ISSN No:-2456-2165

Steganography: Data Hiding using Cover Image

Nikhil Garware, Pravin Shinde, Vinod Patel, Navjeetsing Patil , Yogendra Patil
Department of Computer Engineering
JSPM's Bhivarabai Sawant Institute of technology and Research,
Maharashtra ,Pune.

Abstract:- Steganography is the technique which is used to provide secured communications between two or more users . This technique basically works on the principal of breaking the image into multiple parts and then hiding the data which is to be transmitted to other user's . By using this technology we can hide and send the information in the from of digital images , videos and audios . We have used multiple algorithms to provide extra security to the encrypted image . Algorithms used include LSB (Least Significant Bit) and the MSB (Most significant Bit). For the encryption and the decryption of the image we use the AES (Advanced Encryption Standard) Algorithm . Iterative approach is used by the design with the block size of 128bit and key size 256bit.

Keywords:- *Steganography, Encryption , Decryption , Image hiding , Advanced encryption standards(AES) , LSB(Least significant Bit), MSB (Most Significant Bit), Cryptography , Compression and Decompression.*

I. INTRODUCTION

In greek the word used for 'covered writing is said to be Steganography . In this technique we hide the message in such a way that the message cannot be read by the unauthorized users of the system .Steganography conceal that the generated secret message has been sent successfully and safely . Cryptography is a technique that scrambles the message such that no one can read the original message whereas steganography is the technique in which we hide the message in any of the mentioned formats like digital image , video or audios . The steganography uses a secret key for the decryption process . Without the decryption key the message cannot be decrypted . There are multiple algorithms which are used for the steganography of the image some of the examples are LSB algorithms , MSB algorithms , Huffman code algorithms .

Steganography and cryptography are used to provide information securities with the help of third parties but they can be compromised as none alone is perfect. If it is suspected that there is a conversation taking place between two end then the purpose of steganography is compromised. A solution to this is the combination of both the techniques i.e . Steganography and cryptography . When we use both of these techniques together the message is first encrypted and then the message is processed for the further hiding process . We can say that when steganography and cryptography work together the security if the hidden message transmission is amplified.

II. KEY POINTS OF THE PROJECT

- **Least Significant Bit (LSB) :**Human languages are not recognized by the computer system The computer system only uses the binary language format , which means the computer only knows the language which is in the form of 0 and 1 . Whenever we write any file or instruction for the computer language it is first converted into the binary format and then it is further processed by the system . If we write hello the system dose not know what dose hello means so as a result the system converts the String 'Hello ' in the binary format , the binary representation of the hello is ' 01101000 01100101 01101100 01101100 01101111' . To get the least significant bit we have to take the last digit of every byte so that we get the LSB. So in the example given above the LSB for the word hello would by 01001 .

Similarly every image also has its binary digits code which represents the image. While using the image steganography we are going to change the last digit of the byte and add the binary digit which contains the encoded message. In this we way we are going to hide the complete message into the image without making major changes in the image or the data.

- **Most Significant Bit (MSB):** The MSB method is same as the LSB method , the only difference the LSB and the MSB is the LSB selects the Least significant bit where-as the MSB selects the Most significant bit . By considering the example of the hello message which we have saw above , now we have the MSB of hello message which is represented by '00000'. This digits are changed in order to hide the secret message inside the image . As we only change the First bit (in MSB) or the Last bit (In LSB) there is not much of difference between the two images i.e. the image before hiding data and the image after hiding data. The is minor color difference which goes un noticed to the common human eye .

ISSN No:-2456-2165

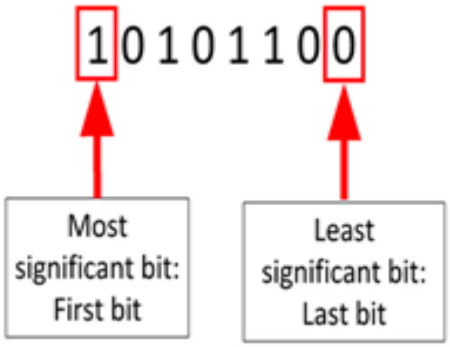

Fig 1:- MSB / LSB

- **Decryption Process:** As the image is encrypted and sent to the other receiving end , the user in the other end has to decrypt the image in order to find the secret message sent by the first user. For the decryption process the user has to enter the password of the key which is provided by the first user . As the user provides the key or the password the message from the image is retrived and displayed to the user .

