RA Journal of Applied Research
ISSN (e): 2394-6709
||Volume||4||Issue||01||Pages-1344-1348||January-2018||
Index Copernicus ICV: 74.25, DOI: 10.18535/rajar/v4i1.01

Color Image Steganography Techniques - A Review

Harender Singh[1], *Manjeet Singh*[2]

[1]M.Tech Scholar, ECE Department, Geeta Engineering College Panipat
[2]Assistant Professor, ECE Department, Geeta Engineering College , Paniapt

Abstract: Steganography is defined as the study of covert communication. Steganography ordinarily deals with the ways of hiding. The presence of the communicated data in such a way that it remains secret. It provide secrecy between two communicating parties. In color image steganography, secrecy is achieved by embedding data into cover image and gives a stego-image. There are various types of steganography techniques each have their advantages and disadvantages. In this paper, we review the comparison between two different steganography method name as Jsteg and JMQT that are used to implement a color image steganography. In section 1st we have discussed about introduction.

Keywords: Steganography, Cryptography, LSB, JSteg , JMQT, DCT, PSNR

INTRODUCTION

In today's world, the basic need of every growing area is communication. Everyone wants the privacy and security of their communicating data. In our daily life, we use different path ways like telephone or internet for sharing and transferring the information, but it's not safe at appropriate level. In order to share the information in a confidential manner two techniques could be used. These techniques are cryptography and steganography. In cryptography, with the help of encryption key message is modified that is known to transmitter and receiver only. No one can access the message without using the encryption key. However, the encrypted Message transmission may easily arouse attacker's suspicion, and the message that is encrypted may be intercepted, attacked or decrypted forcedly. In order to conquer the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communication essentially means "to hide data in pain sight".

Thus, steganography is hiding a secret message in such a way that other cannot discern the presence of hidden data. In steganography the process of hiding information data inside may be any multimedia content like image text, audio , video is used for" embedding". The remaining paper consist of given following section: 1. Steganography (how to use and types) 2. Network steganography techniques 3. Conclusion and Future work. In section 2nd we will have discussed about steganography history, steganography Techniques and Factors affecting steganography.

STEGANOGRAPHY

When a steganographic system is developed, it is important to consider what the most appropriate cover Work should be, and also how the stegogramme is to reach its recipient. In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A great deal of attention is paid to

RA Journal of Applied Research
ISSN (e): 2394-6709
||Volume||4||Issue||01||Pages-1344-1348||January-2018||
Index Copernicus ICV: 74.25, DOI: 10.18535/rajar/v4i1.01

ensuring that the secret message goes unnoticed if a third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end.

A) Network steganography techniques

There are three types of Network Steganography . They are :-

1. HICCUPS : it refers to Hidden Communication System for Corrupted Network. HICCUPS is an intra-protocol Steganography system which modifies frames protocol specific fields and their content. It is especially suitable for WLAN.

2. LACK: It refers to Lost Audio Packets Steganography. As their name imply , these techniques exploit lost packets, corrupted packets, and hidden or unused data fields in the VoIP transmission protocol.

3. Protocol Steganography: it is a common name for a group of methods that use another aspect of IP: packet header fields. These field are like sophiscated address labels that identify the contents of data packets to the recipient. All types of protocol steganography are very hard to detect as no trace of them remains anywhere in the network.

In order to brief discussion about these three techniques is that , LACK hides information in packet delays, HICCUP disguises information as natural "natural" or noise, and protocol steganography hides information in unused data fields.

B. Steganography Terminology

Steganography have two terms that is message and cover image. Message is the confidential data that needs to hide and cover image is the carrier that used to hide the message in it.

