Volume 3, Issue 12, December 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Improved Secure Data Transfer Using Tiny Encryption Algorithm and Video Steganography

Manisha Yadav, Mauli Joshi, Akshita
PDM College Of Engg For Women
Bahadurgarh Haryana, India

Abstract: The "Secure data transfer" is a web application which deals with security during transmission of data. Security for the data is required, as there is always a chance for someone to read those secret data. The security is implemented by using steganography. Steganography is the good art of hiding information in ways so as to prevent detection of hidden messages. This paper designs software which tries to alter the originality of the data files into encrypted form using Tiny Encryption Algorithm .This Algorithm is to be designed for simplicity and better performance. In an encryption scheme, information is encrypted using tiny encryption algorithm that changes it into an unreadable cipher text. After encryption, the encrypted data is embed in a video by using the concept of steganography and then this video file sent via email. The application should have a reversal process as of which should be in a position to decrypt the data to its original format upon the proper request by the user.

Keywords:-Encryption, steganography

I. INTRODUCTION

"Secure Data Transfer" is mainly designed for providing security to data. In this the sender encrypts the data in some form by using "Tiny Encryption Algorithm". Tiny Encryption Algorithm requires less memory. It uses simple operations and it is easy to implement. While encrypting the data in some form, the key is entered by the sender. The key is use to provide security to the system. The key is known only to the sender and the receiver. After entered the key the data is encrypted then the encrypted data is embed in a video by using the concept of steganography. The steganography will read the video and encrypted data and takes whole it as a video. Then this video is sent via mail. So whenever the third person tries to open the video, only video is visible to them. The receiver will receive the video. Then the receiver will de-embed the encrypted data from the video. The application of decryption is done when the receiver enters the same key. This is how the data is transferred from sender to receiver in a secured manner.[13]

II. TINY ENCRYPTION ALGORITHM

The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm. Tiny Encryption Algorithm minimizes memory and maximizes speed. It is a Symmetric block cipher. TEA seems to be highly resistant to differential cryptanalysis. It achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text) after only six rounds. In this research we inspected the most common methods in the cryptanalysis of a block cipher algorithm. [1]

The following notation is necessary for our discussion.

- Hexadecimal numbers will be subscripted with "*h*," e.g., 10 = 16. *h*
- Bitwise Shifts: The logical left shift of *x* by *y* bits is denoted by $x << y$. The logical right shift of *x* by *y* bits is denoted by $x >> y$.
- Bitwise Rotations: A left rotation of *x* by *y* bits is denoted by $x <<< y$. A right rotation of *x* by *y* bits is denoted by $x >>> y$.
- Exclusive-OR: It is logical operation of addition of n-tuples and is denoted by $x \oplus y$.

The Tiny Encryption Algorithm is a symmetric type cipher that uses algebraic operations. A double shift causes all bits of the data and key to be mixed iteratively. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). Time performance on a workstation is very impressive. [4]

In block cipher the plain text is entered and applying the transformation or round function changes into the cipher text. In Feistel cipher the text is encrypted and the encrypted text is divided into two halves at one half the round function F and sub key is applied and the output of F is exclusive-OR(XOR) with other half. Then swap the two halves Each round follow the same steps except the last round in the last round there is no swapping of two halves.[5]

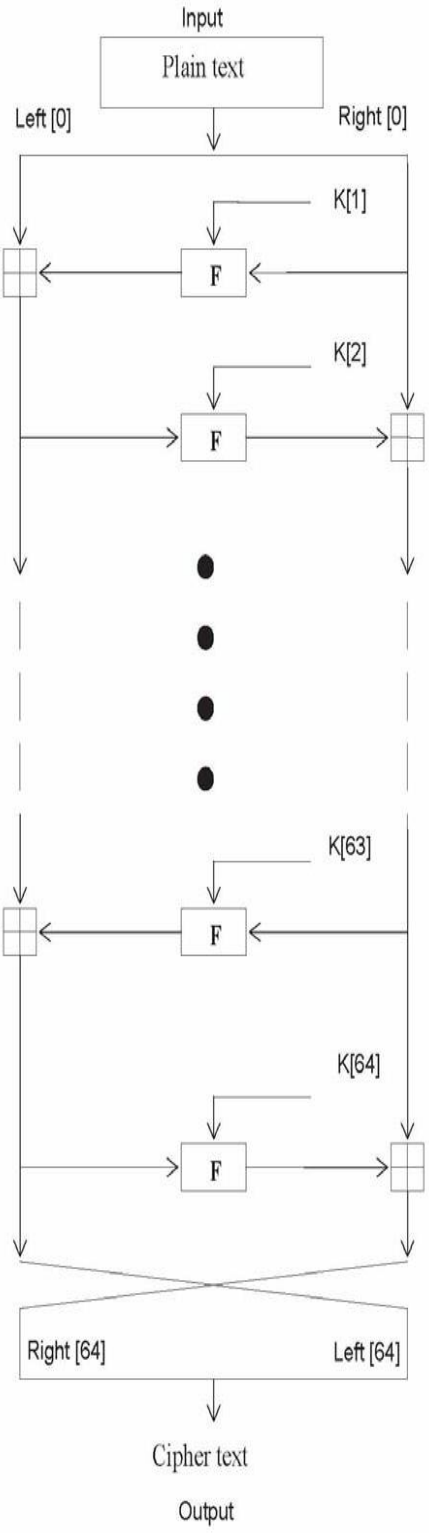


Fig 1: Diagram for Encryption—[13]

The inputs to the encryption algorithm are a plaintext block and a key K .The plaintext is P = (Left [0], Right [0]) and the cipher text is C = (Left [64], Right [64]). The plaintext block is split into two halves, Left [0] and Right [0]. Each half is used to encrypt the other half over 64 rounds of processing and then combine to produce the cipher text block.

