S.G. Gino Sophia, K.Padmaveni, Linda Joseph / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1492-1496

# Four key Secured Data Transfer Using Steganography and Cryptography

**S.G. Gino Sophia, K.Padmaveni, Linda Joseph**
School of Computing Sciences and Engineering Hindustan University

## Abstract

**Steganography and cryptography are used to send the data in a confidential way. Steganography hides the existing message and cryptography will confuse the message. The transformation of plain text to cipher text is called as encryption. The transformation of cipher text to plain text is called decryption. Encryption and decryption are controlled by keys. Hashing, symmetric and asymmetric algorithms are cryptographic techniques. There is a difficulty to find the hidden messages. For this purpose various transformations like DCT, FFT, FFT, and 2DDCT are used. A system is proposed in this paper to develop a new technique along with a newly enhanced security model in which cryptography and Steganography are used. In cryptography DES algorithm is used to encrypt a message and part of the message is hidden in 2DDCT of an image and the rest of the message will generate two secrete keys for the generation if high security.**

**Keywords:** Steganography, Cryptography, Data hiding, 2DDCT, DES algorithm

## I. INTRODUCTION

Information security is called cryptography [3]. Some techniques included in cryptography are the merging of words with images, microdots and the different ways of hiding the data in storage. Cryptography mainly concern with the conversion plain text into cipher text. This process is called encryption. The reverse of this process is called decryption. The four objectives in modern cryptography are:(i)Confidentiality(unauthorized person will not be able to understand the data)(ii)Integrity(The data can't be altered in the storage between sender and receiver)(iii)Authentication(confirmation from the sender and receiver side) (iv)Non- repudiation(at the later stage the sender will not be able to refuse the data which is about for transmission). Steganography, this hides information by embedding the messages within other. Replacement of useless bits or used data is the work performed by it. If the encryption is not allowed Steganography is used or otherwise encryption is supplemented by Steganography. This encrypted file may also hide information's. The hidden messages will not be seen if the encrypted file is deciphered. Data hiding: The other part of the program is protected on changing the decision of a design from the extensive modification. For better confidentiality security we use both cryptography and Steganography in this paper to develop one system. DES algorithm is a secured technique for cryptography and Steganography methods. Our idea is based on combining these techniques the intruder may find the original data, to get a highly secured system for data hiding. In data hiding the following are performed.

The part of a message which is encrypted will be hidden instead of hiding message which is highly encrypted.

The encrypted message which are unhidden will be converted into two secrete keys.

To get the original text along with keys for Steganography and cryptography, two extra keys and the reverse process of the key generation should be known. So the aim of the project is to develop system which is more secured and even if the messages from stegno images are retrieved from somebody [1], it becomes meaningless for any existing cryptographic techniques.

## II. BASIC CONCEPTS AND RELATED WORK

For security there are many aspects. One of the aspects for confidential communication is that of cryptography. The specific security requirements [8] for cryptography are confidentiality, authentication and integrity, on-repudiation.

The following describes the four types of algorithms:

(a)**Public key cryptography (PKC):** uses one public key for encryption and uses other private key for decryption.

(b)**Key distribution centre single key (KDC)**: A single key is shared with the key distribution centre. Key management and authentication is performed by KDC for communication key distribution is essential.

(c)**Shared secrete key:** Both source and destination share the secrete key. It is also called as challenge response protocol.

(d)**Hash function:** To encrypt data irreversibly a mathematical transformation is used. The other technique for communication is Steganography [7]. It transfers the messages by which it can't be detected. The information can be hidden in audio,

video, text, images, or code [11] which is digitally representative.

### A. DES algorithm for cryptography

DES algorithm is a cipher block, which encrypt data in 64 bit block. It is a symmetric algorithm which uses same algorithm [13] and key for encryption and decryption. This algorithm encrypts and decrypts the blocks of data containing 64 bits under 64 bit key controls.

- **Advantages of using DES algorithm**

(i)The security of this algorithm resides in the key
(ii)More secured as the length of the key is increased.

