To Improve Data Security by Using Secure Data Transmission

Manisha Yadav

M.tech (cse)

Pdm college of engineering for women

Bahadurgarh Haryana,India

ABSTRACT*: The "Secure data transmission" is a software solution which provides security during transmission .Present day security is the main issue that the third person attacks on the data. To provide security Tiny Encsryption Algorithm (TEA) is used. TEA is used for encryption and decryption of data. Encryption plays a cordial role in security. Encryption alters the data in unreadable form. Encrypted file embed in a video file by using steganography. Steganography is the concealing of secrete data inside image, video, audio. That video file sends via an email .On the receiver end receiver receive the video file and decrypted it by using Tiny encryption Algorithm (TEA). Then de-embed the information by steganography .This is the process that we are discuss in the paper .*

The goal of our project is to design a tool for providing security to the system during transmission of data. The project is developed using graphics in java swings.

Keywords- *Steganography, Tiny Encryption Algorithm, Encryption, Decryption ,Embed ,De-embed.*

1. INTRODUCTION

The project titled "Secure Data Transmission " is designed for providing security during transmission of data. The sender encrypts the data by using "Tiny Encryption Algorithm" because it requires less memory. It uses simple operations and easy to implement.[1]

By using Tiny Encryption Algorithm encrypt the data or information in unreadable form by entering a key by the sender .The purpose of key is to provide security to the information during transmission because key is knows only to the sender and the receiver. The encrypted data will embed in a video file by using steganography .The steganography [10] will read the video file and encrypted data and embed in video. So whenever the third person tries to open the file, only video file is visible. Then this video file is sent via mail.

The receiver will receive the video and de-embed the information from video then enter the proper key decrypt the information .The whole process will discuss in this paper.

Purpose :-

- To implement the Tiny Encryption Algorithm.
- Implementation of steganography.
- Achieve SECRECY

2. MODULUS

There are two modulus of this project one is tiny encryption algorithm and other is steganography.

2.1 Tiny Encryption Algorithm: Tiny Encryption Algorithm is a fast , easy and feistel block cipher. That was developed by David J. Wheeler and Roger M. Needham from Cambridge University. Tiny Encryption Algorithm has 32 rounds and use the algebraic operators to process. The algebraic operators are shifts, additions and XORs. Tiny Encryption Algorithm has 128-bit key length and 64-bit block size. TEA cipher key scheduling is simple anyway. *It* 32-bit addition by delta (∂) constant, delta is golden number ratio.

$$\partial = (\sqrt{5}-1).2^{31}$$

Tiny Encryption Algorithm process data round by round and TEA has 32 round. Each round has two 32-bit half blocks, one is left half and other is second half. Left halves is processed and swapped iteratively and perform the delta operation on the block. The detail of TEA cipher can be described as follow:*[13]*

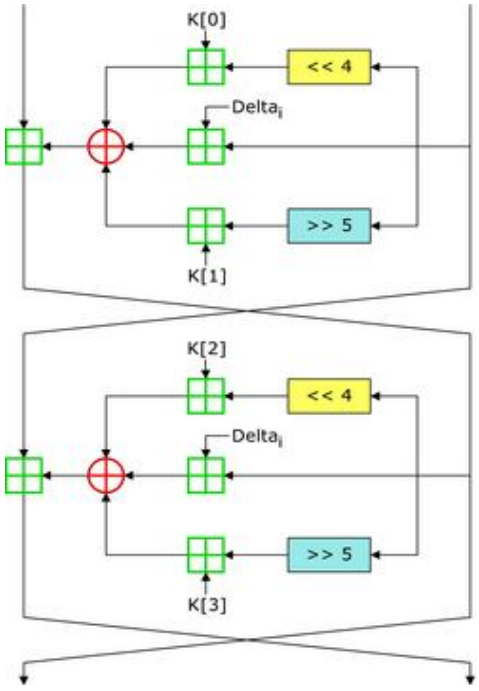


Fig 1: round function[1]

2.2 Steganography:

Steganography is the art of concealing secret data inside image, audio, video file.Various method of stegsnography but video steganography is done by Discrete Cosine Transform (DCT).[6]

DCT Based Steganography [11]

Algorithm to embed encrypted information:-
Step 1: First of all read the video file.
Step 2: Then Read encrypted information that will embed in video.
Step 3: To embed the information in video, divided the video into frames of 8×8 block.
Step 4: Processing each frame from left to right, top to bottom
Step 5: Then DCT will applied to each block. .
Step 6: Then write steganography video.
Algorithm to de-embed the encrypted information:-
Step 1:first read steganography video.
Step 2: Steganography video divided into frames and each frame is broken into 8×8 block of pixels.
Step 3: Processing each frame from left to right, top to bottom subtract 128 in each block of pixels.
Step 4:Then DCT will applied to each block.
Step 5: Then Retrieve the encrypted information.

