Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Robust Image Steganography Technique Using Cryptographic Algorithm

N.Ravali[1], R.V.Divya Lakshmi[2], S.Lakshmee Devi[3] **&** S.Vasanth Naidu[4]

[1,2,3,4]Department of CSE , Lendi Institute of Engineering And Technology , Jonnada , Vizianagaram.

Abstract: *This project allows users to send and receive data through the network. The files are sent in a secured fashion. It uses principles of both cryptography and steganography. Cryptography is used to encrypt the message or file that is to be sent. The problem with cryptography alone is that the intruder knows that some data is being sent over the network and to avoid this,steganography is used, Steganography is the art of hiding the fact that communication is taking place, by hiding information in a carrier file. In this project we hide the encrypted message or file in a carrier file (image) and this innocent looking carrier file is sent over the network. We achieve this by using different steganographic algorithms like: LSB&LSB-1,.We embed the messages or files in encrypted form using different cryptographic algorithm like: Blowfish.This project makes the encryption as optional feature as different applications have different level of requirements***.**

Introduction

In today's information age, the technologies have developed so much that most of the users prefer internet to transfer data from one end to another across the world. So privacy in digital communication is basic requirement when confidential information is being shared between two users.

.

Cryptography

Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [2]. For that information is transforming into an unreadable form which is called cipher text. Only those users who know secret key can decrypt the message into their original form

.

1.1. Symmetric Key Cryptography

In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric – key cryptography is called symmetric-key algorithms. There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks.

List of Symmetric Algorithms

- Data Encryption Standard(DES)
- Advanced Encryption Standard (AES)
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm
- Triple Data Encryption Standard etc

.

2.2. Public Key Cryptography

In public key cryptography there is pair of keys one is secret key and other is public key. In which one is used for encrypting the plain text, and the other is used for decrypting the cipher text

List of public – key algorithms

- Diffie-Hellman

Steganography

Steganography is the art of hiding the fact that communication is taking place, by hiding information. Here we hide the data in a carrier file (image/audio/video). There are different methods to apply the principles of steganography. Some of those are:

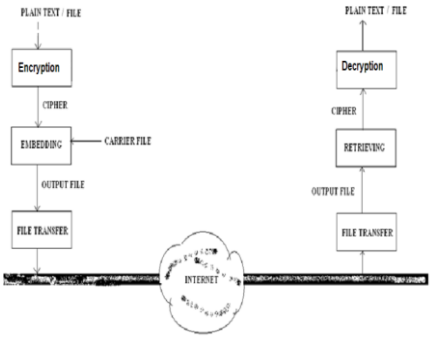
- LSB&LSB-1

Throughout history Steganography has been used to secretly communicate information between people. In olden days there are some methods to pass information secretly, like

- Microscopic images

Proposing System

The proposing system uses the blowfish algorithm which used to encrypt the data and also for both decryption.But with the help of only crypytography the data cannot be in a secured fashion so,LSB technique used for steganography(audio/video/image) where the stego image gives the encrypted format of the blowfish where the data can be hidden in a secured way.



. **Fig:Proposed Architecture**

We use the concept of embedding the message in a carrier file and also the concept of embedding the data file in a carrier file. The generated output file is being sent over the network. This being carried out over the sender's side and the output file sent to receiver's side where the decrypter decrypts the data using one secret key which is private.

Blowfish Algorithm

In this algorithm, we first consider plain text consists of 64 bits which are made into two halves ie., 32 bits. The first 32 bits of left half are XOR'ed and valued with the function 'F' and then XOR'ed with the right most 32 bits to obtain a new value. And the obtained value is again XOR'ed with the next elements in the P2-array and so on the iterations are performed for the successive 15 members of an array. The resulting left and the right half are XOR'ed to produce the entries of p-17,p-18 to produce a cipher text of 64 bits.