### B. 2DDCT algorithm for Steganography

This 2 dimensional discrete cosine transformations is a signal from spatial representation into frequency representation. Than higher frequencies, lower frequencies are more obvious on transforming an image [5] into frequency components. By throwing away higher frequency coefficients without sacrificing too much image quality [15] , reduce the amount of needed data to describe the image.Over simplified Jpeg compressor

- Image is cut into 8x8 pixel of chunks
- Through an 8x8 2DDCT run each chunk
- Resulting coefficients are quantified
- Quantified coefficients are compressed using a losels' methods

Formulae for 2DDCT:

$R_u$=1/√2 if u=0
1 else

$R_v$ = 1/√2 if v=0
1 else

else

$F_{vu}$ = 1/4 $R_v$ $R_u$ $\sum_{y=1}^{N-1}$ $\sum_{x=0}^{N-1}$ $S_{yx}$ cos(vπ 2y+1/2N)cos(vπ 2x+1/2N)

Inverse Discrete Cosine Transform:

Image can be rebuild in the spatial domain from frequencies

IDCT formulae:

$R_u$=1/√2 if u=0
else
$R_v$ = 1/√2 if v=0
1 else

$F_{yx}$=1/4$\sum_{v=0}^{N-1}$ $\sum_{u=0}^{N-1}$ $R_vR_u$ $F_{vu}$cos(vπ 2y+1/2N)cos(vπ 2x+1/2N)

Until the coefficient quantizing is started no image is lost.DCT is perfectly reversible.

## III. PROPOSED SYSTEM

The two different techniques are combined which is based on idea of distortion of message and hiding the existence of distorted message for getting back the original information and retrieve the data which is distorted [2] and regain the actual text by reverse distortion process. Here the system is designed with three modules.

(i)Crypto module for cryptography
(ii)Stegno module for Steganography [10] and
(iii)Security module for more security

### A. Hiding the text

- **Crypto module:**

For the encryption of data the following steps are considered in crypto module [14].

- For encryption the text is inserted
- DES algorithm is applied using 64bit key
- Hexadecimal form cipher text is generates

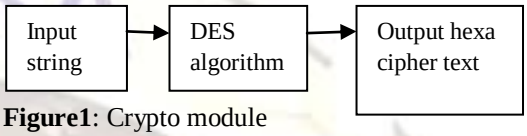


**Figure1**: Crypto module

- **Security Module:**

To our newly developed system an extra security feature is provided by this intermediate module. Cipher text is modified by this module to generate two extra keys [6]. It regenerates the original cipher text on its reverse process. The process of this module before hiding the process follows:

- The alphabets and digits are separated from cipher text
- The digits and the track of the original position of the alphabets are kept in the form of a secrete key (keyC)
- In first step, the first seven characters are separated, the remaining alphabets are added to the end of the separated digits as in the first step by which the second key (keyD) is guaranteed.

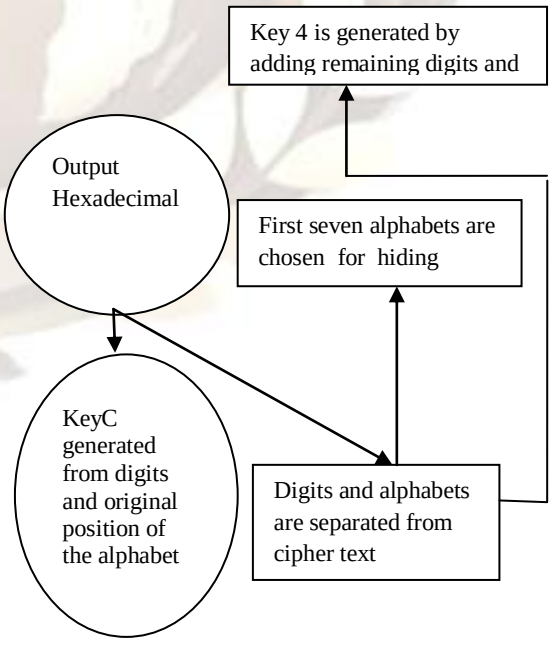


**Figure2:** security module

- **Stegno Module:**

The above guaranteed cipher text are hidden by the following steps:

- From the above discussed security module the seven alphabets are taken
- The alphabets are scrambled using 128 bit key
- 2DDCT of the image is found
- By altering 2DDCT the cipher text is hidden
- Inverse 2DDCT is applied
- Stegno image is found

