A Comparative Study on S – DES algorithm with Secret Key and S – DES with Secret Image Key in Steganography

S.Sabitha
Assistant Professor, PG & Research Department of Computer Science, Vivekananda College of Arts and Sciences for Women (Autonomous), Tiruchengode

ABSTRACT

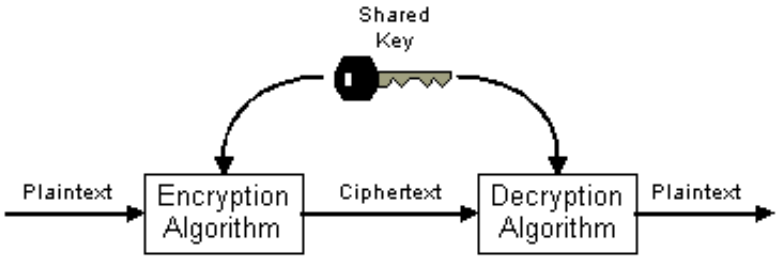
The process of jumbling up the contents of a secret message so as to secure it, is known as cryptography, whereas the process of hiding the very existence of a secret message is known as steganography. The term "steganography" describes the method by which the contents of a secret message are concealed inside some other medium, so as to avoid any kind of detection by an intruder. In this paper, we have proposed two new approaches wherein both cryptography and steganography are used to encrypt the data and also to conceal these encrypted contents in some other medium. In the first method proposed, we have secured an image by converting it into an encrypted text using S-DES algorithm and a secret key and then concealing this encrypted text in some other image, whereas in the second method, we have secured an image directly by encrypting it usingS-DES algorithm and an image key. The contents thus obtained are concealed inside another image so as to hide its very existence. Both these techniques have been tested and it has been observed that they prevent the possibilities of steganalysis also.

Keywords-Steganography, Cryptography, Least Significant Bit (LSB), DES, Stego image, secret key.

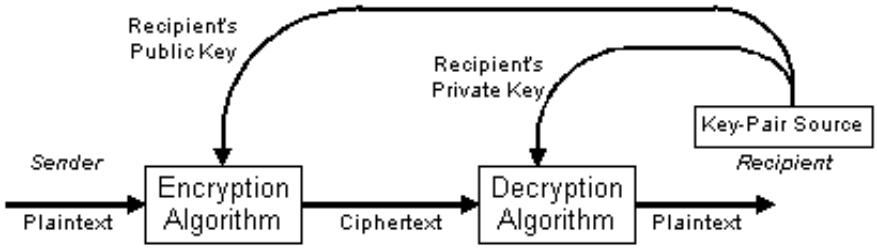
I. INTRODUCTION

In this age of communication and networking, security has become a critical issue for thriving networks. One of the necessary requirements to prevent the theft of data is to secure the information. There are various techniques to secure the information, but the well known and widely used are "cryptography" and “steganography". These two techniques are mostly used and have multiple applications like securing personal files, corporate data, sending confidential and mission critical e-mails etc. The word "cryptography" has been derived form two Greek words "kryptos" meaning "hidden" and "graphein" meaning "to write". So, cryptography can be defined as the study of converting the text message or information from readable format into an unreadable format without using any secret knowledge.

Cryptography intends to encrypt the actual message that is being sent. This message can be encrypted or scrambled by using various mechanisms including mathematical techniques and algorithms to jumble up the data into a non readable, incomprehensible format rendering it un-accessible without any secret knowledge. The encrypted message produced by cryptography can only be decoded or decrypted by a party that possesses the secret key. The generalized cryptographic technique is as illustrated in figure1.



Secret Key Cryptosystem



PublicKey Cryptosystem

Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from the intended recepient knows the existence of the message. The word "steganography" is basically of Greek origin, which means "hidden writing". However in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word "steganography" is often considered similar to "cryptography" and "watermarking", whilst watermarking ensures message integrity and cryptography scrambles the message, steganography hides it. It has been observed that the goal of "cryptography" and "steganography" is the same, but the way this goal is achieved, is different.

