A Study on Steganography to Hide Secret Message inside an Image

D. Seetha[1], Dr.P.Eswaran[2]

[1] Research Scholar, School of Computer Science and Engineering,
[2] Assistant Professor, School of Computer Science and Engineering,
Alagappa University, Karaikudi, India

***Abstract*—** Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. There are many techniques to perform Steganography on electronic media, most notably audio and image files. In this paper, we present a new steganographic technique for embedding messages in BMP image. The main goal of this method, like any Steganography techniques must do, is to hide a text of a secret message in the pixels of the image in such a manner that the human visual system is not able to distinguish between the original and the stegoimage, but it can be easily performed by a specialized reader machine. This paper includes the basis of a wavelet-based low-throughput secret key Steganography system that requires the exchange of a secret key (stego-key) prior to communication. And, a new algorithm to hide data inside image using Steganography technique. The proposed algorithm uses binary codes and pixels inside an image. The zipped file is used before it is converted to binary codes to maximize the storage of data inside the image.

***Keywords*—**Steganography, Image, Steganographic, stegoimage, Hide, Secret Message.

I. INTRODUCTION

In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file. Steganographic systems, can be divided into two categories, one is in which the very existence of the message is kept secret, and non steganographic systems, in which the existence of the message need not be secret. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed. An attempt uses an audio file as a cover media to hide an mobile image without making noticeable changes to the file structure and contents of the audio file based on two Least Significant Bit insertion method of the low part of the audio file, as it has been already proved that modification of LSB creates a minimal change in the audio file format.

The performance of a steganographic system can be measured using several properties. The most important property is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associated measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects , and robustness, which refers to how well the steganographic system resists the extraction of hidden data. Nearly all digital file formats, with a high degree of redundancy, are known for their being used for steganography, the redundant parts refer to those parts capable of change without any possibility to detect the alteration. Image and audio files satisfy this requirement particularly well. In fact, digital images are the most used carrier file formats owing to their popularity on the internet. There are a number of steganographic techniques that enable one to hide a secret message in an image file, all of which have corresponding strong and weak points. Steganographic techniques applicable to specific image formats, including a taxonomy that classifies the techniques depending on the approach used to hide information.

II. IMAGE STEGANOGRAPHY

As stated previously, images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image

steganography techniques will exploit "holes" in the Human Visual System (HVS).

Image Files

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image .The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel .

Moreover, the smallest bit depth in the color scheme is 8,

(i.e.)., 8 bits are utilized to represent the color of each pixel. Both Monochrome and gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that digital color images are known for being saved in 24-bit files and for utilizing the RGB color model. Almost all the color variations for the pixels of a 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8 bits . Thus, in any given pixel, the number of different shades of red, green, and blue can reach 256 that adding up to more than 16 million combinations that finally result in more than 16 million colors.

The most prominent image formats, exclusively on the internet, are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, and to a lesser degree, the portable network graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure.

JPEG compression

If an image is to compress into JPEG format, the RGB color space is first turned into a YUV representation. Through this representation, the Y component represents brightness (or luminance) and the U and V components stand for color (or chrominance). It is known that the human eye is more sensitive to changes in the brightness of a pixel than to changes in its color . Down sampling the color information is taken as an advantage of the JPEG to reduce the size of the file Where the color components (U and V) are splitted in the horizontal and vertical directions and consequently reducing the file size by a factor of 2 . Then, the image is transformed. For JPEG images, the discrete cosine transform (DCT) is used; the pixels can be converted with such mathematical processing by simply "spreading" the position of the pixel values over the image or part of it. With DCT transformation, a signal is transformed from the representation of an image into the frequency domain, this is done by sorting the pixels into (8 × 8) pixel blocks and transforming these blocks into 64-DCT coefficients which are affected by any modification of a single DCT coefficient. The quantization phase of the compression is counted as the next step. Besides it is considered as biological property where the human eye is imposed. Basically, the human eye is known for being capable of identifying small differences in brightness over a relatively large area. The same does not apply when considering the distinction between different strengths in high-frequency brightness . Consequently, the strength of higher frequencies can be reduced without any change in the image appearance. The JPEG format is done by dividing all the values in a block via a quantization coefficient, so the results are made approximate to integer values. The last point is to encode the coefficients by using Huffman coding just to reduce the size.

