TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSIONS

Sujay Narayana[1] and Gaurav Prasad[2]

[1]Department of Electronics and Communication, NITK, Surathkal, INDIA
sujaynarayana@gmail.com
[2]Department of Information Technology, NITK, Surathkal, INDIA
chgauravprasad@gmail.com

ABSTRACT

The science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is concealed. The term 'Steganography' describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This paper introduces two new methods wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One of the methods shows how to secure the image by converting it into cipher text by S-DES algorithm using a secret key and conceal this text in another image by steganographic method. Another method shows a new way of hiding an image in another image by encrypting the image directly by S-DES algorithm using a key image and the data obtained is concealed in another image. The proposed method prevents the possibilities of steganalysis also.

KEYWORDS

Steganography, Cryptography, image hiding, least-significant bit (LSB) method

1. INTRODUCTION

In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has become a critical feature for thriving networks and in military alike. Cryptography and Steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect military messages, E-mails, credit card information, corporate data, personal files, etc.

Cryptography (from Greek kryptós, "hidden", and gráphein, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. The art of protecting information (plain text) by transforming it (encrypting it) into an unreadable format is called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Cryptography encrypts the actual message that is being sent. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key [20]. The general form of cryptographic technique is shown in figure 1.1.

DOI : 10.5121/sipij.2010.1206

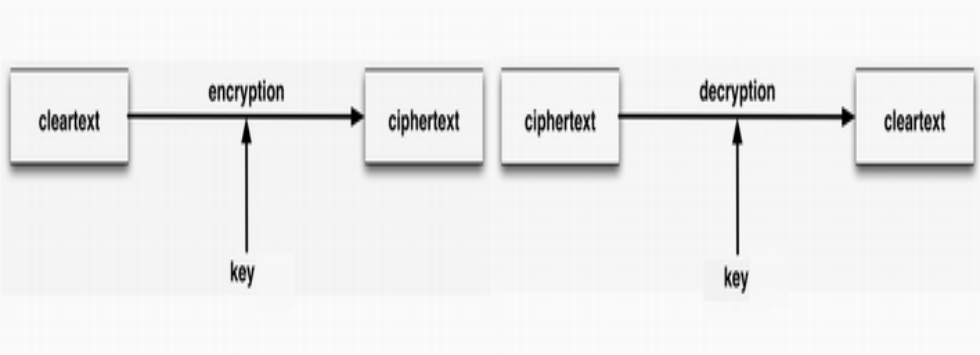

Figure 1.1Cryptographic flow

Steganography(from Greek Stegános, "Covered/hidden", and gráphein, "to write") is the art and science of communicating in a way which hides the existence of the communication[1].Steganography hides the very existence of the message by embedding it inside a carrier file of some type. An eavesdropper can intercept a cryptographic message, but he may not even know that a steganographic message exists. Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography, in contrast attempts to prevent an unintended recipient from suspecting that the data is there. [4].Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. On other hand, steganalysis is a way of detecting possible secret communication using against steganography. That is, steganalysis attempts to defeat steganography techniques. It relies on the fact that hiding information in digital media alters the carriers and introduces unusual signatures or some form of degradation that could be exploited. Thus, it is crucial that a steganography system to ascertain that the hidden messages are not detectable [1013 23].

Steganography includes the hiding of media like text, image, audio, video files, etc in another media of same type or of different type. Later, the message hidden in the selected media is transmitted to recipient. At receiver end, reverse process is implemented to recover the original message [5].

Some terminologies in Steganography [7]:

Payload**:** The information which is to be concealed.

Carrier File**:** The media where 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 inside of a file.

Stego medium = Payload file + Carrier file.

The four basic techniques used for Steganography are:

LSB method: The LSB of carrier medium is directly inserted with the message bit. So LSB of the carrier medium contains the payload.

Injection: Hiding data in sections of a file that are ignored by the processing application. Therefore avoid modifying those file bits that are relevant to an end-user leaving the cover file perfectly usable.

Substitution: Replacement of the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion.

Generation: Unlike injection and substitution, this does not require an existing cover file but generates a cover file for the sole purpose of hiding the message.

