ISSN:0975-9646

Secure Data Transmission using Encrypted Secret Message

Jaishree Singh, Dr. J.S. Sodhi

Department of Computer Science & Engineering,
Amity School of Engineering and Technology
Amity University, Sec-125 NOIDA, (U.P.),India

***Abstract*:- In any communication, security is the most important issue in today's world. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like DCT, FFT and Wavelets etc. In this project we are developing a system in which two techniques, steganography and cryptography are combined, which provides a strong backbone for its security. The scenario of present day of information security system includes confidentiality, authenticity, integrity, non-repudiation. This present work focus is enlightening the technique to secure data or message with authenticity and integrity. In this project work, the secret message is encrypted before the actual embedding process starts. The hidden message is encrypted using Tiny algorithm using secret key and DCT technique is used for embedding and extraction file.**

Keywords: Steganography, Cryptography, Encryption, Data hiding

I. INTRODUCTION

A. Steganography

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing". The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file[1].

B. Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced cryptotechniques ensure that the information being transmitted has not been modified in transit. Cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible.

II. THE PROPOSED SYSTEM

In this proposed system we have the software for data encryption and then embed the cipher text in a cover medium. This system combines the effect of these two methods to enhance the security of the data.

The proposed system encrypts the data with a tiny algorithm and then embeds the encrypted data in a cover file using DCT algorithm. This system improves the security of the data by embedding the encrypted data and not the plain data in cover file. The block diagram of proposed system is as shown in fig.1

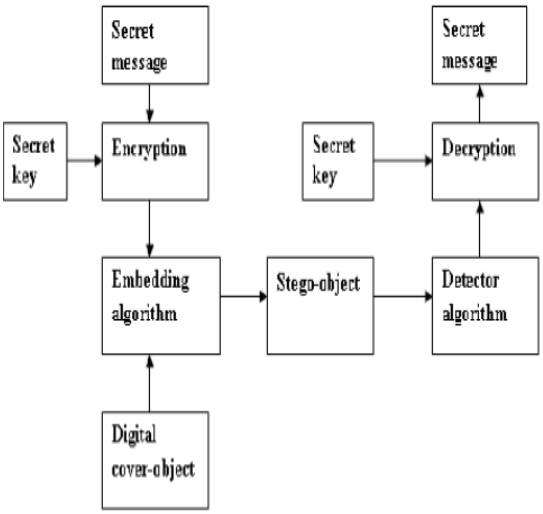


Fig. 1 Block diagram of proposed system

To embed a secret message file in the cover file used two distinct methods:

(1) encrypt the secret message

(2) The encrypted secret message is embed in the cover media

A. Encryption algorithm

This encryption method is simple and efficient and is of symmetric type where only receiver and sender knows secret key. The Secret key length is variable and is of range double precision. At the receiver side during extraction process the decryption ,that is the reverse process of encryption is carried out using the same key to obtain the secret message from

stegno medium. In a nutshell, the reason that we encrypt the message is :

Cryptography + Steganography = Secure Steganography

1) Crypto module
   Text File + Tiny Algorithm = Encrypted File
2) Stegno module
   Encrypted File + DCT Algorithm + Stegno medium = Stegno Object

1) Tiny Algorithm

Tiny Encryption Algorithm the Tiny Encryption Algorithm is a Feistel type cipher (Feistel, 1973) that uses operations from mixed (orthogonal) algebraic groups XOR, ADD and SHIFT. A dual shift causes all bits of the data and key to be mixed repeatedly. 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]). TEA seems to be highly resistant to differential cryptanalysis (Biham et al., 1992) and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text). Time performance on a workstation is very impressive.

2) Encryption Routine

The Encrypt Routine is written in the C language and assumes a 32-bit word size. The 128 bit key is split into four parts and is stored in K[0] - k[3] and the Data is stored in v[0] and v[1].

```
void code(long* v, long* k) {
unsigned long y = v[0], z = v[1], sum = 0, /* set up */
delta = 0x9e3779b9, n = 32 ; /* a key schedule constant */
while (n-->0) { /* basic cycle start */
sum += delta ;
y += (z<<4)+k[0] ^ z+sum ^ (z>>5)+k[1] ;
z += (y<<4)+k[2] ^ y+sum ^ (y>>5)+k[3] ; /* end cycle */
}
v[0] = y ; v[1] = z ; }
```

The constant delta is given as delta = (√5 -1) * 231 i.e. 9E3779B9h and is derived from the golden number ratio to ensure that the sub keys are distinct and its precise value has no cryptographic significance.

TEA uses addition and subtraction as the reversible operators instead of XOR. The TEA encryption routine relies on the alternate use of XOR and ADD to provide nonlinearity. The algorithm has 32 cycles (64 rounds). TEA is short enough to write into almost any program on any computer.

The Tiny Encryption Algorithm (TEA) is a block cipher encryption algorithm that is very simple to implement, has fast execution time, and takes minimal storage space [2].

