International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Steganographical Techniques in Hiding Text Images – System

V.V. Vinoth, E.Kanniga

Abstract*: In this era, internet has become a widespread entity all over the world. Sharing and communicating images, video contributes an essential role in this scientific era. In the meanwhile, secure transition of data has indeed become a major issue. Steganography is one of technology that contributes a vital role in protecting the secret data against an unauthorized access. In this type, secret data can be concealed into a cover file that includes audio, video, text and also image. In this paper, we propose different types of steganography methods for secure transfer of data in a confidential manner. The paper also explores stenographical techniques in terms of text, image and audio. The proposed work compares and discusses the stenographical methods in spatial domain, frequency domain derived under the image technique.

Keywords* : *Communicating Images, Steganography Methods, Image and Audio.

I. INTRODUCTION

Internet has become an efficient and most convenient medium of communication in the world. Much information is being transferred within a fraction of seconds. It has its vital role in various departments such as government sectors, private, especially medical and military [1]. Steganography means writing in a covered manner. It is derived from Greek word called Steganous which means "covered" and graphy takes the meaning of "writing". Steganography is an encrypting technique that hides the message and prevents data in such a way that the hidden message cannot be detected [2]. This technique not only hides the message but also the concept of hiding information [3]. Generally data hiding technique falls into three main categories namely cryptography, steganography and watermarking. Steganography technique conceals the presence of hidden data rather cryptography method [4]. In this modern era image steganography can be considered as best in hiding the secret data [5] that ensures data authentication, data privacy, copyright protection, confidentiality and integrity. The main concept of steganography is to prevent the attention towards the transmission of the hidden message. The steganography terms includes cover file, stego key (K), hidden data (D), embedded function (E) shown in Fig 1.

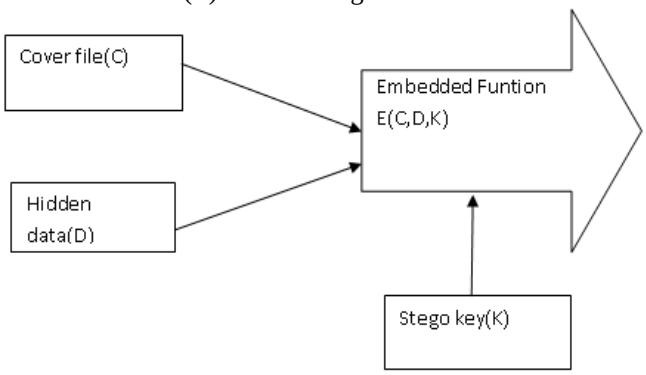

Figure 1: Steganography Model

II. STEGANOGRAPHY PROCEDURE

The fundamental terminologies implied in the steganography process includes: cover media, secret message, stego key and embedding algorithm [6] shown in the Fig 2.The cover message acts as the message carrier that may include image, video, audio, text or any digital media. The secured message is the information which is to be hidden inside the specified media. The secret key embeds the message which is dependent on the hiding algorithms. The embedding algorithm play significant role to embed the secret message inside the cover message[7,8]

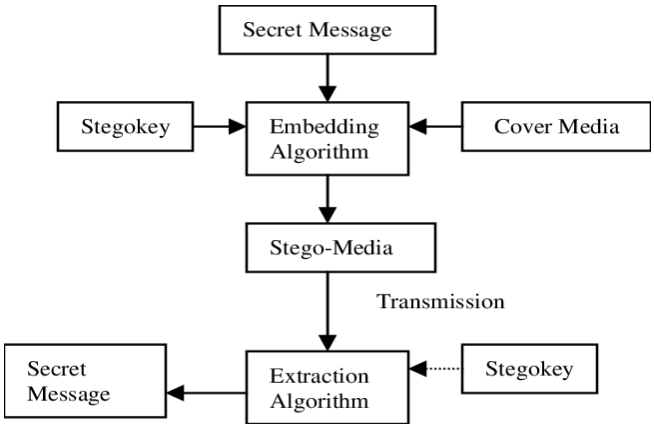

Figure 2 Steganography frame work

III. STEGANOGRAPHY MEDIUM

Information can be hidden in 3 ways of medium in steganography. Text steganography, image steganography, audio steganography. Steganography itself can be categorized as pure, symmetric and asymmetric.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
V. V. Vinoth*, Research Scholar, Department of ECE, Bharath University, Chennai, India.
E. Kanniga, Professor, Electronics and Communication Engineering Head Electronics & Instrumentation Engineering, Bharath University, Chennai, India.