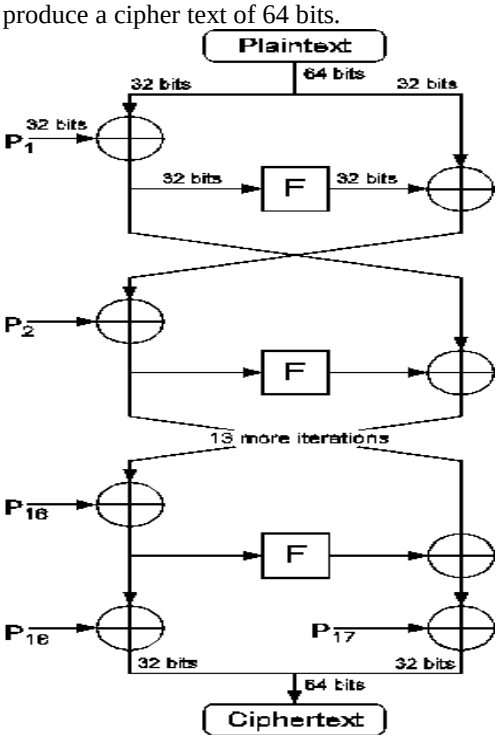


Fig: Blowfish Algorithm

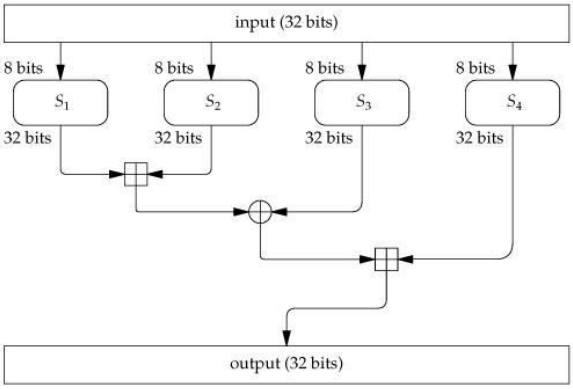


Fig: Graphical representation of F

In this function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XOR'ed together to produce the 32 bits output.

1.2. LSB Approach

LSB is a method in which we replace the least significant bits of a file with the data bits. This is generally applied to images as carrier files. In images there are color values in the form of bytes and just by changing the least significant bits there wouldn't be a considerable change in the color.

Images are created from pixels ie., RGB format Red, Green, Blue. Each pixel having the byte value and having the 8 bits of MSB ie., Most Significant Bit and the LSB value ie., Least Significant Value ie., the last bit is used to hide the data in an image. Using each 3 pixel of image to save a byte of data.