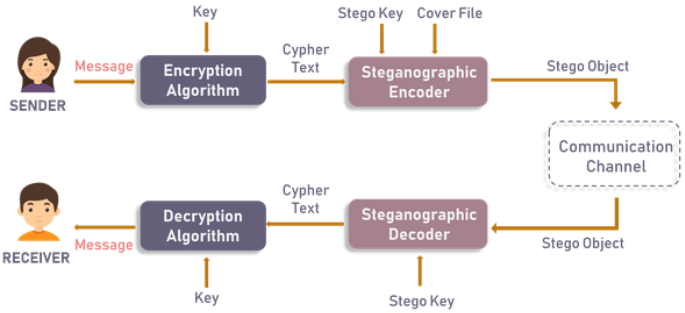

Fig 2:- Steganography process

As displayed in the above figure the sender generates the key and the cipher text and the cover file are attached together and the message is transmitted through the transmission medium to the receiver , the receiver receives the message. For the decryption process the receiver has to enter the key of the password which was set by the sender at the senders end . After entering the password or the key the system validates it , if the key matches then the secret message is retrieved from the cover file and the message is displayed to the receiver . This is the whole process which takes place in the process of image steganography.

III. CHARACTERISTICS

The confidentiality of the message is maintained in any situation.

The message cannot be decrypted without the use of the key or the password which is sent by the sender. So the security of the message is also maintained.

User-friendly GUI makes it easy for the new users to use the system software and perform the operation which user want's to carry out.

IV. ADVANCED ENCRYPTION STANDARD ALGORITHM (AES)

The AES algorithm is a 128 bit symmetric block cipher . We can say that the AES algorithm is the advanced version of the DES algorithm . The AES algorithm user the symmetric key , which means that the encryption and the decryption key both are same. The AES algorithm has the Plain text of 128bit , the key as the 128bit , and the cipher text generated is also of 128 bits. Each round has different key size for the 10 round the key size is :128bit , for the 12 round the key size id 192bit and for the 14 round the key size is 256bit. The maximum size is the 256 bit. The AES algorithm is faster and stronger than DES algorithm.

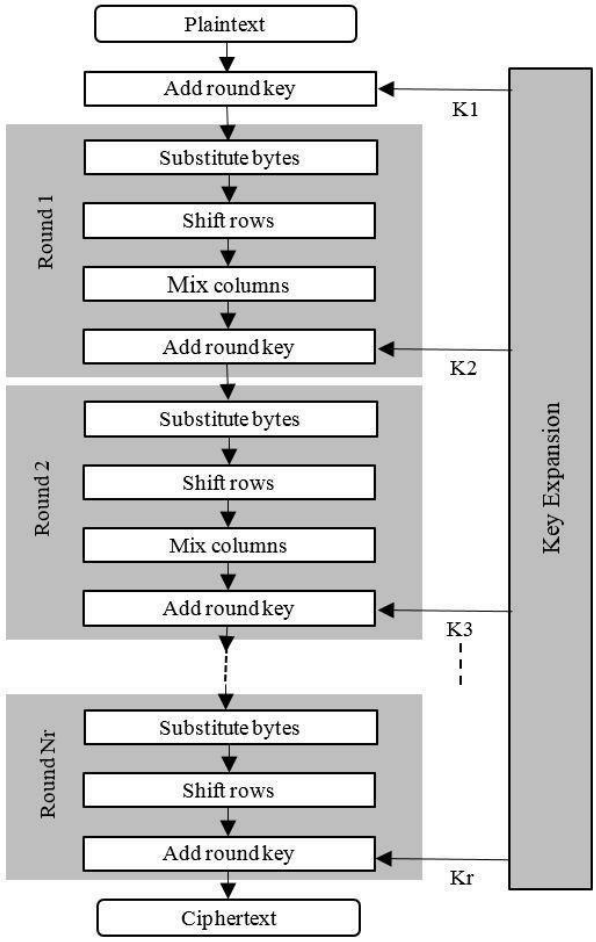

Fig 3:- AES algorithm

V. PROBLEM STATEMENT

The Steganography hides the every information of the data so perfectly that it is nearly impossible to find the difference between the original image and the encrypted image. Steganography can be performed on various files which include audio files, video files and also image files. Digital text is hidden in the image which is performed in our project. The digital text can also be referenced as the secret message.

