ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Secure Data Communication System Using Enhanced Cryptography and Steganography

Darshana Patil[1], Prof. P. M. Chawan[2]

M. Tech Student, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India [1]

Associate Professor, Department of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India [2]

ABSTRACT: Nowadays, security is one of the important issues in our day to day life. Everywhere such as banks, shops etc. we require security. Secret password is the main goal of the password. It can be used to access private information. Because of that data security is one of the most important fields which overcome the problem of data leakage and its misuse. The proposed technique comes under data security which can be used to provide more security. Here proposed technique treat the plaint-text at bit level which is more secure than the compound and intermix characters. Moreover, the main advantage of the technique is that it has its own key generation algorithm and same key is used for both encryption and decryption technique. The encrypted text is after hide behind a carrier using steganography. Hence, use of two modules i.e. cryptography and steganography makes the proposed technique more secure.

KEYWORDS: Encryption key, decryption, symmetric key cryptography, asymmetric key cryptography, Steganography, Peak Signal to Noise Ratio, Cover media, Master file, Least Significant Bit

I. Introduction

In this project, we added two different modules and provide more security to the data. Steganography and cryptography both are different because in case of steganography it involves hiding of data and preventing non-intended observers from learning about its existence while in case of cryptography it involves converting of message to secret message or in unreadable format. In cryptography while using symmetric key new feature to the existing techniques is added. In proposed technique cryptographic key is generated instead of memorizing or providing the separated security mechanism for key transmission. Here we can make the key flexible or be able to change. Steganography is another module which will hide the encrypted message under a cover medium.

In proposed technique we used LSB method for steganography. Image, audio and video all cover medium are used. Steganographic algorithm will change as per the cover medium which is used to hide the information. Each carrier has its own capacity to carry a secret message without making detectable by an attacker. Hence success of steganographic technique is depended on capacity of a carrier and technique. In proposed technique we used both cryptography as well as steganography to hide secret communication.

Steganography can be used to cloak hidden messages in image, image, video and even text files. According to the two most common methods used for hiding information inside a picture, image and video files are LSB (Least Significant Bit) and Injection. In this paper, an image medium was used for the steganography and a more powerful modified LSB (Least Significant Bit) algorithm was employed for encoding the message into the image file.

DOI: 10.15680/IJIRCCE.2017. 0506032

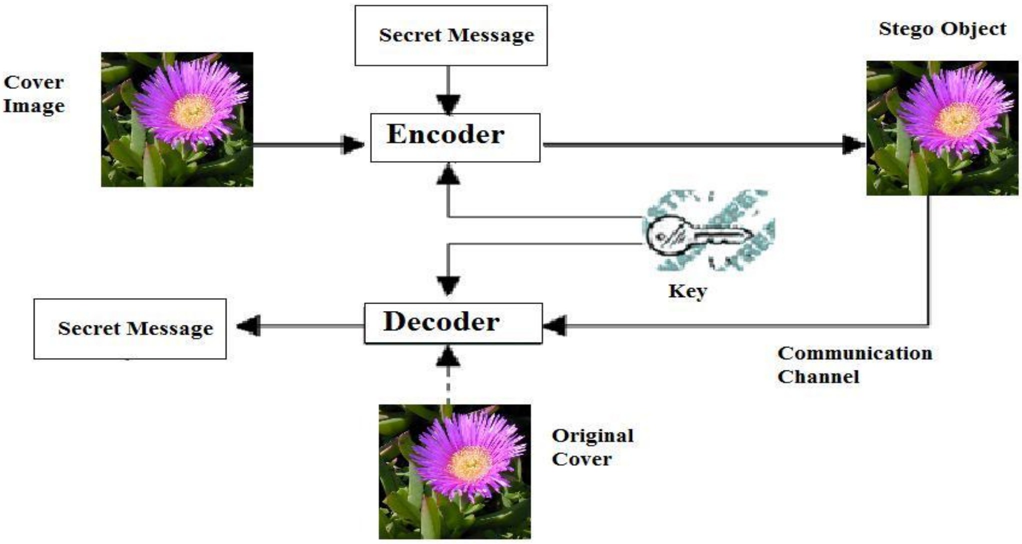

Figure 1. Basic block diagram of message encryption using cryptography and image steganography.

II. LITERATURE REVIEW

1. Cryptography

Cryptography is a practice and study of techniques which are used to provide secure communication. More usually cryptography is all about constructing and analysing the different protocols that prevent reading and stealing of private information from third party or public. In cryptography plaintext is a normal secret text which user wants to hide or transmit. And cipher text is the encrypted plaintext which is in a non-detectable format. Here key plays an important role hence; no one can have access to that data without having key. Different cryptographic algorithms such as AES, DES, MD5, SHA, RSA, IDEA etc. are used. There are three independent dimensions which will classify the cryptographic system.

