Two Layer Security Combining MSB Based Steganography and RSTEG With Cryptography

Sumayya P I, Sheena Kurian K

Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India

sumayya123@gmail.com

Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India

sheenakuriank@gmail.com

Abstract : The sharing of sensitive information along a common communication channel has become inexorable in this internet era. Variant techniques are available to ensure the security of private data according to the specific needs. A new way of securing the data is proposed here which makes use of the combination of two data securing techniques. AES cryptography is utilized in combination with a new steganographic technique. The technique improves the security, as the message is not directly embedded in the cover image, instead a status check is done. Accordingly an indication is provided whether at a calculated bit position of the pixel, the actual message bit or its toggled form is present. The position to be compared with message bit is based on the users choice, which specifies which all color components of the pixel to be used. The proposed method uses the MSB bits of pixels for decision making. Multilevel steganography is done by incorporating retransmission steganography. It is effortful for a snooper to retrieve the actual message as it is very different from the common LSB method. The Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) and the histogram differences can be used to measure the image quality and efficiency of the technique.

Keywords : MSB Based Steganography, AES Cryptography, Filtering algorithm, Retransmission steganography

1. INTRODUCTION

Confidential data loss is huge due to the transmission of private data through the global network. The art of information hiding has received much consideration in the recent years on the point of security of information nowadays. Immense amount of confidential data is being lost every year by cause of interruption by the snoopers. It must be assured that data is not exposed to attack during transmission across the network.

Variety of technologies are available to encrypt data ensuring the privacy and integrity. They ensure that the data remains confidential and cannot be modified.

Security represents the quality of being secure to be free from danger. Different layers of security includes physical, personal, network, communication and information security. Security attacks interrupts the normal flow by implementing different types of techniques over data and network, like interruption, modification, interception, fabrication etc. The Security measures possible to tackle these type of attacks includes preventing and detecting the attacks or responding to or recovering from the attacks. Protection of data from unauthorized users and hackers, and preventing data modification has gained attention due to massive increase in data transfer rate over internet. Cryptography, Steganography, Digital watermarking are some of the techniques to improve the security features in data transfer over internet.

Ciphering techniques are extensively used to encrypt and decrypt data. Sometimes encrypting the data itself is not providing needed security and the hiding of information is needed more. Steganography is the art and science of hiding information. Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between approved parties.

Kryptos is a greek word used to describe anything that is hidden, secret or mysterious which makes up the term cryptography. Cryptography is the study of secret writing, concerning the ways in which information and data can be encoded into another form to prevent disclosure of their contents via eavesdropping, allowing only certain people to see the real message.

Physical security is the best line of protection in order to keep data safe from illegitimate access. However, physical security is not always an option due to cost and efficiency considerations. Most of the computers in a network are interconnected with each other openly, thereby

unveiling their communication and the communication channels that they use.

Cryptography is the state in which security engineering meets mathematics which provides the tools that underlie most modern security protocols. It is probably the key enabling technology for safeguarding distributed systems. Modular arithmetic is integral to modern cryptography and public key cryptosystems in particular. Cryptography is the lore of securing data whereas the science of analyzing and breaking secure communication is cryptanalysis. Classical cryptanalysis involves a combination of application of mathematics, analytical reasoning, pattern finding etc. Attackers who do this cryptanalysis is termed as cryptanalysts. Cryptology enfolds both cryptography and cryptanalysis. Cryptographic algorithm with the possible keys and protocols that makes it work amount to a cryptosystem.

Steganography is the art of embedding secret messages within another seemingly harmless messages. The word Steganography combines the ancient Greek words steganos and graphein, meaning "covered or concealed writing". The benefit of steganography is that the embedded secret message does not attract attention to itself as an object of inquiry. Plainly visible encrypted messages, how unbreakable, will arouse interest, and may in themselves be accusatory in countries where encryption is illegal. Cryptography is the practice of protecting the contents of a message alone, whereas steganography is the practice of concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

For the concealment of information within computer files, a suitable carrier such as text, image, voice, video, or protocol is needed. Digital images are one of the common and most popular cover images due to their frequency on the Internet[2]. Except protocol steganography, all other steganographic methods are independent of the communication protocols used to transmit the data. Multi-level-steganography is based on combining more than one steganographic techniques such that a method is the carrier of another method. Network steganography is based on manipulating the features of a communication protocol in order to send the data secretly. Network steganography is classified into three, Packet modification, modification of packet stream structure and the hybrid methods.