VI. FUTURE SCOPE

In this project we have developed a system which hides the secret data or the secret message inside a image file which is known as the cover file. The message is protected with a password , which is entered by the receiver to retrieve the secret message. This system consists for a symmetric key ,but In the upcoming versions of this system we may try to generate the asymmetric key for the sender and the receiver.

The system may be modified and several changes can be made for making the system more secure so that it could be used by the Military and the intelligence departments.

Updates are under progress to make the system able to hide the data in formats like audio files and video files.

Steganography can also be implemented on printed media so that it becomes easy a secure to transmit the message to the authorized persons without letting others know that the information is being transmitted between two users.

Making changes in the system and making it available in the hospital application and bank application purposes .

VII. LITERATURE SURVEY

- Himani Trivedi And Arpit Rana "A Study Paper on Video Based Steganography",

Description: This paper gives overview of different video steganography methods. From this all the method have their advantages and disadvantages like LSB method has high capacity of embedding of data but low robustness to attack while DCT and DWT is robust against attack but they have less embedding capacity of data.

- Jacob Herison Kennedy1, MD Tabrez Ali Khan2, MD Junaid Ahmed3, MD Rasool4 " Image Steganography Based on AES Algorithm with Huffman Coding for Compressionon Grey Images,"

Description: Huffman coding suffers from the fact that the uncompresser need have some knowledge of the probabilities of the symbols in the compressed files this can need more bit to encode the file if this information is unavailable compressing the file requires two passes.

- Li Liu1, Anhong Wang1,Chin-Chen Chang and Zhihong Li1"A Secret Image Sharing with Deep steganography and Two-stage Authentication Based on Matrix Encoding."

Description: In this paper, a secret image sharing with deep-steganography and two stage authentication was proposed. This scheme is based on matrix encoding to embedded secret shadows into cover images and at most one bit was changed in the embedded block, so secret data does not directly appear in the pixels of the cover image.

- Rutuja Kakade, Nikita Kasar, ShrutKulkarni, ShubhamKumbalpuri, SonaliPatil. "Image Steganography and Data hiding in QR Code"

Description: There are many applications of this technique wherever more security is required. We have considered securing criminal data as one of its applications. The criminal information may be changed for misleading the police department. The data that can be changed or tampered is mainly the type of crime performed, which can be changed for reducing the punishment of the culprit.

- Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali2,Muhammad Naeem "An Improved Imag e Steganography Technique based on MSB using Bit Differencing.

Description: Usually,the LSB are targeted in steganographic systems, therefore using the MSB makes the system more secure. Furthermore, comparative analysis shows that the proposed technique has greater PSNR that shows the effectiveness of the proposed scheme.

VIII. CONCLUSION

Steganography is not being used in many areas as there is no proper awareness about the confidentiality of the data. It should be carried out in bank , military applications as well as hospitals and the needy areas . Steganography is the art of hiding sensitive data without generating unnecessary curiosity and suspicion among foreign party.

REFERENCES

[1]. Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.
[2]. Ashish T. Bhole, Rachna Patel, 2012 Steganography over video File using Random Byte Hiding and LSB Technique, IEEE international conference on computational intelligence and computing research.
[3]. DAVID A. HUFFMAN, Sept. 1991, profile Background story: Scientific American, pp. 54-58.
[4]. B. Karthikeyan, Suddep Gupta, 2016, Enhanced security in steganography using encryption and quick response code, IEEE Wisp Net Conference.
[5]. Avcibas, I. Memon, N. and Sankur, B.: Image Steganalysis with Binary Similarity Measures. Proceedings of the international conference on Image Processing, 3: 645-648. 24-28 June 2002.
[6]. Chiu-Yi Chen; Yu-Ting Pai; Shanq-Jang Ruan, Low Power Huffman Coding for High Performance Data Transmission, International Conference on Hybrid Information Technology, 2006, 1(9-11), 2006 pp.71 – 77.