Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Steganography: Secret Transmission of Data

Prof. Brinda K, Prof. Sudha S,
SITE, VIT University,
Vellore, Tamilnadu, India

Ritika Sharma, Sapana Saini
MCA,SITE, VIT University,
Vellore, Tamilnadu, India

Abstract: In this paper we present a method to enhance data security during transmission by hiding the information into any other data. Steganography is a technique of hiding data within data. This paper is advancement of our previous paper which was based on image encryption. Steganography is the advancement of cryptography as it hides the existence of secret information. The main objective of this paper is to provide a secure steganographic system which can work in efficient manner. This project is proposed for enhancing security of data transmission. In Steganography we hide secret message within a general message and extracts the secret message at its destination. We are using LSB for hiding the data into image and EDES is used for cryptography. This paper is an analysis of steganography for data transmission securely. The proposed process will hide important information into the data image with no information loss.

Keywords: Cipher text, Cryptography, EDES, LSB, Steganography

I INTRODUCTION

In today's world of information and speed it is necessary to protect the sensitive data from unauthorized access while maintaining the speed and accuracy. There are so many algorithms and techniques are present that make the information secure. One of them is steganography. There are many approaches for steganography but all of them have one thing common that they hide the secret message in an object which is sent such as image, audio, video etc. In computerized world cryptography and steganography both are used to protect information but both are different from each other in technical way. [3,4] Encryption and decryption is one of the techniques which makes the information safer during transmission by converting it into unreadable form but there are possibilities that a person can access it as he may be aware of presence of information where, in steganography third person will not be aware of any information as information will be hidden. A person cannot identify embedded message in an image with eyes if the embedding is done correctly. To make technique more powerful we are first encrypting the secret message using EDES algorithm. EDES is enhanced data encryption standard which is advancement of DES algorithm. EDES algorithm takes 64 bit of plaintext and produces 64 bit cipher text. EDES uses key of size 112 bits. There are 2 keys such as each of which are of 56 bit length. There are total 8 numbers of rounds. EDES is more efficient and secure. This encrypted data will be embedded into the image. In this paper we have used LSB for embedding the information into an image. Least significant bit is the unit place in binary system. Secret message can be hided inside all kinds of information such as text. The aim of this project is to hide the data over an image using least significant steganographic algorithm. We can divide steganography in two types which are fragile and robust. In fragile steganography the file will be destroyed if someone will try to change its hidden message. This will make sure that the received file is not tempered. Robust steganography files are not easily destroyable. [9,2,4]Steganographic protocols can be divided into three types: pure Steganography, Secret Key Steganography and Public Key Steganography. Pure Steganography does not require any cipher key such as a stego-key. Secret Key Steganography works in a steganographic system where it is necessary to exchange stego-key before communication. Public Key Steganography is same as public key cryptography. In public key steganography system uses a public key and a private key for secure communication between sender and receiver. Public Key Steganography is more robust compare to other protocols of steganography. Steganography is very much useful as it makes it possible to send secret messages and information without being altered and censored.

2 METHODOLOGY

We are first performing encryption operation on our secret message to obtain high level security and invisibility of message into image. For encrypting we are using enhanced DES algorithm which have 8 rounds of encryption process. EDES uses key of 112 bit which makes it more powerful as it is very tedious task to try all possible 2112 combinations of keys to access the secret message.

© 2013, IJARCSSE All Rights Reserved

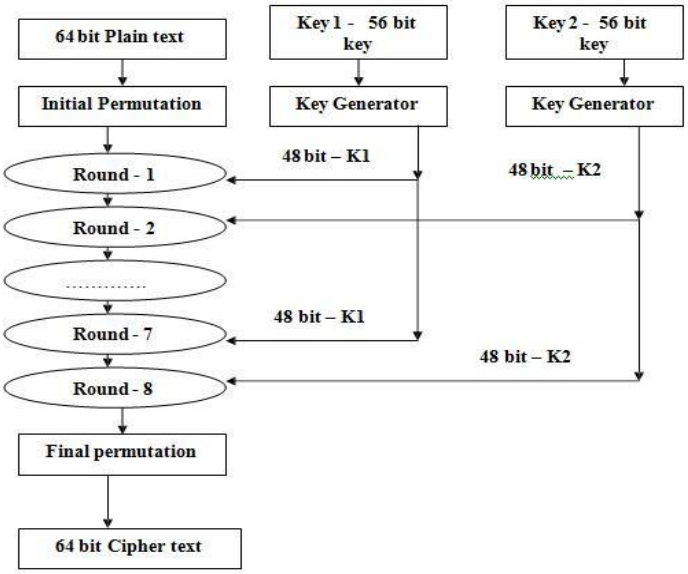

Fig 1. EDES algorithm ref.[8]