Cryptography encodes or encrypts the data or information so as to protect it from an intruder, steganography on the other hand attempts to hide the existence of information or data from the intruder. Combining these two techniques allows for a better private communication. The theme of this research paper is based on the very concept of combining these two terminologies. The basic terminologies used in the steganographic system are: payload: the information which is to be concealed. Carrier file: the media where the payload has to be hidden. Stego-Medium: The medium in which the information is hidden. Redundant-bits: Pieces of information inside a file, which can be overwritten or altered without damaging the file. Steganalysis: The process of detecting hidden information stored inside a file. The generalized steganographic technique is as illustrated in figure 2.

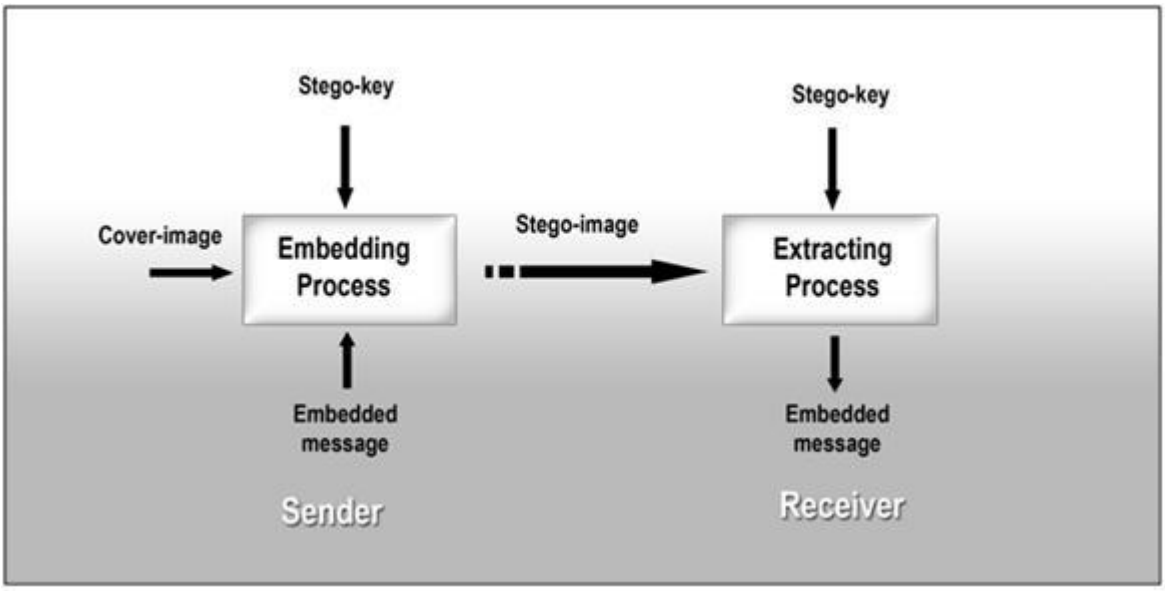


Fig. 2 Generalized steganographic technique.

II. PROPOSED ALGORITHMS

An image file for a computer can simply be regarded as a file having multiple colors and different light intensities on different areas of the image. An image thus can be represented as a collection of pixels stored in a tabular fonn, generally in a matrix therefore helps in processing the image easily. If we consider an image having "i" pixels in the horizontal direction and "j" pixels in the vertical direction, then the total number of pixels in the mage would be[i*j] and this value is also known as the size of the image. Further each pixel value of an image to be stored, can be represented as a collection of bits. As far as grey scale images are considered the number of bits required to represent a pixel is 8. The reason being, in grey scale images the color intensity of a particular pixel will vary from 0 to 255 where the value "0" corresponds to black and the value "255" corresponds to white. This means that the maximum value a pixel could have is 255 and therefore 8 bits are required. Pixel of a grey scale image can be represented as shown in figure 3.

