A Survey Paper on Video Steganography

Ankita Patel[1] Ajay Barot[2]
[1]M.Tech. Student [2]Assistant Professor
[1]Department of Computer Engineering [2]Department of Information Technology
[1,2]UVPCE, Mehsana

Abstract— In today's world security become a major issue, so it is very important to hide the data in such a way that attacker cannot access it. Data is mostly in form of text, image, audio and video. So steganography is a best scheme for hiding the data from attacker. Steganography is a one type of algorithm that can be applied on text, image, audio and video file and the secret data generally in form of text, image, audio and video. The method of hiding secret information in video file is called video steganography. In this paper a review on different video steganography technique are discussed. Different spatial domain, frequency domain techniques of video steganography have been presented in this paper.

Key words: Steganography, Video Steganography, Spatial Domain Steganography, Frequency Domain Steganography, DCT, DWT

I. INTRODUCTION

Steganography is one of the method that hide some information or data behind the multimedia object like text, image, audio and video. When steganography method use text media to hide the data then it's called text steganography. In image steganography, images are used as cover object. When secret data embedded into digital sound then it's called audio steganography. In Video steganography secret data hides in video file. Steganography method can hide the data in such a way that attacker cannot access the data. Steganography method in multimedia object improves the information security during communication. Cryptography is another method that is used to hide the secret information by encrypting the information. The main difference between steganography and cryptography is steganography deals with composing hidden message so that only the sender and receiver know that the message even exists. Other side cryptography is study of hiding information when communicating over an untrusted medium such as internet.

Video is a visual multimedia source that combines a sequence of images to form a moving picture. Video is an electronic medium for the recording, copying, playback, broadcasting, and display of moving visual media. The method of hiding secret information in a video is known as video steganography. Video consist of images as well as audio. Hence, both images and audio steganography can be used for video steganography. Different techniques of video o steganography can be used for video steganography.

II. STEGANOGRAPHY MODEL

Steganography is a technology concerned with ways of embedding a secret message in a cover message. In such a way that existence of the embedded information is hidden. A secret message can be plaintext, cipher text, an image or anything that can be represented as a bit stream.

A. Cover Media

It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data.

B. Stego-Media

It is medium obtained after embedding the secret information.

C. Secret Data

The data or information to be hidden in cover media.

D. Steganalysis

The process of detecting, presence of secret data in cover media.

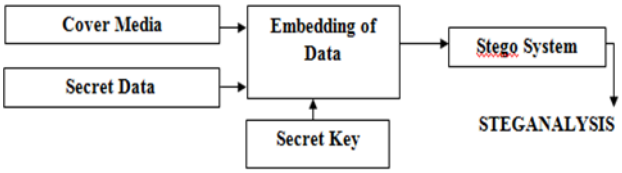

Fig. 1: Basic Model of Steganography

Figure.1 describes the basic framework of Steganography model. The two main concept used here is embedding and extracting process. Embedding process is used hide the secret message in the image as a cover object. A stego key is used to embed the message and no one can extract the information without processing this key. As in extracting process stego image is obtained that is actual image that is holding the secret massage .As the key is used in embedding process it is also used in extracting process. Basically encoding is done at sender side to obtain stego image and decoding at receiver side to obtain secret information

III. TECHNIQUES

A. Spatial Domain Steganography:

It is based on manipulation of pixel of the image. In spatial domain, cover image and secret data modified by using LSB and level Encoding. First, the cover image is decomposed into bit planes and then LSB is of bit planes replaced with secret data fit. LSB substitution is the mostly used steganographic technique. This substitution concept includes embedding at the minimum weighting bit as it will not affect the value of original pixel. This method provides better image quality. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, a secret listener can easily extract the data that we are sending.

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the

human visual system. 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 will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a series of binary number. In LSB substitution the least significant bits of the pixels are displaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The method of embedding differs according to the number of bits in an image (different in 8 bit and 24 bit images).

B. Frequency Domain Steganography:

It is based on modified Fourier transform of the image. In frequency domain, secret data is hidden in significant areas of covered image, which makes data invigorate to attacks such as compression, cropping or image processing methods than LSB approach. This provides an enhanced security level to steganography method and lead to the development of algorithms. This method transforms include DCT, DWT and DFT.

The Discrete Fourier Transform will decompose an image into its sinus and cosines components. It will transform an image from its spatial domain to its Frequency Domain. Due to its computational efficiency the DFT is very popular.

The purpose of the DCT is to transform the value of pixels to the spatial frequencies. DCT is used by many Non-analytical applications such as image processing and signal-processing DSP applications such as video conferencing. The DCT is used in transformation for data compression. DCT is an orthogonal transform, which has a fixed set of basis function. DCT is used to map an image space into a frequency.

