International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY: COMBINED IMPACT OF CRYPTOGRAPHY AND STEGANOGRAPHY

A.M.CHANDRASHEKHAR[1], MADHURA S. HEGDE[2] AARABHI PUTTY[3]

[1]Assistant Professor, Dept. of Computer Science & Engineering, SJCE, Mysuru, Karnataka
[2]M. Tech in Computer Engineering, Sri Jayachamarajendra College of Engineering, Mysuru, Karnataka
[3]M. Tech in Computer Engineering, Sri Jayachamarajendra College of Engineering
Mysuru, Karnataka.

Article Received:12/05/2015 | Article Revised on:19/05/2015 | Article Accepted on:25/05/2015

ABSTRACT
Security of confidential information has always been a major issue from the past times to the present time. Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver whereas cryptography is a method of encrypting data and transmitting it. Both these methods do have their own short comings. This paper present two approaches namely RSA with hash LSB and S-DES with LSB, that uses the advantage of steganography and cryptography for secure data transmission.
Keywords: Cryptography; Stegnography; RSA; Hash LSB; S-DES.

I. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Secrecy and safety of the data being communicated is necessary for everyone. In our daily life, we use many ways like telephone or internet for transferring and communicating information, but it's not safe at a certain level. In order to communicate the information in a secured manner two techniques could be used. These mechanisms are cryptography and steganography.

Cryptography and steganography are well known and popularly used techniques that modifies information or message in order to cipher or hide their existence. These techniques have many applications in upcoming science related fields like computer science and other related fields: they are used to protect credit card information, e-mail messages, corporate data, etc.

Steganography is the art and science of communicating in a way which hides the existence of the communication. A stenographic system thus embeds hidden content in a cover media so as not to arouse an eavesdropper's suspicion. As an example, it is possible to embed a text inside a text, an audio, an image or a video file.

On the other side, the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication is known as cryptography. In this survey paper we will focus only on confidentiality, i.e., the service used to keep the content of information from all but those authorized to have it.

II. OVERVIEW OF STEGANOGRAPHY

The word Steganography has a origin in Greek word which means concealed writing. The word "steganos" means "covered " and "graphical " means "writing" . Thus, steganography is not only

the art of encapsulating data but also hiding the fact of transmission of dern data. Steganography hides the secret data in a separate file in such a way that only the recipient knows the presence of original message.(Fig1)

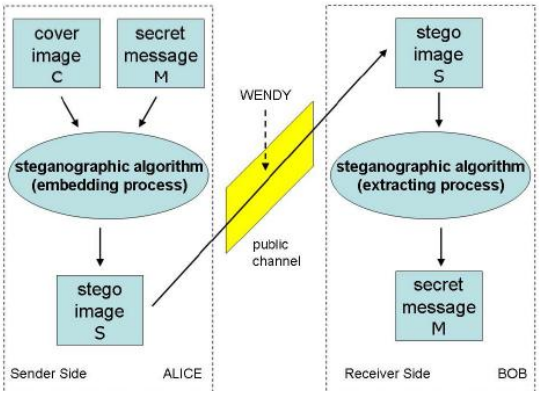

Fig1. Steganographic method

Steganography is broadly classified into six categories:

1. Spatial Domain Methods[7]: This method embeds the secret data directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Sub classes of spatial domain techniques are as follows: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labeling or connectivity method vii) Pixel intensity based

2. Spread Spectrum Technique[7]: In this method the secret data is spread over a wide frequency bandwidth. The concept of spread spectrum is used in this technique. It is a very robust technique mostly used in military communication because the ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover.

3. Statistical Technique[7]: In this technique it involves the splitting of cover into blocks and then embedding one message bit in each block. Also the message is embedded by changing several properties of the cover. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique[7]: The secret message is embedded in the transform or frequency domain of the cover, in this approach. This is a more complex way of hiding message in an image. Different transformations and algorithms are used on the image to hide message in it. Transform domain techniques are sub-classified such as i) Discrete cosine transformation technique (DCT) ii) Discrete Fourier transformation technique (DFT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits.

