Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 4, April-2016

A Review paper on dual staganography

Ms, Bharati D, Bhatiya[1]

[1]*Electronics Department,Shri K J Polytechnic, Bharuch,Gujarat,India*

Abstract — Steganography is a process of hiding of a secret message within an ordinary message and extracting it at the destination. Anyone else viewing the message will fail to know that it contains secret/encrypted data. Several Steganography techniques have been developed and successfully applied till now. The issue we need to look for is the degree of security and the complexity of the steganography model. The process of using steganography along with any other cryptography algorithm is called dual steganography. This technique presents a two level secure and robust approach which makes it quite difficult for hackers to identify the hidden data.

This paper is a review of various steganography techniques. It also and presents possible approaches for dual image steganograph. *Keywords-* **Dual *Steganography, Image steganography, Video steganography, steganalysis,LSB substitution***

I. INTRODUCTION

In the recent years mankind has witnessed rapid growth of high speed networks and so information communication including images and videos has become very easy and fast. Also digital data communication has become very popular because of several distinct advantages it offers such as high quality, higher SNR , ease of compression, high fidelity copying etc. At the same time one cannot ignore data security issues while communicating confidential data over public networks.

Steganography is an art of hiding data into another covering media in a way that only the intended receiver knows that a secret message is hidden in the cover and detects message.[1] The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" means "writing" defining it as "covered writing".[2] Steganography should not be confused with cryptography. It is different than cryptography in a way that it hides the existence of the secret messages itself. The person viewing the cover data will not have any idea of hidden information. So the person will not attempt to decrypt it as in the case of cryptography. Digital steganography has many applications in today's world. It can be used as a digital watermarking or to maintain the confidentiality of valuable data from possible sabotage, theft and unauthorized viewing. The Basic Steganography model is shown in fig 1.

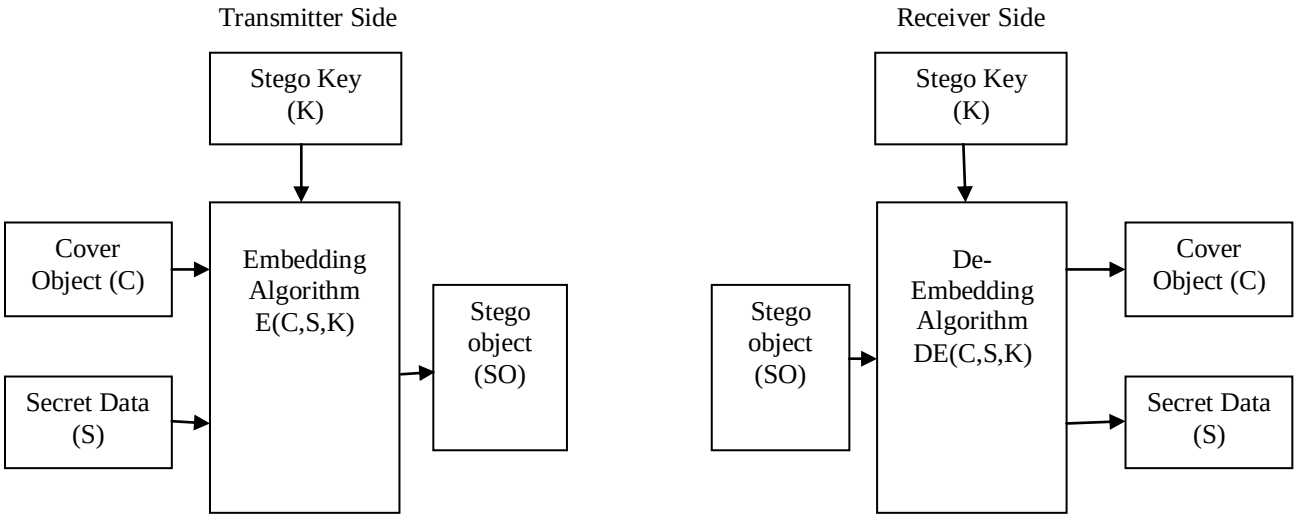

Fig 1. The stagenography model

The model consists of a Cover object (C), Secret data (S) and stego Key (K). The secret message is embedded into cover object which is called the Carrier. Secret data can be any type of confidential data i.e. plain text, cipher text or other

image.[3]. Key is mainly used to ensure that only recipient having the decoding key will be able to retrieve the secret message from the cover object. With the help of 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. The Stego object (SO) which is the output of the process is cover object with embedded secret data.