B. Embedding algorithm

1) Discrete Cosine transform (DCT)

According to the method presented in this paper, the message is inserted into the DCT domain of the host image. The hidden message is a stream of "1" and "0" giving a total number of 56 bits. The transform is applied to the image as a multiple factor of 8x8 blocks. The next step of the technique after the DCT is to select the 56 larger positive coefficients, in the low-mid frequency range. The high frequency coefficients represent the image details and are vulnerable to most common image manipulation like filtering [11] compression [12] etc. Our scheme is applied to the whole image and since robustness is the main issue, the low and mid frequency coefficients are the most appropriate. The selected coefficients *ci* are ordered by magnitude and then modified by the corresponding bit in the message stream. If the *i*th message bit ***s(i)*** to be embedded is "1", a quantity *D* is added to the coefficient. This *D* quantity represents the persistence factor. If the message bit is "0", the same quantity is subtracted from the coefficient. Thus the replaced DCT coefficients are

DCT (new) = DCT+1*D for s(i)=1;
Else
DCT (new) =DCT-1*D for s(i)=0.

DCT can separate the image into High, Middle and Low Frequency components. To hide information we need to set a threshold value for the DCT coefficients depending on the quality of the images.

C. Description of Proposed Work

When the system is executed GUI is displayed for login window, from here user can login to enter into the system and new user can register himself. If any registered user forget his password, this system has an option of forgot password. Database is provided to store user id and passwords. The system provides the process for encryption, decryption, embedding, and de-embedding. The Encryption window provides option for selecting secret message file, for this system the secret message file is text file. Embedding window to embed the message in cover file to get stegomedium and the press save button to save the stegomedium. In Home window press dembed button in home window to extract the secret message from stegomedium and then press decrypt button to get the original file which is in readable form. And press exit button to get out of the home window.

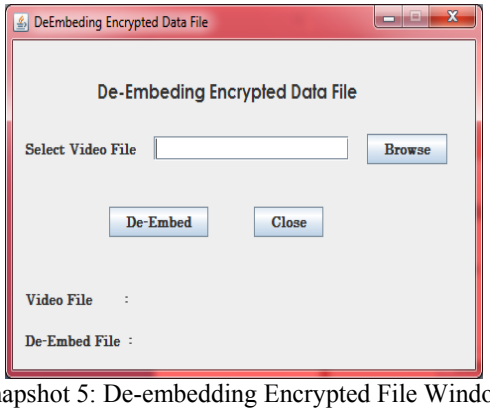
Secret key is required at the time of encryption at sender side and same secret key is required at receiver side to decrypt the dembeded file .Secret key must be known to both sender and receiver. If the incorrect key is entered it is not possible to

Snapshot1:Login Window

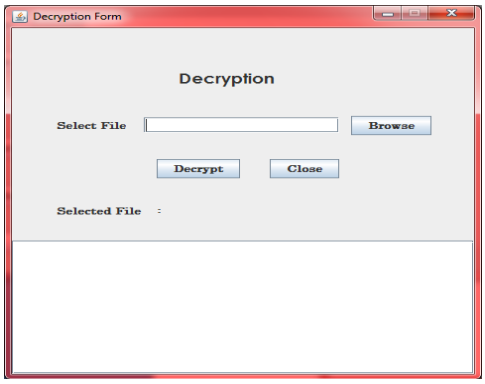
Snapshot 2: Home Window

Snapshot 3: Encryption Window

Snapshot 4: Embedding Window



Snapshot 5: De-embedding Encrypted File Window



Snapshot 6:Decryption Window

As our eye is not very sensitive so therefore after embedding a secret message in a cover file our eye may not be able to find the difference between the original message and the message after inserting some secret text or message on to it.

III. CONCLUSION

This system provides two level of security, first by encryption, second by steganography. Tiny encryption algorithm is block cipher algorithm. It is simple and fast. This System uses Tiny algorithm for encryption which is very secure and the DCT transformation Steganography techniques are very hard to detect.

IV. FUTURE WORK

As future work, we intend to study more steganalytic techniques i.e. detecting whether a particular file contains any form of embedding or not. We also plan to extend our system so that it can hide digital files in other digital files, for example hiding Audio files in Videos files etc.

REFERENCES

[1] Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar "Cryptography of Video InformationIn Modem communica-tion", Electronics And Energefics, vol.11, pp. 115-125, 1998

[2] Wheeler D., and R. Needham. TEA, a Tiny Encryption Algorithm, Proceedings of the Second International Workshop on Fast Software Encryption, Springer-Verlag, 1995, pp. 97-110.

[3] National Institute of Standards, Data Encryption Standard, Federal Information Processing Standards Publication 46. January 1977

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[6] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[7] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[8] C. Cachin, "An Information-theoretic Model for steganography", in proceeding 2nd Information Hiding Workshop, vol.1525, pp.306-318,1998

[9] Neil F. Johnson, Zoran uric,Sushil. Jajodia, " Information Hiding: steganography and Watermarking – Attacks and Countermeasures", Kluwer Academic Press, Norwrll, MA,New York, 2000

[10] J. Zollner, H. Federrath, H. Klimant,et al.,"Modeling the Security of Systems", Steganographic in 2nd Workshop on Informafion Hiding,

Portland, April 1998, pp. 345-355. proceeding of IEEE, pp. 1062-1078, July1999.

[11] N. F. Johnson and S. Katzenbeisser, .A survey of steganographic techniques., in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[12] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996

[13] M. M Amin, M. Salleh, S. Ibrahim, M .R. Katmin, and M. Z. I. Shamsuddin," Information Hiding using Steganography", IEEE 0-7803- 7773-March 7,2003

[14] Advanced Steganography Algorithm usingencrypted secret message, Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Application (IJACSA) Vol-2 No.3, Page19-24,March 2011.