JPEG Steganography

Previously, it was believed that steganography could not be used with JPEG images owing to the lossy compression, which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise. Data in most of the steganographic systems seems to be embedded into the non-zero discrete cosine transform (DCT) coefficients of JPEG images.

OutGuess: OutGuess is provided by Provos as a UNIX source code for which there are two widely known released versions. The first one is the OutGuess-0.13b, which is exposed to statistical analysis, and the second is OutGuess-0.2, which includes the ability to safeguard statistical properties. Hereafter, OutGuess refers to OutGuess-0.2. There are two stages representing the embedding process of OutGuess. The first of which is that OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0s and 1s.Soon after modifications are made

to the coefficients already left during embedding to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be subjected to a chi-square attack.

MB: Model-based steganography (MB) can be defined as a general framework for conducting both steganography and steganalysis by simply using a statistical model of the cover media. The MB method for JPEG images is capable of having high message capacity while remaining secure against many first-order statistical attacks .

YASS: Yet another steganographic scheme (YASS) belongs to JPEG steganography, but does not conceal data in JPEG DCT coefficients directly. Instead, an input image in the spatial domain is divided into blocks with a fixed large size, called big blocks (or B-blocks). A later stage is to randomly select within each B-block, an 8 × 8 sub-block known as embedding host block (or H-block). Then via using error correction codes, secret data is encoded and embedded in the DCT coefficients of the H-blocks. Finally, the entire image is compressed and distributed as a JPEG image after inversing DCT on the H-blocks.

`

III. HIDING SECRET MESSAGE

3.1 Convert Text to Byte

Data is converted into the bytes that are each character in message is converted into its ASCII equivalent. Moreover if message is password protected**,** then while retrieving message, the retriever has to enter the correct password for viewing the message.

For example:
If we are taking the character “a” in the message then “a**=“**01100001 is stored in byte array. Because ASCII value for “a” is 97 and binary equivalent is 01100001.

3.2 Hide the text in the Image

At 8 bit of the color that is processing, with alteration 2 least significant bit , Significant changes that we sighted system can detect changes in color is not in it. In this case leas significant bits have 4 state Which is shown in Table.

11	**10**	**01**	**00**

If we want to store information in 2 bit, at the worst situation 2 bit became symmetry.

For example:
If the red number is a 10111011 pixel, and we want to store the information in 2 least significant bit, at the worst situation the red color number alternated to 10111000, examinations shows that HVS cannot distinguish this alteration. So our idea was it, we insert our information into colour’s least significant bits. It is obviously that each character is 8 bit, so with storing it's bits into 2 least LSB, we can store the information in the image.

3.3 Message Embedding In Digital Image

Hiding image involves embedding the message in to the digital image. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these value often range from 0-255**.** In order to hide the message, and data is first converted into byte format and stored in a byte array. The message is then encrypted and then embeds each bit into the LSB position of each pixel position. It uses the first pixel to hide the length of message (number of character).Suppose we only change the last two bits are the bits that determine the “one place”, and the “two place” **.**

