An Approach for Steganography in Security Systems

M.Angulakshmi, M.Deepa, M.B.Benjulaanbumalar, K.Santhi, M.Lawanyashri

Abstract*: Techniques for hiding secret data or information play an important role with the rapid growth of multimedia content transfer and secret communications of data. Steganography is the art of hiding data or information in such a ways that prevent detection. Steganography is used for transferring hidden data in an appropriate carrier like audio, video, image etc from one place to other place through public channel. Many different carrier files can be used like audio, video, TCP/IP header file, but digital images are the most popular because images are used very frequency on internet now days. For hiding secret data or message in images, there is a large variety of Steganography techniques available and all of them have respective strong points and weak points. Different applications used for steganography technique have different requirements. In this paper we survey different steganography techniques for hiding the secret data and prosed a method by combining different methods.

***Index Terms*: Audio , Image,Steganography, Text, Video.**

I. INTRODUCTION

Steganography is a word which means covered writing. Steganography is used in process of hiding a secret message (the embedded message) within a larger source in such a way that an outsider cannot detect the presence of any secret message. Now days in Internet one of the most important issues is the security of information which we transfer from one place to another. Art and science of invisible communication of secret information is referred as steganography. It is accomplished by hiding information in some other transfer medium. This is a unique technique which is used to conceal the data which is already hidden. This technique is a new method to conceal the important data so that others could not access. In this hidden message can be sent in text format or in image format. Now days this technique is very helpful in sending the confidential data, monitoring piracy, to send secret data etc. Although many data hiding methods have been proposed by various authors, the specific requirements of each information hiding method vary with the application. This study aims at providing a test to outline the best and current steganography technique.

II LITERATURE REVIEW

In the related work, the usage of LSB method developed by Chandramouli is most common method which is used to hide the information. [1], by applying the filter, transformation on the cover media and masking. WeiqiLuo,[2] proposed LSB matching revisited steganography of image and edge adaptive scheme in which according to the size of secret message or information we can select the embedding regions. For large embedding rates smooth edge regions are used and sharper regions are used for lower embedding rate. [3] Based on chaos and Euler, paper proposes an image stenographic method. Theorem in which hidden message or information can be recovered by the use of orbits and there is no need to extract the hidden message from original image. Hassan Mathkour [4] use a new Image steganography method based on LSB replacement technique and differencing pixel value. This method involve replacement of least significant bits(lsb) in order to hide the secret colored message or information image with the advanced LSB method where in accordance to range specified for the colour images the bit replacement takes place. Dobisicek [5] paper proposed a model of authentication for steganography to detect any attack on the transformed image based on a verification code by modifies two coefficients of the Discrete Wavelet Transform in cover image. Neil Provo [6] has proposed another technique to counter the unauthorized attack like statistical attack which is called as Out Guess .In this process or method modifications are made to the coefficients so that stego-image histogram should match the cover image histogram. Pavan [7] has disused about the steganography field used in spatial, transform and compression regions of digital images. Spatial region is comparatively better than transform region. Steganography techniques used are based on the application type and its design. But more data hiding could lead to loss of the image quality. Mohammad Shirali-Shahreza [8] has discussed about the different steganography software that are used in hiding the images. The study says about which tool is better for the steganography. The study shows all the pros and cons of the software used in steganography. Chen Ming [9] have discussed about the different file formats have different formats for sending data .Each technique have its own pros and cons. The person who needs to send the data has to decide that which technique he want to use, keeping in mind about the security issues. MankunXu [10] Based on least square method, paper proposed a Model Based steganography method which is used to estimate the embedding rates of sending message.

Revised Manuscript Received on December 22, 2018.

M.Angulakshmi ,School of Information Technology and Engineering,,VIT, Vellore, India.
M.Deepa, (Corresponding Author**),** School of Information Technology and Engineering, VIT, Vellore, India.
M.B.BenjulaAnbuMalar, School of Information Technology and Engineering, VIT, Vellore, India.
K.Santhi, School of Information Technology and Engineering, VIT, Vellore, India
M.LawanyaShri, School of Information Technology and Engineering VIT, Vellore, India.