5. Distortion Techniques[7]: In this technique a sequence of modification is applied to the cover by the encoder. The secret message is stored by distorting the signal. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering[7]: These techniques embed the information in the more significant areas rather than hiding it into the noise level. These techniques hide information by marking an image. Steganography only hides the information whereas watermarks become a portion of the image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

III. OVERVIEW OF CRYPTOGRAPHY

Cryptography protects information by transforming it into an unreadable format. It is useful to achieve from Greek, it literally means “covered writing” confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called cipher-text via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the cipher-text into plaintext.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key (i.e., a password) that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.(Fig2)

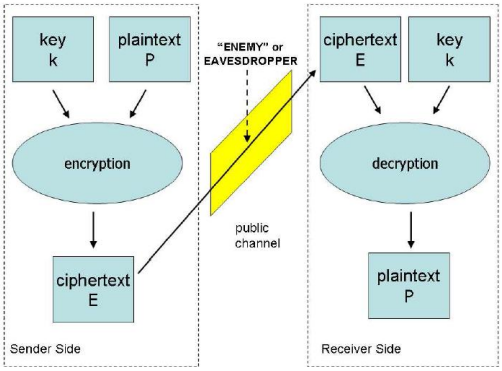

Fig2. Symmetric-key Cryptographic Model.

Cryptography and steganography are cousins in the spy craft family: the former scrambles a message so it cannot be understood; the latter hides the message so it cannot be seen. A cipher message, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not.

In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the ”enemy” is able to access the content of the cipher message, while cryptography fails when the ”enemy” detects that there is a secret message present in the steganographic medium.

The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages.

IV. RELATED WORK

In [1] author has proposed two security approaches, namely cryptography and steganography, where cryptography only changes the format of information and steganography hides complete information in the cover media. Problem with these approaches are, intruder can easily get to know that the data is encrypted if only cryptography is used and if the hidden data is retrieved by intruder he can understand it easily if only steganography is used.

In [2] the LSB technique is described, in which some information from the pixel of the carrier image is replaced with the message information so that it cannot be observed by the human visual system. But one of the major disadvantage associated with LSB method is that intruder can retrieve the hidden message easily.

Because of the short comings of the security methods we propose a study in this paper on various stego-cryptographical methods and their advantages.

V. STEGO-CRYPTOGRAPHIC MODEL

A model which combines techniques, cryptography and steganography, of data security is stego-cryptographic method. In this method the data to be transmitted is encrypted first and then it is embedded in the image. Finally the stego image is transmitted over the network.

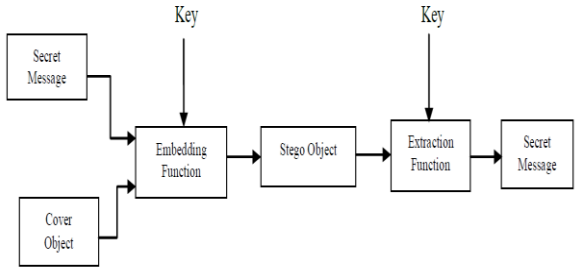

Fig 3. Stego-Crypto Model

A. RSA Encryption with Hash LSB Encoding

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel’s and then message bits are embedded into these RGB pixel’s independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue

pixel LSB as illustrated in Fig. 3. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image.

k = p % n …… (1)

where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the receiver.

This approach of image steganography is using RSA encryption technique to encrypt the secret data. Encryption includes a message or a file encryption for converting it into the cipher text. Encryption process will use recipient public key to encrypt secret data. It provides security by converting secret data into a cipher text, which will be difficult for any intruder to decrypt it without the recipient private key. At the start of this process we take cipher text encrypted from the secret message to be embedded in the cover image. In this process first we converted cipher text into binary form to convert it into bits. Then by using hash function it will select the positions and then 8 bits of message at a time will be embedded in the order of 3, 3, and 2 in red, green and blue channel respectively. The process is continued till entire message of bits will got embedded into the cover image.

B. S-DES algorithm with LSB Encoding

S-DES encryption (decryption) algorithm takes 8-bit block of plaintext and a 10-bit key to produce an 8-bit ciphertext. The encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution that depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function fK again and finally, the inverse permutation of IP (IP-1). The function fK takes two 8-bit keys which are obtained from the original 10-bit key. The 10-bit key is first subjected to a permutation (P10) and then a shift operation is performed.

