Different Techniques of Image and Video Steganography: A Review

Article · January 2015

CITATIONS
6

READS
777

3 authors, including:

Harbinder Singh
University of Castilla-La Mancha
50 PUBLICATIONS **432** CITATIONS
SEE PROFILE

Shikha Sharda
Punjab Remote Sensing Centre
13 PUBLICATIONS **109** CITATIONS
SEE PROFILE

Different Techniques of Image and Video Steganography: A Review

Abhinav Thakur[1], Harbinder Singh[2], Shikha Sharda[3]
[1,2]Electronics and Communication Department ,Baddi University
[3]Electronics and Communication Department, UIET Panjab University
([1]harbinder.ece@baddiuniv.ac.in,[2]abhinav28libra@gmail.com, [3]shikhasharda29@gmail.com)

***Abstract*- Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. It can also be defined as an invisible communication that hides the existence of the communicated message so that the message does not attract the attention from eavesdroppers and attackers. The main objectives of steganography are robustness against various image processing attacks, capacity of the hidden data and undetectability. This paper explores the different methods of image and video steganography that are used to hide the message in digital carriers.**

***Keywords*- Frequency domain, Image steganography, Spatial domain, Video steganography**

1. INTRODUCTION

In today's scenario of high speed internet, people are worried about the information being hacked by attackers. However, the safety and security of long distance communication remains an issue. So in order to overcome this problem many algorithms of steganography have been proposed.

The word steganography is derived from the ancient Geek words steganos meaning "covered, concealed, or protected" and graphein meaning "writing". There are other two technologies which are closely related to steganography [1]. One of them is watermarking. In a digital watermarking technique, a signal is permanently embedded into digital data like audio, image, video and text. It can be detected or extracted afterwards to confirm the authenticity of the data. Second is the fingerprinting, in which unique marks are embedded in the copies of carrier object that are supplied to different customers. Basically, these two properties are used for intellectual property protection [1].

The idea and practice of hiding information has been used in various forms for thousands of years. Five hundred years ago, Jerome Cardan, an Italian mathematician, proposed a Chinese ancient method of secret writing where a paper mask with holes is used. In this method, user needs to write his secret message in such holes after placing the mask over the blank sheet of paper. Then take the mask off and fills the black parts of the page and in this way the message appears as innocuous text [2].

The performance parameters that can used to measure the quality of the stego video or image are Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). One of the most important properties of the steganographic system is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. The other properties are the robustness which refers to how well the steganographic system resists the extraction of hidden data and capacity, which is the maximum information that can be safely embedded in a work.

There are different kinds of file format that can be used for steganography, but the image and audio files are used by researchers for their studies because they have high degree of redundancy [3]. There are four different file formats that are used for steganography are shown in Fig.1.

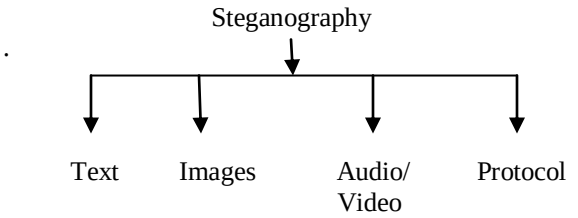

Fig. 1 Different categories of steganography

This paper is organized as follows. Section II discusses the spatial domain and frequency domain techniques used in image steganography. Section III describes video steganography techniques. Finally, section IV gives the conclusion.

II. IMAGE STEGANOGRAPHY

In image steganography, a secret data (image or text) can be embedded in the cover image. A basic model of image steganography is shown in Fig. 2.

Let X represents the cover image and Z the stego-image. Let K be a secret key and M be the secret message that the sender wishes to send. Then E_m represents an embedded message and E_x represents the extracted message. Therefore,