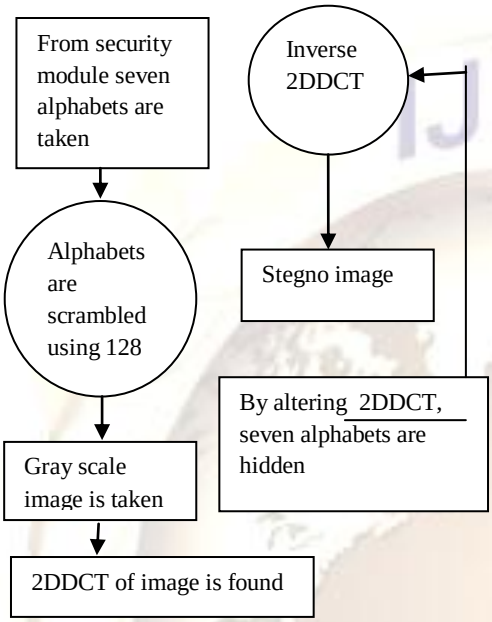


**Figure3:** Stegno module

**B. Retrieving text**

- **Stegno Module(reversing process):**

To retrieve the cipher text the following steps are considered in stegno module:

- 2DDCT of the original image is taken
- 2DDCT of the stegno image is taken
- Difference of 2DDCT coefficient is taken
- From LSB of 2DDCT bits are retrieved from the hidden seven alphabets
- The distorted seven alphabets are constructed
- Using keyB unscramble the distort seven alphabets
- Original seven alphabets are retrieved

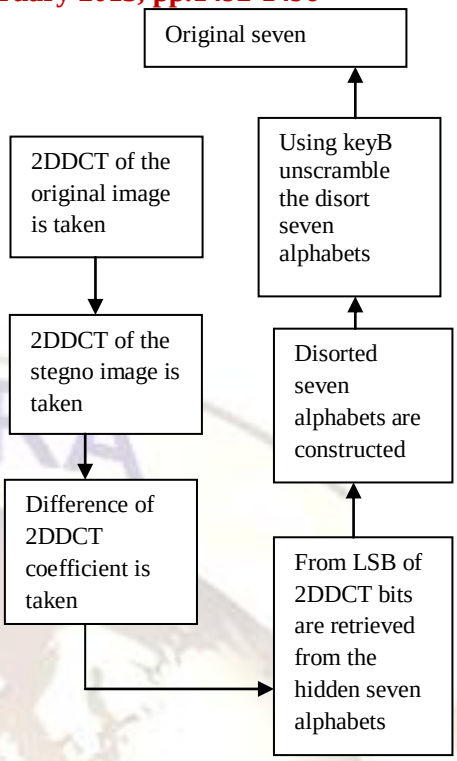


**Figure4:** stegno module (reverse process)

- **Security Module(reversing process):**

For retrieving the cipher text the following steps are considered in the security module:

The seven characters are clubbed with the alphabets of keyD

The cipher text is reconstructed using keyC and keyD from digits and alphabets.

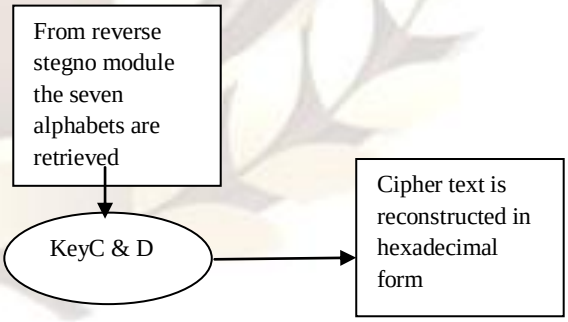


**Figure5:** security module (reversing processing)

- **Crypto Module(Reversing Process):**

For retrieving the original text the following steps are Considered in crypto module:
Retrieved cipher text is taken from the above
Reverse DES algorithm by using keyA
Original message is obtained.

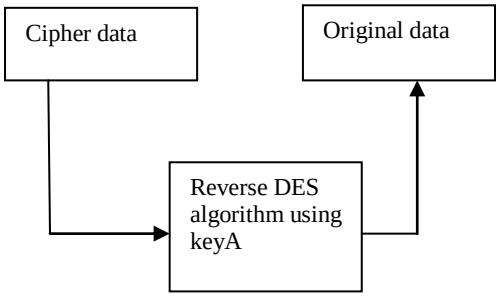


**Figure6:** crypto module (reversing process)

## IV. IMPLEMENTATION DETAILS

By VC6.0 platform using VC++ this project is developed. The three modules taken part are
a) Crypt module
b) Security module
c) Stegno module

### A. Algorithm for the proposed system:

In DES algorithm we are getting the cipher text as hexadecimal form [9].

Data is encrypted in units which are smaller than the defined block size.

