Image Security Using Steganography And Cryptographic Techniques

R.Nivedhitha[1], Dr.T.Meyyappan,M.sc.,M.Phil.,M.BA.,Ph.D[2]
Research Scholar[1], Associate Professor[2]
Department of Computer Science & Engineering,
Alagappa University,Karaikudi.
Tamil Nadu,India.

Abstract- **Steganography is the art of hiding the fact communication is taking place, by hiding information in other information.Many different carrier file formats can be used,but digital images are the most popular because of their frequency on the internet.This paper introduces two new methods where in cryptography and steganography are combined to encrypt the data as well as to hide the data in another medium through image processing . This paper securing the image by encryption is done by DES algorithm using the key image. The encrypted image can be hide in another image by using LSB techniques,so that the secret's very existence is concealed. The decryption can be done by the same key image using DES algorithm.**

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

I. INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography word is of Greek origin and essentially means concealed writing. Protection of the transmitted data from being intercepted or tampered has led to the development of various steganographic techniques.

Cryptography involves converting a message text into an unreadable cipher.A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers Cryptography systems can be broadly classified into symmetric-key systems and public key systems. The symmetric key systems uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message.The public-key systems that use a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key.

Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

The steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes" [3]. It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or

not they have hidden messages encoded into them, and, if possible, recover the hidden information. The cryptanalysis is the process of encrypted messages can sometimes be broken the cipher message is otherwise called as code breaking,although modern cryptography techniques are virtually unbreakable.

The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image. In this paper, the secret message is embedded within the image called cover-image. Cover-image carrying embedded secret data is referred as stego-image.

This paper organized in Sections.Firstly I describe the introduction of Steganography and Cryptography Techniques under the heads of Introduction in Section-I. Subsequently I have gone through the literature review in Section-II. In Section-III, the proposed work described in detail.In Section-IV, the experimental result is described in detail. Finally, this paper concluded and mentions its further enhancements under future scope in Section – V respectively. All used references used during writing of this paper are mention in under head of references.

II. LITERATURE SURVEY

The word steganography is originally derived from Greek words which mean “Covered Writing”. It is defined as "hiding information within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected" [1]. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [2, 4,5,7].

In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [10].

Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text . This method is credited to Cardan and is called Cardan Grille [4].

This section attempts to give an overview of the most important steganographic techniques in digital images.The most popular image formats on the internet are Graphics Interchange Format (GIF), Joint PhotographicExperts Group (JPEG), and to a lesser extent - the Portable Network Graphics (PNG). One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh [1], who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography.

The survey of Johnson [6] appeared in the “Information hiding” book, which limits its distribution compared to a Journal paper which can be more affordable. The classification, herein, of the techniques and that of Johnson are different. Johnson classify steganography techniques into: Substitution systems, transform domain techniques, spread spectrum techniques, statistical methods, distortion techniques, and cover generation methods. Johnson survey neither talks about the history of steganography nor its applications.Johnson work has not included test images that can allow readers visualize the concepts.

III. PROPOSED WORK

A. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) shall consist of the following Data Encryption Algorithm (DES). These devices shall be designed in such a way that they may be used in a computer system or network to provide cryptographic protection to binary coded data. The method of implementation will depend on the application and environment. The devices shall be implemented in such a way that they may be tested and validated as accurately performing the transformations specified in the following algorithms.

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key1. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process.

A block to be enciphered is subjected to an initial permutation ***IP***, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation ***IP-1***. The key-dependent computation can be simply defined in terms of a function ***f***, called the cipher function, and a function ***KS***, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function ***f*** is given in terms of primitive functions which are called the selection functions ***Si*** and the permutation function ***P***. ***Si***, ***P*** and ***KS*** of the algorithm are contained . Blocks are composed of bits numbered from left to right, i.e., the left most bit of a block is bit one.

In this proposed paper, 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.