E_m: X⊕ K⊕ M ⟶ Z
∴ E_x (E_m(x,k,m)) ≈ m,∀x ∈ X, k ∈ K, m ∈ M

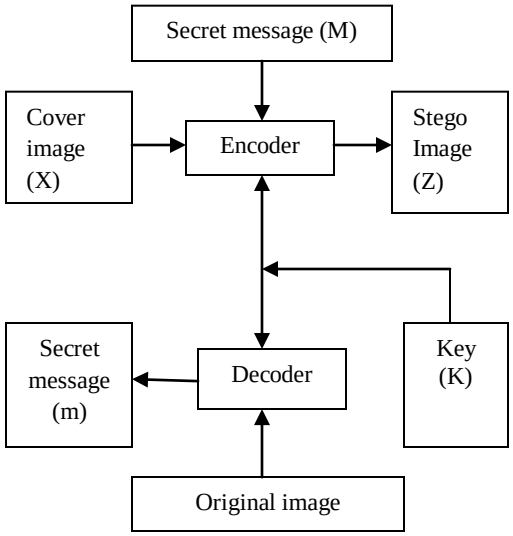

Fig.2 Encoder and decoder of steganographic system

A. Spatial Domain Steganography Technique:

In this approach, the least significant bits of the cover image are replaced with secret image without modifying the complete cover image. LSB is the most common and simplest method for data hiding [4]. Another method of steganography was proposed to hide a secret data into a gray cover image [5]. In this, a cover image is partitioned into blocks of two consecutive pixels. This technique of hiding the secret data gives better result as compare to LSB techniques. The main drawback of LSB technique is the ease of extraction. So to overcome this drawback researcher found better way for embedding the secret message so that it don't attract the eavesdroppers.

B. Frequency Domain Steganography Techniques:

The data can be easily transmitted through internet at very high speed but security remains an issue. Spatial domain techniques are more prone to attacks. Many other algorithms have been proposed by researchers which are less exposed to image processing attacks. A histogram shifting method based on DCT coefficients was proposed for data hiding [6]. Cover images are partitioned into different frequencies. In this approach, secret data is embedded in the high frequency. This method improves the hiding capacity of secret data and quality of the stego images. On reversing the frequency domain stego image back to spatial domain image, this method of histogram shifting may cause underflow and overflow problems.

In last few years, wavelets are being used in most of the steganography techniques. It has been observed that wavelets based techniques are more robust against image processing attacks as compare to LSB based techniques. Prabakaran G. [7] introduced a new and secured algorithm for hiding a large-size data into a small size cover image. In this method, scrambling of secret image is done by Arnold transformation [8]. Discrete Wavelet Transform (DWT) is used to decompose the secret and cover images.

There are three different image quality parameters named as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Maximum Difference (MD) that are used to measure the image quality of stego-image [7].

- Mean Square Error (MSE)

  $MSE= \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2$

- Peak Signal to Noise Ratio (PSNR)

  $PSNR= 10 \log \left(\frac{C_{max}^2}{MSE}\right)$

- Maximum Difference (MD)

  $MD= \text{Max}(|C_{xy} - S_{xy}|)$

Where x and y represents image coordinates, M and N are the image dimensions, S_{xy} is the stego image obtained after encoding and C_{xy} is the cover image. C_{max}^2 is the maximum value in the image. Greater the value of PSNR better is the image quality.

III. VIDEO STEGANOGRAPHY

In video steganography, secret data is embedded in cover video. A basic model of video steganography is shown in Fig. 3.

In this section, some important techniques of video steganography are discussed in brief. One of

the simplest and common methods is Least Significant Bit (LSB) technique. In this method, LSB of cover video is replaced by secret data [9]. But this technique of hiding the secret data is not much effective as the data may lose after some file transformations [10] and [11]. A new method based on Discrete Cosine Transform (DCT) transformation has been introduced [12]. The main focus of this paper is to increase the capacity to hide the secret data.

