Review And Comparative Study Of Dual Stegnography Techniques For Embedding Text In Cover Images

Prof Ms. Ashwini B. Akkawar, Prof. Komal B. Bijwe

Abstract— In recent years, the rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. One of the best techniques for secure communication is Steganography-a covert writing. The process of using steganography in conjunction with cryptography,called as Dual Steganography, develops a sturdy model which adds a lot of challenges in identifying any hidden and encrypted data. Encrypting any secret data before hiding in the cover object will provide double protection. In this paper we have discussed about the three different techniques of dual stegnography for embedding text in cover images such as Image steganography combined with DES encryption pre-processing, Dual layer security of data using LSB Image steganography method and AES encryption algorithm and last Stegnography inside stegnography. The Merits and drawbacks of each technique and their comparative study and decide whether which technique is more useful in future.

Index Terms— Dual Steganography, Cryptography, DES, AES, LSB.

1 Introduction

STEGANOGRAPHY is an information hiding technique developed in recent years. It is a procedure that makes use of human perceptive sense of visual or aural redundancy to digital multimedia, and that embeds the secret information in the public media to transfer digital media carrying confidential information to achieve covert communications [1]. Steganography is different from cryptography. The goal of cryptography is to provide secure communications by transforming the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it cumbersome for a third person to find out the message. Unlike steganography, sending encrypted information may draw attention. Accordingly, cryptography is not the good solution for secure communication but only part of the solution. Both techniques can be used together to better protect information [3]. The basic steganography model is shown in Fig.1

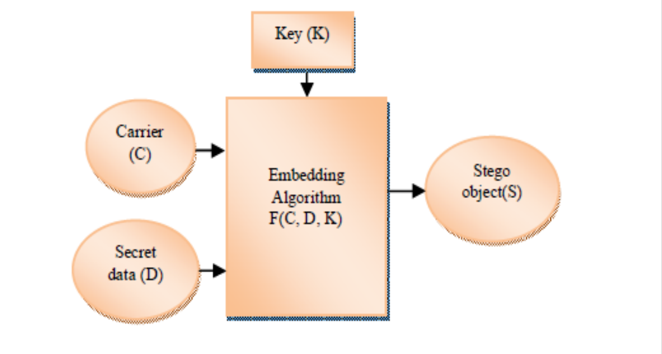


Fig. 1. The basic stegnography model

The basic model consists of Carrier(C), Secret Data(D), Stego Key(K).

1. Carrier is the cover object in which the message is embedded.
2. Secret data can be any type of confidential data that can be plain text, cipher text or other image.
3. Key mainly used to ensure that only recipient having the decoding key will be able to extract the message from a cover-object.
4. By using the embedding algorithm, the secret data is embedded into the cover object in a way that does not change the original image in a human perceptible way.
5. Finally, the stego object which is the output of the process is the cover-object with the secretly embedded data[4].

2 Dual Steganography Techniques

In this paper we have discussed about the three different techniques of Dual Stegnography.
1. Image steganography combined with DES encryption pre-processing.
2. Dual layer security of data using LSB Image steganography method and AES encryption algorithm .
3. Stegnography inside stegnography.

2.1 Image Steganography Combined With DES Encryption Pre-Processing

A. DES Encryption

DES uses a 56-bit key and an additional 8-bit parity bit, resulting in the largest 64-bit packet size. This is an iterative block cipher, using the technology known as the Feistel, which will encrypt the text block half. The use of sub-key pair, half of which application circulatory function, and then the output with the other half to "exclusive or" operator followed by the exchange of the two and a half, this process will continue, but in the end a cycle of non-exchange. DES uses 16 cycles, using

- *Ms. Ashwini B. Akkawar is currently pursuing masters degree program in computer science & engineering, P.R.Pote College of Engineering & Technology ,Amravati ,India. Email: ashu.b.akkawar28@gmail.com*
- *Prof. Komal B. Bijwe is working in Department of CSE, P.R.Pote College of Engineering & Technology ,Amravati ,India. Email: komalbijwe@gmaill.com*

xor, replacement, substitution, four basic arithmetic shift operations[1].