II. Survey of available Stagenography techniques

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication [4]. In modern approach, depending on the nature of cover object, steganography can be divided into five types.

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

The discussion here is limited to Image and Video Steganography.

2.1 Image Steganography

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion
- Algorithms and transformations

Each of these techniques can be applied, with varying degrees of success.

Review of related study has been conducted on various hiding methods like as Least Significant Bit (LSB), Discret Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT).

LSB [5] insertion is a very simple and common approach to embedding information in an image in spatial domain. The limitation of this approach is vulnerable to every slight image manipulation. Converting image from one format to another format and back could destroy information secret in LSBs. Stego-images can be easily detected by statistical analysis like histogram analysis. This technique involves replacing N least significant bit of each pixel of a contained image with the data of a secret message. Stego-image gets destroyed as N increases. Ahuja and Kaur [11] proposed an image based steganography algorithm that combines LSB with high data hiding capacity, high confidentiality as distortions which can cause suspiscions for the intruders, are removed through filtering techniques and two level high security is applied in the model. Mamta and Sandhu [12] proposed a robust image steganography technique based LSB insertion and encryption.

In frequency domain data can be made secret by using Discrete Cosine Transformation (DCT) [6, 9]. A modification of a single DCT co-efficient will affect all 64 image pixels in that block. One of the modern techniques of Steganography is Discrete Wavelet Transformation (DWT) approach [7, 8]. Battacharya et al. [10] proposed a steganographic technique for hiding multiple images in a color image based on DWT and DCT. Ghasemi et al. [13] proposed to embeds data in IWT coefficients by using a mapping function based on Genetic Algorithm and increase the hiding capacity with low distortions. Peng et al. [14] proposed a method that allows embedding more data bits into smooth blocks while avoiding large distortion generated by noisy ones and thus enables very high capacity with good image quality. Yang et al. [15] proposed a simple reversible data hiding scheme based on IWT. This model shows that both the host media and secret message can be completely recovered, without distortion, if the stego images remain intact.

Prabakaran Ganesan and R. Bhavani [16] proposed a high secure steganography scheme hiding a 256×256 size gray secret image into a 512×512 size gray cover image with different combination of Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). Pixel Value Adjustment (PVA) is first performed on cover image. The secret image values are scrambled by using Arnold transform. The DWT /IWT is applied on both cover and scrambled secret

image. Blending process is applied to both images and compute Inverse DWT/IWT on the same to get the stego image. One nice feature of Haar wavelet transform is that the transform is equal to its inverse.

2.2 Video stagenography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information [4]. The advantage of using video files in hiding information is primarily because video is more secure against hacker attacks due to the relative complexity of video compared to image files and audio files. Video based steganography techniques are mainly classified into spatial domain and frequency domain based methods. Frequency domain techniques are mainly based on discrete cosine transforms (DCT) and wavelet transforms. S. Suma et. al. [17] proposed an integer wavelet transformation in cover video so as to get the stego-video. Where as Li. et. al. in [18] proposed a DCT method for hiding the secret message.. Daniel Socek et. al. [19] proposed a novel video encryption with steganography in digital videos. Tamer Shanableh [20] proposes two data hiding approaches using compressed MPEG video. Subtlety, video-based steganography techniques generally takes such analysis into account and tries to maintain the statistics of the carrier before and after message hiding. Kaushik Dasgupta et. Al. [21] proposed an optimised video steganography using GA(genetic Algorithms).