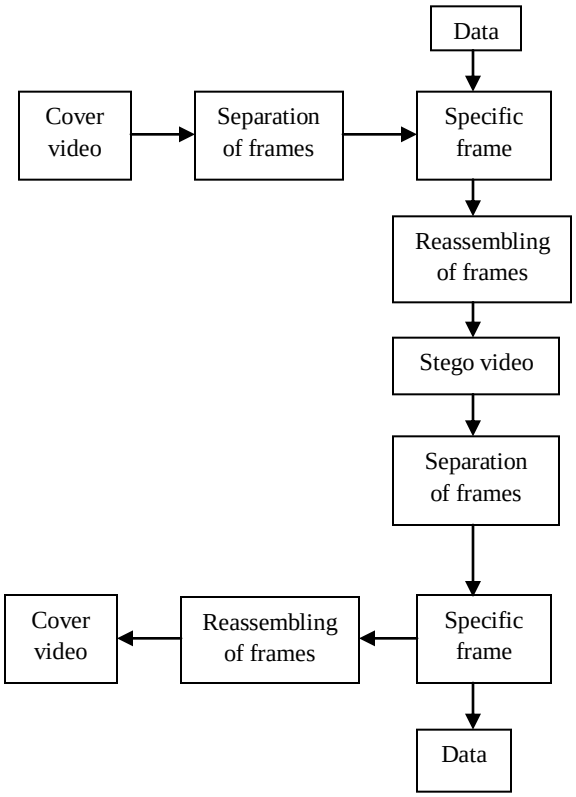

Fig.3 Video steganography model

A. Spatial Domain Steganography Techniques:

A methodology based on Least Significant Bit (LSB) was introduced [13] in which secret data is embedded into the LSB of the host video frame. The quality of the stego video can be measured by using performance parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). A secure technique of video steganography was proposed [14]. This method provides index to secret data and the index is then placed in a video frame. At the receiving end, inspite of searching the whole video, the secret data can be retrieved from stego video with the help of index. This will reduced the computational time as compare to other existing methods. An improved method of data hiding based on back propagation neural network method was proposed [15]. In this method, neural network is used to perform XOR operation. Secret data is embedded into avi video format by using LSB substitution technique.

B. Frequency Domain Steganography Techniques:

A high payload capacity video steganography method was introduced [16]. It uses Lazy lifting wavelet transform technique for hiding the secret information. Firstly wavelet is applied on the video frames and then LSB substitution method is used to hide data in the coefficients of video frames. A new data hiding technique based on Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) was proposed [17]. This is based on the Markov-process in JPEG image steganalysis and used to detect the hidden message in stego video. A wavelet and Bit Plane Complexity Segmentation (BPCS) based video steganography method was introduced [18]. In this paper, 3-D SPIHT-BPCS steganography and motion-JPEG 2000-BPCS steganography are discussed. This technique results in high payload capacity.

VI. CONCLUSION

Steganography is the technique that provides confidential communication between two parties. In this paper, main techniques of image and video steganography are discussed. Each steganography technique must satisfy the three main objectives (imperceptibility, capacity and robustness).

In image steganography, it has been observed that frequency based techniques are more robust as compared to spatial domain techniques. The embedding of secret data in the DWT domain gives better result as compare to LSB and DCT embedding.

In case of video steganography, wavelet transform based techniques are more robust. Also the combination of LSB and wavelet transform can improve the performance of the steganographic system. LSB based techniques results are also good and can be improved by combining this technique with artificial intelligence, fuzzy logic neural network. It is the fast growing and upcoming field and has a great scope for research and development.

REFERENCES

[1] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[2] S.B. Sadkhan., "Cryptography: Current status and future trends", in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.
[3] T Mrkel,JHP Eloff and MS Olivier ."An Overview of Image Steganography,"in proceedings of the fifth annual Information Security South Africa Conference, 2005
[4] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSB substitution", Pattern Recognition, vol 37, pp.469-471, 2003.
[5] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.
[6] Yih-Kai Lin, "High capacity reversible data hiding scheme based upon discrete cosine Transformation", The Journal of Systems and Software 85 (2012) 2395– 2404.
[7] Prabakaran. G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].
[8] Lingling Wu et al., "Arnold Transformation Algorithm and Anti-Arnold Transformation algorithm", the 1st International conference on information Science and Engineering (ICISE2009).
[9] C.S. Lu: , "Multimedia security: steganography and digital watermarking techniques for protection of intellectual property". Artech House, Inc (2003).
[10] J.J. Chae and B.S. Manjunath:, "Data hiding in Video" Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).
[11] Provos, N., Honeyman, P., "Hide and Seek: An Introduction to Steganography" IEEE Security & Privacy Magazine 1 (2003).
[12] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.
[13] MrudulDixit, "Video Steganography", International Conference on Pervasive Computing (ICPC) 2015.
[14] Balaji R., "Secure Data Transmission Using Video Steganography", IEEE international conference on Electro/Information Technology (EIT) 2011
[15] Richa K., "Video Steganography by LSB Techniqueusing Neural Network", Sixth International Conference on Computational Intelligence and Communication Networks 2014
[16] Patel, K., "Lazy Wavelet Transform Based Steganography in Video", International conference on communication systems and network technologies (CSNT) 2013.
[17] Qingzhong Liu,"Video Steganalysis Based on the Expanded Markov and Joint Distribution on the Transform Domains Detecting MSU Stego video" 2008. ICMLA '08. Seventh International Conference on Machine Learning and Applications.
[18] Noda, H., "Application of BPCS steganography to wavelet compressed video", Image Processing, 2004. ICIP '04. 2004 International Conference on (Volume:4)