International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 8 34 - 38

Comparative Analysis of Hybrid Algorithms in Information Hiding

Mrs. S. Guneswari
Research Scholar
PG & Research Department of Computer Science
Sudharsan College of Arts & Science
Pudukkottai – 622 10
Tamilnadu, India

R. Balu
Research Supervisor,
PG & Research Department of Computer Science
Sudharsan College of Arts & Science
Pudukkottai – 622 10
Tamilnadu, India

Abstract: In this present work, propose comparative algorithms to conceal information into the image using steganography method. The proposedalgorithms use binary codes and pixels inside an image. The zipped file is used before it is transformed to binary codes to make the most of the storage of data inside the image. By applying the algorithms, a system called Steganography Imaging Information System (SIIS) is developed. The system is then tested to see the viability of the proposed algorithm. Different sizes of data are stored inside the images and the PSNR (Peak signal-to-noise ratio) is also captured for each of the images tested. According to the PSNR value of each image, the concealed image has a higher PSNR value. Therefore, this new steganography algorithm efficiently hides the data in the image.

Keywords: *BMP, Cryptography, , Image Hiding, LSB, Steganography.*

*****

1. Introduction

Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio file.

Where cryptography scrambles a message into a code to obscure it meaning, steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography's role is gaining prominence.

What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. or a file is hidden inside a carrier file, the data is usually encrypted with a password. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements :

The cover media(*C*) that will hold the hidden data

The secret message (*M*), may be plain text, cipher text or any type of data

The stego function (*Fe)* and its inverse (*Fe-1*)

An optional stego-key (*K*) or password may be used to hide and unhide the message.

2. Related Work

Hiding data is the process of embedding information into digital content without causing perceptual degradation [1]. In data hiding, three famous techniques can be used. They are watermarking, steganography and cryptography. Steganography is defined as covering writing in Greek. It includes any process that deals with data or information within other data. According to Lou et al. [2], steganography is hiding the existence of a message by hiding information into various carriers. The major intent is to prevent the detection of hidden information.

Research in steganography technique has been done back in ancient Greek where during that time the ancient Greek practice of tattooing a secret message on the shaved head of a messenger, and letting his hair grow back before sending him through enemy territory where the latency of this communications system was measured in months [3]. The most famous method of traditional steganography technique around 440 B.C. is marking the document with invisible secret ink, like the juice of a lemon to hide information. Another method is to mark selected characters within a document by pinholes and to generate a pattern or signature [3]. However, the majority of the development and use of computerized steganography only occurred in year 2000 [4]. The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme [5]. There are several steganography techniques used for hiding data such as batch steganography, permutation stehanography, least significant bits (LSB), bit-

plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS).

Research in hiding data inside image using steganography technique has been done by many researchers, for example in [6-10]. Warkentin et al. [6] proposed an approach to hide data inside the audiovisual files. In their steganography algorithm, to hide data, the secret content has to be hidden in a cover message. El-Emam [7], on the other hand, proposed a steganography algorithm to hide a large amount of data with high security. His steganography algorithm is based on hiding a large amount of data (image, audio, text) file inside a colour bitmap (bmp) image. In his research, the image will be filtered and segmented where bits replacement is used on the appropriate pixels. These pixels are selected randomly rather than sequentially. Chen et al. [8] modified a method used in using the side match method. They concentrated on hiding the data in the edge portions of the image. Wu et al. [10], on the other hand, used pixel-value differencing by partitioning the original image into non-overlapping blocks of two consecutive pixels.

This research uses a similar concept introduced by El-Emam [7]. A bitmap (bmp) image will be used to hide the data. Data will be embedded inside the image using the pixels. Then the pixels of stego image can then be accessed back in order to retrieve back the hidden data inside the image. Two stages are involved. The first stage is to come up with a new steganography algorithm in order to hide the data inside the image and the second stage is to come up with a decryption algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stego image.