Discrete Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in image because wavelet separately partitions the high frequency and low frequency information pixel by pixel. This scheme mainly addresses the capacity and robustness of the data hiding system. Discrete Wavelet Transform (DWT), which transforms a discrete time signal to a discrete wavelet representation. The wavelet transform describes a multi-resolution decomposition process in terms of expansion of a signal onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization property

IV. Related Work

A.J. Mozo et al. [6], In this paper, They describe research and software implementation in the field of video steganography. Because of security threats today through modern malevolent technology, confidential information is at risk such as medical records and banking or financial data. They focused on using Flash Videos (.flv file extension) because of its simple file structure, its relatively small size compared to other video file formats, and its popularity in video-hosting websites.

Mohamed Elsadig et al. [7], In this paper, They described the Least Significant Bit insertion (LSB) method on video images or frames, in addition to the usage of the human vision system to increase the size of the data embedded in digital video streaming. For future work in order to hide information in the output frame one can employ other methods of image steganography, which are appropriate for this project.

Duanquan Xu et al. [8], In this paper, Fragile digital watermarking scheme is proposed, in which the watermark is made up of time information and camera ID, the secret key is generated based on the video feature This watermarking scheme can detect and locate the modification of the video, including frame cut, foreign frame insertion and frame swapping etc. This scheme is only suitable for AVS video coding standard. After reading this paper I conclude that this scheme can also be used in various other standards.

Constantinos Patsakis et al. [9], In this paper, new effective steganographic classifier is presented which has very good properties. The novelty of the proposed method is the use of compressive sensing, that seems to have big impact on steganalysis. The classifier that is presented has very good properties as it succeeds in finding the original image in all tests, while the calculations needed can be easily made in a few seconds in moderns computers, without any special configuration.

ShengDun Hu et al. [10], have proposed a novel Video Steganography which can hide an uncompressed secret video stream in a host video stream with almost the same size. Each frame of the secret video will be Non-uniform rectangular partitioned and the partitioned codes obtained can be an encrypted version of the original frame. These codes will be hidden in the Least 4 Significant Bits of each frames of the host video This algorithm can hide a same-size video in the host video without obvious distortion in the host video.

Hong Zhao et al. [11], In this paper 3D Discrete Cosine Transform (DCT) is used to capture this correlation. Statistical features sensitive to data hiding such as absolute central moments, skewness, kurtosis, and Markov features are used as classifying statistics. Unsupervised K-means clustering is used to distinguish between the cover- and the stego-videos. Effectiveness of the proposed scheme is tested using 40 standard videos. This scheme is capable of detecting the presence of hidden message in the stego-you tube videos. Further research direction includes exploiting more sensitive features to data hiding and using more powerful unsupervised classifier.

Khushman Patel et al. [12], have proposed a modified encoding technique which will first transform the video using a Lazy Lifting Wavelet transform and then apply LSB in the sub-bands of the video that has been obtained. The proposed approach to video steganography utilizes the visual as well as the audio component. The lazy wavelet transform is applied to the visual frames, and the data is stored in the coefficients of the visual component. The length up to which it is stored is hidden using LSB in the audio component. The proposed technique does not affect the higher and lower ends of the frequency distribution of the signal. Moreover, it has a high payload capacity and low computational requirements.

Hui Ye et al. [13], have proposed a novel video steganalytic scheme based on the spatial-temporal correlation of motion vectors. The proposed scheme employs 324-dimension features from Markov matrix of motion vectors in each sliding window constituting of eight inter-coded frames

without overlapping. The proposed scheme performs better in detecting existing motion vector-based steganographic methods than previous related steganalysis schemes.

Sunil. K. Moon et al. [14], In this paper, Steganography is used to hide the messages inside other harmless messages in a way that does not allow any enemy to even sense that there is a second secret message present while the purpose of computer forensics is that it provides security from covert communication dealing with digital data and covert communication channel. In this paper author used video as cover media for hiding the secret message and used computer forensics as tool for authentication. Authors aim is to hide an image and text behind a video file. Suitable algorithm such as 1LSB, 2LSB, 4LSB is used and 4LSB method found to be good for hiding more secret information data. This work currently done in .avi file can be extended to any other video file format. Frequency domain techniques can be used for further security improvement.