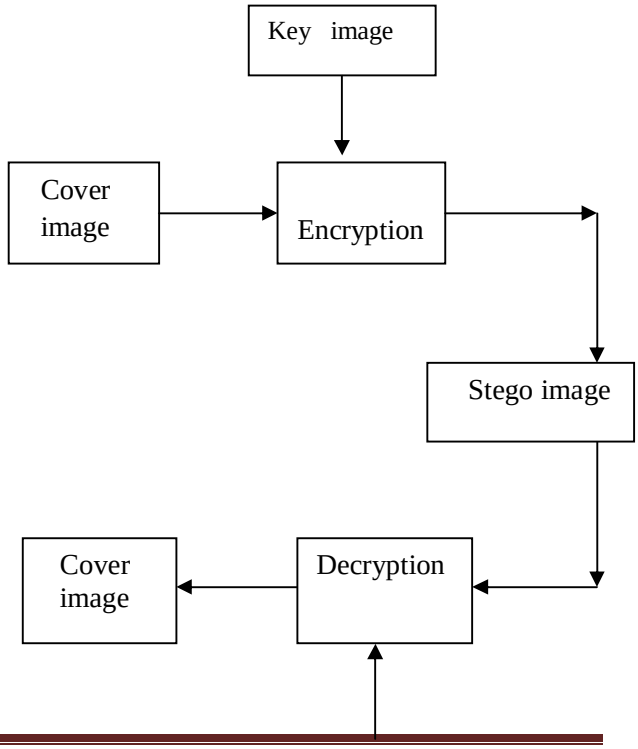
The 10-bit key is first subjected to permutation (P10) and then a shift operation is performed. The output of the shift operation then passes through permutation function that produces a 8- bit output (P8) for the first sub key (K1). The output of the shift operation agaifeeds into another shift and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

$$\text{Ciphertext} = IP^{-1}(f_{k2}(SW (f_{k1}(IP (\text{plaintext})))))$$
$$K_1 = P8 (\text{shift} (P10 (\text{key})))$$
$$K_2 = P8 (\text{shift} (\text{shift} (P10 (\text{key}))))$$
$$\text{Plaintext} = IP^{-1} (f_{k1}(SW (f_{k2}(IP (\text{ciphertext})))))$$

In this proposed paper, each byte (pixel) of all the three matrices(R,G,B matrices of payload) are encrypted using 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).In this paper, the encrypted image is embedded within another image called cover-image or carrier image. Cover-image carrying embedded secret image is referred to as stego-image.

B. EMBEDDING THE ENCRYPTED IMAGE IN CARRIER IMAGE

LSB is a simple approach to embedding information in a cover image.The pixel values of encrypted image is hidden in the lsb of pixels of carrier image by merge it with the 2nd lsb of carrier pixel.If the 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. In this procedure LSB algorithm helps for securing the originality of image.



Key image

Figure 1. Hidden Image

C. EXTRACTING THE ENCRYPTED IMAGE IN CARRIER IMAGE

The extracting is reverse to emdedding the encrypted image. In extracting, the carrier image in which the data is hidden is given as an input file. Here the given image is first encrypted and then the encrypted image is hidden in the carrier image.Finally the hidden encrypted image is decrypted. The Least Significant bit technique by which the encoded bits in the image is decoded and turns to its original state and gives the output as a image. The encryption and decryption in order to secure from unauthorized access.

IV. EXPERIMENTAL RESULTS

In this proposed paper securing the image by encryption is done by DES algorithm using the key image. The encrypted image can be hide in another image by using LSB techniques,so that the secret's very existence is concealed. Finally the hidden encrypted image is decrypted as shown in a figure.