The general form of Steganographic technique is shown in figure 1.2

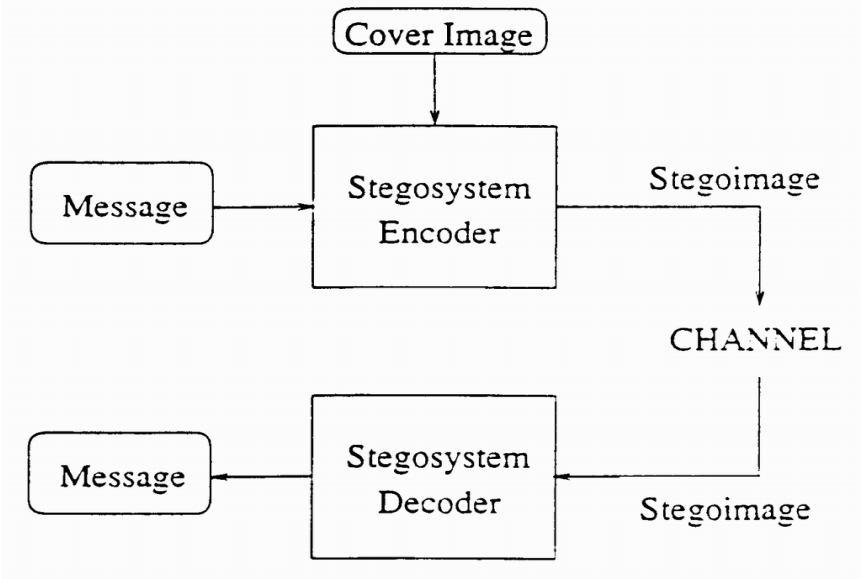

Figure 1.2Steganographic flow

Many ideas and techniques have been proposed to secure data i.e., mainly concealing of text in images. The simple method to do the same is Least Significant Bit replacement method in steganography. But it has its own limitations [2].Steganalysis can be easily done on LSB replacement technique [19]. The new proposed method overcomes this drawback [12 17 21 22].

2. PROPOSED IDEA

To a computer, an image file is simply a file that shows different colors and intensities of light on different areas of an image. We can represent an image in the form of matrix of pixels which helps in image processing. The size of an image is mxn if it is composed of m pixels in the horizontal direction and n pixels in the vertical direction. The total no of pixels in the image will be mxn. Each pixel is indicated by bits. In uint8 class, a gray scale image can be represented in matrix having integers between 0 and 255 to represent the brightness of a pixel. The value 0

corresponds to black and 255 to white.So the total no of bits required to represent a pixel is 8 bits. A RGB color image has three frames of images. These frames altogether represent an image with three matrices of sizes matching the main image format. Each matrix corresponds to one of the colors red, green and blue and gives an instruction of how much of each of these colors a certain pixel should be. So the total number of bits required to represent a pixel of this color image is 24 bits. Hence sending the image is nothing but sending the pixel values of the image. If these pixel values are encrypted, then the whole image will be encrypted. Such an encrypted message can be sent directly which is visible as encrypted data in the channel where it can be known that the data is being sent, or it can be hidden in some other medium where the intruder will fail to find the actual data that is being sent. In this paper, we have proposed two techniques to secure the image that is being transferred.

S-DES encryption (decryption) algorithm takes 8-bit block of plaintext and a 10-bit key to produce an 8-bit ciphertext. The encryption algorithm involves 5 functions: an initial permutation (IP); a complex function fK, which involves both permutation and substitution that depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function fK again and finally, the inverse permutation of IP (IP-1). The function fK takes two 8-bit keys which are obtained from the original 10-bit key [6]. The S-DES algorithm flow is shown in figure 2.1 and figure 2.2.