3. CODE CONVENTION

Main Form.java

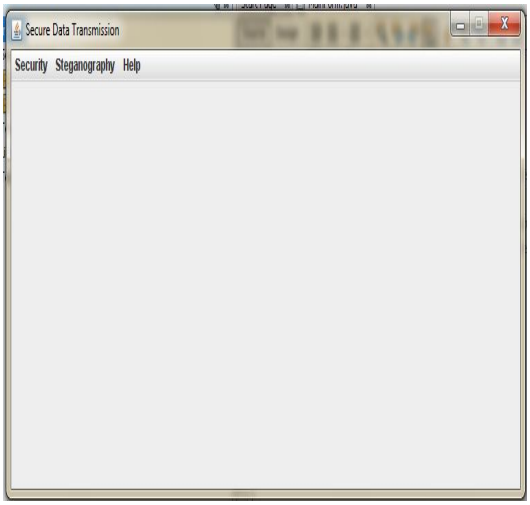
```
import javax.swing.JOptionPane;

import Security.*;

import Stegnography.DembedForm;

import Stegnography.EmbedForm;

public class MainForm extends javax.swing.JFrame

{   EncryptionForm ef;

    DecryptionForm df;

    DembedForm debf;

    EmbedForm ebf;

    public MainForm() {

        initComponents();

    }
```

Embed Form.java

```
package Stegnography;

import java.awt.FileDialog;

import javax.swing.JFrame;

import javax.swing.JOptionPane;

public class EmbedForm extends
javax.swing.JFrame {

    EmbProcess ep;

    public EmbedForm() {
```

4. RESULT OUTPUT SCREENS

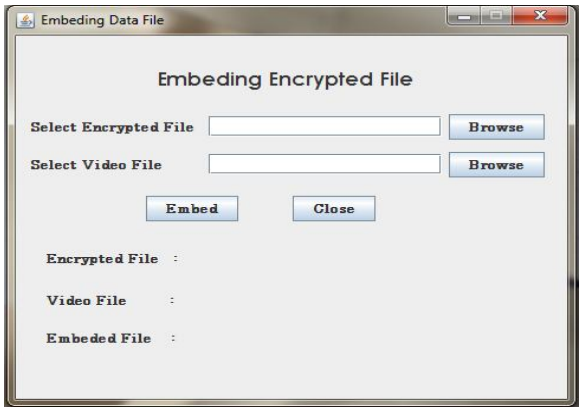
Main Form .java



Encryption of information

To enter the proper key

Browse the file for Embedding



Embeding Process complete

Then the video send via email and Then the reversal process will done in the same manner first de-embed the encrypted information then entering the proper decryption is done and the original information is retrieve by the receiver.

5. FUTURE ENHANCEMENT

To make system more efficient then now . To more concentrate on detect the untraced errors in the coming versions. To correct the errors by using more advance error correction algorithms and the compression of data by using the advance algorithms.

6. CONCLUSION

The software is developed and is tested with the sample data and process according to our requirements .The system performance is more efficient then the existing system. The project meets our primary requirements.

References

[1]. Andem, Vikram Reddy . "A Cryptanalysis of the Tiny Encryption Algorithm", 2003

[2]. Atul Kahate, " Cryptography and Network Security", TMH, 2003

[3]. Behrouz A. Forouzan, (2006)"Cryptography and Network Security", Firstedition, McGraw-Hill.

[4]. Christian Cachin." An information-theoretic model for steganography". Lecture Notes in Computer Science, 1525:306.318, 1998.

[5]. Hernández, Julio César; Isasi, Pedro; Ribagorda, Arturo. "An application of genetic algorithms to the cryptoanalysis of one round TEA". Proceedings of the 2002 Symposium on Artificial Intelligence and its Application, 2002.

[6]. Johnson N. and Jajodia S., "Steganography: Seeing the Unseen," IEEE Computer Magazine, vol. 25, no. 4, pp. 26-34, 1998.

[7]. Kawaguchi, E; Eason RO . "Principle and applications Steganography (Original paper on Steganography)" sept 2008.

[8]. Luis von Ahn and Nicholas J. Hopper. "Public-key steganography" In Lecture Notes in Computer Science, volume 3027,1995.

[9]. Popa R., "An Analysis of Steganographic Techniques," Working Report on Steganography, Faculty of Automatics and Computers, 1998.

[10]. R. Anderson, R. Needham, and A. Shamir. "The steganographic file system". In IWIH: International Workshop on Information Hiding, 1998.

[11]. ―Video Steganography by LSB Substitution Using Different Polynomial Equations‖, A. Swathi, Dr. S.A.K Jilani, International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[12]. An overview of image steganography‖, T Morkel, J.H.P. Eloff, M.S.Olivier.

[13]. Wheeler, D.J., & Needham, R.J. " TEA, a tiny encryption algorithm". In Fast Software Encryption – Proceedings of the 2nd International Workshop,1008, 1998