iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review Paper on Digital Image Steganography Techniques

Prof. Meena S. Chavan[1], Sayali S. Chavan[2]
[1,2]Department of Electronics Engineering, Bharati Vidypeeth Deemed University College of Engineering, Pune

Abstract: ***Steganography means covered writing or secret writing. For this secret writing different steganography techniques have been developed. Encryption of secret information is possible and this encrypted information can be hidden behind the original cover file. The main aim of steganography technique is to hide secret data behind image, because image is the basic form of transmitting information in the visual format. In steganography technique the original message is encrypted also stego key is used for protection and this message is hidden into the original image.***
Privacy, security and protection are three main aspect of secret data communication. The various steganography techniques are compared in this paper and taken review for the secret data communication. Mainly this paper is used to provide background to image steganography methods. It includes properties, applications and analysis of different techniques for development of new steganography technique for images.
Keywords: steganography, secret data communication, stego key, protection, image encryption.

I. INTRODUCTION

Steganography means covered writing or secret writing. Steganography is mainly used to hide secret data behind image, because image is the basic form of transmitting information in the visual format. This technique is used for encryption of secret information such as password; text etc. the original message is converted into encrypted form also stego key gives the protection and this converted message is hidden into the original image in steganography technique.
Steganography is the technique in which hidden messages are written like that only sender and intended recipient, can recognize the existence of the message. Steganography is Greek word and its meaning is “concealed writing” Steganos meaning is “covered or protected”, and graphing meaning is “to write”. Steganography is the technique of hiding the message into the carrier. The carrier used in steganography technique may be text file, image file, video or audio file [9].
As computer network is growing very fastly. With this fast growing computer network security of data becomes a main issue. So data hiding techniques are important. Steganography technique is useful in digital copyrights management, information protection and conceals secrets. Data is the backbone of today’s communication. Communication takes place using Internet to distribute information to the masses. So, the privacy and data reliability are required to protect against unauthorized access and use. The concept of steganography is to embed the hidden object into a considerably larger object such as image, video, audio so that the change is undetectable by the human eye.
All digital file formats can be used for steganography technique. The high scale redundancy formats are more suitable in steganography. Digital images are the most popular cover objects used for steganography, because digital images have a large amount of redundant data. This redundant data is required to hide the messages [2].

II. OVERVIEW OF STEGANOGRAPHY

A. Types of Steganography

There are various types of steganography techniques. Those types of steganography techniques are depending on the file formats which are used for data hiding. Almost all digital file formats can be used for steganography technique. The formats having high degree of redundancy are more suitable in steganography.
Figure 1 shows the different types of file formats which can be used for steganography technique. There are four main types they are as following.

B. Steganography

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

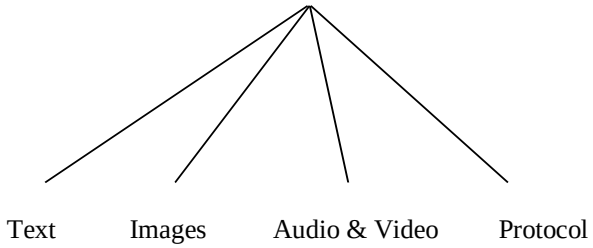


Figure 1: Types of steganography

1) *Text Steganography:* In text steganography text files are used to hide information. In this method, the secret data is hidden behind every nth letter of every words of text message. Different methods are available for hiding data in text file. These methods are as following:
a) Format Based Method;
b) Random and Statistical Method;
c) Linguistics Method.
2) *Image Steganography:* When image is used as cover object for data hiding then it is referred as image steganography. In steganography technique images are the most popular cover objects because there is large number of bits presents in digital representation of an image. In digital images many different image file formats exist, but number if file formats are used for specific applications. For all these different image file formats, different steganographic algorithms exist.
3) *Audio steganography:* In audio steganography data is hiding in audio files. This method hides the data in WAV, AU and MP3 sound files. Different methods of audio steganography are as following:
a) Low Bit Encoding
b) Phase Coding
c) Spread Spectrum.
4) *Video Steganography:* In this technique all kind of files or data is hiding into digital video format. Here video (combination of pictures) is used as carrier for data hiding. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used for data hiding in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI these formats are used by video steganography.
5) *Network or Protocol Steganography:* In Network or Protocol Steganography, information is hiding by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. In the OSI layer network model steganography can be used, where secret channels exists.