3. Proposed Algorithms

A. DES + RSA

Hybrid encryption algorithm, DES algorithm for data transmission because of its higher efficiency in block encryption, and RSA algorithm for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission will be more secure. The proposed system works to hide data which should not be loss single digit. The proposed method based on JAR. JAR stands for Java Archive and it used to aggregate many Java class files and associated metadata and resources (text images and so on) into one file to distribute application software or libraries on the Java platform. The BPCS (Bit Plane Complexity Segmentation) technique is used to embed data into bitmap files. The ultimate goal is to embed as much data as possible into a cover image without detection by human perception or statistical analysis. In BPCS, the noisy region of an image is located on each bitplane as small pixel blocks which have noisy patterns.

B. Hash LSB + RSA

In the problem statement consisting of embedding the secret message in the LSB of each RGB pixels value of the cover image. Before embedding, the secret message is to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach we implemented a technique called Hash-LSB derived from LSB insertion on images. Our research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or intruders. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data. This technique also applies a cryptographic method i.e RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images.

C. LSB + AES

In this work considered a digital color image consists of different pixels. As a colored pixel can be represented as a mixture of red, green and blue color with appropriate proportions. In binary notation, it is represented by a stream of 8 bits. Therefore in total, 24 bits are required to denote a pixel. Thus an image is an array of many bytes each representing a single color information lying in a pixel. In the proposed method, a group of three sequential bytes from such an array is used to embed a bit of the entire message. The proposed technique has two main parts:

i. Changing the secret message (plain text) to cipher text by AES Cryptography

ii.Hiding the cipher into image by a proposed Steganographic technique 128 bits AES cryptographic algorithm takes a password and encrypts the plain text to cipher text.

This cipher text will be embedded into a cover image using our Steganographic technique. In the Steganographic technique, a filtering algorithm has been used to hide the information. The MSB bit specify the area where to embed the secret message. Our algorithm has the concept of randomly select an image and find if it is a darker or lighter image. Lighter image means MSB bits of Red, Green, and Blue component of a pixel contain at least 2 bit 1's and darker image means MSB bits of Red, Green, and Blue component of a pixel contain at least 2 bit 0's. If lighter pixel is greater than darker pixel, we select lighter pixel area to embed message and vice versa. This proposed work gives more security but provides less capacity for embedding information.

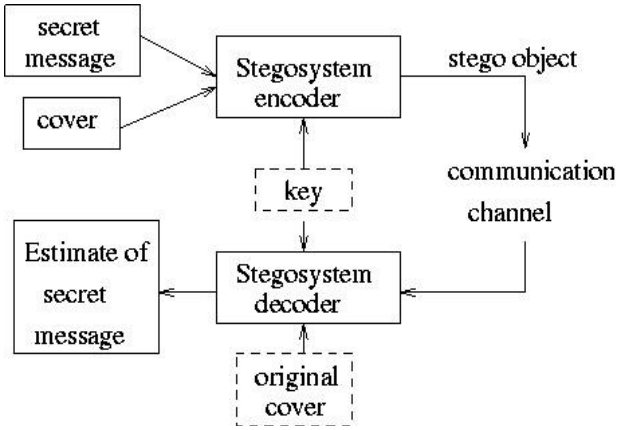

Fig 1. Framework for Steganography

4. Methodology

For the steganography algorithm, Fig. 2 shows the algorithm for embedding the secret message inside the image. During the process of embedding the message inside the image, a secret key is needed for the purpose of retrieving the message back from the image.

From Fig. 2, the secret message that is extracted from the system is transferred into text file first. Then the text file is compressed into the zip file. The zip text file then is used for converting it into the binary codes.

The purpose of zipping the text file is because the zipped text file is more secured if compared with the file that is without the zipped. The contents in the zipped file will significantly hard to be detected and read. Furthermore, this series of binary codes of the zipped text file and the key is a long random codes in which they only consist of one and zero figures. A data hiding method is applied by using this series of binary codes. By applying the data hiding method, the last two binary codes from the series are encoded into a pixel in image, then, next two binary codes are encoded to the next pixel in image, the process is repeated until all the binary codes are encoded. The secret key in this proposed steganography algorithm is playing an essentialrole where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each last two bit is encoded into each pixel in image. This will ensure the original image will not be tempered with too many changes.