- Each round *i* has inputs Left[*i*-1] and Right[*i*-1], derived from the previous round, as well as a sub key K[*i*] derived from the 128 bit overall K.
- The sub keys K[*i*] are different from K and from each other.
- The constant delta $=(5^{1/2}-1)*2^{31}$ =9E3779B h , is derived from the golden number ratio to ensure that the sub keys are distinct and its precise value has no cryptographic significance.

- The round function differs slightly from a classical Fiestel cipher structure in that integer addition modulo 2^{32} is used instead of exclusive-or as the combining operator.[6]

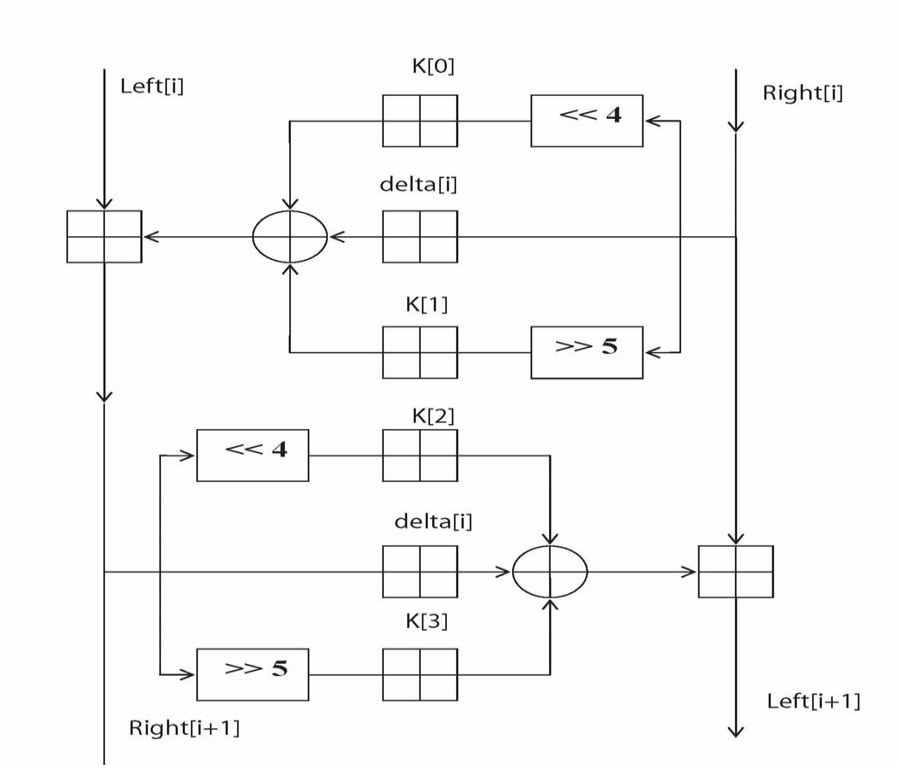


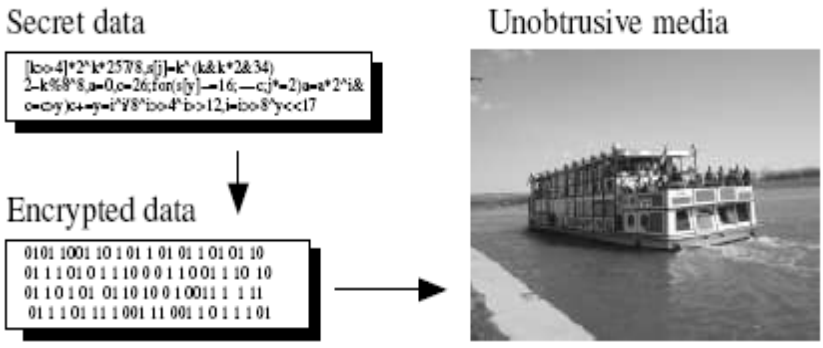
Fig 2: Diagram for Round Function

The round function has the same general structure for each round but is parameterized by the round sub key K[*i*]. The algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). The keys K[0] and K[1] are used in the odd rounds and the keys K[2] and K[3] are used in even rounds.[13]

Decryption is same as the encryption process in the decode routine the cipher text is used as input to the algorithm, but the sub keys K[*i*] are used in the reverse order.

III. STEGANOGRAPHY

Steganography is an art of hiding information within other information. The word steganography means secret writing. Now day's cryptography become very popular science. Cryptography is about concealing the information. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography makes the cipher text invisible to unauthorized users. [10,11]



Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is used to protect important information. Steganography involves hiding information so it appears that no information is hidden at all. If a person tries to views the object that the information is hidden inside will not visible to them therefore the person will not attempt to decrypt the information.

The most common use of Steganography is to hide a file inside other file. When information is hidden inside a file, the data is usually encrypted with a password.[12]

There are various methods used to hide information inside of Picture, Audio and Video files. The two common methods are **LSB (Least Significant Byte)** and **Injection.**

Steganography in Video

DCT(Discrete Cosine Transform) method is used for hiding information inside a video file.

DCT slightly changing the each of the images in the video, the change is minor that does not visible by humans . DCT alters values of certain parts of the images.

For example if part of an image has a value of 7.766 it will round it up to 8.

Video steganography is similar to that Image Steganography, in video steganography the information is hidden in each frame of video that information is not visible the video play as the original video that information is not noticeable by the person that are watching the video.

IV. FUTURE SCOPE

- The correction of errors using various error correction techniques or development of new techniques.
- The compression of data using existing techniques or developing of new techniques.

V. LIMITATIONS

1. It provides the storing of data in an unprotected mode.
2. Password leakage may occur and it leads to the unauthorized access of data.
3. The intruders will affect stegos.

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