2. PREVIOUS WORKS

There are lots of techniques available that implement steganography on different electronic mediums. Minati Mishra et.al, in their work explains about different information hiding techniques[7]. They are classified into Covert channels, Steganography and Copyright marking. The best known Steganographic technique that works in the spatial domain is the LSB, which replaces the least significant bits of pixels with message bits to hide the information. In a LSB embedding, some information from the cover image will be lost always. Embedding directly into a pixel, discards some of the cover's information and replace it with information from the data to hide. J. J. Roque and J. M. Minguet proposed a new variant of the Least significant bit insertion method in their work SLSB (Selected Least significant bits)[3]. Ira. S. Moskowitz et.al, in their work[5], explains the method of using cryptography and steganography in conjunction to improve the security. A subset of methods for providing confidentiality in the communication of digitized information is named as network steganography. Jozef Lubacz et.al in their work[8], provides an overview of the network steganography methods. Rupali Gawade et.al in their work[11], proposed a scheme to transmit a secret message imperceptibly between points over Internet using any encryption algorithm.

3. MSB BASED STEGANOGRAPHY COMBINED WITH RSTEG

A digital image consists of several pixels. In the proposed method color image is used as cover image. A colored pixel can be represented as a mixture of red, green and blue color components in appropriate proportions. In binary notation, a color level is represented by a stream of 8 bits. Thus an image is an array of many bytes each representing a single color information lying in a pixel. A pixel is denoted by 24 bits. In the proposed technique the default LSB technique is improved. MSB bit is used for filtering the pixel, to find whether it is eligible for hiding message bit or not. For more security, AES encryption technique is used.

The proposed technique has three main parts:

i. Changing the secret message (plain text) to cipher text by AES Cryptography
ii. Embedding the cipher into cover image by a proposed steganographic technique
iii. Transmitting the steganogram using retransmission steganography.

3.1 FINDING OUT THE IMAGE TYPE

An image can be darker or lighter. To find out the image type, count the number of brighter and darker pixels in the image. A pixel with MSB bits of Red, Green, and Blue component containing at least 2 bit 1's is a bright pixel. and atleast 2 bit 0's is a darker image. If brighter pixels is greater than darker pixels, select brighter pixels to embed message and vice versa.

3.2 EMBEDDING PROCESS

In an image, color information is arranged byte by byte. A pixel will be represented using 3 bytes R-G-B. A status about the message bit is embedded in the LSB of such a

byte. This byte is chosen from a block of spatially adjacent 3 bytes corresponding to a pixel. The binary representation of the ASCII value of alphabets is embedded in the cover image. The cipher text contains alphabets and special characters, each of them having an ASCII value. ASCII value of 'A' is 65. Thus "A" will be embedded in the cover image as "01000001", the binary representation of 65. The choice where the message bit embedded is determined by the MSB of the 3 bytes. In this case there will be two situations:

i. When the image has more lighter than darker area ii. When the image has more darker area than lighter area

3.2.1 Algorithm for Embedding

1. Get the cover image.
2. Find out the image type.
3. Get the Original message.
4. Encrypt the original message using AES.
5. Convert the cipher bit on consideration into binary number based on its ASCII value.
6. Select the color components of the pixel to which the message to be Embedded (R/G/B/All).
7. Select the first pixel from the cover image.
8. Collect the MSB bits from the pixel's color component bytes.
9. From the MSBs, for lighter image if it contains two bits 1 and for the darker image if it contains two bits 0, select this pixel for hiding message bit. Otherwise, skip this pixel.
10. Convert MSB into decimal number P_n
    a. Compare the value in P_n bit position of the selected color component(s) with the message bit
    b. If it matches, change the LSB of selected pixel's color component(s) as 1(indicate status true).
    c. Else, change the LSB of selected pixel's color component(s), 0(indicate status false).
11. Get the next pixel.
12. Repeat steps 8 to 11 until reached the end of message.
13. Save the stego image.