In this case, symmetric and asymmetric models exchange keys before transmitting the messages whereas pure steganography does not exchange any information [9]. This technique is mainly based on the type of media in which the information is hidden. The next section discusses three different Medium of through which data is hidden. Steganography uses text, images audio and also some network protocols used in the network transmissions. Image steganography is generally preferred media due its impact on the public. Cameras and digital images are technically advanced to transmit the digital images to the nodes [10]. The main advantage of hiding the message in the image is that text messages do not distort the image.

i. Steganography in Text Medium

In text steganography, the secret data is being embedded in the text files shown in (Fig 3). There are three methods for transmitting the information embedding with the text files namely:

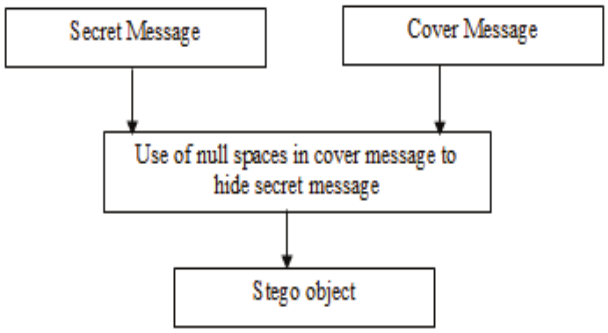

Figure : 3 Text Steganography

Format model: In Format based model, the text data includes the insertion of spaces, resizing the text, change of style in order to hide the secret information

Random model: This model encrypts the characters in a random sequence manner.There occurs another model embedded in this method called statistical model [11] that analysis statistical properties that includes mean, variance that measures the quantity of replicated messages that should be hidden in the text.

Linguistic model: It is a synthesis of syntax and technical semantic models. It considers linguistic properties and altered text with its own structure that considers the space where the information is being hidden. It also finds syntactical flaws and a value is assigned to the synonyms in which the information is encoded in the actual text image.

ii. Steganography in Image Medium

In this type of encryption, images (Fig 4) are used as a cover entity for securing the digital images. Image file consists of data that comprises both compressed form and uncompressed type. Here the data securing or hiding is done in two ways. One is spatial domain and another category is frequency domain. Manipulating the pixels in image is called spatial domain[12] and frequency domain model is done by altering the Fourier transform of an image data. Generally stegano technique works on three classes of images such as GIF images, BMP format images and JPEG images. Today's internet world completely uses JPEG format as it provides heavy compression percentage and also sustains the nature of the image quality in terms of PSNR value.For JPEG compression discrete cosine transformation[13] is deployed on every block of the image which is then used for data compression. This technique also resembles Fast Fourier Transform where data is converted into frequencies sets. Transformation matrix are quantized in a matrix table containing coefficients. Thus by evaluating the inverse quantized coefficients jpeg image is evolved.

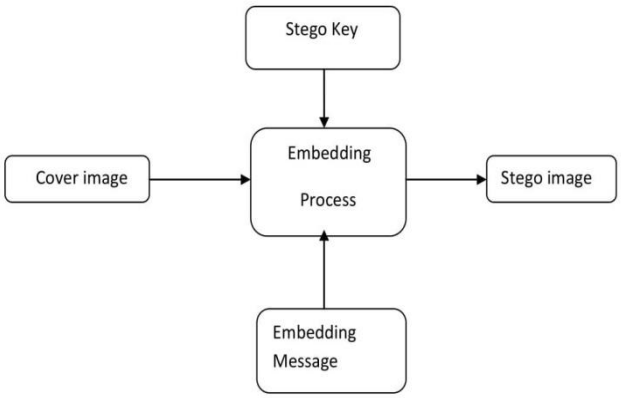

Figure 4 Image Steganography

iii. Audio Steganography

This type of encryption technique embeds the secret information within the digital sound (Fig 5) It includes sound files such as WAV, AU and MP3. Audio steganography holds three methods for encoding the data. They are as follows:

a. **Encoding low bit:** Its application falls in mobile phones and it embeds the data while encoding the low bit rate of audio by managing the synchronization between message hiding and speech encrypting.

b. **Encoding Phase model**: Entire audio stream file is splitted into file blocks and it enclosed the entire secret message into phase of the primary block. Its advantage is its low capacity.

c. **Encoding spread spectrum**: Its application lies in radio frequency. Information are spread through frequency spectrum. The quantum calculation is taken in a discrete manner of host by locking the phase. The main advantage of this type of encoding is that chip rate is higher and able to hide large data.

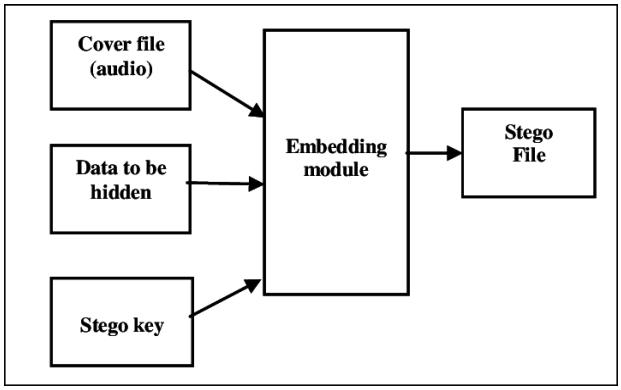

Figure : 5 Audio Steganography

IV. DISCUSSION

In the past one decade, steganography has dragged the world's attention mainly on the image coverage medium. The paper discusses about the steganography layout, its types, methods and medium such as text, audio and image shown in Fig 6a and 6b.Steganography holds advantages that overcomes cryptography models. The techniques used in the steganography models are used for the determining the stego images by providing security for images and also for the data enclosed within the image, audio , video or image[14] as well. Some steganalysis tools are also implemented to detect the files which is hidden in any type of the image.[15] Though there exists many mediums for transmitted secret data image steganography holds the prior position among all other models which is efficiently decoded.