Begin

Input: Cover_Image, Secret_Message, Secret_Key;

Transfer Secret_Message into Text_File;

Zip Text_File;

Convert Zip_Text_File to Binary_Codes;

Convert Secret_Key into Binary_Codes;

Set BitsPerUnit to Zero;

Encode Message to Binary_Codes;

Add by 2 unit for bitsPerUnit;

Output: Stego_Image;

End

Fig. 2 Algorithm for embedding data inside image.

Once the message is hidden inside the image, this message can be extracted back from the stego image. Fig. 3 shows the algorithm for extracting the secret message from the stego image. In order to retrieve a correct message from the image, a secret key is needed for the purpose of verification.

From Fig. 3, for the data extracting method, a secret key is needed to detect whether the key is match with the key that decodes from the series of binary code. Once the key is matched, the process continues by forming the binary code to a zipped text file, unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

Begin

Input: Stego_Image, Secret_Key;

Compare Secret_Key;

Calculate BitsPerUnit;

Decode All_Binary_Codes;

Shift by 2 unit for bitsPerUnit;

Convert Binary_Codes to Text_File;

Unzip Text_File;

Output Secret_Message;

End

Fig. 3 Algorithm for extracting data from stego image.

The main focuses of this proposed steganography algorithm are the use of transferring secret message to a text file, zipping file, a key, converting both zipped file and key into a series of binary codes, and the use of encoding each last two binary codes into pixels in image. The image quality is still robust where the distortion and colour changes of images are reduced to the minimum or zero-distortion. Secret message, on the other hand, is difficult to be stolen by steganalysis.

The proposed steganography algorithm consists of two image embedding techniques which are data hiding method and data retrieving method. Data hiding method is used to hide the secret message and the key in cover image while data retrieving method is used to retrieve the key and the hidden secret message from stego image. Hence, data or in particular a secret message, is protected in image without revealing to unauthorized party.

Both from Figs. 2-3 show that 2 layers of security are maintain within the system. However, the secret key is used for verification process in order to retrieve the correct message back from the image. This secret key is also embedded together with the data inside the image. Therefore, when a user is transmitting the image via the internet, that image contains the data and the secret key as well. However, the data can only be retrieved from the image using the system.

5. Result and Discussion

Based on the proposed algorithm, we develop a simple system, which implements the algorithm. We name the system as Steganogrphy Imaging Information System (SIIS). Based on the framework for the system as seenin Fig. 1, SIIS imposed on 2 layers of security. The first layer is for the login purpose and the second layer is for the hiding and retrieving purposesbe used by user to send it via internet or email to other parties without revealing the secret data inside the image. If the other parties want to reveal the secret data hidden inside the image, the new stego image file can then be upload again using the system to retrieve the data that have been locked inside the image using the secret key.

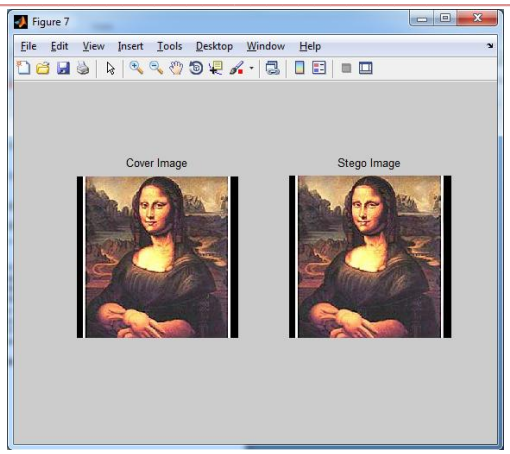

Fig. 4 (a) Original image (b) Stego image.

We then tested the algorithm using the PSNR (Peak signal-to-noise ratio). PSNR is a standard measurement used in steganograpy technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have.

If the cover image is *C* of size *M* × *M* and the stego image is *S* of size *N* × *N*, then each cover image *C* and stego image *S* will have pixel value *(x, y)* from *0* to *M-1* and *0* to *N-1* respectively. The PSNR is then calculated as follows:

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \tilde{y}_i)^2$$

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\mathrm{dB}$$

Note that MAX is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAX value is 255.

If the stego image has a higher PSNR value, then the stego image has more quality image. Table 1 shows the PSNR value for two stego images in Figures4. The PSNR is calculated using the equation of PSNR in Eq. (1). Based on values of PSNR from Table 1, the PSNRvalues show that the stego images have quality images without compromising of the original image.

