RESEARCH ARTICLE OPEN ACCESS

A Simple Steganography Technique for Hiding Data into Image

Satwant Singh[1], Proff. Lekha Bhambhu[2]
Research Scholar[1], Head of the Department[2]
Department of Computer Science and Engineering
JCDMCOE, Barnala Rd, Sirsa
Haryana - India

ABSTRACT

Steganography is the process by which we can hide the data into the image. Steganography and Cryptography both are different. As in cryptography a person can easily detect by naked eye that there is some change in the data but in steganography a person cannot detect by naked eye that's why it is the art of hiding data into image. In this paper the technique of LSB is used by randomly selecting the pixels and use them for embedding. Mat lab is used to develop a tool that is GUI interface and easy to use for hiding data.

Keywords:- Steganography, Image, Matlab

I. INTRODUCTION

Steganography is the process by which we can hide date into image and any audio file. In today's world security is the main concern. Steganography is the way to achieve security. Internet has become important and the most effective and fastest media for communication. Although, it there are many problems such as copyright, hacking, eaves dropping etc. But the need for secret communication is always remains. Now a days the importance of reducing a chance of the information being detected during the transmission is major concern. So some solutions are made so that effective and secure communication would be done in order to refuse consideration of the attacker or network hacker. Cryptography and Steganography are two fields available for data security. Steganography comes from Greek and literally means, "Covered writing". It is the art and science of writing of hidden message in such a way that no one can see the message instead of the receiver. Steganalysis is the process used to test the characteristics of hidden& science helps in designing the text message. Steganography is generally similar with cryptography because these two processes are similar in the way that they both are used to protect secret information. The main difference between them is the representation of the message bcos in case of steganography the message is visible and looks similar but in cryptography it shows that some changes are made through and moreover cryptography scrambles a message so it cannot be understood but on the other hand Steganography hides the message so it cannot be detect.

A message in cipher text might create a suspicion on the side of recipient while an invisible message created with Steganographic algorithm will not give any attention of data hidden. Focus at detecting secret information hidden in a cover image/audio and video files using Steganographic tool, Steganalysis has been interest since the end of 1990's.With the wide spread of Steganographic tool on the internet, the Hackers/attacker may communicate in a secret way with the help of Steganography and to avoid this the research on Steganography and Steganalysis is becoming more and more important. Since Steganography is used to hide the existence of communication, it has been applied to covert communication, watermarking and fingerprinting that assume to be holding the promise for copyright protection.

The main aim of steganography is secret communication. Therefore, steganography try to prevent that no one can detect that such communication is taking place. Essentially, steganographic systems should identify the redundant (insignificant)bits of cover files or medium. Therefore, any modifications to these redundant bits should not destroy the integrity of these mediums. As a result, preserving the integrity of cover files enhances the undetected ability of steganography (Anderson and Petit colas, 1998). Usually, hiding secret data using steganography adds as light change to the stage file properties. It makes difficult even impossible to detect that any communication had taken palace. Additionally, even if the hiding method used is publically known, nobody should be able to prove the existence of hidden data. However, detectability could be mainly achieved by adding no visible changes to the cover file. After the data hiding process, people have to see no visible traces in the stage file. Hence, If someone detects and proves that some data is hidden into the image then our method of steganography becomes unsuccessful.

What is Digital Image???

Digital image is the 2D array of m*n pixels. In the image processing the digital image refers to the two colours that is white and black

$$F\,(x, y)$$

Image is represented by the Function f(x,y) where x and y are the co ordinates of the pixel and F is the brightness of the point (x,y).The Pixel represents the value of the x & y and the co ordinate (0,0) is located at the top, left corner of the image. The value of *x* increases moving from left to right, and the value of *y* increases from top to bottom. In digital image processing, an imaging sensor converts an image into a discrete number of pixels. The imaging sensor assigns to each pixel a numeric location and a gray level or colour value that specifies the brightness or colour of the pixel.

Prosperities of the image:

Image Resolution

The number of rows and columns of image are called the resolution. An images made of *m* columns and *n* rows has a resolution of $m \times n$. This image has *m* pixels along its horizontal axis and *n* pixels along its vertical axis.

