Assured Data Communication Using Cryptography and Steganography

G.Sateesh[1], E.Sai Lakshmi[2], M.Ramanamma[3], K.Jairam[4], A.Yeswanth[5]

[1] *Associate Professor,* [2,3,4,5] *Students*

Department of CSE, Lendi Institute of Engineering and Technology, vizianagaram.

***Abstract*— Now days in the world of communication, securing the information is Main criteria while communication in the network. Usually users exchange the confidential data and documents during communication. So, that Security is important criteria in Communication. Security and communication are inseparable words. In order to provide security to the data we are using cryptography and Steganography techniques together. This paper proposes Assured Data Communication by Using Cryptography and Steganography together. The combination of these two techniques can provide robust platform for secured data communication System. Here, We Create a Cipher text (Encrypted) of text message Using Cryptography Techniques and then we hide the Cipher text into Multimedia Using Steganography [1] techniques. We used SDES algorithm in Cryptography for data Encryption and Decryption, LSB Method of Steganography to hide Cipher text into image. This Proposed System provides high Assured Communication System. So that Intruders fail to crack data Communication even in Non-Secure channels.**

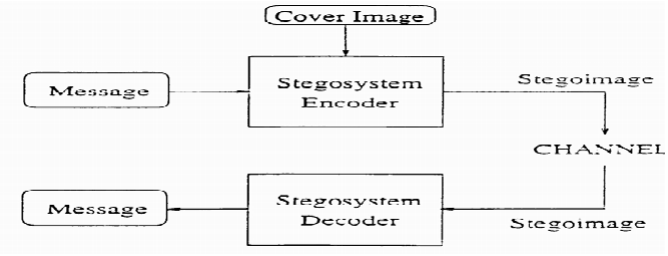
***Keywords*— Cryptography, Steganography, SDES, image hiding, least significant bit method**

I. INTRODUCTION

The Security of the data transmission place crucial role in Communication Networks. A Communication System is reliable as long as it provides high level of Security. Usually, Users Exchange the Personal Sensitive data or important documentation. In this type of case users want a Security , Integrity , authentication and Confidentiality of exchanged data most be provided to user over a the transmission medium. Present days, Internet is multimedia is very popular, a huge amount of data is exchanged every second in over non secure channel, which may not be safe. Therefore, it is essential to protect the confidential data from intruders. To protect the sensitive data; Cryptography and Steganography techniques Used. Cryptography is the Science of keeping the transmitted data Secure. Using Cryptography techniques we are provide the assured (secure) data transmission. It provides Encryption process for assured (secure) communication. The Encryption process is applied before transmitting the message and decryption process applied after receiver receives the encrypted message. Steganography is science of hiding the object in multimedia medium. In our proposed paper we took image as multimedia medium. It conveys the data by concealing it in other medium such as image or audio which is called the cover object. The information hiding process is applied before transmission and the extraction process is applied after receiving. The main difference between cryptography and steganography based on the existence of the secret message. Cryptography encrypts the message and transmits it; anyone can view the encrypted message, but is very difficult to be understood, especially if it has been encrypted with strong cryptographic algorithm. Steganography conceals the secrete message existence by hiding it in cover object

A. CRYPTOGRAPHIC FLOW

B. STEGANOGRAPHIC FLOW



Above 2 flow diagrams represent the clear view of the Cryptography and Steganography concepts and how they implemented. In our proposed system we are combining both these techniques and create robust and secure communication system which can resist from intruders attack but it certain minor limitations [2] that's not matter at all.

