MULTI-LAYERED SECURITY FOR PRIVATE COMMUNICATION (USING STEGANOGRAPHY AND CRYPTOGRAPHY)

[1]Sahil Agarwal, [2] Barkha Khattar , [3] Dr. Inder Singh

[1,2] Scholar, [3]Assistant Professor (Senior Scale),

Centre for Information Technology- COES, UPES-Dehradun, (India)

ABSTRACT

Communication has always been an integral part of human existence and innovation. In this age of technology, data transmission has become important in order to communicate. This paper proposes the use of enhanced form of Least Significant Bit method for Steganography and Triple Data Encryption Standard algorithm for encrypting the message. The proposed method will encrypt the message and embed it into the cover image in the red, green and blue channels of each pixel in random method, making use of linked list data structure. We are making use of the least significant bit and also one bit before it in each pixel, chunking three pixels, to store the message and the address of the next pixel and those chunked together along with it. The recipient, on receiving the image will have to log in using a valid username and password and then can de-embed the message, followed decrypting the message. We are using the enhanced version of steganography and the classical method for cryptography, making it a multi-layered secured system for private communication, which can be used the secret agencies or government agencies or even by the defence to communicate in a secret way even if the network is unsecured.

Keywords: Cryptography, Linked-List, LSB Technique, Secret communication, Steganography, triple-DES

I. INTRODUCTION

In this age of cyberspace revolution, people are diving into the world of internet that can be used without any restriction or strict regulation. There are some people, known as intruders, who secretly keep an eye on the communication which is taking place between the sender and the receiver. Intruders, having malicious intention or purpose can reveal the message to others or can alter it to mislead the recipient. For the purpose of secretly transmitting the message over the network, steganography and cryptography has been used from a long time. Steganography[1], a term which was first recorded in the year 1499, is the type of information hiding method[2], that conceals a message or a file into a cover object, such as digital image[3]. Cryptography is the practice and study of techniques for secure communication, so that the third party cannot read the message. Cryptography allows data to be hidden from the third party, whereas steganography is to keep others from thinking that the information even exists.

II. PROPOSED SYSTEM

2.1. Cryptographic Techniques

Cryptography is the science of keeping the transmitted data secure [4]. It provides data encryption for secure communication [5]. There are two basic types of cryptographic algorithms, which are, symmetric key algorithm and public key algorithm. Algorithm which uses same key for encryption and decryption is known as symmetric key algorithm and algorithm which uses different keys for encryption and decryption is known as public-key encryption.

In this system, the encryption process is achieved using triple Data Encryption Standard algorithm. Triple DES algorithm is a symmetric-key block cipher, which applies Data Encryption Standard three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm. The encryption algorithm using 3DES is:

ciphertext = EK3(DK2(EK1(plaintext)))

i.e., DES encrypts with K1, DES *decrypt* with K2, then

DES encrypt with K3. The decryption algorithm using 3DES

is:

plaintext = DK1(EK2(DK3(ciphertext)))

i.e., decrypt with K3, *encrypt* with K2, and then decrypt with K1.

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K1 and K2 are independent, and K3 = K1.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 x 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 x 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meeting- the-middle attacks.

Keying option 3 is no better than DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations simply cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST) and not supported by ISO/IEC 18033-3.

In general Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack the effective security it provides is only 112 bits. Keying option 2 reduces the key size to 112 bits. However, this option is susceptible to certain chosen-plaintext or known-plaintext attacks and thus it is designated by NIST to have only 80 bits of security.

2.2. Image Steganography

Steganography is the art of hiding that the communication is even taking place as the original information is buried into the cover digital medium. Different types of carrier formats can be used, but digital images are more popular because of their frequency over the network. Before selecting an image as a cover image, precaution should be taken to check that the image is of good quality. There are three types of steganography techniques

used for image, which are: 1) LSB Techniques; 2) Masking and filtering Techniques; 3) Algorithms and transformation techniques.

In this system, enhanced version of Least Significant Bit method is being used. It is widely used method for embedding message into an image. To understand this method, we shall be clear about the least significant bit. LSB is the bit of lowest value. In the proposed system, we shall be using LSB and also a bit before the LSB, chunking it together to make a linked list containing the message bit and also the address to the next bit chunked together to hold the same.