Image Definition

The number of shades that one can see is called the image definition. The bit depth of an image is the number of bits used to encode the value of a pixel. For a given bit depth of *n*, the image has an image definition of 2^n, meaning a pixel can have 2^n different values. For example, if *n* equals 8 bits, a pixel can have 256 different values ranging from 0 to 255. If *n* equals 16 bits, a pixel can have 65,536 different values ranging from 0 to 65,535 or from -32,768 to 32,767.

II. LITERATURE SURVEY

M. Goljan in [2007] proposed by cryptography, which aims to make communication unintelligible to those who don't possess the right keys. Once a third party can reliably identify which images contain secret messages, the stenographic tool becomes useless. Another important factor is the choice of the cover image. The selection is at the discretion of the person who sends the message. Images with a low number of colours, computer art, and images with unique semantic content should be avoided as cover images.

Zhe Wang [2008], proposed to identify the Least - Significant- Bit (LSB) steganography in the digital signals such as images and audio that the length of hidden data can fix signal samples can be estimated with high precision. The new steganalysis approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. To evaluate the robustness of the proposed steganalysis approach, bounds on estimation errors are developed.

An approach proposed by Andrew D. Ker [6], proposed to identify the spatial domain Least Significant Bit Matching (LSBM) steganography in gray scale images, which is proved much harder than for its counterpart, LSB replacement. The Histogram Characteristic Function (HCF), for the detection of steganography in colour images but ineffective on gray scale images.

A. Daneshkhah [2010], proposed the two bits of message is embedded in a pixel in a way that not only the Least Significant Bit (LSB) of picture element is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, but the point is in each embedding process only one alternation in one bit plane is allowed to happen. It is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for steganalysis algorithm.

Q. Huang [5] proposed the problem in LSB Matching Revisited (LSBMR) algorithm to make regions selection on images to find suitable area. By counting on each pixel we can decide if it should be protected. It can improve the visual imperceptibility and detectability of the LSB matching method. By adjusting the parameters of neighbour pixels, the max embedding capacity can be increased as needed.

Samir Kumar Bandyopadhyay[13] proposed Steganography is the art of writing hidden messages in such a way that no one; apart from the sender and intended recipient even understand there is a hidden message. Altering the LSB will only cause minor changes in colour. While this technique works well for 24-bit colour image files, steganography has not been as successful when using an 8-bit colour image file, due to limitations in colour variations and the use of a colour table. Colour table is organized as- the first three bytes correspond to RGB components and the

Last byte is reserved or unused.

III. METHODOLOGY & PROPOSED SYSTEM

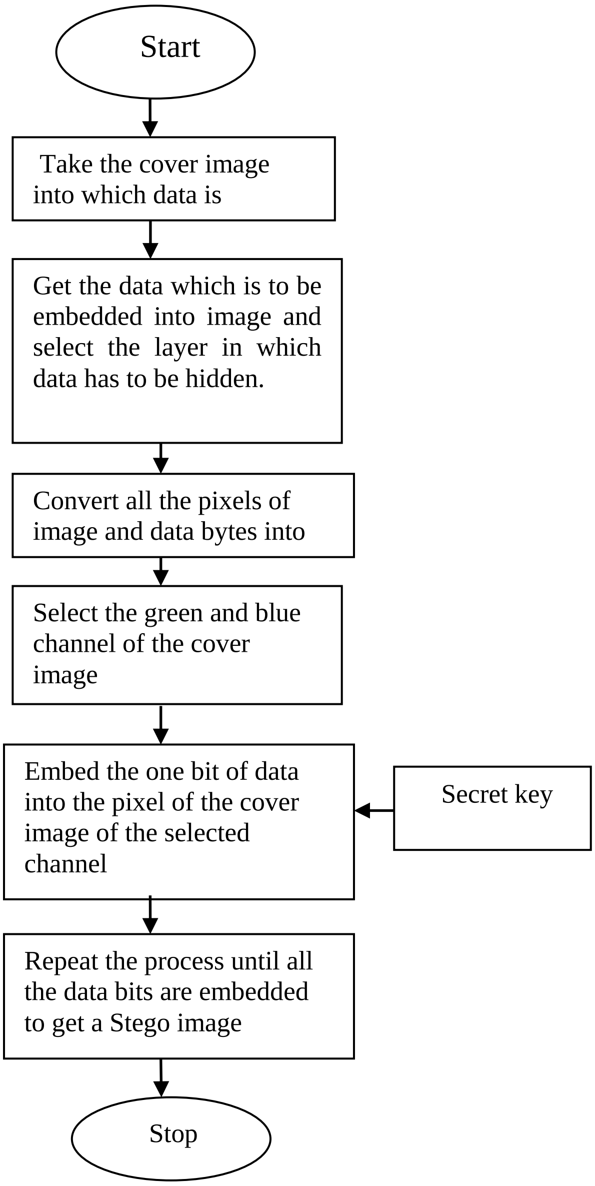
In modern digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same colour pixels repeated in a row. By applying the encrypted data to this redundant data in some random or non conspicuous way, the result will be data that appears to have the "noise" patterns of regular, non encrypted data. A trademark or other identifying symbol is hidden.