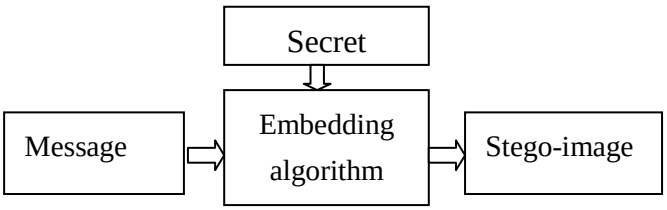

Fig 1: Steganography process

C. Steganography Techniques

1. Spatial Domain Methods: In the intensity of pixel ,the secret data is embedded.. It means Few pixel values of the image are directly changed in procedure of hiding data. Spatial domain techniques are classified into following parts:

i) Least significant bit (LSB) ii)Edge based data embedding method iii) Pixel value differencing (PVD)method iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling orconnectivity method vii) Pixel intensity based.

i) LSB: this is most commonly used method for hiding data. In this method the embedding process is done by changing the least significant bits of image pixels with secret data data bit. The image generate after embedding is similar to Real image due to the changes in the LSB of image pixel does not bring so much variation in the image.

ii) BPCP: In this method image are used by measuring their complexity. Complexity is used to notice the noisy block. By this method bit plan of noisy block are replaced by the binary patterns mapped of a secret data.

iii) PVD: In this segmentation, for embedding the data two consecutive pixels are selected. Payload is determined by using the difference between two consecutive pixels and it refers as for identifying whether both the pixels related to an edge area or smooth area.

2. Spread Spectrum Technique: The spread spectrum technique is used in this method. Secret data is spread over a large bandwidth. The signal

RA Journal of Applied Research
ISSN (e): 2394-6709
||Volume||4||Issue||01||Pages-1344-1348||January-2018||
Index Copernicus ICV: 74.25, DOI: 10.18535/rajar/v4i1.01

to noise ratio in each frequency band should be very small because it creates difficulties to detect the presence of data. Although the parts of data are clear from several bands, still enough information present would be there in other bands to recover the data. Although it is difficult to remove completely the presence of data without destroying the cover entirely. This type of robust techniques is generally used in military forces.

3. Statistical Technique: In this statistical technique input data(message) is embedded by changing some properties of the cover. In this method the cover is splitting into blocks and then embedding one message bit of every block. It modifies the cover block only. when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique: In this technique; the transform domain and frequency domain of cover is used to embed the message. This is one of the most complex method of data hiding in an image. The message is hide in an image by using different algorithm and transformations. Transform domain techniques are classified as

i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits

5. Distortion Techniques: In this method, the secret message is saved by signal distorting. A series of

modification is applied by the encoder to the cover. The differences between the original cover and

the distorted cove are measures by decoder to detect the modifications sequence and then recover the secret message.

6. Masking and Filtering: In this techniques the information is hiding by marking an Image. Steganography only hides the information while watermarks becomes a nectar of the image. More significant area is used to embed the data in this technique rather than hide the data at noisy level. Due to lossy compression there is no threat of image destruction in Watermarking techniques. This method is used 24-bits

D. Factors Affecting a Steganographic Method

The effectiveness of any steganographic method can be determined by comparing stego-image with the cover Image. There are some factors that determines the efficiency of a technique. These factors are:

1) Robustness: Robustness attacks attempt to diminish or remove the presence of a watermark. Although most techniques can survive a variety of transformations, compression, noise addition, etc. Embedding multiple copies of the mark using inverse transformations can increase the resistance to these attacks.

2) Imperceptibility: The imperceptibility means disappearance of a steganographic algorithm. Because it is the first and essential requirement, since the stability of steganography lies in its capability to be unnoticed by the human eye.

3) Capacity: Steganographic capacity is considered as the size of data embedded within a cover image (KB). . The size of the hidden information relative to the size of the cover image is known as embedding capacity. the embedding capacity is likely to be larger than the steganographic capacity.

4) PSNR (Peak Signal to Noise Ratio): The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. *Higher the*

RA Journal of Applied Research
ISSN (e): 2394-6709
||Volume||4||Issue||01||Pages-1344-1348||January-2018||
Index Copernicus ICV: 74.25, DOI: 10.18535/rajar/v4i1.01

value of PSNR, better the image quality.

