International Journal of Management, IT & Engineering
Vol. 12 Issue 8, August 2022,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Increasing Security of Images through Image Steganography: A Review

Prof. Pankaj Nandan
Associate Professor in Computer Science
Govt. College for women, Kathua (J&K)
Rakhi Billawaria
Lecturer in Computer Science
GDC Reasi, J&K.

Abstract

The image processing is the method which is employed to process the image pixels for different objectives. The image data is very sensitive. In order to provide security to image data, various techniques has been proposed in the present times. Among these numerous proposed methods, image steganography is one of the most efficient techniques and methods which provide greater protection 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 discussed and reviewed in terms of various parameters.

Keywords: Steganography, Information hiding, image properties.

Introduction

Digital image processing is a quickly growing technology which is employed in medical, defense, agriculture, transmission and encoding and many other fields. The method processes digital images as input to extract some significant aspects from it as an output. Image processing is an important process of analysis and manipulation of the digital images to advance image quality by submitting some efficient algorithms on it.

1. Steganography is very famous and unique instrument for concealing any kind of information into cover media (audio, video, image, text) in such a way that no one can imagine that a secret data exists behind the cover media.

2. It provides more protective communication between two intended parties. Performance of steganography depends on two important factors. The first one, embedding efficiency deals with 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.

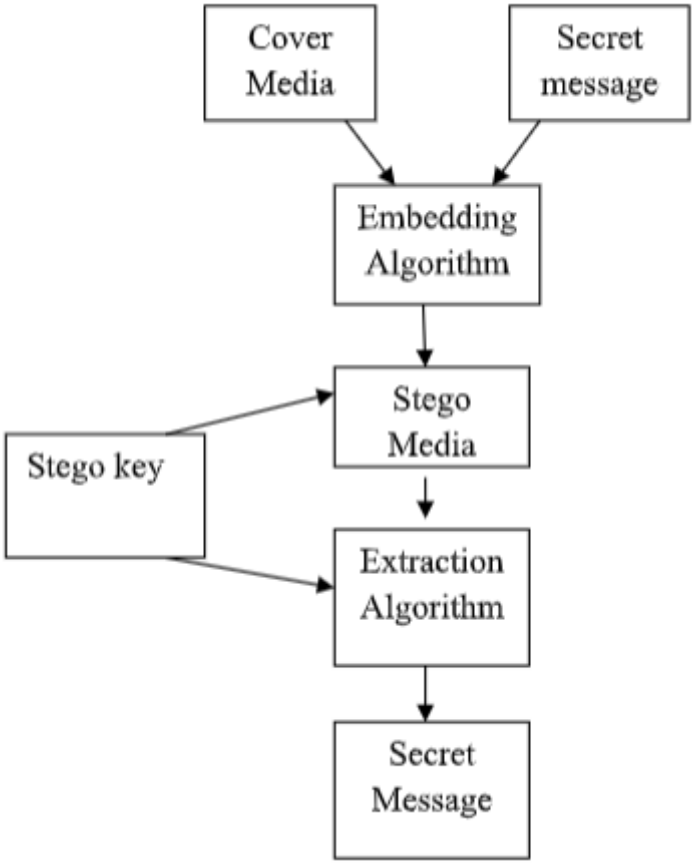

Figure:Common Stegangraphic Model

Video Steganography

In video steganography, a secret data is concealed into a cover video. Video has an enormous capacity to hide secret data than a cover image. Video decomposes into a number of frames and then the encoded secret message is implanted into a selected video frame which bestows greater security than image steganography. The process of message embedding dependsupon two techniques i.e. spatial domain and transform domain.

Spatial Domain VideoSteganography: There are multiple methods which are extensively employed 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 one of the famous techniques 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 concealing ability of LSB method can be enhanced by employing 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 inserting 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 collection of pixels that shows 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 sensitive data. Each pixel is the amalgamation 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 databehind 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 method, inserting of secret message depends on the DCT coefficients. If any DCT coefficient value is above from a specific threshold then that will be a possible location for the insertion of secret data. This technique is employed in general image compression formats like JPEG and MPEG. It divides an image into a number 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 method 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 shows the low frequency part denoted as L and collect the variation on the right which highlights 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. Reiterate these operations until all the columns are covered. Finally we will get 4 sub-bands indicated as LL, LH, HL and HH respectively. The LL is a low frequency sub-band that looks analogous to the original image. LH, HL and HH are the middle and high frequency sub-bands that comprises 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.

EVALUTION AND ANALYSIS

Mapping Study Plan Execution:

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

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 andleft 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 divergent video steganography methods for concealing secret

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.

4. CONCLUSION

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

Bibliography

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.

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

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.

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.

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 .

Niels Provos, Peter Honeyman.(2003): “Hide and Seek: An Introduction to Steganography”, IEEE SECURITY and PRIVACY, MAY/JUNE 2003.

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.

Ramadhan J. Mstafa and Khaled M. Elleithy, “A highly secure video steganography using hamming code (7,4)”, 2014.

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.

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