B. LSB Steganography Combined with Digital Image

The LSB (Least Significant Bit) which hides the secret information to the least significant bit of carrier information, is the most classic and simplest steganography algorithm, which also features of a large capacity and concealment. It is still widely considered most practical and applied up to today.The LSB steganography uses the secret information instead of the last bit of the image pixels value, which is equivalent to superimposing a weak signal upon the original carrier signal, and therefore it's difficult to realize visually[1].

C. Image Steganography Combined with Encryption

In order to improve the imperceptibility of steganography algorithm, the steganography combined with encryption algorithm,which reach the goal by changing the matching relationship between carrier image and secret information. At the transmitting terminal, we firstly choose the appropriate image as the carrier, and then encrypt text information or documents designed to hide by DES encryption followed by using the LSB steganography algorithm to hide the encrypted information in the image. At the receiving terminal,firstly extract the encrypted information from the carrierimage by the algorithm which is contrary to steganography algorithm, and then recover the hidden information by DES decryption algorithm[1].

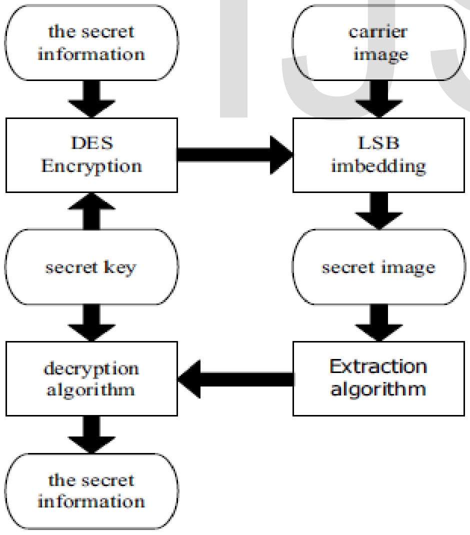


Fig. 2. The flowchart of image stegnography combined with encryption

2.2 Dual layer security of data using LSB Image Steganography method and AES encryption algorithm

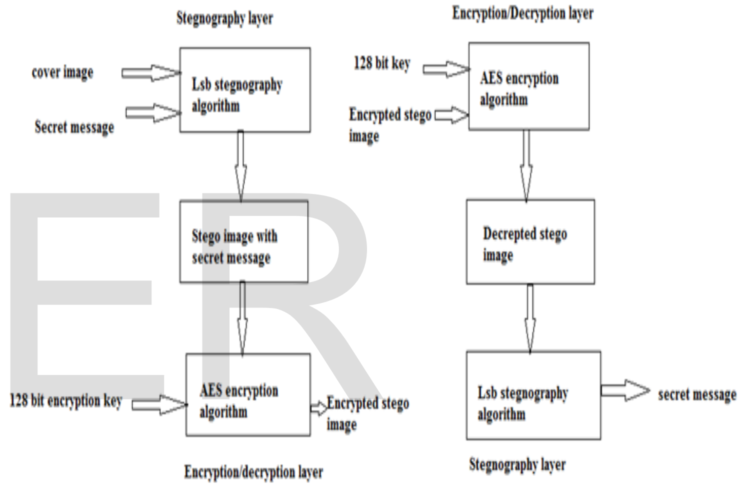
This technique consists of two layers, namely Steganography Layer and Ecryption/Decryption Layer.

A. Steganography Layer

In this process first we have to provide two inputs to the LSB steganography algorithm. First input is cover image in which secret message is embedded and second is secret message itself. Output of this process is Stego Image (image with secret message)[2].