III. BLOCK DIAGRAM OF STEGANOGRAPHY

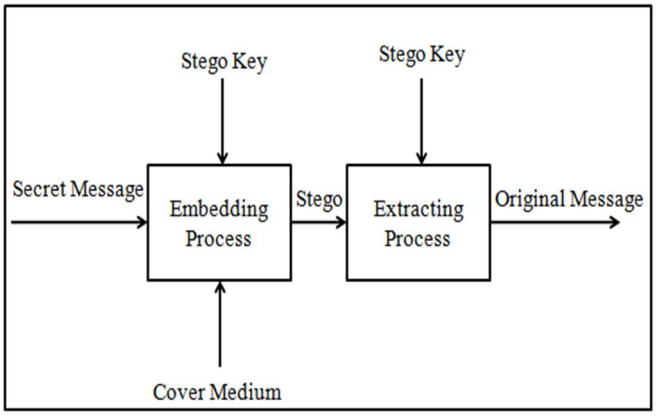


Fig. Block Diagram of steganography

A. *Secret Message*

This is the key data or message which is to be sending out without any destruction to proper destination.

B. Cover Medium

This is the medium which carries the secret message from sender to receiver. All type of files can be used as cover medium such as Text, image, audio, and video.

C. Encoder

This is the main block which embeds the secret message into cover image to produce stego image. LSB or DKL technique can be used for encoding. LSB replacement technique is mostly used. This technique replaces LSB of cover image pixel with secret message bits.

D. Stego Key

It is a sequence of statistics created by the sender for the embedding process and should be employed by the receiver to recover the embedded message. A person cannot access the undisclosed information without the stego key.

E. Stego Image

It is the embedded image formed by hiding secret data into cover image.

F. Extracting process

This block performs reverse operations on stego image for retrieving original image and secret data faithfully.

IV. RELATED WORK

A. LSB Algorithm

The LSB data hiding technique is one of the simplest methods for inserting data into digital signals in noise free environments. LSB (Least Significant Bit) replacement is the process of adjusting the LSB pixels of the carrier image. In LSB both the cover file and the secret message will be converted into the binary format. Then the LSB of some bytes of covered file will be replaced with the sequence of bytes secret message. Generally the right most bit is considered as LSB as it has the least impact over the quality of cover file. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is distorted to the bit of secret message. For JPEG image, the direct substitution of steganographic techniques is not possible hence it will use lossy compression. So it uses LSB substitution for embedding the data into images.

Three main aspect of secret data communication are privacy, security and protection. Least Significant Bit (LSB) technique is used for hiding messages in an image. This technique is harder to extract the original message for unauthorized people. low capacity and more distortion such limitations occur due to hiding process, and because of this distortion the image quality may be degraded, by using color plane process improved approach can be achieved.

B. LSB and SPIHT Based Compression Method

In this method the message image is compressed by using the SPIHT method of lossless compression and then it is encoded in to the other image. Image contains a combination of RGB layers. If we consider a pixel has an 8 bit value then each pixel has the value in the range of 0 to 255.

In this algorithm the secret message image compress by SPIHT and convert in to a binary sequence. Then divides the binary sequence in to a blocks and change the order of block using a key-based randomly generated permutation, concatenates the permuted blocks can be changed in to a permuted binary sequence, and then utilizes the Least-Significant-Bit (LSB) approach to embed the permuted binary sequence into image. When the pixel value changing is completed all the images are placed in a sequential manner. In the decoding side the message image is decoded and decompressed so that we can get the message image [2].

C. DKL Algorithm

Security is very important factor in steganography. So to increase security new technique is developed that is DKL Algorithm. Using DKL algorithm secret message is transferred to the receiver in not identified by any other user or any hacker. So security is provided over the network. Comparison between LSB algorithm and DKL algorithm can be done on the basis of different parameters Mean Square Error, Peak Signal Noise Ratio, Relative Payload and Rate of Embedding such as .to avoid data hacking,

data encryption is done.

Sometimes LSB algorithm is not capable to maintain quality while retrieving original data. So to maintain high robustness and less corruption DKL algorithm is preferred. The key length varies for every cover image based on its pixel. The algorithm can be called "Differing Key Length. The integrity of the hidden messages cannot be destroyed in case of DKL technique.