The original message is first encrypted using Advanced Encryption Standard. A cover image for hiding the data is chosen and according to its type, embedding is to be done. MSB bits of the pixel color components are taken into consideration in order to embed a status about the message bit. Get the decimal representation of the MSB bits as P_n. Go through every pixel in the image and find whether to hide the message bit in the selected pixel or not. Check whether value at P_n bit position of pixel color component and message bit matches. If yes, indicate the status as true, otherwise false.

3.3 EXTRACTING PROCESS

At first collect the Stego image saved after the embedding process. For the extraction process the procedures for embedding should be reversed.

3.3.1 Algorithm for Extraction

The algorithm to do extraction of the message from the Stego Image is as follows,

1. Get the Stego image.
2. Find out the image type.
3. Get the first pixel of the stego image.
4. Collect the MSBs of the color component bytes.
5. If MSBs contains two bits 1 for a lighter image and two bits 0 for the darker image, select this pixel for extracting the message bit, else skip the pixel.
6. Convert MSB into decimal number, P_n.
    a. Check the LSB of the selected color component.
    b. If it is 1, collect the P_n bit of the selected pixel component as the cipher bit.
    c. If it is 0, collect the cipher bit by toggling the P_n bit of the selected pixel component.
7. Get the next pixel.
8. Repeat steps 4 to 7 until the whole cipher text is extracted.
7. Decrypt the cipher text using AES to get the original message.

If the pixel is supposed to hold the cipher bit, get the decimal representation of the MSB bits as P_n. Check the status at the LSB bit of the pixel color component. For a true status, extract the cipher bit as such as present in the P_n bit position of the selected color component of pixel and for a false status toggle the P_n bit.

3.4 MULTILEVEL STEGANOGRAPHY

Multilevel steganography is the process in which atleast two steganographic techniques are utilized. The idea behind is that even after detection of the upper level method which is the carrier of the lower level method, the secret message is left unreadable to an intruder. Network steganography, is a branch of steganography, based on manipulating the features of the communication protocol. Retransmission steganography is introduced to transmit the stego image obtained from the proposed MSB based method.

3.5 RETRANSMISSION STEGANOGRAPHY

RSTEG uses a retransmission mechanism to exchange steganograms. Sender and receiver, aware of the steganographic procedure reliably exchange packets during their connection. At some point during the connection the receiver intentionally doesn't acknowledge

a successfully received message. In the context of RSTEG, a sender replaces original payload with a steganogram rather than sending the same packet again during retransmission. When the retransmitted packet reaches the receiver at an agreed upon time, the receiver can extract the hidden information using the proposed extraction method.

4. EVALUATION MEASURES

A 24-bit image is used as the cover image. Commonly used measures of image quality for comparing stego images with cover results are Mean Square Error, Peak Signal-to-Noise Ratio and hisogram. **Mean Square Error (MSE)**

MSE is a risk function which measures the average of squares of difference between the estimator and what is estimated. Thus the estimator quality can be assessed by the mean square error. MSE between two images can be given by

$$MSE = \frac{\sum_x \sum_y (|A_{ij} - B_{ij}|)^2}{i=1\ j=1\ x * y}$$

Where A(x,y) and B(x,y) are the images.

 Peak Signal-to-Noise Ratio (PSNR)

PSNR is a performance measure for evaluating image distortion. It is classified under the difference distortion matrices and can be applied on stego images.

$$PSNR = 10 \log_{10} \left(\frac{C^2_{max}}{MSE} \right)$$

where, C^2_{max} holds the maximum value in the image.

The PSNR value of the proposed technique will be better than other methods providing an efficient way to embed a message into the image without producing clear distortion. In most cases cover image will be of less significance. Thus a suitable cover image according to user's choice to carry the message can be chosen.