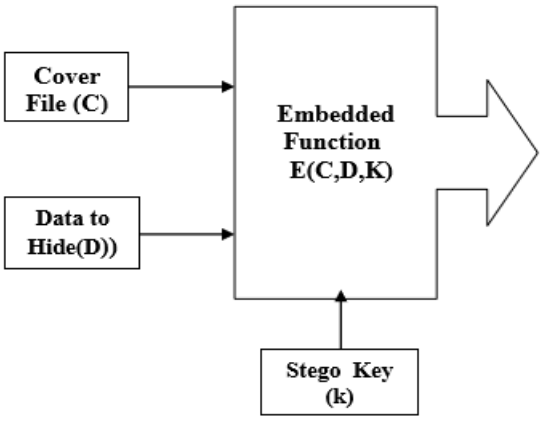

Figure1: **Steganography Diagram**

A. APPLICATIONS OF STEGANOGRAPHY:

Steganography applications are:-

- It hides data in another data in form of message that can text, image, audio or any kind of media.
- The communications becomes more secure and safe.
- TV broadcasting, access control for distribution of the digital contents
- TCP/IP packets in which unique id is embedded into any media format
- Protection of altering of the data
- Highly confidential data could be safely circulated to and from the companies

IV TYPES OF STEGANOGRAPHY

Steganography can be classified into pure steganography, symmetric steganography and asymmetric steganography. In pure steganography there is no need for any exchange of information but in symmetric and asymmetric steganography, we need to exchange the keys before sending the messages[11][12]. Type of media being used to hide the information in steganography is a very important. Medium which are commonly used are text, images, audio, video and network protocols like tcp/ip header files used in network transmissions of information. Image Steganography is generally more popular among all mediums because of its harmlessness and attraction [13][14]. Through the increased used of the internet and ease of comfort and flexibility in sending information, exchange of greetings through digital media is increasing day by day. Advancement in technology related to design of cameras and digital images includes saving of image in cameras and then transferring it to PCs. Secondly, the text messages or information hidden in the original images does not destroy the image and there are methods which only change one bit in pixel of an image which is not noticed and almost negligible on its quality[15][16]. The major drawback of steganography is that we can hide very small amount of information of data in the media selected. Some methods are following.

- Encoding secret information in text/documents media
- Encoding secret information in audio media
- Encoding secret information in images media

A. Text Steganography: Text Steganography hide the secret information in text files through various methods:

- Format based technique
- Random and statistical technique
- Linguistic technique

B. Format based technique: In order to hide the stenographic text or message this technique modifies the existing original text. This method includes insertion of spaces, changing of the style of text, resizing the text to hide message in it.[17][18][19]

C. Random and statistical technique: Random technique hides the characters which appear in random sequence in the original information which we embed in text. Statistical technique determine the statistics such as variance, means and chi square test which is used to measure the amount of duplicate message that can be hide within the given text[20][21][22].

D. Linguistic technique: Linguistic technique for steganography is a combination of syntax and semantics techniques. Linguistic method also considers the linguistic properties of modified text which is generated in the process of steganography, and uses linguistic structure as the space in which information are hidden by use of it. Syntactic method is used to ensure that structures are syntactically correct and proper for hiding process. In this method the text should be syntactically correct because if we change the grammar it will affect the original text. In Semantic technique we can give or assign the value to synonyms and information can be encoded or embedded into original words of text. [23][24][25]

E. Audio Steganography: Hiding secret information into digital sound or audio is called as audio Steganography. Audio Steganography techniques can be used to embed messages in AU, WAV and MP3 audio files. There are three methods that are used in audio steganography are: Low bit Encoding method, Phase Encoding method and Spread Spectrum Encoding method [26][27][28].**Low Bit Encoding**: It is widely used in audio communications for example, mobile communications and VOIP. It is used to perform the task of embedding the message while during low bit-rate speech encoding; pitch period prediction is conducted, so to maintain synchronization between message hiding and speech encoding is important in this process. [29][30]

F. Phase Encoding: In this method splitting of the original audio file into small blocks is done and hides the whole secret sequence message into the phase spectrum of the first block[31][32][33]. One disadvantage of the phase encoding technique is that less amount of message is stored or we can say that message capacity of message is less which is going to store in first block.

G. Spread Spectrum Encoding: we can say that it is a form of radio frequency

communication. In this method data is sent using the spread spectrum in which encoding is intentionally spread across same as the frequency spectrum spread across. One Particular technique in this is DSSS (Direct Sequence Spread Spectrum) in which signals are spread by multiplying it by a certain max length pseudorandom sequence, which is called as chip[34]. Then start and end quanta calculation is taken by the discrete, sampled nature of original signal for phase locking purpose. In the end as a result we get the higher chip rate and we can hide maximum information or message in that chip.

H. Image steganography: Images are considered as cover object which is used for steganography. Digital images are used to store image files. An image file can store data or information in compressed or uncompressed format. In Image Steganography method, data hiding techniques can be classified into two methods. They can be spatial domain and frequency domain. Spatial domain method can be used by direct manipulation of pixels in an image. In Frequency domain method the Fourier transform of an image is modified. Steganography algorithm which is used in these methods can be applied on three types of images. They are Palette based images (GIF images), JPEG images and Raw images (BMP format). We can say that one of the most popular formats which we use on internet is JPEG (Joint Photographic Expert Group) because it provide large compression ratio and also provide maintain high image quality by measuring PSNR value of image.

