: "m" has ASCII value 109.

(109)10 = (01101101)2

If Data is embed in the above pixel then the resultant pixels are as follows:

RED (Pi) = (134)10 = (10000110)2

BLUE (Pi) = (14)10 = (00001111)2

GREEN (Pi) = (108)10 = (01101010)2

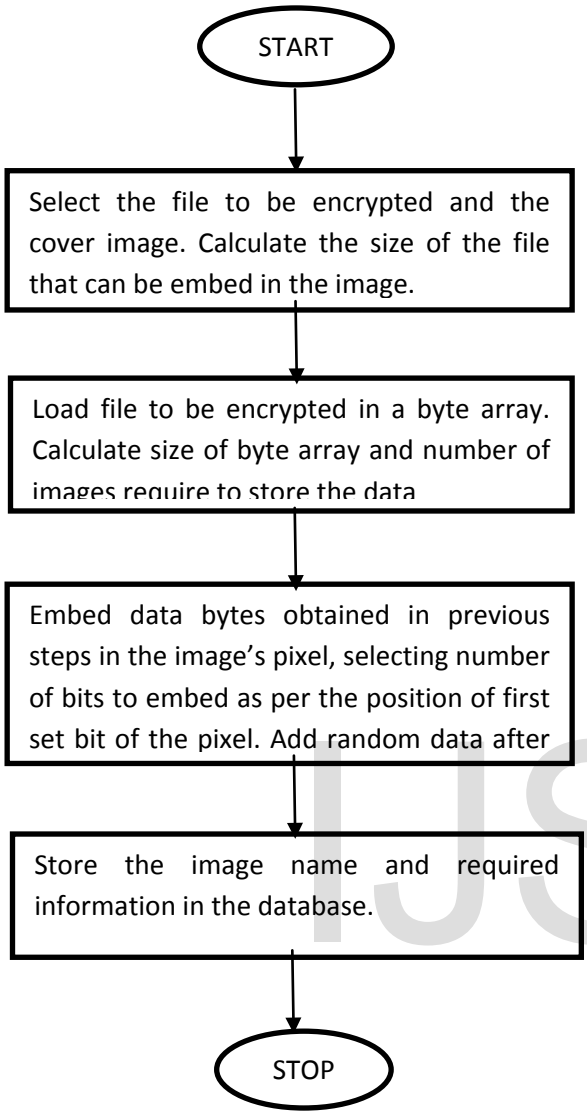
(Yellow colour represent the bits of data)

If the data bits are less than bits that can be replaced then we add random data following that bit in the remaining pixels of image.

Fig. 3 Image before embedding of data

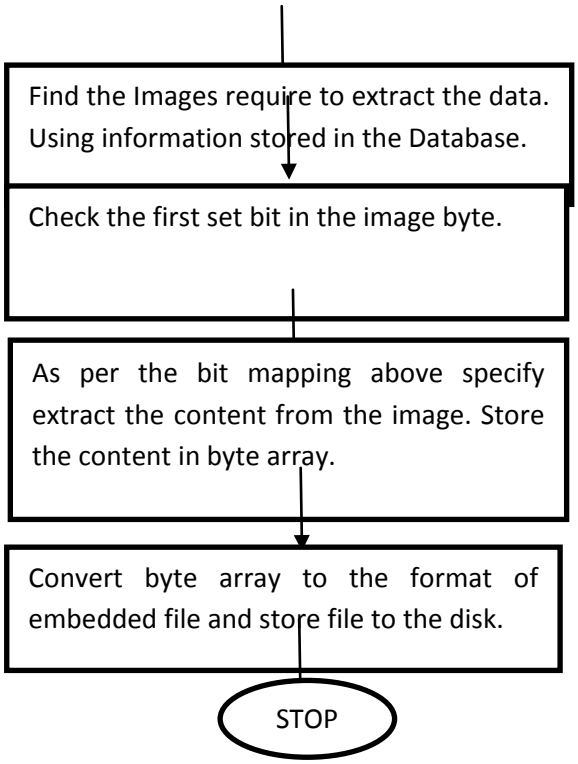
Fig. 4 Image after embedding of data

Encoding Process:



Encoding process using enhanced LSB substitution technique.

Decoding Process:



Decoding process using enhanced LSB substitution technique.

Encoding process

- The file to be hidden is selected by the user.
- Selected file is encrypted using AES 256 bit encryption.
- Encrypted file is converted to a byte array, and calculate the number of images required to hide file. For each RGB component of pixel, calculate the number of bits that can be stored, on the basis of position of first set bit and replace those bit from file to be hidden.
- After all the data is hidden, add random data to remaining pixel positions.
- Store image name and all the relevant information in the database.

Decoding Process

- Retrieve the images required to containing data of file to be extracted.

- For each RGB component of image's pixel do the following check the position of first set bit in the component.
- On the basis of first set bit, extract number of bits from the image.
- Add the bits to form a byte, when the byte is add to byte array.
- Once all the data is retrieved, decrypt the data using AES 256 bit encryption. Send the decrypted file to user

7. APPLICATIONS

Steganography helps in confidential communication and secret data storingSteganography provides us with:

Potential capability to hide the existence of confidential data

Hardness of detecting the hidden (i.e., embedded) dataStrengthening of the secrecy of the encrypted data

- ☐ Protection of data alteration
- ☐ Access control system for digital content distribution
- ☐ Media Database systems

8. FUTURE SCOPE

Steganography, though is still a fairly new idea. There are constant advancements in the computer field, suggesting advancements in the field of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A hopeful advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack.

What is scary is that such a small file of only one or two sentences may be all that is needed to commence a terrorist attack. In the future, it is hoped that the technique of Steganalysis will advance such that it will become much easier to detect even small messages within an image.

REFERENCES

[1] R. Chandramouli and NasirMemon, *"Analysis of LSB Based Image Steganography Techniques"*, IEEE, no. 1019-1022, february 2001

[2] Atallah M., Al-Shatnawi, *"A New Method in Image Steganography with Improved Image Quality"*, Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907–3915

[3] Chi-Kwong Chan and L.M. Cheng, "*Hiding data in images by simple LSB substitution*",Elsevier Computer Science Pattern Recognition, 37 (2004),No. 469 – 474

[4] AnindyaSarkar,UpamanyuMadhow and B. S. Manjunath,"Matrix *Embedding With Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography"*, IEEE Transactions On Information Forensics And Security, VOL. 5, NO. 2, JUNE 2010

[5] WeiqiLuo, Faniqun Huang and Jiwu Huang, *"Edge Adaptive Image Steganography Based on LSB Matching Revisited"*, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 2, June 2010

[6] KshetrimayumJenita Devi, "*A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique*", Department of Computer Science and Engineering, National Institute of Technology-Rourkela Odisha, No. 1-40, May 2013

[7] T. Morkel, J.H.P. Eloff, M.S. Olivier, *"An Overview Of Image Steganography*", Information and Computer Security Architecture (ICSA) Research Group