5. CONCLUSION

A new concept of Steganography is introduced in the proposed system. The goal of the technique is not to increase the capacity of the message but we try to make it difficult to the unauthorized person to determine the presence of a secret cipher. In ordinary Least Significant Bit Steganography technique the LSB bit of the image is replaced with the message bit. The proposed algorithm does not just replace the message bit but it would replace the status of the message bit. Moreover, Cryptography is merged with it so that the secret message can be secured by two security layers. Instead of inserting the message bits in the cover image, a status is embedded in the LSB to get idea about the message bit. Also RSTEG is done, making very difficult for a steganalyst to detect the presence of a message in the image. In cases where a specific cover image itself is needed to hide the data, checking for the amount of space present to hide the image should be taken into consideration. The quality of proposed technique can be found out using the evaluation measures, Mean square error, Peak Signal-to-noise ratio and histogram of the cover image. Thus the proposed technique fulfills the needs of an efficient steganographic technique.

REFERENCES

[1] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin Ashis Kumar Mandal and Md. Delowar Hossain, "*An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography",* 3rd international Conference on informatics, electronics & vision 2014

[2] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "*An overview of image steganography*" New Knowledge Today Conference Sandton, pp. 1-11 , 2005.

[3] J.J.Roque and J.M.Minguet, "*SLSB: Improving the Steganographic algorithm LSB,*" Proceedings the IberoAmericanz Congress on Information Security (CIBSI), Montevideo, pp. 398408, 2009.

[4] N.F. Johnson and S. Jajodia, "*Exploring Steganography: Seeing the Unseen*", Computer Journal, 1998.

[5] I. Moskowitz, G. Longdon and L. Chang, "*A New Paradigm Hidden in Steganography",* Proc. 2000 Workshop on new security *paradigms*, Ireland, pp. 41-50.

[6] Tobby Sharp, " *An implementation of key-based digital signalnsteganography*",Proc. 4th International Workshop on Information Hiding, USA, vol. 2137,pp. 13-26 , 2001. [7] Minati Mishra, Priyadarsini Mishra and Flt. Lt. Dr. M.C. Adhikary , "*Digital image data hiding techniques: a comparative study*", ANSVESA, 7(2), 105-115 , 2012, ISSN-0974-715X

[8] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Princi*ples and Overview of Network Steganography",* IEEE Communications Magazine • May 2014 , 0163-6804

[9] Sujata Edekar and Rajeswari Goudar , "*Capacity boost with data security in Network Protocol Covert Channel"* , Computer Engineering and Intelligent Systems, ISSN 2222-1719 (Paper),ISSN 2222-2863 (Online)Vol.4, No.5, 2013

[10]D. D. Dhobale, Dr. V. R. Ghorpade, B. S. Patil and S.B.Patil, "*Steganography by hiding data in TCP/IP headers*", 2010 International conference on advanced computer theory and engineering(ICACTE) [11] Rupali Gawade, Priyanka Shetye, Vaibhavi Bhosale, and P N.Sawantdesai, "*Data Hiding Using Steganography For Network Security*", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014

[12] W. Bender, D. Gruhl, N. Morimoto and A. Lu "*Techniques for data hiding* ", IBM Systems Journal, vol. 35, nos. 3&4, 1996.

[13] M. Owens, "*A discussion of covert channels and steganography"*,SANS Institute, 2002 .

[14] J. K. Mandal and M. Sengupta, "*Steganographic Technique Based on Minimum Deviation of Fidelity (STMDF).*", Proceedings of Second International Conference on Emerging Applications of Information Technology, IEEE Conference Publications, pp 298–301 , 2011.

[15] Adam Berent, "*Advanced Encryption Standard Simplified*", ABI Software Development

[16] Kawaguchi, E. and Eason. R., "*Principle and applications of BPCS-Steganography*", Proc. Multimedia Systems and Applications Conference,USA, vol3528, pp.464-473 , 1998.