D. BPCS and IWT Technique

In image steganography technique data hiding or embedding process is done in bit planes of sub band wavelet coefficient which is obtained by using integer wavelet transform (IWT). Bit-Plane Complexity Segmentation Steganography (BPCS) Technique is used to increase data hiding capacity. Error Control Coding is used in the system, which can reduce the Bit Error Rate (BER) of extracted hidden data when the stego image receives some channel distortion.

Using Integer Wavelet Transforms (IWT) reversible image compression methods have been developed. Using IWT image compression, reconstruction of original image is easy and perfect image can be achieved. Also IWT method has lower compression rate as compared to DWT based compression method. The hidden message can be retrieved in lossless manner if the communication channel is ideal. When communication channel is not ideal, the extracted message have some erroneous bits in output. To increase the robustness of the secret message for non-ideal communication channel, we introduce the linear error control coding.

V. CONCLUSION

In the era of fast information interchange using internet and World Wide Web, Steganography has become essential tool for information security. There are many techniques for Image Steganography. The most important aspects of steganography technique are high data hiding capacity; provide more security and less degradation in image quality during recovery of image.

REFERENCES

[1] Xiaochun Cao, Senior Member, IEEE, Ling Du, Xingxing Wei, Dan Meng, Member, IEEE, and Xiaojie Guo, Member, IEEE "High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation" IEEE TRANSACTIONS ON CYBERNETICS, VOL. 46, NO. 5, MAY 2016
[2] M.J.Thenmozhi1, Dr.T.Menakadevi2 "A New Secure Image Steganography Using Lsb And Spiht Based Compression Method" IJOER, Vol-2, Issue-3 March-201
[3] S. Udhayavene∗, Aathira T. Dev and K. Chandrasekaran "New Data Hiding Technique In Encrypted Image: DKL Algorithm" Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015) Computer Science and Engineering, National Institute of Technology, Karnataka, Surathkal, Mangalore 575 025, India
[4] Prashant Johri, Arun Kumar, Amban. Galgotias University, Greater Noida "Review Paper On Text And Audio Steganography Using GA" International Conference on Computing, Communication and Automation (ICCCA2015
[5] Han-Zhou Wu, Student Member, IEEE, Yun-Qing Shi, Fellow, IEEE, Hong-Xia Wang and Lin-Na Zhou "Separable Reversible Data Hiding for Encrypted Palette Images with Color Partitioning and Flipping Verification" 2015 IEE
[6] Deepali G. Singhavi, Dr. P.N.Chatur "A New Method for Creation of Secret-FragmentVisible-Mosaic Image for Secure Communication" ICIIECS'15 2015 IEE
[7] Smita Kuldiwar, Deepa Parasar "Reversible Color Transmission of Compressed Fragment–Visible Mosaic Image" 2015 IEEE International Conference on Computational Intelligence and Computing Research
[8] Tomáš Denemark, Mehdi Boroumand and Jessica Fridrich "Steganalysis Features for Content-Adaptive JPEG Steganography" 2015 IEEE
[9] Richa Khare, Dr. Kuldeep Raghuwanshi "A REVIEW OF VIDEO STEGANOGRAPHY METHODS" International Journal of Research in Advent Technology Volume 2, Issue 1, January 201
[10] Bingwen Feng, Wei Lu, Wei Sun "Secure Binary Image Steganography Based on Minimizing The Distortion on The Texture" 2013 IEE
[11] Gunjan Nehru, Puja Dhar "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 201
[12] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," J. Telecommun. Syst., vol. 52, no. 4, pp. 2237–2247, 2013.
[13] G. Horng, Y. H. Huang, C. C. Chang, and Y. Liu, "(k, n)-image reversible data hiding," J. Inf. Hiding Multimedia Signal Process., vol. 5, no. 2, pp. 152–164, Apr. 2014.
[14] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 40, no. 5, pp. 1280–1293, Oct. 2010.
[15] A. Dabrowski, E. R. Weippl, and I. Echizen, "Framework based on privacy policy hiding for preventing unauthorized face image processing," in Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC), Manchester, U.K., Oct. 2013, pp. 455–461
[16] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005
[17] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 456–465, Sep. 2008.
[18] D. Coltuc, "Improved embedding for prediction based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011
[19] X. Li, B. Ying, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011
[20] K.Thangadurai and G.Sudha Devi, PG and Research Department of Computer Science, Govt., Arts College (Autonomous), Karur, India. "An analysis of LSB