There are three methods in which Cryptography is carried out.

1. To transform or convert plain-text to cipher text.

Here Plaintext in converted into cipher text using different cryptographic algorithm.

2. To choose the number and type of keys for encryption

Some methods which is used with cryptography are

- Secret key
- public key
- digital signature
- hash function

3. To process the plain text.

Here an output block is produced for each input block which is processed by a block cipher one at a time.

2. Steganography

Steganography is a technique in which we hide the data or information by using a carrier file. It is done by using carrier file and embedding file. Here carrier file must be larger than that of the embedding file as its carries the data of the embedding file. The result is called as stego file which contains the secret message. There are different aspects of information security and one of the important aspects is capacity. Capacity is nothing but the amount of information that can be hidden in the carrier file.

There are three types of steganographic techniques which are as follows:

1. Pure steganography
2. Public key steganography
3. Secret key steganography

1) Pure steganography:

In pure steganography there is no use of any private key for embedding the data into the carrier file. Secrecy is only the aspect for pure steganography. Basically, this type of steganography is used to hide the secret information or data which is to be transmitted by using various encryption decryption algorithms. Carrier file can be an image, audio or video.

2) Secret key steganography:

In secret key steganography we used same procedure as pure key steganography but here only by using a secret key. It is an also symmetric key steganography where same key is used for both embedding and extraction of data from carrier file. Key used in these techniques is secret i.e. not known to anyone other than sender and receiver.

3) Public key steganography:

In public key steganography we used two types of keys i.e. private key and public key. Private key is used for encryption where public key is used for decryption and it is in public database. As per the cover medium we used steganography is divided into four types such as text steganography, image steganography, audio steganography, video steganography.

- **Text steganography:** This is the most common method of steganography. By using this method we use text message to hide a secret message.
- **Image steganography:** Image is one of the most popular carriers or cover medium used for steganography. By using embedding algorithm and the secret key secret message is hid behind a digital image.
- **Audio steganography:** There are different methods which are most commonly used for audio steganography such as Phase coding, LSB coding, Spread spectrum, Echo hiding, Parity coding. In audio steganography we embed the information in an speech or in an audio cover medium.
- **Video steganography:** Video Steganography is a technique in which we can hide large file inside a video where video is used as a cover medium.

III. THE PROPOSED TECHNIQUES

1] Cryptographic Technique

Proposed technique simply read text block and securely transmit the text block over the network.

A. Encryption Technique

Encryption is done by using following four steps:

1) Read the text block

Here we simply receive the original data that user want to send to the receiver.

2) Convert text block into a binary format
0100000101101110001000000100010101101110110100001
1000010110111001100011011001010110010000100000100
0011011100100111100101110000011101000110111101100111
0111001001100001011100000110100001101001011000110010

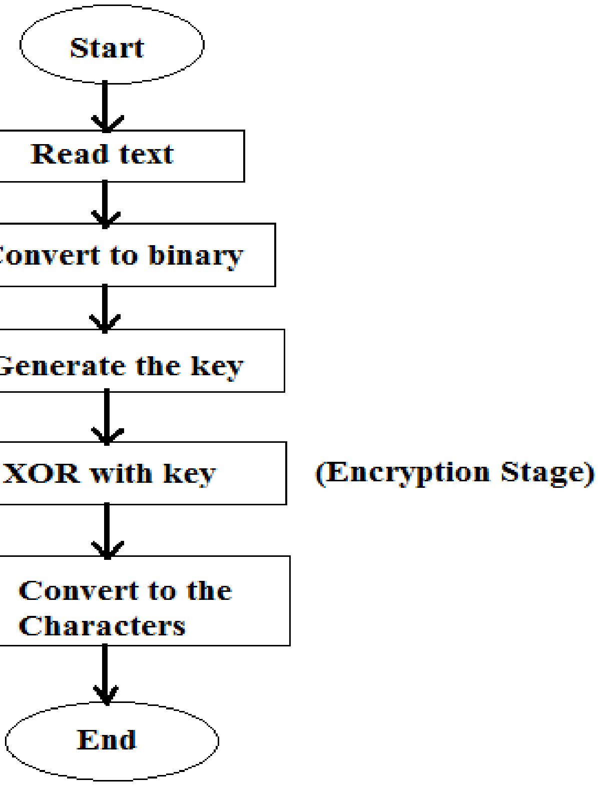

Figure 2. The main stages of the encryption algorithm.

