International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 3 Issue 3 ǁ March. 2015 ǁ PP.61-66

A Steganography LSB technique for hiding Image within Image Using blowfish Encryption Algorithm

Tawfiq S. Barhoom, Sheren Mohammed Abo Mousa
Faculty of Information Technology The Islamic University of Gaza

ABSTRACT: Steganography refers to information or a file that has been hidden inside a digital image, video or audio file. There are different carrier file formats can be used such as Text Steganography, Image Steganography, Audio/Video Steganography, but Image Steganography are the most popular because of their frequency on the Internet. It is the first common methods used for hiding the information in the cover image. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. steganographic algorithm for 8bit (gray scale) or 24 bit (colour image) is presented in this paper. Sometime steganography will not cover the total security of secret massage. So an additional security need to the secret massage. For this purpose blowfish encryption Algorithm is used in the proposed Steganographic system This work is concerned with implementing Steganography for images, with an improvement security and image quality.
The experimental result shows that the stego-image is visually indistinguishable from the original cover-image It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to cover up the very existence of the embedded data. and that the algorithm has a high capacity and a good invisibility.
Keywords: Steganography, cryptography, LSB, blowfish.

I. INTRODUCTION

A major issue for computer network is to avert important information from being disclosed to Unauthorized users. for this reason encryption techniques were introduced . most encryption techniques have an easy implementation and are widely used in the field of information security.

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing" (Greek words "stegos" meaning "cover" and "gratia" meaning "writing")(Das and Tuithung 2012).there are many type of Steganography such as: text Steganography ,audio/video Steganography and image Steganography.

Generally a steganographic system consists of cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide information, steganography gives a large opportunity in such a way that someone cannot know the presence of the hidden message. The goal of modem steganography is to keep its information undetectable(Karim 2011).

1. Steganographic Process Model

In steganographic model, message is the data that the sender wishes to remain it confidential. It can be plain text, cipher text, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number Password is known as *stego-key*, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the stego-object. the Figure 1 shows the Steganographic Process Model

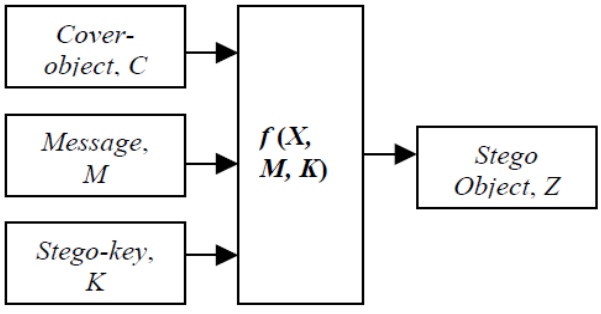

Figure 1: Steganographic Process Model

On the other hand, cryptography is not concerned with hiding the existence of a message, but rather its meaning by a process called encryption. The word cryptography is derived from the Greek word kryptos, meaning 'hidden'(Challita and Farhat 2011). Its method used for secure communication(Thangadurai and Sudha Devi 2014).

Cryptography is now an important research area where the scientists are trying to develop some good encryption algorithm so that intruders cannot intercept the encrypted message. There are two types of modern classical cryptographic (i) symmetric key cryptography : The same key is used for encryption and for decryption. (ii) Public key cryptography where we use one key for encryption and another key for decryption purpose(Chatterjee, Nath et al. 2011).