As seen in the various references, there are several different algorithms and methods are available for embedding of data into images and Extraction of data from the image. Most of the steganography methods are developed using the spatial domain (LSB substitution) and in the DCT domain (by changing the discrete coefficients). The main aim is to use the random pixels selected by the random number generator that is used for data hiding and then these random pixels can be used for embedding and extraction. So for obtaining the above said objective, in the algorithm, firstly there is embedding of data. It is done by implementing the following steps in a sequential manner:

- Select the image which will be used to embed data.

- Then convert the data into character format which will be embedded into image.
- Then we will select the 1 Dimensional image only that is RGB
- Convert all the pixels of image and data bytes into binary.
- Select the green and blue channel of the cover image.
- Then embed each bit into each pixel of the image into the channel which is selected
- Repeat the process until all the data bits are embedded to get a stego image.

In the end we will get the stego image which will look similar to the original image .Now the data is hidden into that image. In the same way the reverse process is used to extract the message that is hidden into the image .But for that we need the key that is used in the algorithm. The algorithm designed and processed in MATLAB platform.


Start
Take the cover image into which data is
Get the data which is to be embedded into image and select the layer in which data has to be hidden.
Convert all the pixels of image and data bytes into
Select the green and blue channel of the cover image
Embed the one bit of data into the pixel of the cover image of the selected channel
Secret key
Repeat the process until all the data bits are embedded to get a Stego image
Stop

Mat lab is used for this project. MATLAB stands for Matrix Laboratory. MATLAB was written originally to provide Easy access to matrix software developed by the LINPACK (linear system package) and EISPACK (Eigen system package) projects. MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming environment. Furthermore, MATLAB is a modern programming language environment: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming. These factors make MATLAB an excellent tool for teaching and research. MATLAB has many advantages compared to conventional computer languages (e.g. C, FORTRAN) for solving technical problems.

RESULTS

CHAMPIONS OF EUROPE
CHELSEA
FOOTBALL CLUB
CHELSEA FC · 2012

Normal Image

CHAMPIONS OF EUROPE
CHELSEA
FOOTBALL CLUB
CHELSEA FC · 2012

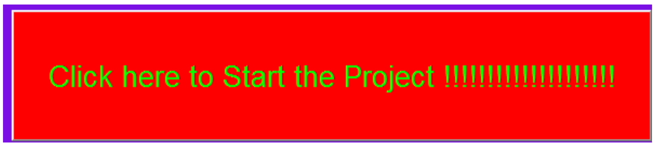
Stego image

As we can see there is no difference in both images. A person can not detect that which one is stego image and which one is normal one. The only way a person can detect is using the Matlab tools and the technique by which these images are encrypted.

Image	**Resolution**	**Size of image**	**Format**
Normal image	**480*547**	**35.8kb**	**Jpg**
Stego image	**480*547**	**35.9kb**	**jpg**

The images shown below will tell the process through the designed technique in matlab using gui interface

1-Firstly this box appears and click on it



Click here to Start the Project !!!!!!!!!!!!!!!!!!!!