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Results

We are using Java language to implement our proposed work**.**

Embedding message in a carrier file

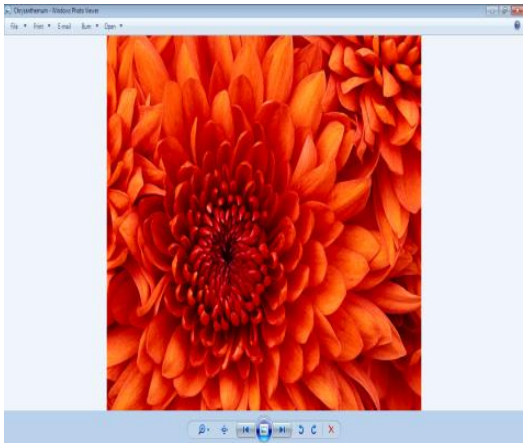


Fig: Embedded Image

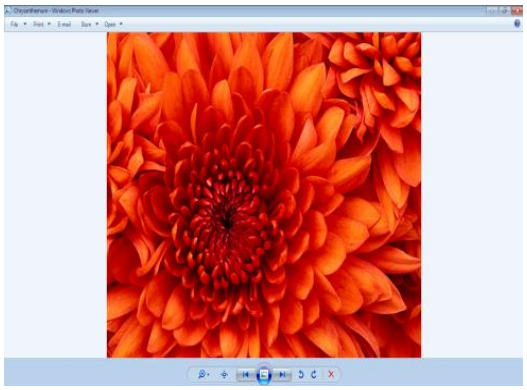


Fig: Original Image

Embedding data file in a carrier file

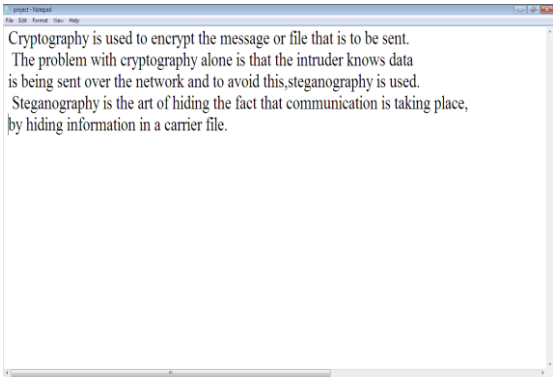


Fig: Plain Text

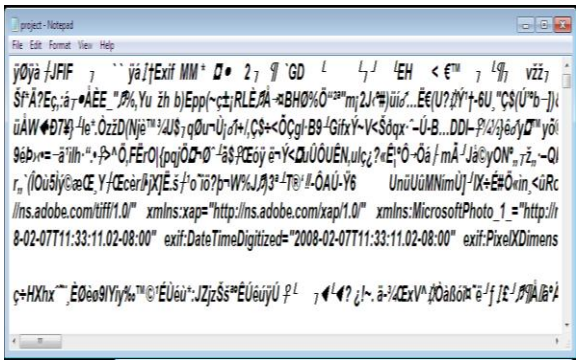


Fig: Cipher Text (embedded data file in image)

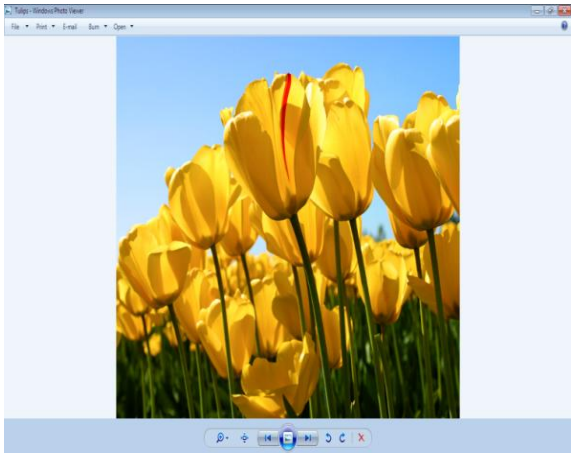


Fig: Original Image

Conclusion

In this we have combined the steganography and cryptography for providing higher security. We have enhanced the existing LSB method by adding a random function to it which is more complex because of its dynamic behavior**.** To be able to achieve a very reliable, sturdy yet simple software package that would really help people in sending the confidential data safely and securely was our main goal. We hope that the application would be easy and practical to use. All these above techniques works upto the expectations as we have observed by experimentation with more than hundred carrier images and different data and files.

We can also send the data from sender to receiver with the help of an IP address.

References

[1]Principles of Information Security, --Michael E. Whitman and Herbert J.Mattord

[2]Antti Hamalanen, Matti Tommiska and Jorma Skytta, "6.78 Gigabits Implementation of the IDEA Cryptographic Algorithm", 12th conference on Field Programmable Logic and Applications, Montpellier, France, Sept 2002.

[3]Miroslav Dobsicek, In Article "Modern Cryptography", Czeck Technical University in Prague.

[4]Ross J. Anderson, Fabian A.P. Petitcolas, "On The Limits of steganography", IEEE Journal of selected Areas in communication, 16(4), 474-481, May 1998.

[5]Mohammad Ali Bani Younes, Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", IJCSNS International Journal of Computer Science & Network Security, Vol 8, No 6 , June 2008.