2. CRYPTOGRAPHY AND STEGANOGRAPHY

Cryptography and Steganography are well known and widely used techniques that control information in order to cipher or hide their existence respectively(Raphael and Sundaram 2011). Figure 2 shows the combination of cryptography and Steganography

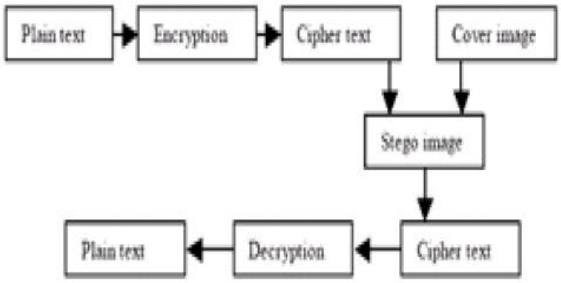

Figure2: Combination of cryptography and steganography(Thangadurai and Sudha Devi 2014)

Image steganography focused on hiding data inside cover images for security. Images have a lot of visual redundancy in the sense that our eyes do not usually care about superfine changes in color in an image region. One can use this redundancy to hide text, audio or image data inside cover images without making significant changes to the visual perception. Image steganography is becoming popular on the internet these days since a steganographic image, which just looks like any other image, attracts a lot less attention than an encrypted text and a secure channel(Gupta and Garg).

In this paper we proposed Steganography For Hiding Image within Image based on encryption was proposed combines the traditional encryption and information steganography.. It not only makes the secret information transmission "incomprehensible" and "invisible", but makes the steganographic system have a higher anti-detection performance. There are already a bunch of techniques available for this purpose and Least Significant Bit (LSB) Steganography is one of them. LSB steganography is a very simple algorithm where higher bits of the color channels of hidden images are stored in lower few bits of the color channels in the cover image.

II. LSB BASED DATA HIDING TECHNIQUE

The most common and simplest Steganography approach is the least significant bits (LSB) insertion. the secret messages are embedded directly. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding (Islam, Siddiqa et al. 2014). The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels:
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 10000001
Result:
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits which were actually altered. LSB insertion requires on average that only half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to hide the next character of the hidden message.

The advantages of Least-Significant-Bit (LSB) steganographic data embedding are that it is simple to understand, easy to implement, and it produces stego-image that is almost similar to cover image and its visual infidelity cannot be judged by naked eyes.

A good technique of image steganography aims to three aspects. First one is capacity (the maximum data that can be stored inside cover image). Second one is the imperceptibility (the visual quality of stego-image after data hiding) and the last is robustness. The LSB based technique is good at imperceptibility but hidden data capacity is low because only one bit per pixel is used for data hiding. Simple LSB technique is also not robust because secret message can be retrieved very easily once it is detected that the image has some hidden secret data by retrieving the LSBs(Akhtar, Johri et al. 2013).

III. HIDING IMAGE WITHIN IMAGE

To a computer, an image is a collection of numbers that comprise 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 is represented by 8 bits.

Sometime steganography will not cover the total security of secret massage. So an additional security need to the secret massage. For this purpose blowfish encryption system is used in the proposed Steganographic system.

IV. BLOWFISH ENCRYPTION ALGORITHM

Blowfish is a symmetric block cipher that can be effectively used for encryption of data(Thakur and Kumar 2011), meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits and is suggested as areplacement for DES. Blowfish is public domain, and was designed by Bruce Schneier in 1993 (Gatliff 2003). The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors at a rate of one byte every 26 clock cycles. The algorithm is compact and can run in less than 5K of memory(Agrawal and Mishra 2012).

V. RELATED WORKS

Many research works have been carried on Steganography. for the purpose of secured secret image embedding. Following are the few related works carried out by various research groups:

Study by (Morkel, Eloff et al. 2005) intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Other study by(Thangadurai and Sudha Devi 2014) presents the detail knowledge about the LSB based image steganography and its applications to various file formats. we also analyze the available image based steganography along with cryptography technique to achieve security.

Other study by(Karim 2011) introduces a best approach for Least Significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden information. It is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. in LSB methods, hidden information is stored into a specific position of LSB of image. For this reason, knowing the retrieval methods, anyone can extract the hidden information. In this study, hidden information is stored into different position of LSB of image depending on the secret key. As a result, it is difficult to extract the hidden information knowing the retrieval methods. they have used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images. The value of PSNR gives better result because their proposed method changes very small number of bits of the image.