Volume 5 Issue V, May 2017
ISSN: 2321-9653

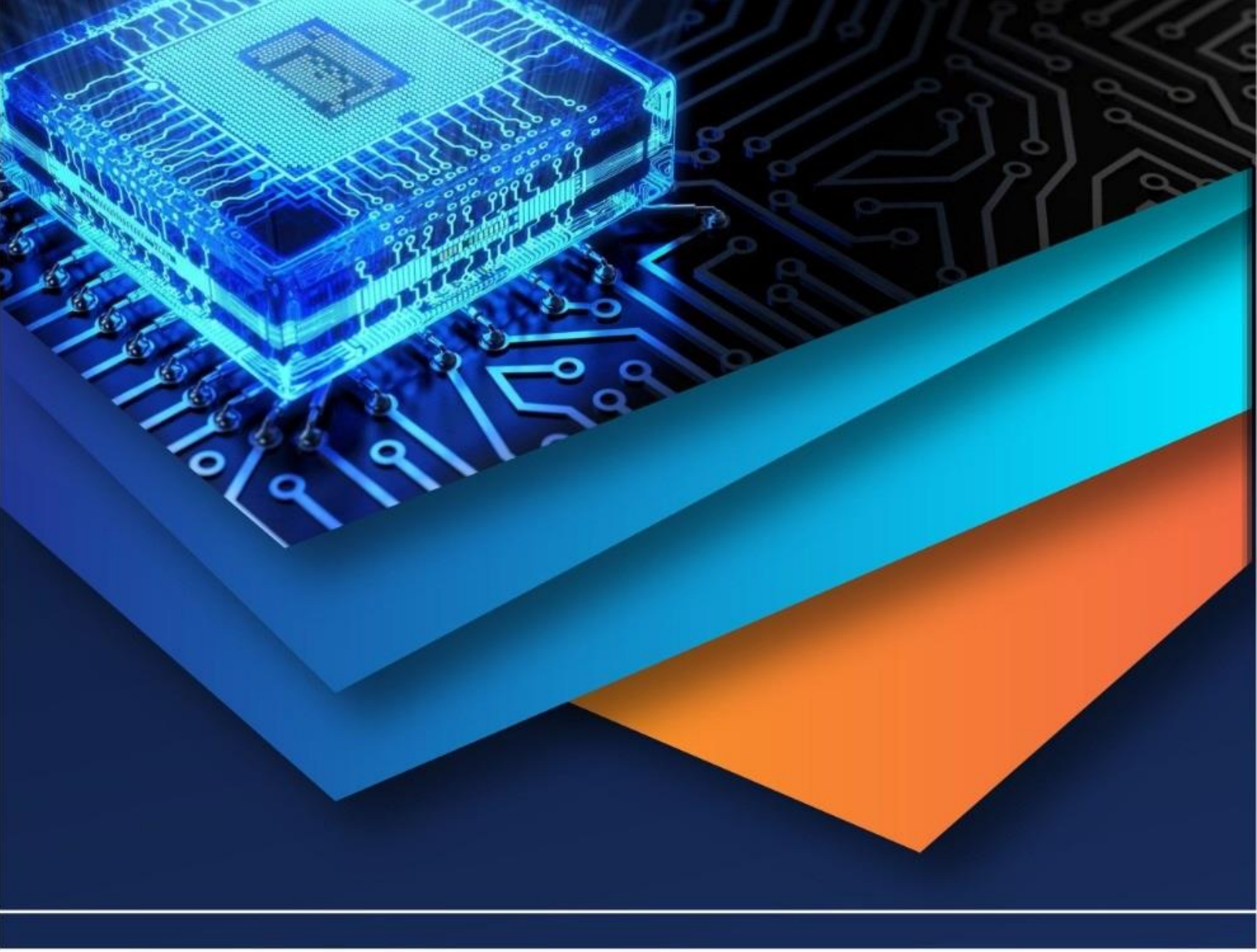
Based Image Steganography Techniques" 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDI

[21] M. S. Hsieh and D. C. Tseng, "Image subband coding using fuzzy inference and adaptive quantization," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 33, no. 3, pp. 509–513, Jun. 2003

[22] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007

[23] M. Cancellaro et al., "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Process. Image Commun., vol. 26, no. 1, pp. 1–12, Jan. 2011.

[24] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.W. Hong, T. S. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY