Image Steganography Technique to Increase Security of Images: A Review

Shilpa Goyal
Department of Computer Engineering
Govt. Engineering College Bikaner
Bikaner, India
sgoyal.ecb@gmail.com

Maninder Singh Nehra
Assistant Professor CE department
Govt. Engineering College Bikaner
Bikaner, India
maninder4unehra@yahoo.com

ABSTRACT

The image processing is the technique which is used to process the image pixels for different purposes. The image data is very sensitive. To provide security to image data, various techniques has been proposed in the recent times. Among the various proposed techniques, image steganography is one of the most efficient technique which provides greater security to the image data. In the image steganography the sensitive data can be hidden inside the image. The two steps are involved to implement image steganography, in the first step properties of the image are analyzed and in the second phase encoding scheme is implemented to generate final steganography image. In this paper, various techniques of an image steganography are analyzed and reviewed in terms of various parameters.

Keywords

Steganography, information hiding, image properties

1. INTRODUCTION

Digital image processing is a rapidly growing technology which is used in medical, defense, agriculture, transmission and encoding and many other fields. The method processes digital images as input to extract some important features from it as an output. Image processing is an essential process of analysis and manipulation of the digital images to improve image quality by applying some efficient algorithms on it [1]. Steganography is a very popular technique for hiding any kind of information into cover media (audio, video, image, text) in such a manner that no one can imagine that a secret data exists behind the cover media [2]. It provides a secure communication between two intended parties. Performance of steganography depends on two important factors. The first one, embedding efficiency refers to the amount of secret data can be hidden in the cover media. The second one is embedding payload, refers to the capacity of the cover media to hide as much as data with minimum distortion.

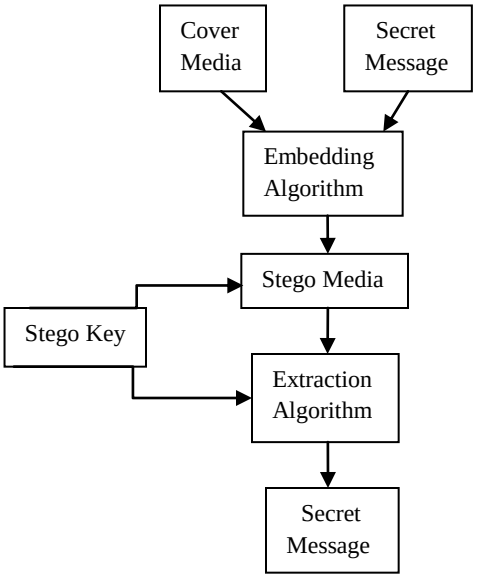

Fig. 1 General stegographic model

1.1.Video Steganography

In video steganography, a secret data is hidden into a cover video. Video has a large capacity to hide secret information than a cover image. Video decomposes into a number of frames and then the encoded secret message is embedded into a selected video frame which provides greater security than image steganography.

The process of message embedding is based on two techniques i.e. spatial domain and transform domain.

Spatial Domain Video Steganography

There are several methods which are widely used for video steganography, based on spatial domain. These methods change the image pixel values for hiding secret data.

A. Least Significant Bit (LSB)

It is a very popular method for hiding the bits of secret message in the least significant bits of cover image pixels. The resulted stego image looks very similar to the original image [3]. The hiding capacity of LSB method can be increased by using up to 4 least significant bits of each pixel which is also quite hard to detect. This method is very simple and less robust. It has high embedding capacity, high visual quality and high detectability.

B. Pixel Value Differencing (PVD)

In this method, for embedding a secret message, the cover image is divided into non-overlapping blocks of two consecutive pixels. To determine how many bits of secret message should be embedded inside a cover image, the difference between two consecutive pixels values is computed [4]. Large difference value is to be considered in edge area and small difference value is to be considered in smooth area. Human eyes are very sensitive to the noise in smooth area rather than in the edge area. So the difference value is replaced by another value to embed the secret message bits. This method has high imperceptibility and high embedding capacity.

C. RGB based Steganography

A digital image is a group of pixels that represent light intensities at various points. An image can be stored as 24-bit (RGB) or 8-bit (Gray scale) files. A 24-bit colored image is quite large, however it provides more space for hiding secret information. Each pixel is the combination of three primary colors (Red, Green, and Blue), which are individually represented by 1 byte (8 bits). RGB steganography method overcomes the problem of sequential fashion and the use of stego key for selection of pixels [5].