Aaron Sharp et al. [15], have chosen to apply their multidimensional DST attack to video steganography. They had chosen to attack a scheme which encodes information in multiple steganographic domains of the video sequence, using image-based steganography and motion-vector steganography. The process of encoding information in the video sequence where information is encoded 2-dimensionally within individual frames of the video, as well as 3-dimensionally within the motion vectors of the video. They believe this scheme represents a robust system that would be exceptionally difficult to combat using existing steganographic attacks. Attack will utilize 2D and Time (3D) DST attacks to combat the multi-dimensional video steganography scheme. The process of attacking the video sequence as follows: First, the video sequence is decomposed into a train of 2D images or frames. Next each frame of the sequence is attacked using the 2D DST transform. Lastly, this resultant sequence is attacked using the Time (3D) DST attack.

Parag Kadam et al. [16], In this sender encrypt data and image separately using AES algorithm, hides encrypted data in encrypted image using LSB technique, system auto generate the all 3 respective keys. Sender sends the file through existing mail system. Receiver can perform operation as per respective keys like if he has only data hiding and image decryption key then he can only get the image in original form or if he has data hiding and data decryption key then he can get original data. Algorithm work well only small size of data, so capacity is very low. In future research Apply another algorithm, use cover as a video file & try to hide more information. So improve the capacity of data hiding.

Mritha Ramalingam, et al. [17], They described how to transmit maximum hidden data without losing the video quality and size. In order to achieve this goal, in this system they are using the encryption key for sequential data encoding and decoding. The performance of the steganography approach has been evaluated using video images in bit mapped (bmp) format in Red, Green, and Blue (RGB) components. This algorithm works well for bitmap video images. It is found that the proposed method allows embedding secret data of different length in the cover-video images without varying the size of the original images Further, this algorithm can be modified to embed any type of data in any format of video files and the work will continue to focus on increasing the capacity, security, and robustness.

Seema et al. [18], This paper described an analysis approach with effective frame selection, partial information storage per frame and referenced mask based embedding is suggested to improve the steganography process in video objects. In first stage, the effective frame selection analysis is performed using entropy method on which the information hiding is effective. The frame analysis is performed based on content level analysis. The adaptive mask over the frame is identified using frequency based analysis over the image in second stage. At third level, LSB approach is applied over the mask to perform information embedding. The work is applied on real time images.

Hemant Gupta et al. [19], In this paper, proposed method for replacing one or two or three LSB of each pixel in video frame and apply Advance encryption standard (AES). It becomes very difficult for intruder to guess that an image is hidden in the video..

Pragya Agarwal et al. [20], have presented different video watermarking techniques by analyzing their performances, time taken for watermarking, co-relation of the extracted watermark with the original one, and some other important factors. Digital video watermarking is a technique developed to help in copyright protection of video files. Digital video files can be easily copied and shared among many people on the Internet. So, it's extremely necessary to protect the copyright and ownership right of the video files with the help of digital watermarking. All the three video watermarking schemes mentioned in this paper are not perfect. In future, a watermarking scheme can be found which is robust under all the attacks like frame dropping etc, still the imperceptibility of the watermarked frame should not be compromised. Also the time complexity of the scheme should be reduced to some extent.

Palak Patel et al. [21], In this paper, they proposed combined strategy of cryptography, steganography and digital watermarking to hide secure image with watermark logo inside cover image. They use DCT, DWT, SVD and RSA approach. Using DCT, encrypted watermark logo is hide inside Secure image, results in Stego image. This Stego image is hiding inside cover image using DWT and SVD. Their approach can be used to transmit secure information like copyright information of company, movie with their respective image, finger-print or thumb impression of particular person. This method can be used for security purpose. Thus would be beneficial to nation for over all security.

Kasim tasdemir et al. [22], a high efficiency video coding (HEVC) is the most recent video codec coming after currently most popular H.264/MPEG4 codec. In this paper, pixel domain steganography applied on HEVC video is targeted for the first time. Temporal correlation remains strong enough for more than 40 frames. Finding a practical way of incorporating more frames in feature extraction stage is a future work

V. CONCLUSION

In today's world steganography scheme becomes more useful scheme for hiding the data from attacker. This paper present review on video steganography. Steganography and Cryptography are two popular ways of sending vital

information in a secret way. One hides the existence of the message and the other distorts the message itself. By using both one can achieve better confidentiality and security.