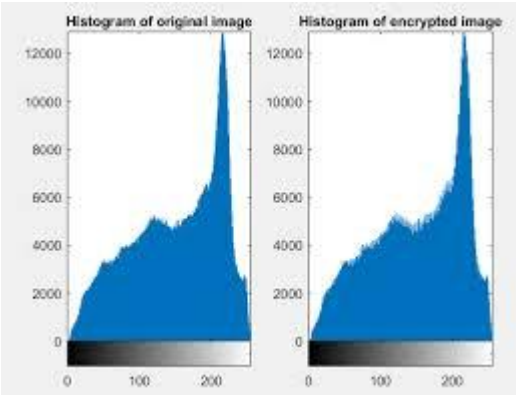

Figure 6a Image Steganography

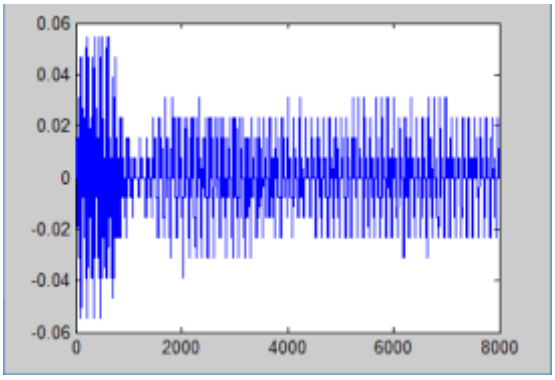

Figure 6b. Audio Steganography

V. CONCLUSION

The proposed paper describes the fundamental ideas of steganography, its methods, categories and types and its medium through which secret information are transmitted. The paper also clearly depicts the steganography medium and it is found that image steganography is ahead when compared to the other mediums where all types of images that BMP, GIF and JPEG are used for secure transmission using discrete cosine transformation and Fourier transformation series. The proposed paper also furnishes the spatial and frequency domain categories of image medium thus concluding that image steganography are widely implemented rather other medium of transforming the secure data or text messages.

REFERENCES

1. V. Potdar and E. Chang, "Gray level modification steganography for secret communication," in Proceedings of the IEEE International Conference on Industrial Informatics, Berlin, Germany, 2004.
2. B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).
3. Chandramouli R., Kharrazi M., and Memon N., "Image Steganography and Steganalysis: Concepts and Practice", International Workshop on Digital Watermarking (IWDW), Seoul, pp. 35-49, October 2003.
4. Saman Shojae Chaeikar, Azizah Bt Abdul Manaf and MazdakZamani. Comparative analysis between Master key and InterpretativeKey Management (IKM) Framework to provide utilization guidelinefor researchers and developers. Cryptography and Security inComputing, ISBN: 978-953-51-0179-6. Publisher online InTech.2012.
5. J.C.Judge, Steganography: past, present, future. SANS Institute publication, , 2001.
6. Derek Upham, Jsteg, http://zooid.org/ Paul/crypto/jsteg.
7. K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168, 2004.
8. Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287
9. Navdeep, Ms Neha Goyal, Hide Text in Images using Steganography and a Review of methods and Approach for secure steganography, International Journal of Research in IT and Management, Vol.6, No.5, 2016.
10. Haz Malik, Steganalysis of qim steganography using irregularity measure, Proc. of the 10th ACM workshop on Multimedia and security, ACM Press, pp. 149-158, 2008.
11. A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp 283-286, 2007.
12. M. Goljan, J. Fridrich, and T. Holotyak, New blind steganalysis and its implications, IST/SPIE Electronic Imaging: Security, Steganography of Multimedia Contents VIII, vol. 6072, pp. 1-13, 2006.
13. Y. Wang and P. Moulin, Optimized feature extraction for learning-based image steganalysis, IEEE Trans. Information Forensics and Security, vol. 2, no. 1, pp. 31-45, 2007.
14. Nandagopal, V., Geeitha, S., Kumar, K. V., & Anbarasi, J. (2019). Feasible analysis of gene expression–a computational based classification for breast cancer. *Measurement*, *140*, pp.120-125.
15. Nandagopal, V., Maheswari, V., & Anbarasi, J. (2019). Pyrolysis Electricity Generation and Biomass. Journal of Computational and Theoretical Nanoscience, 16(2), pp.428-429