www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-6, Dec 2017
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Information Security: A Review on Steganography with Cryptography for Secured Data Transaction

Kodge B. G.

Department of Computer Science, Swami Vivekanand Mahavidhyalaya, Udgir, India

**Corresponding Author: kodgebg@gmail.com*

Received: 10/Oct/2017, Revised: 24/Oct/2017, Accepted: 18/Nov/2017, Published: 31/Dec/2017

Abstract— This is an age of universal electronic connectivity & due to advanced hackers and crackers, the importance of security increases day by day. To protect the data from hackers and crackers, we prepared a very simple technique which avoids hacking of secret data. In this paper, we used two methods of encryption technique like- 1. Cryptography - converts plain text into coded form 2. Steganography- hides secret data into images. If we use each technique individually then there may be possibilities of decoding of data within some time limit. So, to avoid this and to provide powerful security, we combined both above mentioned techniques to encrypt and hide text data into the bits of bitmap image for secured data transaction.

Keywords—Steganography, Cryptography, Image Processing, Information Security

I. INTRODUCTION

In 1994, the Internet Architecture Board (IAB) issued report entitled "Security in the Internet Architecture" (RFC 1636). The report stated the general consensus that the Internet needs more & better security. In today's wireless network world, although there are many solutions for wireless access, lots of things are remains to do in this field. There are some open research topics, one of them is – steganography with cryptography. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security. Cryptography systems can be broadly classified into symmetric-key systems that use a single key 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. In Cryptography, 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[1].

A. Steganography

The word steganography comes from Greek language. 'tegnos' means cover and 'graphia' means writing. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphein meaning "to write". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter [8]. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. In this method, simply text file hides in a bmp i.e. image file [2]. Here, the least significant

bit of each 24 bit pixel can be changed without greatly affecting the quality of the image. The result is that we can hide a 2.3 megabyte message in single digital snapshot having resolution 2048 by 3072 pixels.

More specifically, steganography is the art and science of communicating in a way which hides the existence of the communication. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. As an example, it is possible to embed a text inside an image or an audio file. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. In this paper they have focus only on confidentiality, i.e., the service used to keep the content of information from all but those authorized to have it [11].

B. Cryptography

The term cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Cryptology prior to the modern age was almost synonymous with encryption. Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

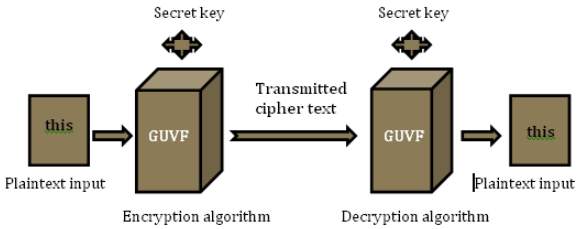

Figure 1. General Model of Encryption Technique

The general encryption technique has five ingredients like-

1. Plaintext
2. Encryption algorithm
3. Secret key
4. Cipher text
5. Decryption algorithm

Accordingly, here in this paper I have made an attempt to shown how to transform secrete data by decoding and hiding the information digitally in an image without disturbing the inner geometry of sample image. This paper is organized in five sections like, Introduction, Problem Domain and its Solutions, Methodology, Results and Conclusion.

II. PROBLEM DOMAINS AND ITS SOLUTIONS

A. Review

All of us have dreamed of secret communication language, well the aim of this paper is to provide powerful security by combining steganography with cryptography for secured data transaction along with removing deficiencies of pervious methods like-

- In previous method they directly replaces LSB of image byte by 1 bit of text byte, while we firstly apply mask(254-11111110) by using logical AND operation on each image bytes before replacing it, so that data will be correctly transferred.
- They replace 2 bits of image bytes, but we replace 1 bit, so that no one can feel or see any changes in image.
- In this method, decoding process is time consuming as compare to previous method, so that it's difficult to decode message for hackers.

B. Processes

The followings are the list of steps/processes for encrypting and hiding text data into the bits of bitmap images.

- Plain text / secret message is converted into coded form by using one of the existing cryptography techniques.
- Convert that coded text into its binary equivalent.
- Then we take image bytes from an RGB image & apply mask (254-11111110) by using logical AND operation, so that all LSB bits will sets to zero.
- The first few pixels store length of message.
- Then the remaining LSB bits of each image bytes are replaced by message bits.

The last step e. repeats for all message bits. And for decoding, reverse process of coding is used.