II. RELATED WORKS

Previously their exist some works like our proposed system but they are using either Cryptography or Steganography techniques of it and also some works like both together

(Cryptography and Steganography) also exist but they are not strong enough .Some of related works are failed in the secret data firstly are converted into a series of symbols to be embedded in a notation system with multiple bases. In this case, the particular bases used are determined by the degree of local variation of the pixel magnitudes in the host image. Due to this related works are fail to overcome the problems Changes stegoimage (cipher text hidden image) like colour changes in the image. Colour change in image may give the chance to intruders attack. A modification to the least significant bit matching (LSBM) steganography was introduced in our proposed system. This modification provides the desired choice of a binary function of two cover pixels rather than to be random as in LSBM. To increase the level of security, a combined data encoding and hiding process was proposed in our paper. This process was used to overcome the problem of image colour changes after the embedding process. The LSB steganography technique was developed in it based on embedding the secret message into the sharper edge regions of the image to ensure its resistance against image steganalysis [5] based on statistical analysis. In our proposed system avoid the colour changes in it.

III. PROPOSED SYSTEM

In our proposed system, we use both Cryptography (for encryption and steganography) and Steganography (for data hiding in the multimedia object) techniques together [4].

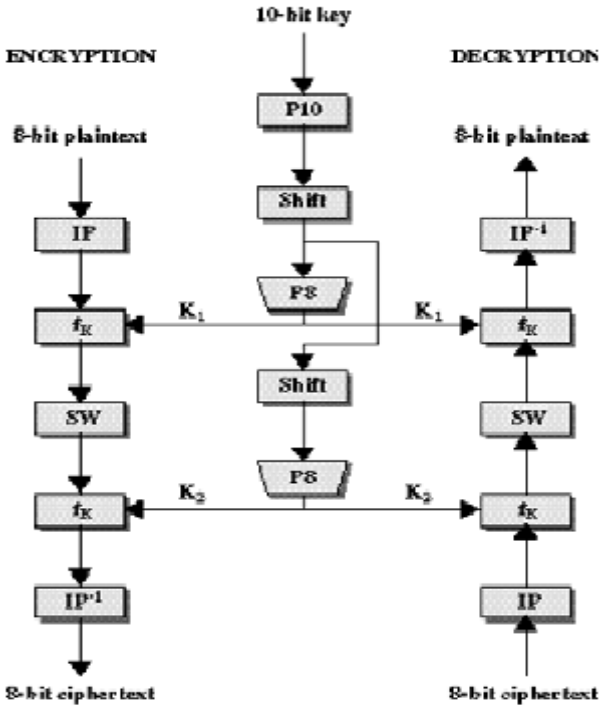
A. Cryptography

Cryptography is the study of means of converting information from its normal comprehensible form into an incomprehensible format. The algorithm used in this is Simplified Data Encryption Standard (SDES) [6].

IN SDES ALGORITHM

- Input(plain text):10bits
- Output(cipher text):10bits
- Rounds:2
- Round keys are generated using permutations and left shifts
- Encryption: initial permutation, round function, switch halves
- Decryption: same as encryption ,except round keys used in opposite direction

SDES ALGORITHM



$$\text{Ciphertext} = IP^{-1}\left(f_{K_2}(SW(f_{K_1}(IP(plaintext))))\right)$$

$$K_1 = P8(Shift(P10(key)))$$

$$K_2 = P8(Shift(Shift(P10(key))))$$

$$\text{Plaintext} = IP^{-1}\left(f_{K_1}(SW(f_{K_2}(IP(ciphertext))))\right)$$

In *above* algorithm

IP –Initial permutation

f_{k1}, f_{k2} – Round functions with keys k_1, k_2

SW - Shift operation

K_1, K_2 .Secret keys

B. Steganography

Steganography [7] is the study of means of concealing the information in order to prevent hackers from

detecting the presence of the secret information. In this project, we use a JPG or PNG image as a cover object. The technique used in this is Least Significant Bit (LSB method)[12]. This method modifying the rightmost bit in each byte by replacing it with a bit from the secret message. LSB method is more significant than MSB method .In LSB method we are not seen the any difference between original image and stego image [11] (data hidden image).