III. Dual Steganography

Many steganography techniques have been proposed by researchers and have been successfully developed also. The main drawback is if the hackers have any idea about the hidden message they can perform steganaysis of the stego object and can recover the hidden message. The possible solution for this is to apply a two layer security. That is to combine steganography with any other security technique is called **dual steganography**. The PSNR achieved so far for steganography using video file as a cover object is in the range of 28 db to 32 db.
For example : A technique that uses LSB embedding algorithm twice.[3]

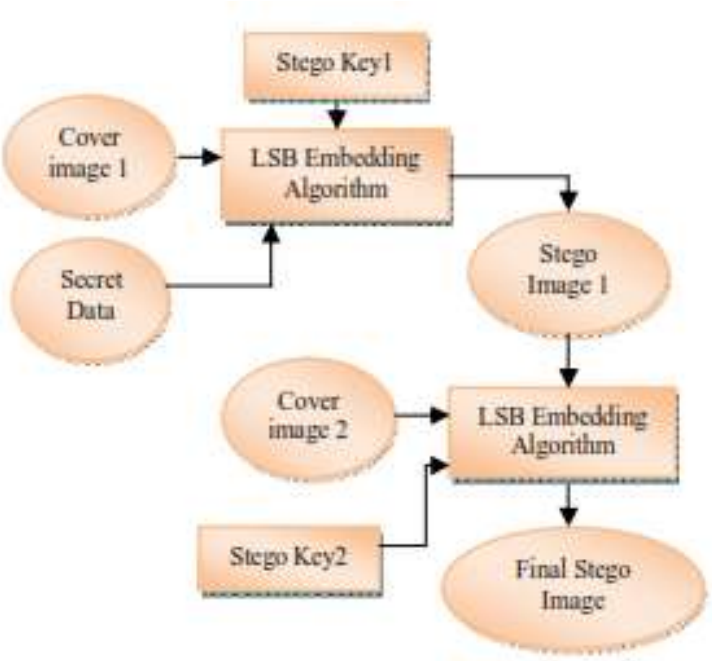

Fig 2. Data Hiding Process

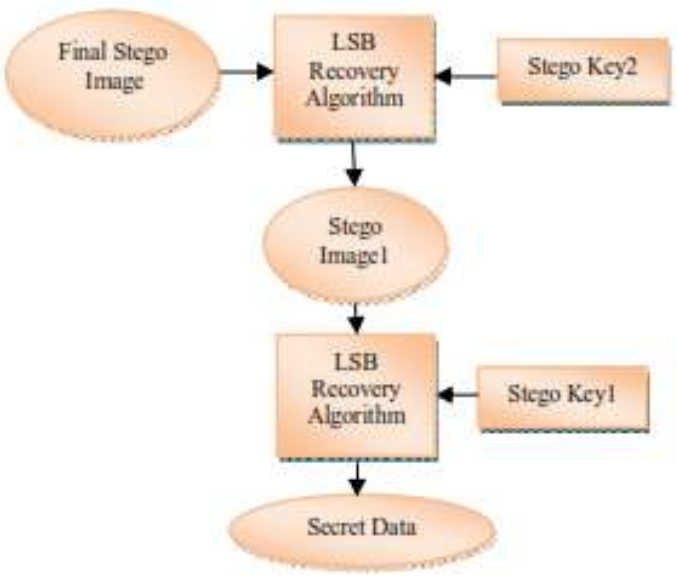

Fig 3. Data Extraction Process

IV. Alternatives for dual steganography

As LSB insertion is a very simple and basic technique, even using it twice may not provide protection against possible steganalysis attack. So in order to have a robust steganography model some other technique must be used for atleast one level. It would be highly desirable not to use LSB insertion for any of the level.

The possible combinations for level one and level two can be as follows.

1. Using neural network and DCT/DWT.
2. Using genetic algorithm and DCT/DWT
3. Using neural metwork and genetic algorithm.

Other combinations are also be possible and algorithms can be developed and tested for various image processing parameters.

V. Conclusion

Many different steganography techniques are available and researchers are continue developing new techniques, The methods of steganalysis also advance rapidly. Since a two layer method provides better security against steganalysis, it must be employed. In the two layer protection also any combination of the available techniques can be used. Ofcourse LSB insertion may be avoided. The most important application of steganography is in the transmitting high security information and also in the field of digitalwatermarking. Authors would certainly wish to protect their work against illegal use and distribution.