REFERENCES

[1] Shivani Kundra, Nishi Madaan, "A Comparative Study of Image Steganography techniques". International Journal Of Science And Research (IJSR), Volume 3 Issue 4, April 2014, ISSN: 2319-7064
[2] Rakhi, Suresh Gawande "A Review On Steganography Methods" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 10, October 2013, ISSN (Print) : 2320 – 3765, ISSN (Online): 2278 – 8875
[3] Gurwinder Kaur, Navdeep Singh Sethi, Harinderpal Singh "Novel LSB Approach for Steganography" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-4, Issue-7)
[4] Douglas Lyon "The Discrete Fourier Transform, Part 1" JOURNAL OF OBJECT TECHNOLOGY, Published by ETH Zurich, Chair of Software Engineering ©JOT, 2009 Vol. 8, No. 3, May-June 2009
[5] A.M.Raid, W.M.Khedr, M. A. El-dosuky, Wesam Ahmed "Jpeg Image Compression Using Discrete Cosine Transform - A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.5, No.2, April 2014 DOI : 10.5121/ijcses.2014.520439
[6] A.J. Mozo, M.E. Obien, C.J. Rigor, D.F. Rayel, K. Chua, G. Tangonan "Video Steganography using Flash Video (FLV)" I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, 5-7 May 2009 978-1-4244-3353-7/09/$25.00 ©2009 IEEE
[7] Mohamed Elsadig, Miss Laiha Mat Kiah, Bilal Bahaa Zaidan, Aos Alaa Zaidan "High Rate Video Streaming Steganography" 2009 International Conference on Future Computer and Communication 978-0-7695-3591-3/09 $25.00 © 2009 IEEE
[8] Duanquan Xu, Jiangshan Zhang, Baochuan Pang "A Digital Watermarking Scheme Used for Authentication of Surveillance Video" 2010 International Conference on Computational Intelligence and Security 978-0-7695-4297-3/10 $26.00 © 2010 IEEE
[9] Constantinos Patsakis, Nikolaos Aroukatos "A DCT steganographic classifier based on compressive sensing" 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing 978-0-7695-4517-2/11 $26.00 © 2011 IEEE
[10] ShengDun Hu, KinTak U "A Novel Video Steganography based on Non-uniform Rectangular Partition" IEEE International Conference on Computational Science and Engineering 978-0-7695-4477-9/11 $26.00 © 2011 IEEE
[11] Hong Zhao, Hongxia Wang, Hafiz Malik "Steganalysis of YouTube Compressed Video Using High-Order Statistics in 3d DCT Domain"" 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing978-0-7695-4712-1/12 $26.00 © 2012 IEEE
[12] Khushman Patel, Kul Kauwid Rora, Kamin Singh, Shekhar Verma "Lazy Wavelet Transform Based Steganography in Video" 2013 International Conference on Communication Systems and Network Technologies 978-0-7695-4958-3/13 $26.00 © 2013 IEEE
[13] Hui Ye, Weiming Zhang, Yuanzhi Yao, Cong Kong, Hao Huang, and Nenghai Yu "Motion Vector-Based Video Steganalysis Using Spatial-Temporal Correlation"2013 6th International Congress on Image and Signal Processing 978-1-4799-2764-7/13/$31.00 ©2013 IEEE
[14] Sunil. K. Moon, Rajeshree. D. Raut "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security" Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013) 978-1-4673-6101-9/13/$31.00 ©2013 IEEE
[15] Aaron Sharp, Qilin Qi, Yaoqing Yang, Dongming Peng, and Hamid Sharif "A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform 2013 IEEE International Conference on Signal and Image Processing Applications (ICSIPA) 978-1-4799-0269-9/13/$31.00 ©2013 IEEE
[16] Parag kadam, Mangesh Nawale, Akash Kandhare, Mukesh Patil "Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique" Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22,978-1-4673-5845-3/13/$31.00©2013 IEEE
[17] Mritha Ramalingam, Nor Ashidi Mat Isa "A steganography approach for sequential data encoding and decoding in video images" 2014 International Conference on Computer, Control, Informatics and Its Applications 978-1-4799-4575-7/14/$31.00 c 2014 IEEE.
[18] Seema, Mrs. Jyoti Chaudhary " A Multiple Phase Model to Improve Video Steganography" 2014 Sixth International Conference on Computational Intelligence and Communication Networks 978-1-4799-6929-6/14 $31.00 © 2014 IEEE
[19] Hemant Gupta, Dr. Setu Chaturvedi "Video Data Hiding Through LSB Substitution Technique" International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 32-39 Issn(e): 2278-4721, Issn(p):2319-6483
[20] Pragya Agarwal, Ankur Choudhary "Protecting Video Data Through Watermarking: A Comprehensive Study" 978-1-4799-4236-7/14/$31.00c 2014 IEEE
[21] Palak Patel, Yask Patel "Secure and authentic DCT image steganography through DWT –SVD based Digital watermarking with RSA encryption" 2015 Fifth International Conference on Communication Systems and Network Technologies 978-1-4799-1797-6/15 $31.00 © 2015 IEEE
[22] Kasim Tasdemir, Fatih Kurugollu, Sakir Sezer "A Steganalysis System Utilizing Temporal Pixel Correlation of HEVC Video" 978-1-4799-4874-1/14/$31.00 ©2015 IEEE.