Other recent study by(Akhtar, Johri et al. 2013) concerned with implementing Steganography for images, with an improvement in both security and image quality. The one that is implemented here is a variation of

plain LSB (Least Significant Bit) algorithm. The stego-image quality is improved by using bit-inversion technique. In this technique, certain least significant bits of cover image are inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of modified LSBs. Thus, less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stegoimage. By storing the bit patterns for which LSBs are inverted, message image can be obtained correctly. To improve the robustness of steganography, RC4 algorithm has been used to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This process randomly disperses the bits of the message in the cover image and thus, making it harder for unauthorized people to extract the original message. This method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.

Another recent study by(Ren-Er, Zhiwei et al. 2014) studied image steganography combined with pre-processing of DES encryption. When transmitting the secret information, firstly, encrypt the information intended to hide by DES encryption is encrypted, and then is written in the image through the LSB steganography. Encryption algorithm improves the lowest matching performance between the image and the secret information by changing the statistical characteristics of the secret information to enhance the anti-detection of the image steganography.

Another study(Das and Tuithung 2012) presents a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

In October 2011(Khalil 2011) present the possibility of Hiding short audio message inside a digital image and encrypt the audio message before hiding it in image file.

Other study by (Sharma and Shrivastava 2012) present a new steganographic algorithm for 8bit(grayscale) or 24 bit (colour image), based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. in this n LSB of cover image ,from a byte is replaced by n MSB of secret image. the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived.

However, which (Sharma and Shrivastava) present maybe solved the problem of security for steganography Many research which have been mentioned of ways to improvement security and image quality of steganography , but there are many security gaps which no one of experts was be able to solve it. Data hidden and the elimination of threats and attacks in steganography also can not be solved, Therefore we proposed a new Algorithm to hidden data in steganography approach , and we think it will be more secure than previous method and solve their problem.

VI. THE PROPOSED APPROACH

A digital image consists of different pixels. In this approach we used gray scale and color image. As we know, a colored pixel can be represented as a mixture of red, green and blue color with appropriate proportions. In binary notation, a color level 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 approach, a group of three sequential bytes from such an array is used to embed a bit of the entire message.

The proposed technique has main parts:

1. Changing the secret message (plain text) to cipher text by blowfish Cryptography
2. Take secret key from the cover image that select pixels randomly then store this key in the stego image
3. Hiding the cipher into image by a proposed Steganographic technique.

blowfish Cryptographic algorithm encrypts the plain text to cipher text, and take the secret key (used the key for encryption and decryption)from the cover image that select pixels randomly and store this key in the stego image (using key store for decryption) This cipher text will be embedded into a cover image using our Steganographic technique.

Figure3.shown Overall structure of the proposed technique.

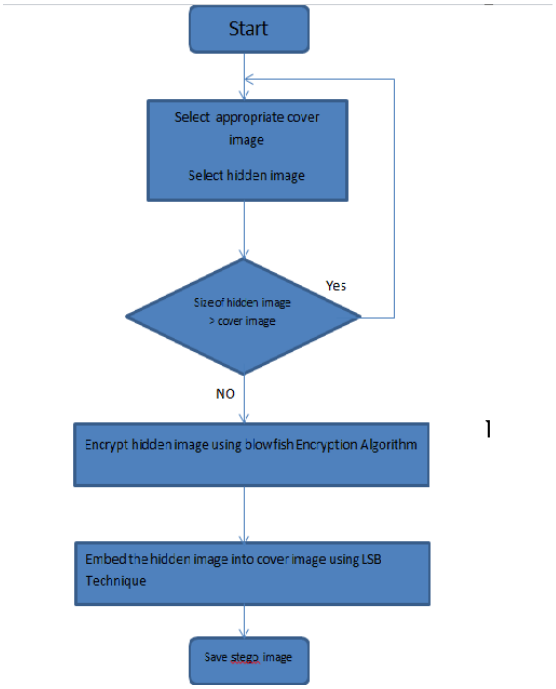

Figure3:Overall structure of the proposed technique

VII. EXPERMENTAL RESULT

Experimental results are given to demonstrate the performance of our proposed method. We used some standard RGB (true color) images as the cover image. Small size image is used as the hidden information.