We can only alter the original pixel color value by 3. We use four colours in two pixels to store 8 bits character, the first color in first pixel: r7 r6 r5 r4 r3 r2 r1 r0. The second color in first pixel: g7 g6 g5 g4 g3 g2 g3g2. The third color in first pixel: b7 b6 b5 b4 b3 b2 b5b4. The first color in second pixel: r7 r6 r5 r4 r3 r2 r7 r6 of these character bits in the lowest red pixel, tow more in the lowest green pixel, the two in the lowest blue pixel and the two in the lowest red other pixel as follows. The first color in first pixel: r7 r6 r5 r4 r3 r2 c1 c0 The second color in first pixel: g7 g6 g5 g4 g3 g2 c3c2. The third color in first pixel: b7 b6 b5 b4 b3 b2 c5c4 .The first color in second pixel: r7 r6 r5 r4 r3 r2 c7c6.
If we take an example of pixel (255, 64, 64) with character “a”, then we can obtain**:** Original pixel=(11111111,01000000,0100000) **”**a” = 01100001 New pixel = (11111101, 01000000,0100000) New pixel =(253,64,64)
Here we can notice that the new pixel of (253, 64, 64) is almost the same value as the old pixel of (255, 64, 64). So there will not be noticeable color difference in the image.

For storing the text "save the text in the image" into the
image, we should save 26 character in the 104 colour, so at the image 24 bit BMP format we have 3 byte at any pixel, so, for storing the text, we proceed our image and store it's information at 33 pixels.

Figure 1: It shows one image before storing the text in to the image**.**

Figure (1)

For storing the text "save the text in the image" into the
image, we should save 26 character in the 104 color, so at the image 24 bit BMP format we have 3 byte at any pixel, so, for storing the text, we proceed our image and store it's information at 33 pixels**.**

At figure 2, after storing the text we see

Figure (2)

IV. *TO FIND THE PIXEL VALUES BY USING ALGORITHM*

The algorithm is going measure the intensity of the pixel and then hides' data by random pixel selection with a goal to hide maximum data in each pixel without creating extra unnatural noise. For perform the operation and find pixels whit higher intensity we obtains average color elements in this image. The number is a boundary to determine the elements whit higher intensity, these are elements that have greater average are more color intensity. Thus the intensity of pixels in the image are selected and scatter in a pixel selection is created. Elements selected are higher intensity pixels and have more than scatter.

Figure (3)

In figure 4, pixels higher than the average color images are marked with black color

Figure (4)

The total number of pixels in figure 5 is 215232 that number of pixels marked is 58468 To determine pixel whit more Intensity, we can add factor k to mean, whatever K is more than the specified number of pixels is less. If k=50 that number of pixels marked is 23405. For more efficient and find pixel of image that have a certain complexity, we divide image to block n*n. To pixels with more intensity than its neighbouring areas to be compared and we do operations to find the pixel with higher intensity on each block.

CONCLUSION

In this paper, discussed about the one of the other main uses for image steganography is for the transportation of highlevel or topsecret documents between international governments also it allows for copyright protection on digital files using the message as a digital watermark. This paper reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting.

ACKNOWLEDGMENT

First and for most, I own my whole hearted thanks to god for his merciful guidance and abundant blessing. I would like to express my humble gratitude to my parents who have taken over the great task of educating and providing me with lots of strength and courage.

REFERENCES

1. Image Steganography Techniques: An Overview. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi.
2. A Low-throughput Wavelet-based Steganography Audio Scheme. P. Carrión1, H.M. de Oliveira1, R.M. Campello de Souza1. 1Federal University of Pernambuco - UFPE, C.P. 7.800, 50.711-970, Recife - PE, Brazil.
3. Steganography Based on Payload Transformation. **K** B Shiva Kumar , K B Raja, R K Chhotaray, Sabyasachi Pattnaik. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.
4. Steganography Algorithm to Hide Secret Message inside an Image. Rosziati Ibrahim and Teoh Suk Kuan. Computer Technology and Application 2 (2011) 102-108.
5. A New Method to Steganography Whit Processing Picture in Three Colors (RGB). Khosravi, Sara,Abbasi Dezfouli, Mashallah, Int. J. Comp. Tech. Appl., Vol 2 (2), 274-279. ISSN:2229-6093.
6. A New Steganographic Method for Embedded Image In Audio File. Dalal, Khamael & Mohammed.
   SEGMENTATION AND HISTOGRAM GENERATION USING THE HSV COLOR SPACE FOR IMAGE RETRIEVAL. Shamik Sural, Gang Qian and Sakti Pramanik.