Transform Domain Video Steganography

Transform domain technique does not hide the secret data behind the image pixels [6]. This method is basically used for transforming image pixels from time domain to frequency domain before hiding a secret data. There are two most widely used steganography techniques as follows:

A. Discrete Cosine Transform (DCT)

In this transformation technique, embedding of secret message depends on the DCT coefficients. If any DCT coefficient value is above from a specific threshold then that will be a potential place for the insertion of secret data. This technique is used in common image compression formats like JPEG and MPEG. It splits an image into a no. of spectral sub-bands along with its visual quality (high, middle and low frequency components). It is more suitable for low frequency sub-band.

B. Discrete Wavelet Transform (DWT)

DWT is a well-known transformation domain technique in which wavelets are discretely tested [7]. There are two operations i.e. horizontal and vertical. Firstly, scan the pixels from left to right in horizontal plane. Then, perform addition and subtraction operations on neighboring pixels. Store the sum on the left that represents the low frequency part denoted as 'L' and store the difference on the right which represents the high frequency part of the original image, denoted as 'H'. Repeat these operations until all rows are covered. Secondly, scan the pixels from top to bottom in vertical plane. Then, perform additional and subtraction operations on neighboring pixels. Store the sum on the top and the difference on the bottom. Repeat these operations until all the columns are covered. Finally we will get 4 sub-bands denoted as LL, LH, HL and HH respectively. The LL is a low frequency sub-band that looks similar to the original image. LH, HL and HH are the middle and high frequency sub-bands that contain detailed information about an image i.e. edges and textures of an image [8]. It is more suitable for embedding without being notice by the human eyes.

2. RELATED WORK

TABLE 1: COMPARISION OF IMAGE STEGANOGRAPHY TECHNIQUES

Ref. No.	Author	Year	Techniques Description	Outcomes	Limitations
[9]	Ramadhan J. Mstafa and Khaled M. Elleithy	2014	Secret data is encoded by using hamming code and then embedded into randomly selected video frame.	High embedding efficiency, highly secure and gives high PSNR (> 51dB) values.	When embedding capacity increases up to 90 Kbits in each frame, results in some degradation of visual quality.

[10]	Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale	2015	Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) video steganography techniques and random LSB audio steganography technique are used.	Highly secure and reduces embedding distortion.	-----
[11]	Ramadhan J. Mstafa and Khaled M. Elleithy	2015	BCH encoding and Discrete Wavelet Transformation is used to hide secret message inside a selected video frame. The algorithm is tested under two types of videos which contain slow and fast motion objects.	High embedding payload (6.12 Mbytes), High visual quality and hidden ratio is approximately 28.12%.	Non robust against all attacks and LSB method is susceptible to many attacks.
[12]	Pillai,Mundra Mounika,Pooja JRao,Padmamala Sriram	2016	K-mean clustering technique is applied on image and then data insertion is done in each cluster.	High imperceptibility and security.	-----
[13]	C. Lalengmawia, A. Bhattacharya	2016	Advanced Encryption Standard algorithm is proposed to generate random pixel positions and determines the size of Least Significant Bits for embedding the information dynamically.	High embedding capacity, high visual quality and security.	This method is applicable only for uncompressed image formats.
[14]	N.Jothy and S.Anusuyya	2016	Integer Wavelet Transform (IWT) method is applied on image to transmit the secret information to the receiver independently.	High visual quality and high PSNR values compared to other methods.	------
[15]	Ramandeep Kaur,Pooja,Varsha	2016	The proposed hybrid approach based on video steganography is a combination of RSA asymmetric key based encryption, Edge detection, Identical match and 4LSB substitution techniques.	High visual quality, high security, high embedding capacity (128 KB), high PSNR and low MSE & BER.	------
[16]	Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi	2016	Two meta-heuristic approaches are combined with LSB method i.e. Local Search (LS) and Stochastic Local Search (SLS) are applied on image.	This combined method improves the effectiveness and performance of the LSB method and also gives infinity PSNR.	Only single LSB method is not so effective to hide secret message in JPEG image.

3. EVALUTION AND ANALYSIS

3.1. Mapping Study Plan Execution:

In this column, the description of the plan for execution is given step wise.

A. Conduction of Search

The various data bases like IEEE Xplore and Springer are searched with different strings and it is found that total number of 328 research papers have been published in the recent years. In the table 2, the individual database results are given.

TABLE 2: SEARCH STRING RESULT OF VARIOUS DATABASES

INDEX	DATABASE	RESULT
1	IEEE Xplore	143
2	Springer	185
TOTAL		**328**

B. Criteria for Efficient Result Extraction

The study is being conducted to check the authentication of the 328 papers which are searched with the search string criteria from the different databases. The 328 papers have been put into the plagiarism checker tool and we are only left with 223 papers which are unique and not copied from anywhere. The unique papers are analyzed manually and it is found that only 115 papers which represent different video steganography techniques for hiding seceret message behind the cover video and remaining papers are based on other steganography techniques. The search string is based on video steganography. In the end result we achieved only 40 papers which represent the security concerns of the video steganography.

