ISSN 2395-1621

Data Hiding using Steganography

[#1]Vinod Patel, [#2]Nikhil Garware, [#3]Pravin Shinde, [#4]Navjeetsing Patil

vinodpatel1221@gmail.com

[#1234]Department of Computer Engineering

JSPM's Bhivarabai Sawant Institute of technology and Research,
Maharashtra ,Pune.

ABSTRACT

Steganography is the art of hiding the fact that 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. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications.

ARTICLE INFO

Article History

Received: 9th December 2019

Received in revised form :

9th December 2019

Accepted: 11th December 2019

Published online :

12th December 2019

Keywords: Steganography, Data Hiding, Encryption and Decryption

I. INTRODUCTION

The use of the internet and wireless communications has been rapidly growing and occupying a wide area in everyday life. Millions of users generate and interchange large amount of electronic data on a daily basis in diverse domains. However, the issue of privacy and security is on the top of the crucial concerns which determine the diffusion of such applications into the daily life. Hence, cryptography turns to become the key for the reliability and effectiveness of the embedded Technologies.Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

II. PROBLEM STATEMENT

Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this study, we proposed a new framework of an image steganography system to hide a digital text of a secret message.

III. LITERATURE SURVEY

[1] 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.

[2]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.

[3] 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.

[4] 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.

[5] Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali2, Muhammad Naeem "An Improved Image 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.

IV. PROPOSED SYSTEM

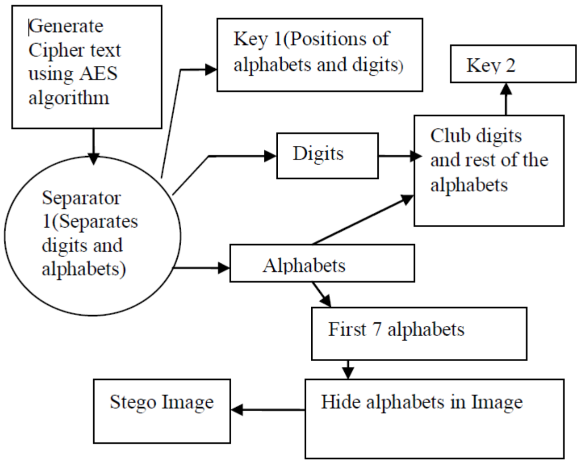

Fig 1. Proposed System for hiding text

Hiding Text

- Generate the cipher text in hexadecimal form by AES algorithm [13] in the form of alphabets (A, B, C, D, E, F) and digits (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).
- Separate the alphabets and digits with the help of Separator 1 and keep track of the original position of the alphabets and digits in the form of the first key (**Key 1**).
- Take the first 7 characters of the alphabets; this part will be hidden in the image.
- Take the rest of the alphabets and combine with the digits; this will form the second key (**Key 2**)
- Hide the 7 characters in the Image as mentioned in 2.2.

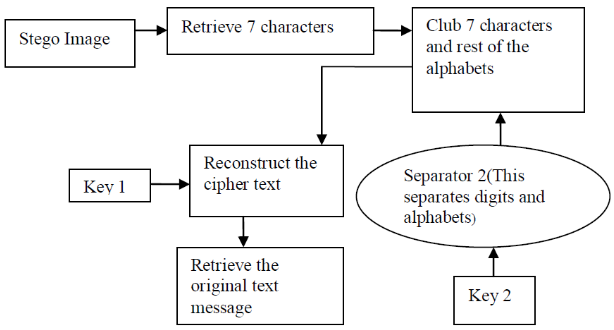

Fig 2.Proposed System for retrieving text

Retrieving Text

- Retrieve the 7 characters from the image.
- Separate alphabets and digits from **Key 2** with the help of Separator 2.
- Add back the rest of the alphabets from **Key 2** to 7 characters retrieved from the image.
- Reorganize the alphabets and digits with the help of the **Key 1** to get back the original cipher text in hexadecimal form.

- Regenerate the original text message from the cipher text with the help of AES algorithm.

V. CONCLUSION

Though Steganography is not implemented in wider ways but it can be the best security tool. 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 HighPerformance Data Transmission, International Conference on Hybrid Informat ion Technology, 2006, 1(9-11), 2006 pp.71 – 77.