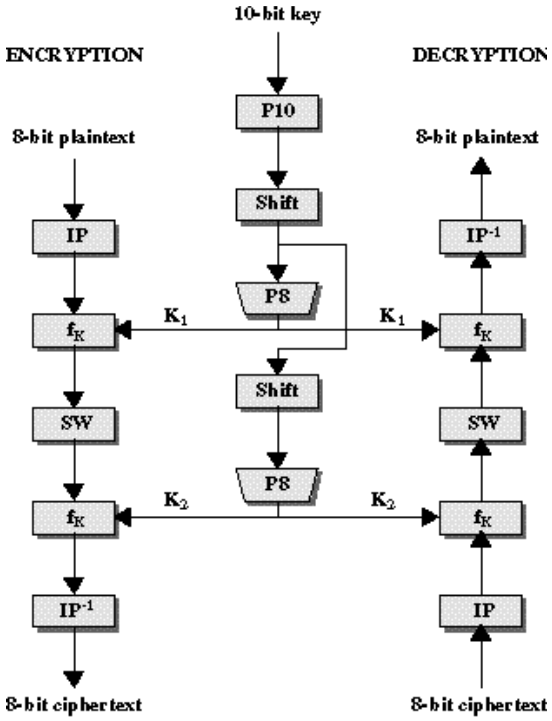

Figure 2.1S-DES algorithmflow

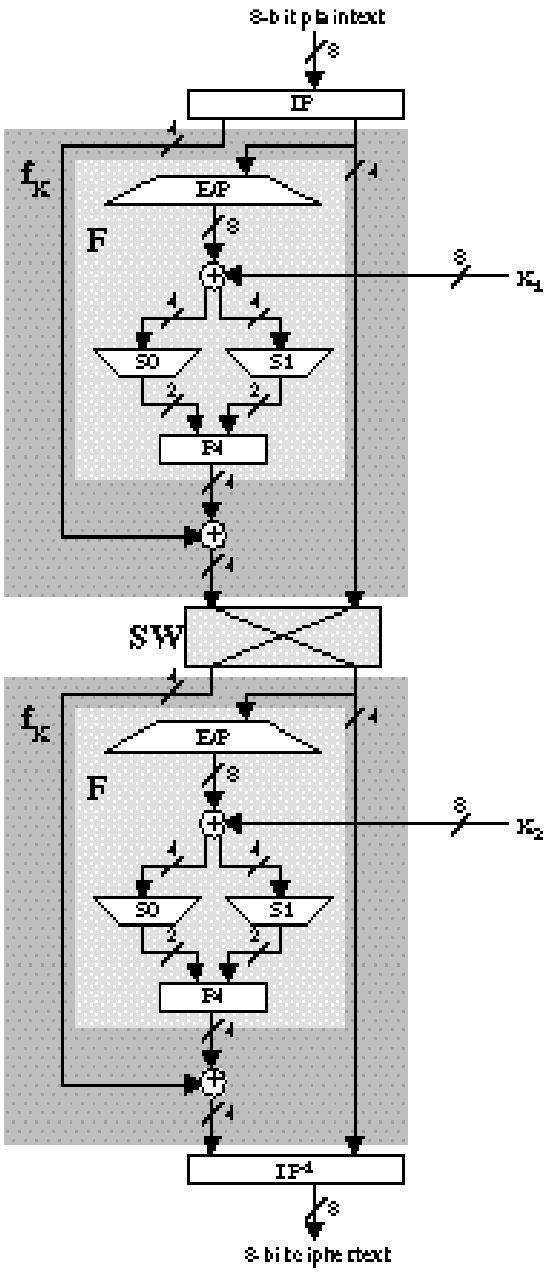

Figure 2.2S-DES Algorithm in detail

The 10-bit key is first subjected to a permutation (P10) and then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces a 8-bit output (P8) for the first sub key (K1). The output of the shift operation again feeds into another shift and (P8) to produce the 2nd sub key (K2) [18].We can express encryption algorithm as superposition:

$$\text{Ciphertext= } IP^{-1}\left(f_{K_2}(SW(f_{K_1}(IP(pla\,\text{int}\,ext))))\right)$$

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

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

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

Considering a 24-bpp color image, the image is split into three matrices (frames) each matrix containing pixels indicating the intensities of Red, Green and Blue. If m by n is the dimension of that image, then there will be mxn number of pixels in that image. Hence, the matrices corresponding to Red, Green and Blue intensities will also have mxn number of pixels.