(a) (b)

Figure4: Original cover image

The hidden information used in our proposed approach is shown below:

(c) (d)

Figure5: Hidden information

A and b image are used as cover image. These images are shown in Fig. 4. The hidden information which is used to hide into cover image is shown in Fig. 5. Hidden information is inserted into cover image after applying blowfish encryption algorithm that hide image **c** in cover image **a** and hide image **d** in cover image **b**. The resulting image is called stego image.

The stego images resulted from our proposed approach is shown in Figure 6.

Figure6:Resulted stego image

the result of the stego-image is visually indistinguishable from the original cover-imageو any attacker can not show any Difference between cover imge and stego image. the proposed approach improvement security and image quality.

VIII. CONCLUSION

In this paper, steganography has its place in security. Though it cannot replace cryptography totally, it is intended to supplement it. for use in detection of unauthorized, illegally copied material, is continually being realised and developed. Also, steganography can be used for covert data transmission. Steganography can be used along with cryptography to make an highly secure data high way. The LSB technique provides an easy way to embed information in images, but the data can be easily decoded. The proposed approach used in this paper encrypts the secret information using blowfish Encryption before embedding it in the image.

REFERENCES

[1]. Agrawal, M. and P. Mishra (2012). "*A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm*." International Journal of Engineering and Advanced Technology (IJEAT) 1(6): 79-83.

[2]. Akhtar, N., P. Johri and S. Khan (2013). *Enhancing the Security and Quality of LSB Based Image Steganography*. Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, IEEE.

[3]. Challita, K. and H. Farhat (2011). "*Combining steganography and cryptography: new directions*." International Journal of New Computer Architectures and their Applications (IJNCAA) 1(1): 199-208.

[4]. Chatterjee, D., J. Nath, S. Dasgupta and A. Nath (2011). *A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm*. Communication Systems and Network Technologies (CSNT), 2011 International Conference on, IEEE.

[5]. Das, R. and T. Tuithung (2012). *A novel steganography method for image based on Huffman Encoding*. Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on, IEEE.

[6]. Gatliff, B. (2003). "*Encrypting data with the Blowfish algorithm.*" Embedded Systems Programming 16(8): 28-35.

[7]. Gupta, A. and R. Garg "*Detecting LSB Steganography in Images*."

[8]. Islam, M., A. Siddiqa, M. P. Uddin, A. K. Mandal and M. Hossain (2014). *An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography*. Informatics, Electronics & Vision (ICIEV), 2014 International Conference on, IEEE.

[9]. Karim, M. (2011). *A new approach for LSB based image steganography using secret key*. 14th International Conference on Computer and Information Technology (ICCIT 2011).

[10]. Khalil, M. (2011). *Image Steganography: hiding Short Audio Message within Digital Images, JCS&T*.

[11]. Morkel, T., J. H. Eloff and M. S. Olivier (2005). *An overview of image steganography*. ISSA.

[12]. Raphael, A. J. and V. Sundaram (2011). "*Cryptography and Steganography- A Survey*." International Journal of Computer Technology and Applications 2(3).

[13]. Ren-Er, Y., Z. Zhiwei, T. Shun and D. Shilei (2014). *Image Steganography Combined with DES Encryption Pre-processing*. Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on, IEEE.

[14]. Sharma, V. K. and V. Shrivastava (2012). "*A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize detection*." Journal of Theoretical and Applied Information Technology 36(1): 1-8.

[15]. Thakur, J. and N. Kumar (2011). "*DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis*." International journal of emerging technology and advanced engineering 1(2): 6-12.

[16]. Thangadurai, K. and G. Sudha Devi (2014). *An analysis of LSB based image steganography techniques.* Computer Communication and Informatics (ICCCI), 2014 International Conference on, IEEE.