Using cipher feedback mode, DES is converted into stream cipher. With the same key more than one message is encrypted and different initialization vector is used.

Cipher feedback mode (CFB) is same as the block cipher. Here encryption is not parallelizable only decryption is parallelizable [12] and it has random access property. It is self recovery with respect to synchronization errors.

*A. Hiding text:*

Cipher text is generated in hexadecimal form by DES algorithm in the form of alphabets like .
With the help of a intermediate the alphabets and digits are separated and the original position of the alphabets and digits are kept tracked in the form of first key(keyA).

The first seven characters of the alphabets are taken and hidden in the image
The rest of the alphabets are taken and combined with digits. This form the second key

Then the seven characters are hidden in the image mentioned in image 2.2

*B. Retrieving text*

From the image the seven characters are retrieved

From keyB with the help of seperator2 the alphabets and digits are separated

From keyB the rest of the alphabets are added back to seven characters which are retrieved from the image

With the help of the keyA the digits and elements are reorganized to get back the original cipher data in the form of hexadecimal

The original message from the cipher text is regenerated with the help of DES algorithm.

### C. Advantage of the proposed system:

The proposed system is highly secured because

Let's the combination of two secured techniques
a) DES for cryptography
b) 2DDCT for Steganography

- NNumber of keys:
Four keys are used in this system
a) For scrambling the cipher text one 56 bit private key
b) For DES algorithm one 64 bit private key
c) For retrieving the original data two extra private generated key
The system is highly secured by using these two extra generated keys.

## V. CONCLUSION

The summary of this project is mentioned in the following points:

- AThe new system with the combination of cryptography and Steganography using 4 keys is introduced.
- TThe method used for encryption using DES algorithm is very secure and it is the main advantage of this system. The 2DDCT transformation Steganography is very difficult to detect.

## REFERENCE

[1] **O**wen, M.," A discussion of covert channels and Steganography", SANS institute, 2002
[2]J. Zollner, H.federrath, H.klimant, et al.,"modeling the security of systems:, steganographic in 2nd workshop on information hiding,Portland,april 1998, pp.345-355.July1999.
[3] D.R.Stinson, cryptography: Theory and practice, Boca Raton, Press, 1995.ISBN: 0849385210
[4] 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.
[5] Marvel, L. M., Boncelet Jr., C.G.&Retter, C.,"Spread spectrum Steganography", IEEE Transactions on image processing,8:08,1999

[6] Alain C.Brainos II East Carolina university," Study of Steganography and The Art of Hiding information", November 13,2003.
[7] Dunbar,B.,"Steganography techniques and their use in an Open-Systems environment", SANS Institute,Januray 2002
[8]Stinsown,D."Cryptography: Theory and Practice"
[9] Neil F.Johnson, Zoran uric, Sushil jajodia," Information hiding: steganography and watermarking attacks and countermeasures", Kluwer academic press, Norway, MA, Newyork, 2000.
[10] N.Provos, P.Honeyman," Detecting Steganography content on the Internet". Transformation", ZEICE Tram. [11]Chandramouli, R., Kharrazi, M.& Memon,N.,'Image proceedings of the 2nd Workshop on Digital Watermarking, October 2003.
[12] R A Isbell,"Steganography: Hidden Menace or Hidden saviour", Steganography white Paper, IO May 2002
[13] Domenico Daniele Bloisi, Luca Iocchi: Image based steganography and cryptography, Computer Vision theory and applications volume1, pp.127-134
[14] E.T.Lin and E.J.Delp,"A Review of Data Hiding in Digital Images", JUNE 20001
[15] Ros J.Anderson,Fabien A.P.petitcolas," on The Limits of Steganography", IEEE Journal of Selected Areas in Communications,16(4):474-481,May 1998.
[16]http://www.xdp.it

## About Authors:

**S.G. Gino Sophia** , M.Tech Computer Science and Engineering working as a Selection Grade Assistant professor, Hindustan university, Chennai has 9 years of teaching experience and has published 7 international journal / conference papers.

**K.Padmaveni**, ME Computer Science and Engineering working as a Selection Grade Assistant professor, Hindustan university, Chennai has 8 years of teaching experience and has published 9 international journal / conference papers.

**Linda Joseph**, ME Computer Science and Engineering working as a Senior Scale Assistant professor, Hindustan university, Chennai has 7 years of teaching experience and has published 8 international journal / conference papers.