REFERENCES

[1] Shailender Gupta, Ankur Goyal & Bharat Bhushan. " Information system for using Least Significant bit Steganography and Cryptography" International Journal Modern Education and computer science. Vol 6.pp27-34,2012
[2] T.Sharp, "An implementation of key based digital signal Steganography",Proc. Information hiding Workshop,Springer,vol.2137 pp 13-26,2001.
[3] Ketki Thakre and Nehal Chitaliya "Dual Image Steganography for Communicating High security information." International Journal for communicating high security information. ISSN :2331-2307,volume-4,Issue-3 July 2014.
[4] *Samir K Bandyopadhyay "A tutorial review on steganography" Conference proceedings of IC3-International conference on computing" organized by UFL(University of Florida) and JIITU on April 21 2008 pp 105-114.*
[5] Chan, C. K. and Cheng, L. M. 2003. "Hiding data in image by simple LSB substitution". *Pattern Recognition* 37:469-474.

[6] Iwata, M., Miyake, K., and Shiozaki, A. 2004. *"Digital Steganography Utilizing Features of JPEG Images",* IEICE Transfusion Fundamentals, E87-A, 4:929-936.
[7] Po-Yueh Chen* and Hung-Ju Lin, "*A DWT Based Approach for Image Steganography",* International Journal of Applied Science and Engineering 2006. 4, 3: 275-290
[8] Ali Al-Ataby and Fawzi Al-Naima, "*A Modified High Capacity Image Steganography Technique Based on Wavelet Transform",* The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010
[9] Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "*Steganographic Approach for Hiding Image in DCT Domain",* International Journal of Advances in Engineering& Technology, July 2011.
[10] Battacharya, T. N. Dey and S.R.B. Chauduri, 2012. " A session based multiple image hiding technique using DWT and DCT." Int. Journal. Computer. Application., 38: 18-21
[11] Ahuja, B. and M. Kaur, 2009. High capacity filter based steganography. Int. Journal . Recent Trends Eng., 1: 672-674.
[12] Mamta, J. and P.S. Sandhu, 2009. Designing of robust image steganography technique based on LSB insertion and encryption. Proceedigs of the IEEE International Conference on Advances in RecentTechnologies in Communication and Computing, Oct. 27-28, IEEE Xplore Press, Kottayam, Kerala, pp: 302-305. DOI: 10.1109/ARTCom.2009.228
[13] Ghasemi, E. J. Shanbehzadeh and B.Z. Azami, 2011. A steganographic method based on integer wavelet transform and genetic algorithm. Proceedings of the International Conference on Communications andSignal Processing, Feb. 10-12, IEEE Xplore Press, Calicut, pp: 42-45. DOI: 10.1109/ICCSP.2011.5739395
[14] Peng, F., X. Li and B. Yang, 2012. Adaptive reversible data hiding scheme based on integer transform. Signal Processing., 92: 54-62. DOI:10.1016/j.sigpro.2011.06.006
[15]Yang, C.Y., C.H. Lin and W.C. Hu, 2012. Reversible data hiding for high-quality images based on integer wavelet transform. J. Inform. Hiding Multimedia Signal Processing., 3: 142-150.
[16] Prabakaran Ganesan and R. Bhavani "A high secure and robust image steganography using dual wavelet and blending model" Journal of Computer Science, 9 (3): 277-284, 2013 ISSN 1549-3636
[17] S. Suma, "Improved Protection in Video Steganography using compressed Video Bitsterams," in International Journal on Computer Science and Engineering, Vol. 02, No. 03, pp. 764–766, 2010.
[18] Y. Li, H.-X. Chen, and Y. Zhao, "A new method of data hiding based on H.264 encoded video sequences," in Proc. IEEE Int. Conf. Signal Processing, ICSP, pp. 1833–1836, 2010.
[19] D. Socek, H. Kalva, Spyros S. Magliveras, O. Marques, D. Culibrk and B. Furht, "New approaches to encryption and steganography for digital videos," in Proc. Multimedia Systems, Springer-Verlag 2007.
[20] Tamer Shanableh, "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering," in Proc. IEEETransactions on Information Forensics and Security, VOL. 7, NO. 2, pp. 455-464, 2012.
[21] Kousik Dasgupta ,Jyotsna Kumar Mondal and Paramartha Dutta. "Optimized Video Steganography using Genetic Algorithm (GA)" International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013. pp. 131-137.