In the process of compression of JPEG image, image is divided into 8*8 blocks and after that DCT is applied on each block of image. Discrete Cosine Transformation method or technique is used for data compression in this case. It is similar to Fast Fourier Transform method and after that DCT converts data (pixel values) into small sets of frequencies. In the end quantization table is used to quantize the resultant DCT coefficient matrix.
Quantization table which is a matrix contain DCT coefficients. After that the process of inverse DCT of quantized coefficients is evaluated and jpeg image is obtained.
I. Jpeg-Jsteg: In the process of Steganography of image, there is a JPEG information hiding tool known as jpeg-jsteg. It hides the information into LSB of the quantized DCT coefficients where the values of it is not equal to 0,1,-1.The main drawback of this technique is that it has less capacity to hide the information also modifying low frequency coefficients cause a distortion which can be detectable or detectable by a steganographic technique available.

V PROPOSED METHOD

As mentioned in the above section of this paper, almost all steganography research done in the JPEG transformation domain method of image steganography shows that, in this method it divides a given original cover image into non-overlapping blocks of 8*8 pixels of that image. Since the research is going on to increase the capacity of message hiding by proposing a new steganography technique based on JPEG and quantization table is a continuous process in field of image steganography to make it more secure and flexible to use.

VI CONCLUSION

Now day's steganography is an interesting topic for image cover media. In this paper we provide an overview of different type of steganography and introduce some methods of steganography which help to hide the secret data or information in some given media. These methods are more useful for detecting the stego images and data hidden in it. It also focuses on the security of message or information which is embedded in the image or some other media and we can easily calculate the high embedding rate by the use of quantitative steganalytic technique available.

REFERENCES

1. M. Shirali-Shahreza , "A new method for real time steganography",International Conference on Signal Processing.vol.4 Nov 2006.
2. Y.Ying Chung, fang FeiXu, "Development of video watermarking for MPEG2 video" TENCON-IEEE Region 10 conference, Nov2006.
3. C. Lu, J. Chen and K. Fan, "Real-time Frame- Dependent Video Watermarking in VLC Domain", Signal Processing: Image Communication. vol. 20, pp. 624–64, 2005.
4. J. Cummins, P. Diskin, S. Lau ,R. Parlett ."Steganography and digital watermarking" School of Computer Science, The University of Birmingham. 2003.
5. C. Lu, J. Chen, H. M. Liao, and K. Fan, "Real-Time MPEG2 Video Watermarking in the VLC Domain "Proc.of 16th International Conference on Pattern Recognition, Vol. 2, , pp. 552-555, Aug 2002.
6. M. Angulakshmi. I. NagarajanA "Survey on Multi-Relational Database Based Classification Approaches", International Journal of Applied Engineering Research, vol 9, 2014.
7. M. Angulakshmi,. "Big data analytics–Areview". International Journal of Pharmacy and Technology, vol. 8, pp. 4634-4639, 2016.
8. H. Dewangan, M. Angulakshmi,. I. Nagarajan,."Multiprocessing optimization - Parallel quick sort using open MP". International Journal of Pharmacy and Technology. vol. 8, pp. 15633-15639, 2016.
9. A.Sharma, P.Patidar, M. Angulakshmi. "Overview of features of smartphone OS- android, ios and window phone 8", International Journal of Pharmacy and Technology, vol 8(4), pp. 25347-25351, 2016.
10. R.Rathi,.S.Sudha, K. Brindha., M. Angulakshmi, G.Haripriya, M. Teja, "effective evaluation of prediction accuracy using optimation algorithm", International Journal of Pure and Applied Mathematics, 2017.
11. M. Angulakshmi, G.G. Lakshmi Priya,, "Automatic brain tumour segmentation of magnetic resonance images (MRI) based on region of interest (ROI)." Journal of Engineering Science and Technology, Taylor & series. vol. 12, pp. 875-887, 2017.
12. M. Angulakshmi, G. G. Lakshmi Priya. "Automated brain tumour segmentation techniques — A review". International Journal of Imaging Systems and Technology.Wiley. vol .27, pp. 66-77, 2017.
13. M. Angulakshmi, G. G Lakshmi Priya. "Walsh Hadamard kernel-based texture feature for multimodal MRI brain tumour segmentation". International Journal of Imaging Systems and Technology. vol.28, pp. 254-266, 2018.
14. M.Deepa, M. Anand ,"Availability Modelling of Fault Tolerant Cloud Computing System". International Journal of Intelligent Engineering and Systems, vol.10, pp.154-165, 2017.
15. M. Deepa, M. Anand, "An Approach to Evaluate the Availability of System in Cloud Computing Using Fault Tree Technique". International Journal of Intelligent Engineering and Systems, vol.10, pp .245-255, 2017.
16. M. Deepa , M. Anand, "Risk - based availability modelling and reputation management on fault tolerant cloud computing