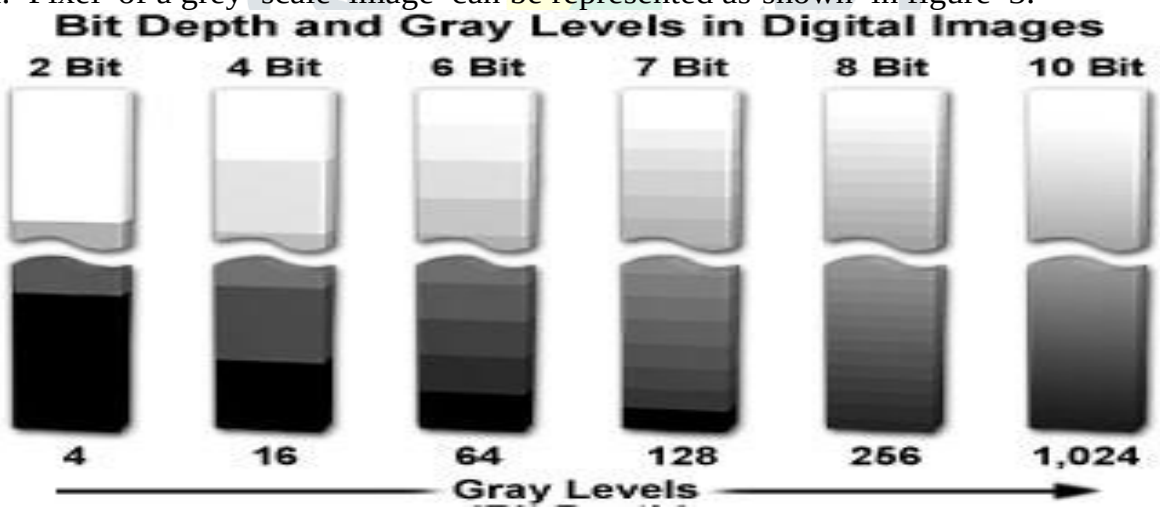


Fig. 2 Generalized steganographic technique.

III. S-DES ALGORITHM

In this paper we have proposed two new approaches to secure/protect the have proposed two new approaches to secure/protect the image being transferred, from the intruder. The encryption technique we have used to encrypt the data is S-DES algorithm. This algorithm takes as input, an eight bit block of plaintext and an encryption key which is 10 bits long and produces an eight bit ciphertext block as an output. S-DES algorithm comprises of five different functions which takes 8- bit plaintext as an input and produces 8-bit ciphertext as an output. These functions are: an initial pennutation function represented

by (IP); a more complex function represented by (fK), involving both pennutations and substitutions. These pennutations and substitutions depend solely on the input key; a fair & simple pennutation function that shifts two parts of the input data; (fK) is used again and finally the inverse pennutation function (IP -1) which inverses the initial pennutation.The flow of S-DES algorithm is shown in figure 5 & 6.