The output of the shift operation then passes through a permutation function that produces a 8-bit output (P8) for the first sub key (K1). The output of the shift operation again feeds into another shift and (P8) to produce the 2nd sub key (K2).We can express encryption algorithm as superposition:

$$\text{Ciphertext} = IP^{-1}\left(f_{K_2}(SW(f_{K_1}(IP(plaintext))))\right)$$

$$K_1 = P8(Shift(P10(key)))$$

$$K_2 = P8(Shift(Shift(P10(key))))$$

$$\text{Plaintext} = IP^{-1}\left(f_{K_1}(SW(f_{K_2}(IP(ciphertext))))\right)$$

In this approach, each byte (pixel) of all the three matrices(R,G,B matrices of payload) are encrypted using S-DES algorithm and an image comprised of encrypted pixels is formed. The key used to encrypt each pixel is of 10-bit length and is obtained from the pixels of key image. The pixel values of red, green and blue intensities of each pixel of key image are combined to get a 24-bit value. The first ten bits are selected as the key to encrypt the red intensity pixel of payload image. The middle ten bits will be the key to encrypt the green intensity pixel of payload and finally the last ten bits is the key to encrypt blue intensity pixel of payload image.

So the size of key image must be same as that of payload. If not, then the key image will get resized. Each pixel (24-bit) of the key image is split into three keys(10-bit each).This encrypted.

The pixel values of encrypted image ishidden in the LSBs of pixels of carrier image by Exclusive-ORing it with the 2nd LSB of carrier pixel. If the size of the encrypted image is mxn, then the size of carrier image must be mxnx8 as each encrypted byte requires 8 bytes (pixels) of carrier image. So if the carrier image size is not eight times the size of the payload, then it has to be resized.

Two basic types of LSB modifications that can be used for the embedding schemes are LSB replacement and LSB matching. In LSB replacement, the LSB of the carrier is replaced by the message bit directly. On the other hand, in LSB matching if the LSB of the cover pixel is same as the message bit, then it remains unchanged; otherwise, it is randomly incremented or decremented by one. This

technique, however, requires both the sender and the receiver to have the same original image, which makes LSB matching very inconvenient. LSB replacement method is vulnerable to Steganalysis. To overcome this, in the proposed algorithm, the LSB of carrier medium is not changed directly, but the message bit is Exclusive-ORed with the2nd least significant bit of the carrier byte and the LSB of carrier medium is replace by the result bit. The Exclusive-OR operation of the encrypted bit with the second LSB bit makes the stego image more secured.

VI. CONCLUSION AND FUTURE WORK

In this study we reviewed many papers on steganography and cryptography techniques. We observed that impact of the combination of steganography and cryptography is more on data security when compared to individual techniques. The Stego-crypto approach using S-DES and LSB is noticed to be more secure than the stego-crypto approach using RSA and Hash-LSB. This is because key production in S-DES is more complex than RSA so the confidentiality of S-DES is high. In future, several other combination of cryptographic and steganographic techniques can be used to improve other aspects like authenticity and integrity can be improved.

REFERENCES

[1] "Information security based on steganography and cryptography Techniques: A Review", International Journal of Advanced research in computer science, 2014.

[2] Anil Kumar, Rohini Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering, July 2013.

[3] Sujay Narayana, Gaurav Prasad, "Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions" An International Journal(SIPIJ) Vol.1, No.2, December 2010

[4] DomenicoBloisi, Luca Iocchi, "Image Based Steganography And Cryptography", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[5] "A Survey: A Hybrid Approach to Secure Transmitted Message by Combining Steganography and Asymmetric Cryptography" International Journal of Innovative Research in Computerand Communication Engineering, Vol. 2, Issue 11, November 2014.

[6] R. Chandramouli, N. Memon, "Analysis Of Lsb Based Image Steganography Techniques", International Conference On Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.

[7] Jasleen Kour, Deepankar Veerma, "Steganography Techniques- A Review Paper", International Journal of Emerging Research in Management and Technology, Vol. 3, Issue 5, May 2014.