Example:

ORIGINAL IMAGE

IMAGE WITH HIDDEN TEXT

Through this technique intruders does not understand which one is real image which one data hidden. Our proposed System combining these 2 techniques in Cryptography and Steganography provides high level Security in communication.

C. Algorithm of Proposed System

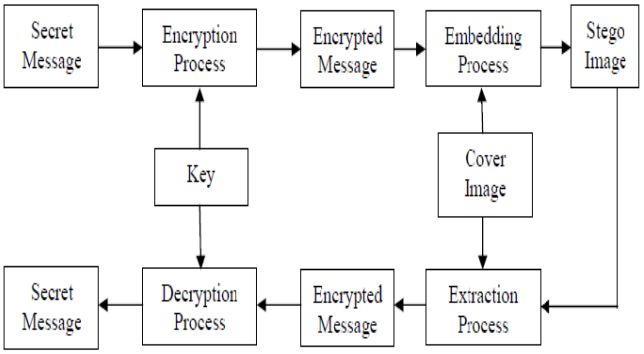
Input: Embed the message.
Output: Message is embedded safely in an image and reconstructed properly

Begin

1. Message.
2. Encrypting message.
3. Implementing LSB Method steganography
4. Embedding data.
5. Stego image.
6. Extraction of embedded message.
7. Encrypted message generation.
8. Decryption.
9. Original Message.

End

D. Proposed System Flow Chart

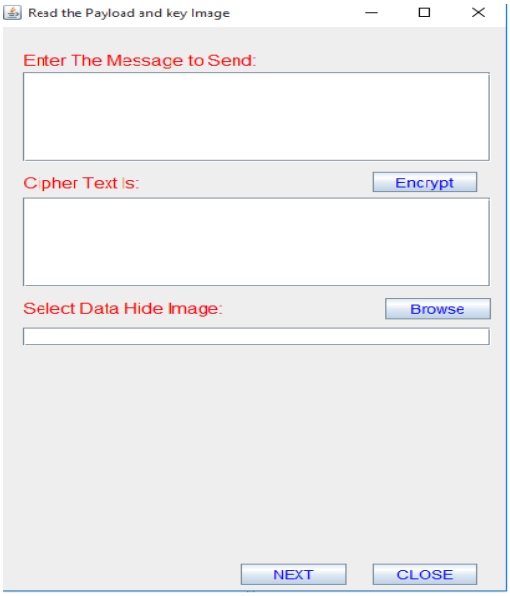


Block Diagram of the proposed system.

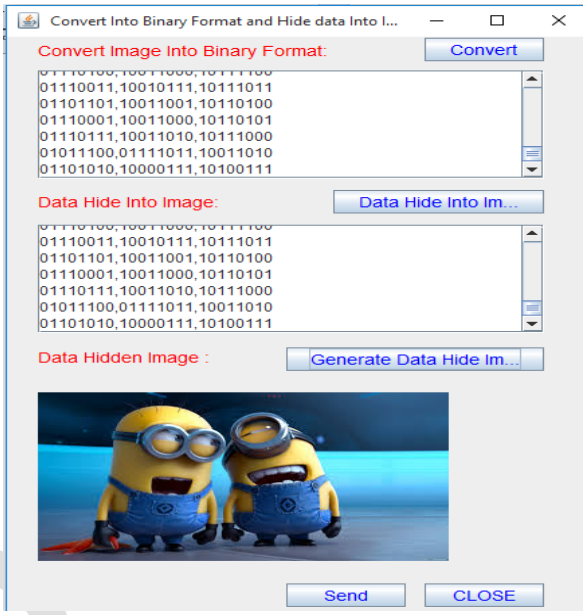
III. APPLICATIONS

- To protect military messages.
- Secure private files and documents
- E-mails Credit card information.
- Hide passwords and encryption keys
- Private sector for tender purposes.