2.1 Image to Text Encryption (Approach I)

Each byte (pixel) of all these three matrices are encrypted using S-DES algorithm and an array of encrypted pixels is created. The dimension of so produced array will be [1, mxn] for each of the three matrices and contains (mxnx8) bits each. Each element of the array is denoted in binary form and split into two parts. The first part contains the first four Most Significant Bits and the second contains the remaining four Least Significant Bits. If we denote the binary value 0000 as ‘A’, 1111 as 'P' and the intermediate values were assigned with the respective letters of alphabet, then the whole array will be converted into the form of text comprising the letters from A to P. If R_Array is the encrypted array produced from Red intensity matrix and similarly G_Array and B_Array for Green and Blue intensity matrices, then the total number of characters present in these arrays will be (mxnx8/4) each.

The total no of letters present in the final cipher text is [(number of characters in R_Matrix) + (number of characters in G_Matrix) + (number of characters in B_Matrix)]

= (mxnx8/4) + (mxnx8/4) + (mxnx8/4)

= (mxnx6)

This encrypted data can be sent to the destination or can be saved so that for an intruder, the data looks like a simple text, though the actual data being sent is an image. The original data (in this case, it is an image) can be decrypted only with the same key which is used for encryption in S-DES.

2.2 Image Steganography (Approach II)

In this approach, each byte (pixel) of all the three matrices(R,G,B matrices of payload) are encrypted using S-DES algorithm and an image comprised of encrypted pixels is formed. The key used to encrypt each pixel is of 10-bit length and is obtained from the pixels of key image.

The pixel values of red, green and blue intensities of each pixel of key image are combined to get a 24-bit value. The first ten bits are selected as the key to encrypt the red intensity pixel of payload image. The middle ten bits will be the key to encrypt the green intensity pixel of payload and finally the last ten bits is the key to encrypt blue intensity pixel of payload image. So the size of key image must be same as that of payload. If not, then the key image will get resized. Each pixel (24-bit) of the key image is split into three keys(10-bit each).This encrypted

data is represented as an image which is hidden in another image called carrier image using Steganography [14 15 16].

2.3Image Steganography: Embedding the encrypted image in carrier image.

The encrypted byte (in Approach I) or the pixel values of encrypted image (in Approach II) is hidden in the LSBs of pixels of carrier image by Exclusive-ORing it with the 2nd LSB of carrier pixel. If the size of the encrypted image is mxn, then the size of carrier image must be mxnx8 as each encrypted byte requires 8 bytes (pixels) of carrier image. So if the carrier image size is not eight times the size of the payload, then it has to be resized [9]. The flow of algorithm for Approach I and Approach II are shown in figure 2.3 and figure 2.4 respectively.