In EDES we take 64 bit plain text which will be divided into two halves of 32 bit. Every round of EDES uses 48 bit sub keys generated from 56 bit two different keys. [8, 1]These sub keys will then perform XOR operation with same size of text bit. Same process will be repeated for eight numbers of times and result of eighth round will be cipher code. EDES is more complex as it provides two different keys one by another. Once we have encrypted the secret message we have to hide this cipher code into image. Before
inserting cipher code we have to convert it into binary form so that we can easily perform the LSB algorithm. There are so many techniques for embedding the information in other data. One of them is LSB method of insertion. [5,6] This is one of the simplest but efficient algorithms for data hiding in steganography. LSB stands for least significant bit replacement. In this algorithm we will replace the least bit of every eight bit with binary coded secret message. This little change in image bit is not affecting the intensity of original image as the only changes are from 0 to 1 or vice versa. The changes are made with the difference of eight bit. For example if we have total 256 bit image then only or less than 32 bits are changed. For example we have taken a part of a 24 bit image i.e. 3 pixels:
10100100 01101101 11101001

00101011 10101101 11100110

11001110 00011010 11001100

If we have to insert our secret message as a number which is 253 and binary representation of this number is 11111101. This binary number is now embedded with our image pixels using least significant bit algorithm. The new resultant image pixels are:

10100101 01101101 11101001

00101011 10101101 11100111

11001110 00011011 11001100

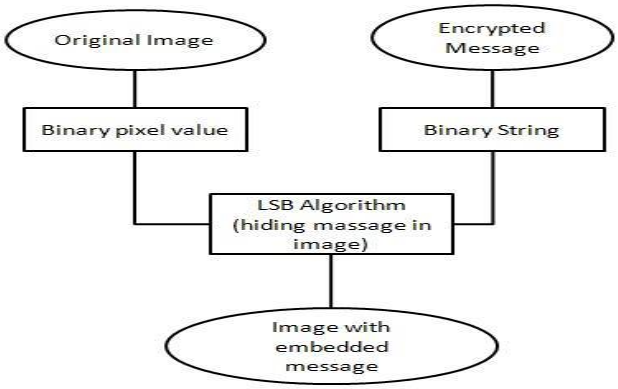

Fig 2 encryption process using LSB

© 2013, IJARCSSE All Rights Reserved

Here change in only bit will not affect the intensity and value of image. Transmission will be very simple process once we have our object ready. The little change in image object cannot be identified with human eyes. In the flowchart it is shown the process of hiding the message in image using LSB and EDES algorithm is used for encryption. This process is held on sender side.

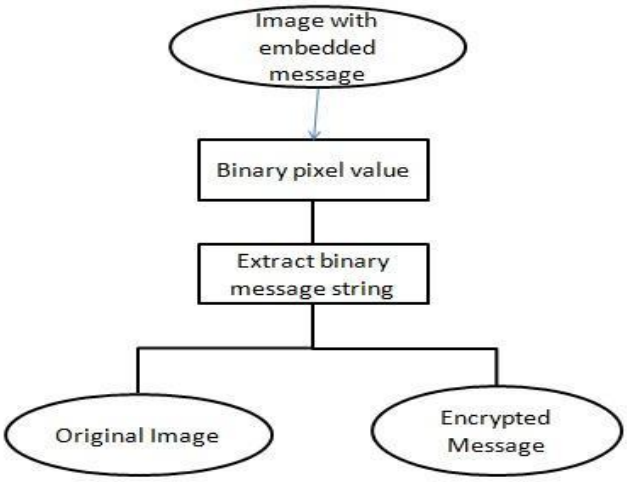

Fig 3 decryption process using LSB

Once we send our object on receiver side same process will be worked out to get the secret message. The receiver end can retrieve the LSB value from the image and can decrypt with same EDES algorithm. Receiver side will first get binary value of image and then binary formatted encrypted message will be extracted using LSB.

3. CONCLUSION

This research paper is based on image steganography. Steganography is a new field in digital world. We have used the least significant bit algorithm for hiding the secret message in an image. LSB is a simple but efficient and reliable algorithm for data replacement compare to other algorithm. We have used enhanced data encryption standard technique for encryption of secret information. The complexity of EDES algorithm makes it more secure. Encrypted message improves the security level of our system.

REFERENCES

[1] Nitin Jain, Sachin Meshram, Shikha Dubey "Image Steganography Using LSB and Edge – Detection Technique"
[2] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy "Implementation of LSB Steganography and its Evaluation for Various File Formats"
[3] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image"
[4] Gabriel Macharia Kamau, Stephen Kimani, Waweru Mwangi "An enhanced Least Significant Bit Steganographic Method for Information Hiding"
[5] Baluram Nagaria, Ashish Parikh, Sandeep Mandliya, Neeraj shrivastav "Steganographic Approach for Data Hiding using LSB Techniques"
[6] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data"
[7] Chi-Kwong Chan∗, L.M. Cheng, "Hiding data in images by simple LSB substitution"
[8] Implementation of Enhanced Data Encryption Standard on MANET with limited computation and energy consumption
[9] Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited"

© 2013, IJARCSSE All Rights Reserved