When using a 24-bit image, a bit of each of red, green, blue channels can be used, since they are each represented by a byte. In other words, one can store three bits in each pixel. Representing a grid for three pixels of 24-bit image:

(00101010 10110100 10101111)
(10001011 01011101 00010100)
(11110010 11010001 00010010)

A number, suppose 180, before being embedded into the above grid using the LSB method has to be converted into the binary form. The binary form of 180 is 10110100. Embedding this into the above grid:

(00101011 10110100 10101111)
(10001011 01011100 00010101)
(11110010 11010000 00010010)

On an average, only half of the pixels in an image are modified using this method. On changing the least significant bit no changes are visible in the image as the intensity of change is very less. One of the disadvantages of LSB method is that it is easily detectable [7]. A slight secure method will be sharing of the key by the sender with the receiver that specifies alteration in certain bits only, making it difficult for the adversary as he would not know which bits to target [8].

III. IMPLEMETATION OF THE PROPOSED SYSTEM

In the proposed system, we shall be making use of the above mentioned techniques for implementation, that is, for encryption and decryption, triple-Data Encryption Standard and for embedding and de-embedding an image, Least Significant Bit method. The proposed system targets to overcome the difficulty faced in the classical method, making it a multi-layered secured system.

3.1. Authentication

First step of this multi-layered secured system is providing the valid username and password for authentication of the sender. Any individual or organization (private, government, military) can make an account, to log into the system. Hence, people having username and password can only send secret message over the network.

3.2. Sender

The sender has to type the message into a text box provided for the message to be typed. 'Encrypt' button has be pressed. On pressing that button the message typed in the text box will be encrypted using the triple- Data Encryption Standard algorithm mentioned above.

The sender then has to load an image into the image box from the saved images. Any image can be selected of good quality. On pressing the 'embed' button, the message is embedded into the cover image in the following manner: the least significant bit and second to the least significant bit, of each channel (red, green, blue) are to be taken together. We will now take the pixel, adjacent pixel and next to the adjacent pixel, that is, three pixels are chunked together to hold the message and the address in coordinate form of the next pixel. It can be represented as follows:

(00101*10* 10110*00* 10101*11*)

(10001*11* 01011*01* 00010*00*)

(11110*10* 11010*01* 00010<u>10</u>)

The italics bits hold the address in coordinate form(x,y). The value for the 'x' coordinate is stored evenly in the 8th bit of each byte of the channel and the value for 'y' coordinate is stored in the 7th bit of each byte. The underlined bits hold the message in both 7th and 8th bit.

Suppose the coordinates of the next pixel holding the message is (0,255). It will be converted into the binary form as: 0 will be 00000000 and 255 will be 11111111. It will be evenly distributed as:

(00101*10* 10110*10* 10101*10*)

(10001*10* 01011*10* 00010*10*)

(11110*10* 11010*10* 00010010)

The underlined bit shall hold the message bit as required.

The start pixel will be used as key and will be sent to the receiver separately. The message will then be transmitted over the network.

3.3. Receiver

On receiving the image, the recipient will be required to login for authentication. The encrypted message from the cover image can then be retrieved using the reverse technology. The message has to be de-embedded after the key has been received. The encrypted message can then be decrypted by the algorithm provided above using triple-DES.

IV. PRECAUTIONS

- The image that the sender is selecting as the cover image should be of good quality.
- The key should be sent separately by the sender.
- Valid username and password has to be provided by the sender.

V. CONCLUSION

We have seen the paradigm shift from batch processing to this era of internet in everything. Hence it has become important to secure communication from being attacked during a secret transmission. The formulation that we have made through this paper may have already been discovered but our implementation is different and involves use of both technologies in a distinct way.

VI. ACKNOWLEDGEMENT

We owe a great debt of gratitude to Dr. Inder Singh, our mentor and guide who helped us to make this project a success. We would also like to thank all our friends and classmates who helped us in the coding.

REFERENCES

[1] R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography”, IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, vol. 16(4), pp. 474−481, 1998.

[2] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (pdf).*Proceedings of the IEEE (special issue)* 87 (7): 1062– 78. doi:10.1109/5.771065. Retrieved 2008-09-02.

[3] Fridrich, Jessica; M. Goljan and D. Soukal (2004). "Searching for the Stego Key".*Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI* 5306: 70–82. Retrieved 23 January 2014.

[4] Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

[5] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.