C. Results

This step illustrates the data of paper publication year wise.

- *Year*
  In the figure 3, it shows the percentage of papers which are being published from 2014 to 2017.

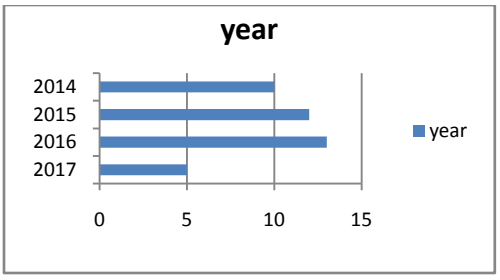

Fig. 3 Percentage of papers published year wise

- *Country of Authors*
  The contribution of authors from China is 25% and rest 30% is published by the European authors. 45% papers have been published by the India authors.
- *Published in Conference or Journals*
  In the Fig 4, it shows the percentage of papers published in Conference or Journals. From the data which is collected from the search string, it is being analyzed that 60% of the papers have been published in the conferences and rest of the 40% papers have been published in journals.

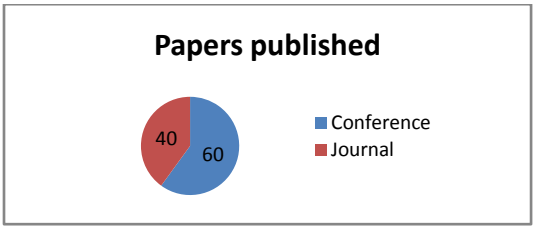

Fig. 4 Paper published for Research

4. CONCLUSION

In this paper, it is been concluded that various techniques has been proposed in the recent times to implement image steganography. The image steganography involves two phases. In the first phase, image properties are analyzed and in the second step technique of image encoding will be applied which will generate final stego image. In future, various techniques of video steganography will be reviewed and analyzed in terms of various parameters.

REFERENCES

[1] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in Image and Signal Processing (CISP), 2011 4th International Conference on, 2011, pp. 1784-1787.

[2] Shashikala Channalli and Ajay Jadhav, "Steganography an art of hiding data", International Journal of Computer Science and Engineering Vol. (3), pp.137-14I, 2009.

[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, (2012): Steganography Using Least Significant Bit Algorithm, International ournal of Engineering Research and applications, vol.2, issue 3, pp: 338-341, May-June2012.

[4] H.C. Wu, N.I.Wu, C.S. Tsai, and M.S. Hwang, "An Image Steganography Scheme Based on Pixel Value Differencing and LSB Replacement Methods", *IEEE Proceedings- Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611–615, Oct 2005.

[5] Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur "A Dynamic RGB Intensity Based Steganography Scheme" World Academy of Science, Engineering and Technology, pp. 630-633, 2010 .

[6] Niels Provos, Peter Honeyman.(2003): "Hide and Seek: An Introduction to Steganography", IEEE SECURITY and PRIVACY, MAY/JUNE 2003.

[7] G. Prabakaran and R. Bhavani, "A modified secure digital image steganography based on discrete wavelet transform", in International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012, pp. 1096-1100.

[8] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel dwt based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612 – 618, 2015, proceedings of the International Conference on Information and Communication Technologies, ICICT, 2014, 3-5 December 2014 at Bolgatty Palace and Island Resort, Kochi, India.

[9] Ramadhan J. Mstafa and Khaled M. Elleithy, "A highly secure video steganography using hamming code (7,4)", 2014.

[10] Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale," Audio-Video steganography", 2015, IEEE, 978-1-4799-6818-3.

[11] Remah Alshinina, Khaled M.Elleithy et al. "A High Payload Video Steganography algorithm in DWT Domain based on BCH (15, 11)". IEEE, 2015, doi: 10.1109/WTS.2015.7117257.

[12] Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram," Image steganography method using K-means Clustering and Encryption techniques", 2016, IEEE, 978-1-5090-2029-4.

[13] C. Lalengmawia, A. Bhattacharya, and A. Datta," Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data", 2016, IEEE, 978-1-4673-9802-2.

[14] N.Jothy, S.Anusuyya," A Secure Color Image Steganography Using Integer Wavelet Transform", 2016, IEEE, 97698542-3234-346-7.

[15] Ramandeep Kaur,Pooja and Varsha, "A hybrid approach for video steganography using edge detection and identical match techniques", 2016,IEEE, 978-1-4673-9338-6.

[16] Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi," Stochastic Local Search Combined with LSB Technique for Image Steganography", 2016, IEEE,9587965-3489-5765-45.