3) Generate the key:
000110100011000010111001

4) Encryption is done by using simple XOR with key
0001010011111001001011011001000111001000110110010
00101011101101100011110111100110001100000101110100
0011010000110100101100011001000000101010001100101011
0001101101000011011100110100101110001011101010110010

B. Decryption Technique

Decryption is done by using following four steps:
1) Read cipher text in binary format:
0001010011111001001011011001000111001000110110010
00101011101101100011110111100110001100000101110100
0011010000110100101100011001000000101010001100101011
0001101101000011011100110100101110001011101010110010

2) Selecting the same specific bit to extract the key:
0001101000110000101111001

3) Decryption is done by using simple XOR with key.

4) Finally convert the stream of bits into a characters
0100000101101110001000000100010101101110110100001
1000010110111001100011011001010110010000100000000100
00110111001001111001011100000111010001101111101100111
01110010011000010111000000110100001101001011000110010

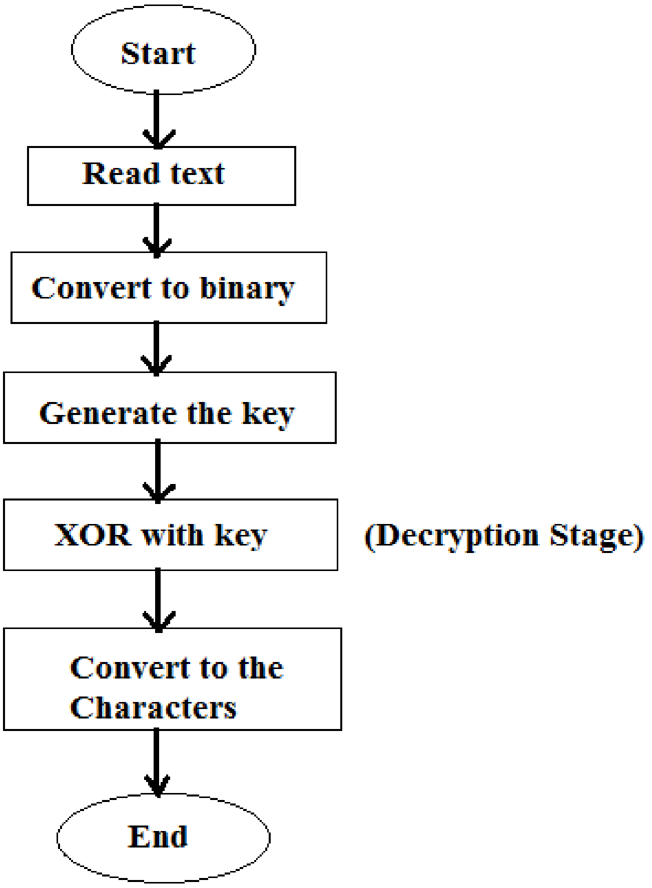

Figure 3. The main stages of the decryption algorithm

2] Steganographic Technique

a) LSB insertion algorithm

Step1: Represent the first character of the data which is to be hidden in binary format.
Step2: Represent the first pixel of the image in binary format.
Step3: The data which is in binary format is extracted bit by bit from left to right.
Step4: Append or prefix zeros to each bit to make it as a 1 byte.
Step5: After appending the zeros, check the value of the byte it is 0 then make it as 2(change the value to 2) and if it is 1 then keep as it is.

Step6: Now take the value of the pixel if the value is 255 or 256 then subtract the value of the data from it else simply add the value.

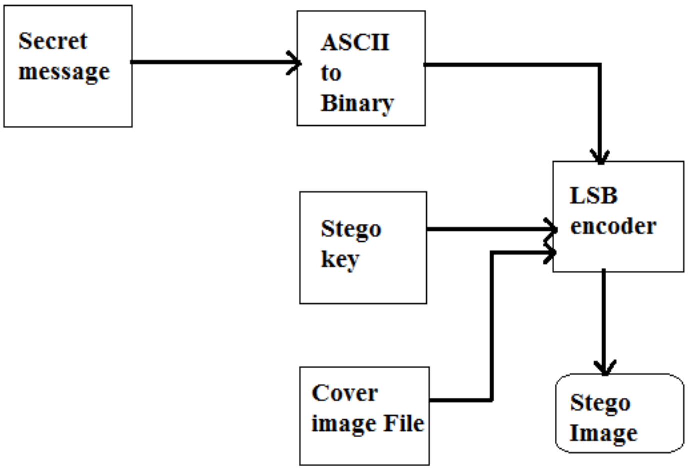

Figure 4. LSB Insertion Mechanism

b) LSB Extraction algorithm (Reverse LSB)

Step1: Extract the byte by byte data from image and represent in binary format.
Step2: Subtract the two values that are extracted and store in temp file.
Step3: Repeat the Step 1 and step 2 till the end of the file.
Step4: Now from temp file every continuous 8 bytes are taken and clubbed them to make it as a 1 byte.
Step5: Last step is to convert the byte by byte data into a character to get the original message.