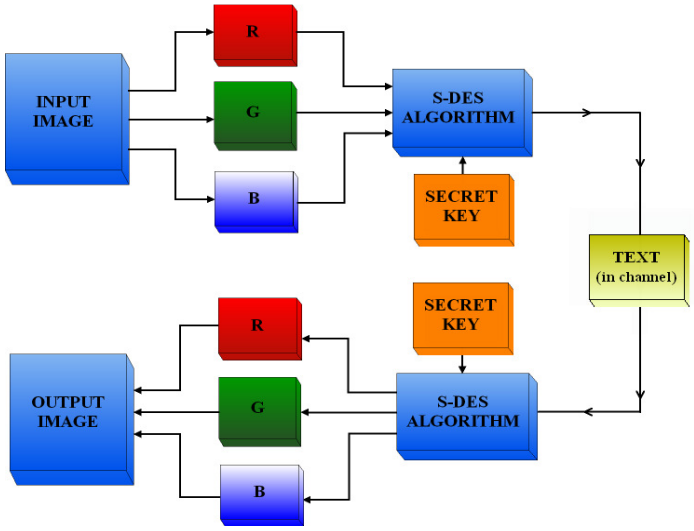

Figure 2.3. Flow of proposed idea

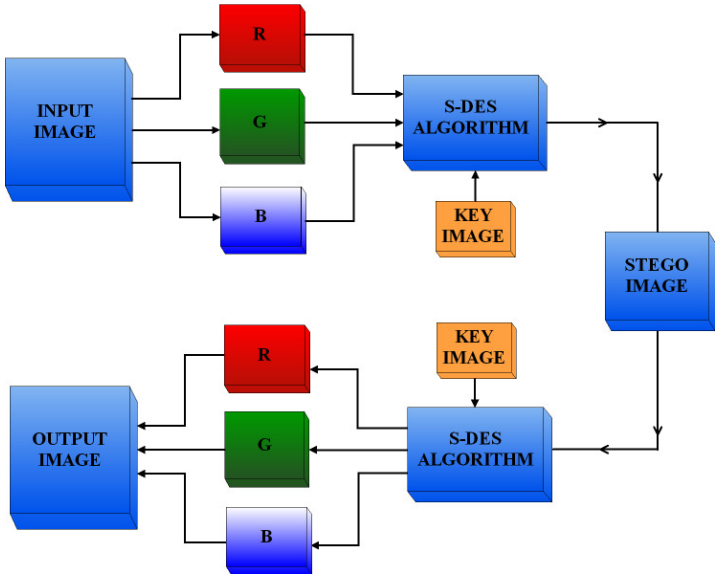

Figure 2.4.Flow of proposed idea

As we know, the least significant bit insertion method is probably the most well known image steganography technique. It is a common, simple approach to embed information in a graphical image file. Two basic types of LSB modifications that can be used for the embedding schemes are LSB replacement and LSB matching. In LSB replacement, the LSB of the carrier is replaced by the message bit directly. On the other hand, in LSB matching if the LSB of the cover pixel is same as the message bit, then it remains unchanged; otherwise, it is randomly incremented or decremented by one. This technique, however, requires both the sender and the receiver to have the same original image, which makes LSB matching very inconvenient. LSB replacement method is vulnerable to Steganalysis [3 8]. To overcome this, in the proposed algorithm, the LSB of carrier medium is not changed directly, but the message bit is Exclusive-ORed with the 2nd least significant bit of the carrier byte and the LSB of carrier medium is replace by the result bit. The Exclusive-OR operation of the encrypted bit with the second LSB bit makes the stego image more secured [11].

3. IMPLEMETATION RESULTS

The above two methods have been successfully implemented using MATLAB. Figure 3.1 'bird.jpg' represents the payload image that has to be concealed. The image pixels were encrypted using S-DES and converted to text form as described. The obtained ciphertext is sent along the channel to the receiving end. The ciphertext obtained by applying S-DES algorithm to payload image is shown in figure 3.2.Once the text is received at receiving end, it is then decrypted to get the image. For an intruder who attacks in the channel, the data looks like a plain text where the actual message passed is an image. Figure 3.3 is the image in receiving end. When compared it with the image at sending end, no pixel differences were found.

Figure 3.1Image at source

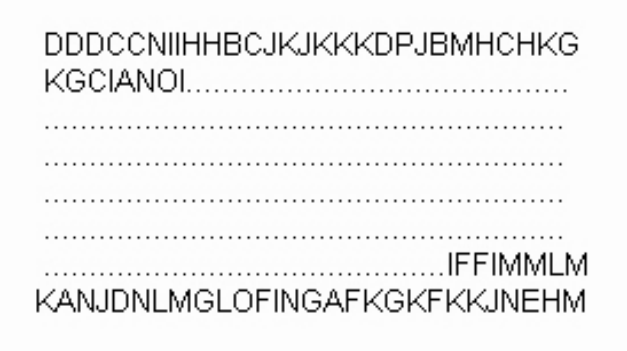

Figure 3.2Obtained ciphertext

Figure 3.3Decrypted image obtained at destination

To be more secure, the ciphertext obtained can be hidden in another image instead of sending it along the channel directly. The image 'bird.jpg' which is the payload is encrypted with the same S-DES algorithm and hidden in the key image 'building.jpg'. The secret key used in S-DES algorithm is a plain text. Figure 3.4 shows the payload image and the image obtained by applying S-DES algorithm to the payload. In figure 3.5 the key image and stego image are shown. This stego image is sent along the channel.There was a slight difference in the histogram of key image and stego image, but this difference is invisible to human eye.We were able to get back the payload image successfully using the decryption key and the decrypted payload was matching with the input payload without any error in any pixel value. The image obtained at receiving end is shown in figure 3.6.