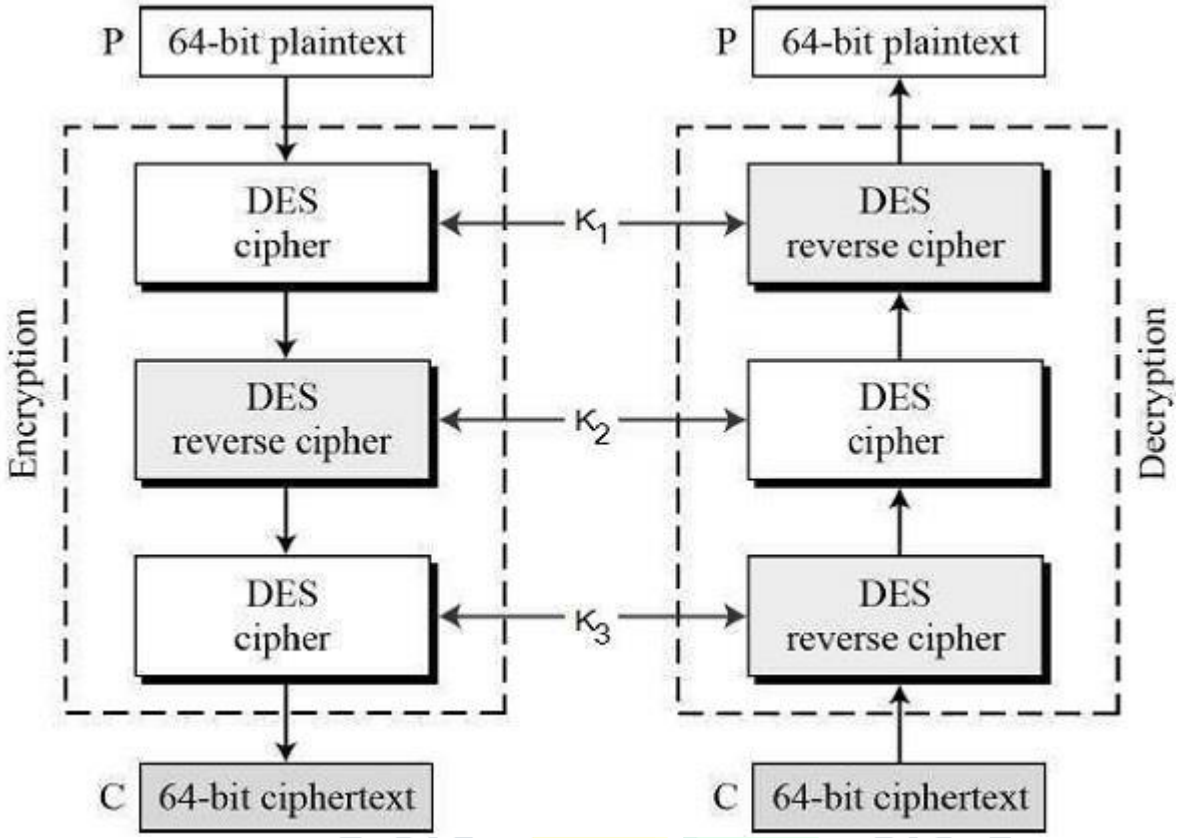


Fig. 3 Detailed S-DES Algorithm

The S-DES algorithm can be expressed as: -
Ciphertext = IP- (fKz(SW(fK1(IP(plaintext)))))
Kl = Pg(Shift(PIO(Key)))
K2 = Pg(Shift(Shift(PIO(key))))
Plaintext = W \fK1(SW(fK2(lP(ciphertext))))) [7]

IV. IMPLEMENTATION & RESULTS

The two new techniques discussed above have been implemented using MATLAB. A. Results obtained with technique 1Payload image to be encrypted. The pixels of this image have been encrypted using the S-DES algorithm. The text obtained after encrypting the image has been printed. This text obtained is also known as the cipher text. This cipher text thus can be sent along the channel to the receiving party. The cipher text received by the receiving party is then subjected to decryption using the same secret key to obtain the image. So these are the results obtained using these two approaches. In the first approach the image to be encrypted is converted into a text file and then this text file can be sending either directly to the receiver or can be hidden inside another image before being sent. Whereas in the second approach the image to be encrypted is encrypted directly using S-DES algorithm. This encrypted data is then hidden inside another image before being sent along the channel towards the receivers end.

IV. CONCLUSION

In this paper we have proposed two new approaches for image steganography. Both these approaches utilize the concept of combination of cryptography and steganography and have been implemented using MATLAB. The results thus obtained provide a means by which secret information can

be sent and received between two parties. Further these two approaches overcome the problem of steganalysis.

V.REFERENCES

[1] William Stallings, Cryptography and Network Security, Principles and Practices, Third edition, Pearson Education, Singapore, 2003.

[2] B. Dunba . A detailed look at Steganographic Techniques and their use in an open system environment, Sans Institute, (2002)

[3] C. Christian. An Information Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT laboratory for Computer Science, 1998.

[4] N. Jhonson, Survey of Steganography Software, Technical Report, january 2002.

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

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

[7] K.Kim, S. Park and S. Lee, "Reconstruction of S2DES S-Boxes and their immunity to Differential Cryptanalysis", Proceedings of the 1993 Korea-Japan workshop on Information Security and Cryptography, Seoul, Korea, 24-26 Oct 1993, pp. 282-291.

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

[9] C.C Chang, T.D. Kieu and YC. 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.

[10] Jiri Fridrich, Du Dui, "Secure Steganographic Method for Palette Images",3'd International Workshop on Information Hiding, pp. 47-66, 1999.