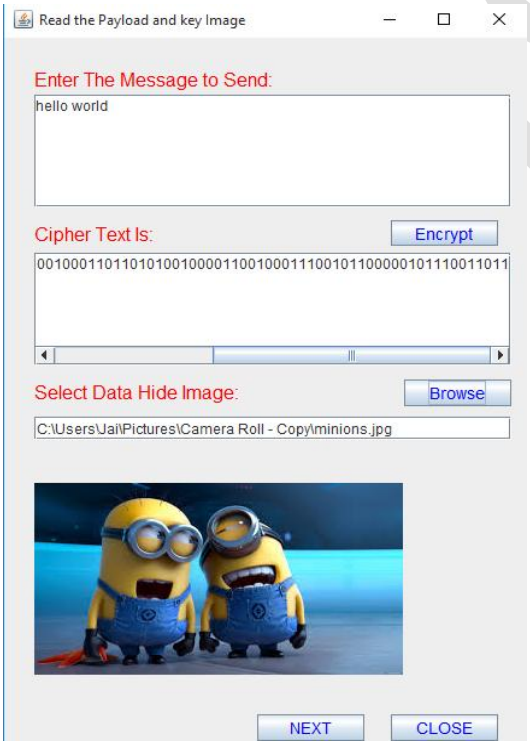
USER INTERFACE



STEANIGRAPHY METHOD



SENDER



RECEIVER

IV. CONCLUSION

This paper introduced the concept of combination of cryptography and steganography. The proposed method provided a higher similarity between the cover and stego pictures is achieved that also yields a better imperceptibility.

As per the results obtained, steganography when combined with encryption provides a secured means of secret communication between two parties.

The future work could be to extended the work further by considering videos, advanced, cryptography and steganography algorithms in this concept

REFERENCES

[1]. Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001 www.strangehorizons.com/2001/20011008/steganography.shtm

[2]. R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Steganography, IEEE Journal Selected Areas in Communications, 16(4), pp. 474-481.

[3]. Johnson, Neil F., and SushilJajodia. "Exploring Steganography: Seeing the Unseen." IEEE Computer Feb. 1998: 26-34

[4]. Westfield, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. pp. 32-47.

[5]. Krenn, R., "Steganography and Steganalysis", http://www.Krenn.nl/univ/cry/steg/article.pdf

[6]. E. Biham, A. Shamir. "Differential cryptanalysis of DES-like cryptosystems," Journal of Cryptology, vol. 4, pp. 3-72, January 1991.

[7]. T. Moerland, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.Liacs.nl/home/tmoerl/priytech.pdf

[8]. A. Ker, "Improved detection of LSB steganography in grayscale images," in Proc. Information Hiding Workshop, vol. 3200, Springer LNCS, pp. 97–115, 2004.

[9]. A. Ker, "Steganalysis of LSB matching in greyscale images," IEEE Signal Process. Lett., Vol. 12, No. 6, pp. 441–444, June 2005

[10]. C. C. Lin, and W. H. Tsai, "Secret Image Sharing with Steganography and Authentication," Journal of Systems and Software, 73(3):405-414, December 2004.

[11]. N. F. Johnson and S. Jajodia, "Steganalysis of Images Created using Current Steganography Software," Lecture Notes in Computer Science, vol. 1525, pp. 32 – 47, Springer Verlag, 1998.

[12]. J. Fridrich, M. Long, "Steganalysis of LSB encoding in colorimages,"Multimedia and Expo, vol. 3, pp. 1279-1282, July 2000.

[13]. KafaRabah. Steganography - The Art of Hiding Data. Information technology Journal 3 (3) - 2004.

[14]. A. Westfeld, "F5-A Steganographic Algorithm: High Capacity Despite Better Steganalysis," LNCS, Vol. 2137, pp. 289-302, April 2001.

[15]. C.-C. Chang, T. D. Kieu, and Y.-C. Chou, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," Proc. of the 2008 International Symposium on Electronic Commerce and Security, pp.16-21, August 2008.