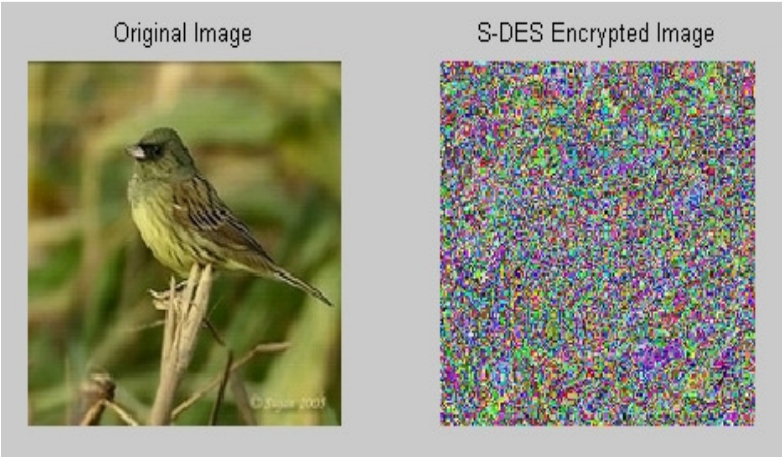

Figure 3.4Original image with S-DES encrypted image

Figure 3.5Key image with stego image

Figure 3.6Image extracted from stego image and S-DES decrypted image

As described in Approach II, we have selected 'map.jpg' as the payload image and it was encrypted using S-DES with the key image ‘key.jpg’. The payload, key image and the encrypted image are shown in figure 3.7. Each pixel of payload is encrypted by using the respective pixel of key image as key for S-DES algorithm. So in case if the key image size is not as same as the payload, then it has to be resized.

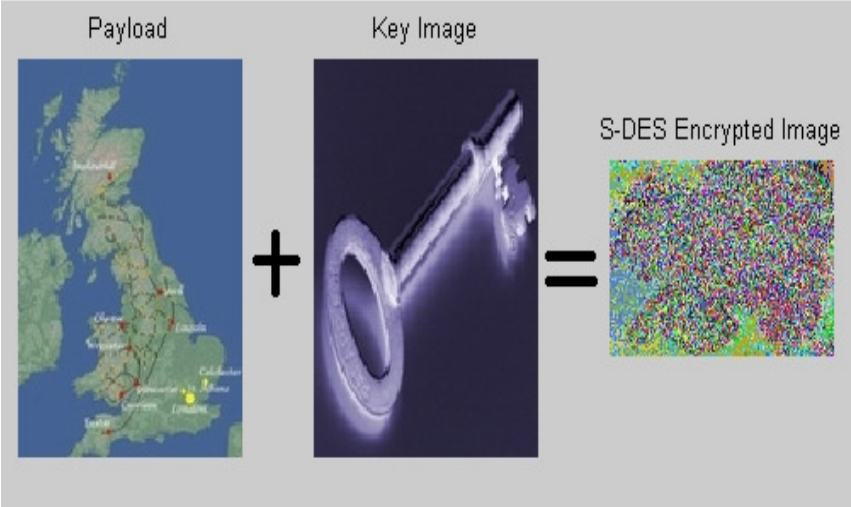

Figure 3.7Payload, Key image and S-DES encrypted image

The encrypted image thus obtained was steganographically concealed in the carrier image 'sunset.jpg' as shown in figure 3.8.For human eye, both the stego image and carrier image looks alike.

Figure 3.8.Carrier image and stego image

At the receiving end, the encrypted image is extracted from the stego image.The encrypted image is then decrypted using the same key image which is used to encrypt. The payload received is shown in figure 3.9. The received payload had same pixel values as that of sent payload.