III. METHODOLOGY

A. Resources

To complete the processes discussed in section II(B), we require few primary things and they are as follows:

- Text file
- Secret key
- BITMAP image file
- Logical AND operation table

1) Structure of text file:

Following five characters are training data for our experiment

G	M	M	G	N
77	71	71	77	78
01000111	01001101	01001101	01000111	01001110

2) Secret key:

a b c d e f g h i j k l m n o p q r s t u v w x y z

G A N E S H J I Z Y X W V U T R Q P O M L K F D C B

3) Structure of bitmap image file:

Header - 54 Bytes	Data - Rest of BMP file

4) Logical AND operation table

A	B	A AND B
0	0	0
0	1	0
1	0	0
1	1	1

Figure 2. Logical AND Truth table

B. Example

The following example showing the practical implementation of Cryptography and Steganography:

1) Applying cryptography

The secret message:

attack postponed until two am

Encrypted message:

GMMGNX RTOMRTUSE LUMZW MFT GV

Converting text bits into binary form-

Taking only first five characters-

G	M	M	G	N
77	71	71	77	78
01000111	01001101	01001101	01000111	01001110

2) Applying Steganography

a) Applying mask on bmp bytes

BMP bytes	10100101	11110000	11000010
Mask(254)	11111110	11111110	11111110
Result of AND	10100100	11110000	11000010

Figure 3. Masking BMP bites

b) Putting text bits in BMP bytes (taking 8 bits for first character)

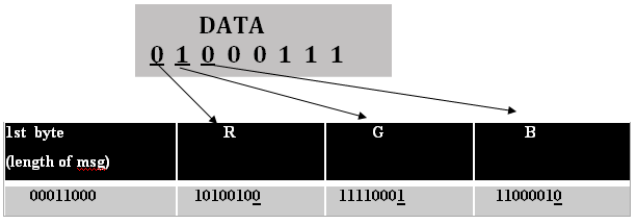

Figure 4. Adding text bits into BMP bites

We performed all the processes in MATLAB through different modules to complete these tasks.

IV. RESULTS

Resulting stego image

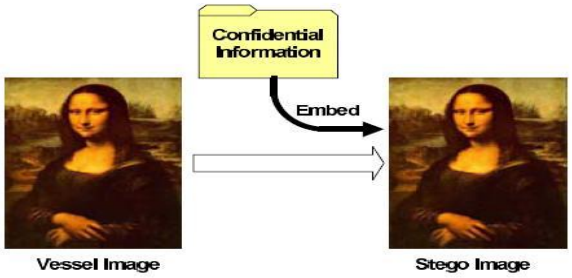

Figure 5. Result of BMP stego image

The above shown Figure5 is an illustration of the processes discussed in the Methodology section of this paper. The Vessel image is an input image taken as a sample for this test. The proposed techniques are applied within this sample image with confidential test information. The outcome of the applied processes is a Stego Image, which can't be differentiated by anyone one with open eyes. The features of this outcome are as follows:

- The secret message is correctly transmitted using this technique.
- None is able to differentiate two images, one having secret message and other without any message i.e. simple image.
- Except sender and receiver no one is able to decode the image to get secret message.
- It provides more complexity which avoids hacking problem.

V. CONCLUSION

The proposed techniques presented in this paper will be very much useful for the current and future digital era. This proposed technique can be used to avoid the problems of hacking and cracking the data while online data transactions. The proposed techniques discussed in this

paper combine both strong methods like, cryptography and steganography for better encryption and data hiding. It's impossible for anyone to decode the message due to its complexity. This proposed technique is useful in defense or any confidential sector for sharing secret plans. It's also useful in the institutions/organizations for private communication for secured information transactions.

REFERENCES

[1] A. Joseph Raphael, Dr. V Sundaram, International Journal of Computer Technology and Applications, Vol 2 (3), ISSN: 2229-6093, pp-626-630

[2] Emil Wolf, Progress in Optics, Vol. 60, Elsevier, 2015, pp-139.

[3] Cryptography and Network Security, forth edition, by William Stallings.

[4] WAYN96 Wayner, P. Disappearing Cryptography, Boston: AP Professional Books, 1996.

[5] Cryptography and Network Security, Principles and practices, second edition, by William Stallings.

[6] The article licensed under the "Code Project Open License" (COPL) by Corinna John.

[7] Digital Electronics by R. P. Jain, BPB Publications.

[8] Domenico Bloisi and Luca Iocchi, IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY, Dipartimento di Informatica e Sistemistica Sapienza University of Rome, Italy.

[9] M. Arora, S. Sharma, "Synthesis of Cryptography and Security Attacks", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.5, pp.1-5, 2017.

Authors Profile

Dr. Kodge B. G. working as an Associate Professor in Department of Computer Science of Swami Vivekanand Mahavidyalaya, Udgir Dist. Latur (MS) India. He obtained M.Sc., MCA, M. Phil. and Ph.D. degrees in Computer Science and Applications and having 14 years of teaching experience. His research areas of interests are GIS and Remote Sensing, Digital Image processing, Data mining and data warehousing, and Information Security. He is published more than 30 Research papers in national/international Journals and proceedings conferences/seminars. He is a recognized Research Guide in Computer Science and member of several academic and professional committees/bodies.