5) MSE (Mean Square Error):Mean Square Error is used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image.

6) SNR (Signal to Noise Ratio): It is the ratio of the signal power and the noise power. It measures the level of a intent signal to the level of background noise.

E. Application of Steganography

i) secret Communication and confidential Data Storing ii) Protection of Data variation iii) Access Control System for Digital Content Distribution iv) E- Commerce v) Media vi) Database Systems.vii) digital watermarking.

In the next section (3rd) we have discussed about conclusion and future work.

CONCLUSION AND FUTURE WORK

In this research work we reviewed a No. of papers on color image steganography techniques. These papers on color image steganography are good enough and have Vast future scope .By reviewing many papers we observed that most of the work on steganography is done in the last few years.

In these years, Jsteg and JMQT are the most widely used method for color image steganography. many researchers have also used the techniques like digital water marking, distortion technique, Jsteg and JMQT method of steganography in their work and maintain a strong means of safe ,accurate and secure information transmission. Most of the papers that are discussed here are taken from various sources like technical books, previous IEEE papers and ITU-T standards.

This review paper is enough for us to start our work in this field. Various security and data hiding techniques are used to implementation of steganography using LSB,ISB, MLSB . different methods are used like JPEG, Jsteg and JMQT etc. In further research we are going to compare the different various methods of color image steganography to make more secure communication.

REFERENCES:

1. Almohammad and G. Ghinea 2015, "Image Steganography and Chrominance Components,"10th IEEE International Conference on Computer and Information Technology (CIT 2015).
2. J.G.Yu1, E.J.Yoon2, S.H. Shin1 and K.Y. Yoo 2015, "A New Image Steganography Based on 2k Correction and Edge-Detection", Fifth International Conference on Information Technology: New Generations 978-0-7695-3099-4/08, April 2015.
3. G. Sahoo1 and R. K. Tiwari2 2015, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2015.
4. N. N. EL-Emam 2014, "Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm," International Journal of Information and Communication Engineering, 4:2, 2014.
5. N.N. EL-Emam 2014, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm," Journal of

RA Journal of Applied Research
ISSN (e): 2394-6709
||Volume||4||Issue||01||Pages-1344-1348||January-2018||
Index Copernicus ICV: 74.25, DOI: 10.18535/rajar/v4i1.01

Computer Science, vol.3(4), pp. 223-232, 2014, ISSN 1549-3636.

6. L. M. Marvel, Member 2014, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 2014.
7. J. He, S. Tang and TingtingWu 2014, "An Adaptive Image Steganography Based on Depth-varying Embedding," Congress on Image and Signal Processing, vol.5, 2014, pp. 660-663, DOI 10.1109/CISP.2008.189
8. S .K. Moon, R.S. Kawitkar 2014, "Data Security using Data Hiding," International Conference on Computational Intelligence and Multimedia Applications 2014.
9. S. M Thampi 2014, "Information Hiding Techniques: A Tutorial Review," ISTE-STTP on Network Security & Cryptography, LBSCE 2014.
10. C.Y. Yang 2014, "Color Image Steganography Based on Module Substitutions," Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication: 2014 ISBN:0-7695-2994-1.
11. D.C. Lou and C.H. Sung 2013, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem," IEEE Transactions on Multimedia, VOL. 6, NO. 3, JUNE 2013.
12. K. Curran, K. Bailey 2013, "An Evaluation of Image Based Steganography Methods," International Journal of Digital Evidence Fall 2013, Volume 2, Issue 2.
13. J. Fridrich, M. Goljan 2012, Binghamton, "Practical Steganalysis of Digital Images – State of the Art," Conference, San Jose CA, ETATS-UNIS (21/01/2012).
14. C.C. Chang, T.S. Chen, L.Z. Chung 2012, "A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol.141, pp. 123–138, 2012.
15. K. Rabah 2004, "Steganography-The Art of Hiding Data," Information Technology, Journal, vol.3 (3), pp. 245-269, 2004, ISSN 1682-6027.
16.