B. Encryption / Decryption Layer

The core of second layer in our system is AES 128 bits Encryption algorithm. The output of first layer is Stego image with embedded secret message in it. In this layer we encrypt the stego image with AES algorithm by providing 128 bits public key for encryption. In the receiver end reverse process is applied by decrypting the stego image[2]. The following two fig.3[A] shows the Embedding and encryption process and fig.3[B] shows how message extraction and decryption is done.



(A) (B)

Fig. 3. (A) Embedding and Encryption Process (B) Extraction and Decryption Process

2.3 Stegnography Inside Stegnography

A. Data Hiding Process

The block diagram for the data hiding technique is shown below in fig 4.

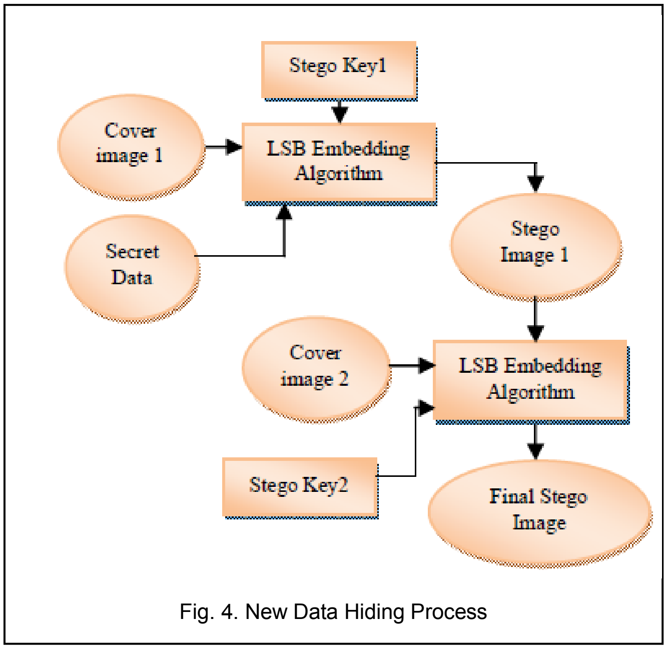


Fig. 4. New Data Hiding Process

Here two cover images are used i.e. coverimage1 and cover image2. For providing more security two stego keys are used which are different from each other. The stego key used is of 10 bit in length. The key can be made of numbers, characters, and symbols but should be of 10 bit length. These keys are hidden in the cover image during the hiding process. This should be known at the receiver side during the decoding process for retrieving the secret file as shown above the secret data has been embedded inside the cover image1 with the help of 4 bit LSB embedding algorithm along with the stego key1 mainly used for security purpose from which stego image1 is generated. Next, the stego image1 is considered as the secret data and hidden inside the cover image2 using 4-bit LSB algorithm and stego key2 after which final stego image is generated[3].

B. Data Extraction Process

The block diagram of data extraction process is presented is shown below in fig 5.

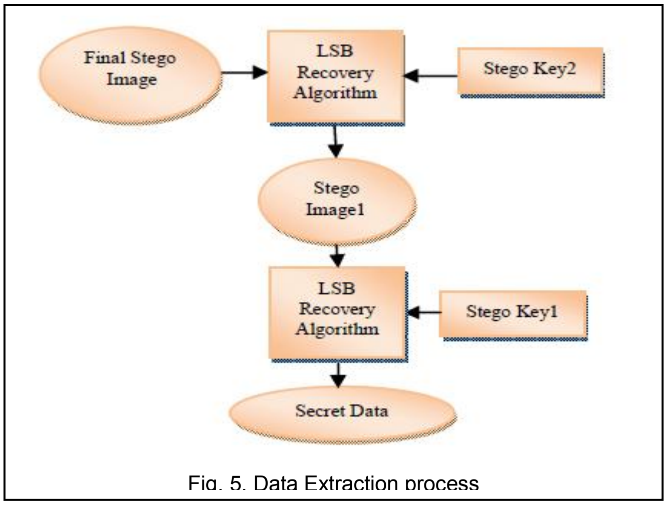


Fig. 5. Data Extraction process

From the final stego image, the stego image1 is extracted using stego key1 and LSB recovery algorithm.Next, from stego image1, secret data is extracted by using stego key2 and same LSB recovery algorithm. The proposed scheme is irreversible one as the cover image is not recovered at the receiver side [3]. The extraction process is strictly blinded as the secret data is extracted from stego image without the original cover image reference. This is done by using the same key at the receiver side whichever was used at the transmitter side. To make the secret data extraction more cumbersome, the concept of hiding the secret data in two planes has been adopted[3].

3 Subject And Methods

Different dual stegnography techniques and their advantages paired with weaknesses are given below in tabular form.

TABLE 1
Comparisons Of Dual Stegnography Techniques

Name Of Technique	Strengths	Weaknesses
1. Image steganography combined with DES encryption pre-processing	1. Encryption algorithm improves the lowest matching performance between the image and the secret information[1]. 2. Improve the security of Steganography. 3. The anti-detection robustness of image steganography combined with pre-processing of DES encryption is found much better than the way using LSB steganography algorithms directly[1].	1. Loopholes are there in DES and 3DES encryption algorithm . 2. The camouflaged appearance of encrypted data may arouse suspicion[3].
2. Dual layer security of data using LSB Image steganography method and AES encryption algorithm	1.AES Encryption algorithm provides better security than DES encryption algorithm. 2. AES algorithm does not have such loopholes like DES and 3DES[2].	1. National Security Agency (NSA) has developed a quantum computer that could crack most types of encryption Algorithms[3].
3.Stegnography inside stegnography	1. Provide two level of security to embbed data . 2.Good perceptual transparency . 3 .High payload capacity.	1. The complete and successful extraction of data needs the knowledge of keys-K1 and K2 which been extracted from blue plane of cover

	4. The secret data is not restricted to images only but also applicable to any text, audio or video. 5. The retrieved secret file is exact the same as that of the original one with 0% of data loss which is the biggest advantage of this method[3].	image[3]**.**

4 Conclusion

In this paper we have compared three different techniques for dual stegnography along with their strengths and weaknesses. The study shows that Image steganography combined with DES encryption pre-processing in which the secret data file is encrypted first using DES algorithm and then embedded using LSB technique improves the security of steganography and anti-detection robustness of image steganography than indivisual LSB. Dual layer security of data using LSB image steganography method and AES encryption algorithm in which secret data file is embedded first in cover image using LSB then resultant stego image is encrypted using AES encryption algorithm. AES Encryption algorithm provides better security than DES encryption algorithm. Finally, stegnography inside stegnography techniques overcome all the drawbacks of previous once and give rise to improved version of dual steganography. In this , two different stego keys are used, so the system is said to be double protected .Hence it is concluded that dual stegnography using stegnography inside stegnography techniques can be a good alternative for secure communication where two level of security is obtained in conjunction with high payload capacity , good imperceptibility and 0% of data loss.

References

[1] Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei," Image Steganography Combined with DES Encryption Pre-processing", *Sixth International Conference on Measuring Technology and Mechatronics Automation*, 2014.

[2] Satwinder Singh and Varinder Kaur Attri," Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", *International Journal of Signal Processing, Image Processing and Pattern Recognition* Vol. 8, No. 5 (2015).

[3] Ketki Thakre, Nehal Chitaliya," Dual Image Steganography for Communicating High Security Information", *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-4, Issue-3 July 2014.

[4] Ms. Ketki Thakre Dr.Nehal Chitaliya," Highly Secured Dual Steganographic Technique: A Retrospective", *International Journal of Engineering Research & Technology (IJERT),*Vol. 2 Issue 10, October – 2013IJERT ISSN: 2278-0181.

[5] Odai M. Al-Shatanawi1 and Nameer N. El. Emam," A New image stegnography algorithm based on MLSB method with Ramdom", *International Journal of Network Security & Its Applications (IJNSA*, Vol.7, No.2, March 2015.