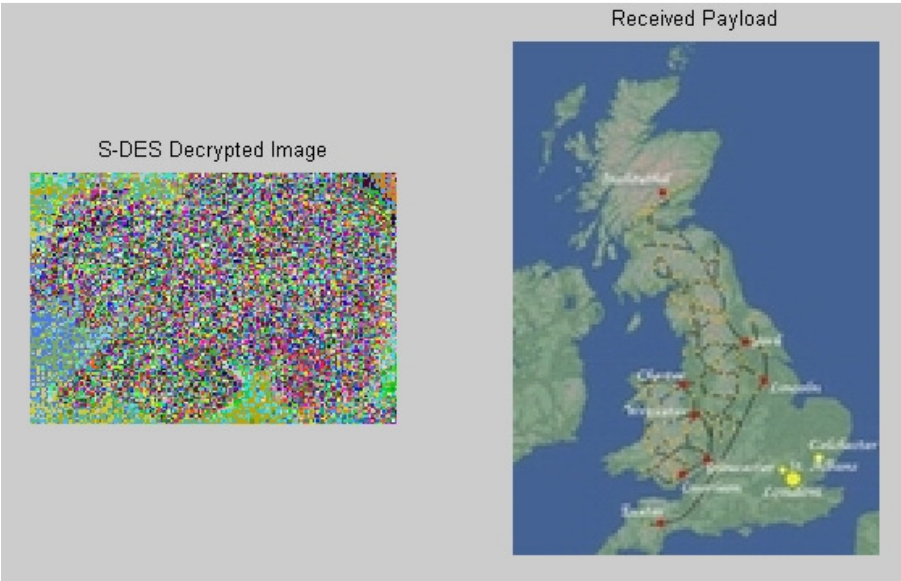

Figure 3.9Original Image with S-DES Encrypted Image

So in first method, the payload image is converted into text and this text is hidden in another image. The secret key used in S-DES algorithm may be a character or number. In second method, the payload image is encrypted directly and this encrypted data is hidden in another image. The secret key used for S-DES algorithm here is an image.

2. ACKNOWLEDGEMENT

It is our privilege to express our sincere gratitude to Dr MuralidharKulkarni, Professor, Department of Electronics and Communication, National Institute of Technology Karnataka, Surathkal for his constant support, encouragement and valuable suggestions throughout the work. We would also like to thank staff of Department of Electronics and Communication and Department of Information technology, NITK, Surathkal for all their help during this work. We are thankful to our parents to whom we are greatly indebted for their support and encouragement.

2.9. CONCLUSION

This paper introduced the concept of combination of cryptography and steganography. It also proposed a new algorithm to overcome steganalysis. The proposed method provided a higher similaritybetween the cover and stego pictures is achieved that alsoyields 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 extend this methodto arrange the text that is obtained by the encryption of image, to form a word or meaningful sentence and new methods to prevent steganalysis, done by other than LSB method.

REFERENCES

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

[2] R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, 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] Westfeld, 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 onElectronic Commerce and Security, pp.16-21, August 2008.

[16] Jiri Fridrich ,Du Dui, "Secure Steganographic Method for Palette Images," 3rd Int. Workshop on InformationHiding, pp.47-66, 1999.

[17] R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice " , International Workshop on DigitalWatermarking, Seoul, October 2004.

[18] K. Kim, S. Park, and S. Lee, "Reconstruction of s2DES S–Boxes and their Immunity to DifferentialCryptanalysis," Proceedings of the 1993 Korea–Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24–26 Oct 1993, pp. 282–291.

[19] S. Dumitrescu, W.X.Wu and N. Memon (2002) On steganalysis of random LSB embedding in continuous-tone images, Proc. International Conference on Image Processing, Rochester, NY, pp. 641-644.

[20] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, PearsonEducation, Singapore, 2003.

[21] Hide & Seek: An Introduction to Stegnography: http:\\niels.xtdnet.nl/papers/practical.pdf.

[22] Y. Lee and L. Chen (2000) High capacity image steganographic model, IEE Proceedings on Vision,Image and Signal Processing, 147(3), pp. 288-294.

[23] T. Morkel, J. H. P. Eloff, M. S. Olivier, ”An Overview of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, SA.

Authors

SujayNarayana received the BE degree in Electronics and Communication from KVG College of Engineering, Sullia, in 2009. He is currently with the Department of Electronics and Communication, National Institute of Technology Karnataka, Surathkal.

Gaurav Prasad received the BE degree in Information Science from P.A College of Engineering, Nadupadavu, Mangalore in 2006 and MTech degree in Information Security from NITK, Surathkal . He is currently with the Department of Information Technology, National Institute of Technology Karnataka, Surathkal.