systems". International Journal of Internet Technology and Secured Transactions- Inderscience. vol.9, pp.37 – 56, 2019.
17. M.Deepa, M. Anand, "Quality of service on performance evaluation- A Survey". Institute of Integrative Omics and Applied Biotechnology (IIOAB).Vol.8, pp. 8-13, 2017.
18. M. Anand , M. Deepa " A Survey on Applications of Grammar formalism In Image Processing". International Journal of Applied Engineering Research, Vol.10, pp. 16021-16034, 2015.
19. K. Santhi., C. Priyadarshini. "Efficiently Allocating the Virtual Machines in Cloud", International Journal of Applied Engineering Research, vol. 9(3). pp. 387-392, 2014.
20. K. Santhi, R. Saravanan. "Facilitate refined keywords search over encrypted data on cloud". International Journal Of Pharmacy & Technology, vol 8(3), pp. 15552-15557, 2016.
21. K.Santhi, R.Patel, "Sheds: A simple and secure cost efficient data storage in heterogeneous multiple cloud". International Journal Of Pharmacy & Technology, vol.8, pp.26058-26065, 2016.
22. K. Santhi, R. Saravanan, "A survey on queueing models for cloud computing,"International Journal Of Pharmacy & Technology, vol8(2), pp. 3964-3977, 2016.
23. K. Santhi, R. Saravanan, "Performance Analysis of Cloud Computing in Healthcare System Using Tandem Queues".International Journal of Intelligent Engineering and System,vol 10(4). pp.256-264, 2017.
24. K. Santhi, R..Saravanan, "Performance Analysis of Cloud Computing Bulk Service Using Queueing Models". International Journal of Applied Engineering Research, vol 12(7), pp.6487- 6492, 2017.
25. K. Santhi, R. Saravanan, "Performance Analysis of Cloud Computing Using Batch Queueing Models in Healthcare Systems". Research Journal of Pharmacy and Technology,vol10(10), pp.3331-3336, 2017.
26. K. Santhi, R. Saravanan, "Performance analysis of cloud computing using series of queues with Erlang service", International Journal. Internet Technology and Secured Transactions, Vol. 9, pp.147–162, 2019.
27. K.P. Shiva Priya, S. Monisha, R. Keerthiga, M. LawanyaShri. , "A comparative analysis of classifier algorithm in defect prediction using cgbr framework", International Journal of Applied Engineering Research , 2015.
28. K.R. ManojPrabhakar, M. LawanyaShri, "Implementation of an issue tracking system in private cloud", International Journal of Applied Engineering Research, 2014.
29. K.S. Tarun Kumar, P. Vignesh Kumar, M. LawanyaShri, "An implementation of storage provisioning in private cloud", International Journal of Applied Engineering Research, 2014.
30. G. Jothipriya, M. LawanyaShri, "Database synchronization of mobile-build by using synchronization framework", International Journal of Engineering and Technology , 2013.
31. M. LawanyaShri, S. Subha ," An implementation of E-learning system in private cloud", International Journal of Engineering andTechnology,2013.
32. M. LawanyaShri, B. Balusamy, B, S. Subha, Energy-aware hybrid fruitfly optimization for load balancing in cloud environments for EHR applications. Informatics in Medicine Unlocked, vol8, pp 42-50, 2017.
33. M. LawanyaShri, S. Subha, B. Balusamy . Energy- Aware FruitflyOptimisation Algorithm for Load Balancing in Cloud Computing Environments. International Journal of Intelligent Engineering and Systems, vol10(1), pp. 75-85, 2017.
34. M. LawanyaShri, B. Balusamy, S. Subha, Threshold-based workload control for an under-utilized virtual machine in cloud computing. International Journal of Intelligent Engineering and Systems, vol9(4),pp 234-241, 2016.
35. .Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.
36. Rajesh, M., and J. M. Gnanasekar. "Sector Routing Protocol (SRP) in Ad-hoc Networks." Control Network and Complex Systems 5.7 (2015): 1-4.
37. Rajesh, M. "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks." International Journal of Pure and Applied Mathematics 118.9 (2018): 407-412.
38. Rajesh, M., et al. "SENSITIVE DATA SECURITY IN CLOUD COMPUTING AID OF DIFFERENT ENCRYPTION TECHNIQUES." Journal of Advanced Research in Dynamical and Control Systems 18.
39. Rajesh, M. "A signature based information security system for vitality proficient information accumulation in wireless sensor systems." International Journal of Pure and Applied Mathematics 118.9 (2018): 367-387.