2-Now it will ask wether you want to encrypt the image or decrypt the image

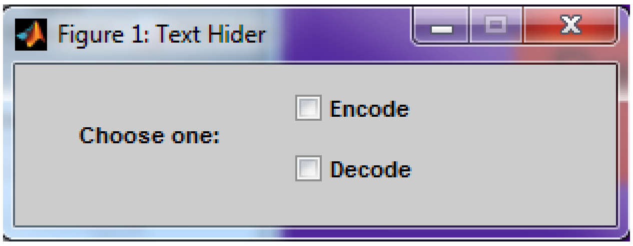


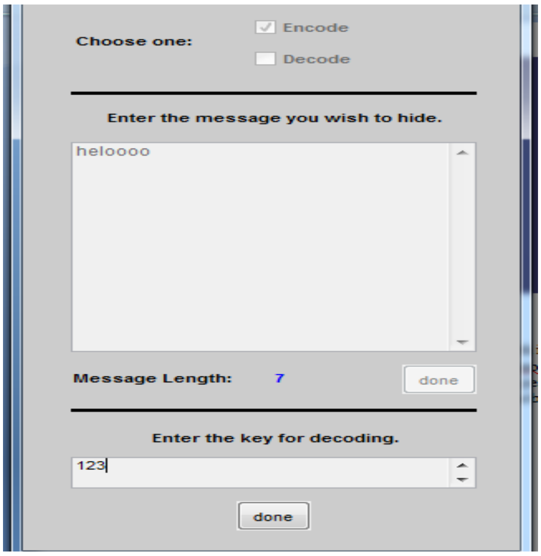
Figure 1: Text Hider

Choose one:

□ Encode

□ Decode

3—after that select the message you want to hide and the key used for this process



Choose one:

☑ Encode

□ Decode

Enter the message you wish to hide.

heloooo

Message Length: 7

done

Enter the key for decoding.

123

done

CONCLUSION

The scheme used in this will secretly hide the data into the image firstly it will encrypt the data that is to be hidden by using the encryption algorithm and then embed into the image. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it..The basic mechanism of the research is explained in this paper and it is somewhat different from pure steganography technique The advantage of our technique is the data file and reference image is going through the open channel separately. The basic result is interception of any one cannot provide desired objective. Second advantage is that any amount of data can be transmitted using the method because it is not depending on the size of image. Final advantage, the said method is not affecting the image. There is no change of quality and colour change of reference image. It is most vital achievement of method.

REFERENCES

[1] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray- Scale Images", IEEE Multimedia, vol.8, no.4, pp.22-28, Oct.200l.

[2] S.Dumitrescu, X.Wu, and Z.Wang,"Detection of LSB Steganography via Sample Pair Analysis", IEEE transactions on signal processing,vo1.51, no. 7, Ju1.2003.

[3] Andrew D. Ker, "Steganalysis of LSB Matching in Gray scale Images", IEEE signal processing letters, vol. 12, no. 6, pp. 441-444, Jun. 2005.

[4] Ali Daneshkhah, Hassan Aghaeinia and Seyed Hamed Seyedi, "A More Secure Steganography Method in

Spatial Domain", Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[5] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010.

[6] Andrew D. Ker, "A General Framework for Structural Steganalysis of LSB Replacement", in Proc.7th Int. Workshop on Information Hiding, 2005, vo1.3427, pp. 296-311.

[7] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", 2nd International conference on Computing, Communication and Networking Technologies, 2010.

[8] Andrew D. Ker, "A Fusion of Maximum Likelihood and Structural Steganalysis", in Proc.9th Int. Workshop on Information Hiding, 2007,vol. 4567, pp. 204-219.

[9] Adel Almohammad and Gheorghita Ghinea, "Image Steganography and Chrominance Components", 10th IEEE International Conference on Computer and Information Technology, 2010.

[10] Jarno Mielikainen, "LSB Matching Revisited", IEEE signal processing letters, vol. 13, no. 5, May 2006.

[11] Xinpeng Zhang and Shuozhong Wang,"Steganography Using MultipleBase Notational System and Human Vision Sensitivity" IEEE signal processing letters.

[12] Ying Wang, Student Member, IEEE, and Pierre Moulin, Fellow, IEEE, "Optimized Feature Extraction for Learning-Based Image Steganalysis" IEEE transactions on information forensics and security, 2007.

[13] Samir Kumar Bandyopadhyay” An Application of Palette Based Steganography”.