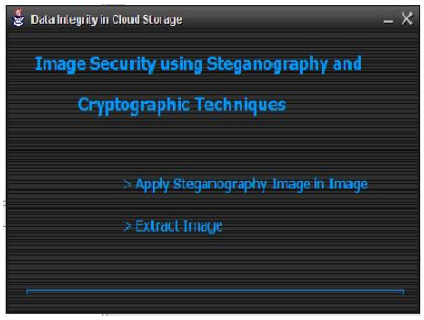


FIGURE-1

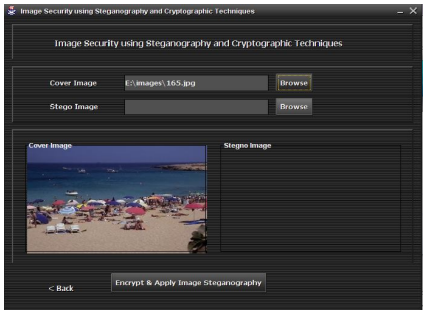


FIGURE-2

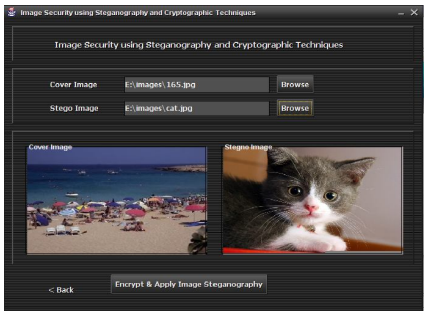


FIGURE-3

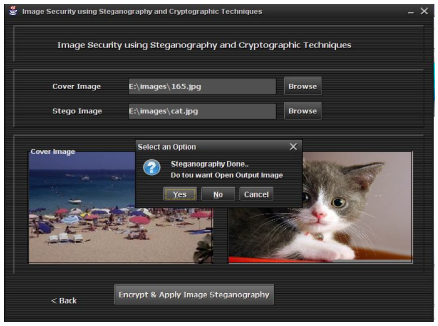


FIGURE-4

FIGURE-5

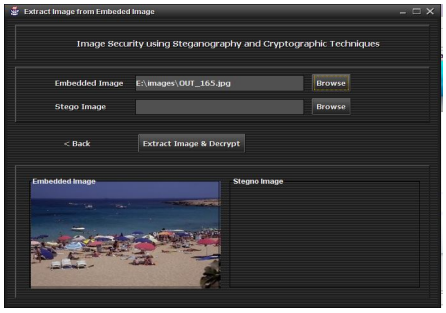


FIGURE-6

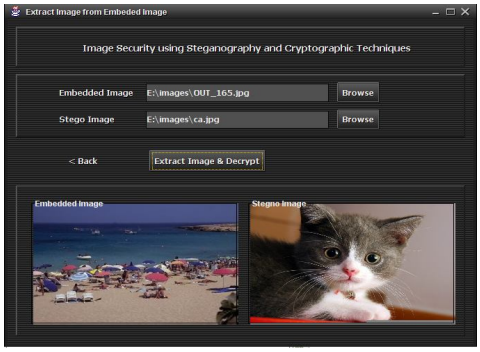


FIGURE-7

V. CONCLUSION

In this paper, we proposed the combination of cryptography and steganography has been achieved by using the DES algorithm and LSB technique. Data encryption standard (DES) is used to encrypt secret image and LSB technique is used to hide encrypted secret image into cover image. To yield better imperceptibility the proposed method provided a higher similarity between the cover and stego pictures as a result.when steganography is combined with encryption a good security was achieved between two parties in case of secret communication, it is hardly attracted from eavesdropper by naked eye. Finally we can conclude that the proposed technique is effective for secret data communication.

The future work could be to extend this method to arrange the text that is obtained by the encryption of image,to form a word or meaningful sentence and new methods can be done by other than LSB method.

REFERENCES

[1] C. Kurak and J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8 Annual Computer Security Applications Conference, 30 Nov-4 Dec, 1992, pp. 153-159.

[2] J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/stenganography/552.php, 2001.

[3] Km. Pooja ,Arvind Kumar , "Steganography- A Data Hiding Technique" International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010.

[4] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2)(1998) 2634.

[5] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, 01 (3)(2003)32-44.

[6] N.F. Johnson and S.C. Katzenbeisser, "A survey of steganographic techniques", in: S. Katzenbeisser and F.A.P. Petitcolas, (ed.) (2000) Information hiding techniques for steganography and digital watermarking, Norwood: Artech House, INC.

[7] P. Moulin and R. Koetter, Data-hiding codes, Proceedings of the IEEE, 93 (12)(2005)2083-2126.

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

[9] 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.

[10] S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

[11] 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.

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

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

AUTHORS BIOGRAPHY

Ms.R.Nivedhitha

Ms. R.NIVEDHITHA is a Research scholar in the Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.Sc., in Information Technology from Alagappa University, Karaikudi, Tamilnadu . She has presented her work in National level conferences. Her areas of research interests include Image Processing.

Dr.T.Meyyappan

Dr.T.Meyyappan received his Ph.D. degree in computer science and Engineering from Alagappa University,Karaikudi,TamilNadu. He has obtained his M.SC.,M.phil.,MBA.,.He is currently working as an associate professor in the Department of Computer Science and Engineering of Alagappa University,karaikudi,TamilNadu. He has presented and published number of papers in International and National Conferences,International and National Journals.His research areas of interest are cryptography,Operation Research, Data Mining, Security and Image Processing.