The pixels of the cover image must fulfill the minimum requirement for the process of data hiding. The minimum image pixel for width is at least 150 while the minimum image pixel for height is at least 112.

Smaller images file size, for example, a BMP image with a sized of 1.0 MB, is proved to be capable of hiding the Secret Message within it. The biggest size of a zipped file to be encoded into a 1.0 MB BMP image by proposed system is 3.16 KB, which means that the size of image can encodes 10553 characters with spaces (or 1508 words or equally to 4 pages of words) underneath the image with near-zero distortion. Both cover and stego images are alike with the images that showed in Fig. 4 with near-zero distortion noticeable by naked eyes. Therefore, the proposed steganography algorithm is a strong yet robust algorithm to produce a stego image which will not be doubted by outsider that the image contains any secret message.

The image file format used in proposed algorithm is focused on bitmap (BMP) format. The BMP file format handles graphics files within the Microsoft Windows OS. Typically, BMP files are uncompressed, hence they are large. The advantage of using BMP files is the simplicity and wide acceptance of BMP files in Windows programs. Thus, this type of image is chosen to be used in our proposed algorithm. Since BMP image has a relatively larger size, the pixels in image are relatively larger as well. Thus, it provides more space for binary codes to be encoded within it. To increase as much as characters that can be hidden, zip technique is used to reduce to total size of file and to enhance the security of the file.

Using the proposed algorithm, we test several sizes of BMP images to see the various sizes of data being stored in the image. Table 2 shows these various results for the testing.

Table 2 shows the comparison of different sizes in BMP image by using the proposed steganography algorithm. These BMP images are used as cover images

Table 1 The PSNR value of stego images.

Images	Reference	PSNR for 1.0 KB
Mona	Stegno Image	32.15
Bhagat	Stegno Image	43.47

Table 2 Comparison of different sizes in bitmap images.

Algorithms	PSNR	Compression Ratio
DES+RSA	43.9328	4.1381
HASH LSB + RSA	41.3377	4.0925
LSB + AES	39.9328	3.8260

6. Conclusion

Cryptography deals with taking a message and making it appear as random noise, unreadable to an outside world. Steganography is not intended to replace cryptography but supplement it. Steganlaysis is the art of detecting the hidden messages embedded in digital media using steganography. Both Steganography and steganalysis have received a great deal of attention from law enforcement and the media. The present work describes a comparative evaluation of LSB steganography for different file formats. The strong and weak points of these file formats in LSB based image steganography are mentioned briefly. One would require a very large cover image to be able to hide a secret message inside a BMP file. The 800 x 600 pixels of BMP image file found to have less web applications. For this reason, LSB based image steganography is used with other file formats.

References

[1] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[2] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information – hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[3] Schneider, Secrets & Lies, Indiana:Wiley Publishing, 2000.

[4] T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H. Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569.

[5] M. Warkentin, M.B. Schmidt, E. Bekkering, Steganography and steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008, pp. 374-380.

[6] N.N. El-Emam, Hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232.

[7] P.Y. Chen, W.E. Wu, A modifed side match scheme for image steganography, International Journal of Applied Science & Engineering 7 (2009) 53-60.

[8] C.C. Chang, H.W. Tseng, A steganographic method for digital image using side match, Pattern Recognition Letters 25 (2004) 1431-1437.

[9] P.C. Wu, W.H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (2003) 1613-1626.

[10] V.Lokeswara Reddy, Dr.A.Subramanyam, Dr.P.ChennaReddy,"Implementation of LSB Steganography and its Evaluation for Various File Formats,"International Journal of Advanced Networking and Applications", Vol. 02, Issue: 05, pages 868-872. (2011).

[11] Kevin Curran, Karen Bailey," An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, fall 2003, Vol.2, Issue.2.

[12] Vivek Kumar, Sandesh Kumar, Lavalee Singh, PrateekYadav,"Implementation of LSB Steganography and its Evaluation for Various File Formats (LSB, JSTEG)", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 6, June – 2013.6.

[13] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J.Modern Education and Computer Science, 2012, 6, 27-34.

[14] Wai Wai Zin, "Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR), Vol.2 Issue 1, January 2013.