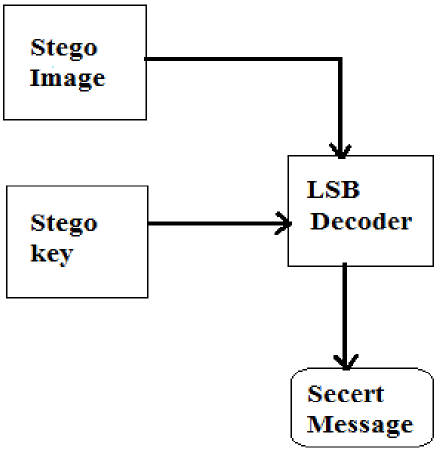

Figure 5. LSB Extraction Mechanism

IV. EXPERIMENTAL RESULTS

1. Performance analysis

Performance measure for image distortion because of hiding of message is done by calculating PSNR value which is given as follows:

PSNR = 10log $(Cmax)_2$ / MSE.

MSE = mean - square – error,
which is given as:
MSE = 1 / MN((S-C) 2.
Cmax = 255.

Here M and N are image dimensions, S is the stego image and C is a cover image. If PSNR value is less than 30 dB then indicates low quality and if it is 40 or above that then high quality. In order to measure the performance several parameter are given as below

Perceptibility: It means embedding the data in cover medium up to a visually unacceptable level.

Capacity: Amount of data can be hidden.

Robustness to attacks: Type of attach on a stego image to read, access or destroy the embedded data.

Figure 6. Grey scale Image

Figure 7. RGB Image

These are the resultant images after the cryptography and steganography. Performance measure of these images are given below.

Technique	Imperceptibility	Capacity	Robust ness
LSB algorithm	High	High	Low

Table 1.Comparison of the characteristics for LSB algorithm

The above table shows that LSB algorithm has high imperceptibility and capacity where has low robustness. Hence, it is one of the most popular technique.

Sr. No	Cover Image	Secrete Message	Stego Image	SNR (dB)	MSE	PSNR (dB)
1	Gray Image	Text file	Grey Images	60.534	0.045	61.80
2	RGB Image	Text file	Images	62.098	0.012	68.25

Table 2. PSNR of Least Significant bits technique

Here the comparison of gray image and RGB image is done over SNR, MSN and PSNR value. Here for both images PSNR value is greater than 40dB which means high quality of images.

DOI: 10.15680/IJIRCCE.2017. 0506032

V. CONCLUSION

In this paper, proposed technique is consisting of two main modules. One is enhanced cryptography and another one is steganography. Here cryptography is enhanced as it is differ from the existing one because it has its own key generation algorithm. Hence no need to provide the separate security for key transmission. Encrypted message is further hide behind a carrier file such as image, audio or video. Hence proposed technique provides a two level of security. It simply goes beyond of embedding a normal data but also embed the encrypted data.

REFERENCES

1. Dipti, K. S. and Neha, B., “Proposed System for Data Hiding Using Cryptography and Steganography”, International Journal of Computer Applications, 8(9), pp. 7-10, 2010.
2. Omar Kassem Khalil, Aissa Boudjella, “An Enhanced Cryptographic Technique for Messages Traveling between Computers”, Sixth International Conference on Developments in E-Systems Engineering, 2013.
3. Alan Siper, Roger Farley and Craig Lombardo, “The Rise of Steganography”, Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005.
4. Niels, P. and Peter, “Hide and Seek: An Introduction to Steganography”, IEEE Computer Society, IEEE Security and Privacy, pp. 32-44, H 2003.
5. Raphael, A. J., and Sundaram, V, “Cryptography and Steganography - A Survey”, International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630, 2011.
6. Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, “An Encrypto-Stego Technique Based secure data Transmission System”, PEC, Chandigarh.
7. Sridevi, R., Damodaram, A., and Narasimham, S., “Efficient Method of Image Steganography By Modified LSB Algorithm and Strong Encryption Key with Enhanced Security”, Journal of Theoretical and Applied Information Technology, pp. 768-771, 2009. Retrieved 21st August, 2012 from http://www.jatit.org.
8. http://en.wikipedia.org/wiki/Autokey_cipher
9. Helen Fouché Gaines, “Cryptanalysis”, Dover, ISBN 0-486-20097-3, 1939.
10. Ibrahim A. Al-Kadi, “The origins of cryptology: The Arab contributions”, Cryptologia, 16(2), pp. 97–126, April 1992.
11. David A. King, “The ciphers of the monks - A forgotten number notation of the Middle Ages”, Stuttgart: Franz Steiner, (ISBN 3-515-07640-9) 2001.