A Survey Paper on Video Steganography

Aparna Asokan
M.Tech Scholar
Department of Information Technology
Government Engineering College, Barton Hill, India

Simi Krishna.K.R
Assistant Professor
Department of Information Technology
Government Engineering College, Barton Hill, India

Abstract— Nowadays, security becomes a major concern, so it is very important to hide data from an unauthorized person who tries to access data in an unauthorized way. Data is generally in the form of text, image, video and audio. As technology grows, the need for hiding data in a secure manner increases. As a result Steganography was introduced. Steganography is a process of hiding data from an unauthorized access. It plays an important role in information security. Steganography has many applications in defence, medical, online transactions etc. It is mainly used whenever confidentiality of information is needed. Steganography algorithms can be applied in different file formats such as text, image, video and audio. Hiding data in video file is known as video steganography. There are many techniques for video steganography. In this paper, an analysis of different video steganography techniques has been presented.

Keywords— Steganography, Video steganography, Spatial domain, Transform domain

I. INTRODUCTION

The Internet's discovery has made many changes in our world. People started to make payments, money transfer, ticket reservation, shopping through the internet. Also the Internet has become a major source of information interchanges. At the same time unauthorized person or group tries to access the interchanged information, that means without any permission information will accessed by others. So there is a need for some techniques to prevent unauthorized attacks on the information.

Information security is necessary for the secure transmission of data. Steganography and cryptography are the means of securing the confidentiality and secrecy of information [1]. These techniques can be used to prevent security attacks on the information. In Steganography the secret text will be embedded in another format of data. In cryptography secret text is converted into cipher text, by knowing the secret key, then only data can be decrypted.

In Steganography the secret message is embedded in the cover message and transmitted in such a way that the existence of information is undetectable [2].A steganographic system consists of three components, namely: Plain text, Cover file and stego file [1]. Steganography is a process that involves hiding of important information (message/Plain text) inside other carrier (cover) data, to protect the message from unauthorized users [3]. Cover file or carrier can be text, image, video or audio in which the message is embedded [1]. The output of steganographic system is the stego file that contains hidden information. According to the cover media there are different steganographic systems such as text steganography, image steganography, video steganography and audio steganography.

In Text steganography the secret data is hidden in a text file and in a binary file. Text can be scrambled or concealed in any way inside a video [4].Text steganography has very high capacity to hide text data in a text file. Image steganography deals with hiding of data in an image. Image is the collection of pixels and the pixels based on their intensities are selected to hide the data [4].Video steganography deals with hiding of data in a video file. That means cover media is a video. Video is a combination of continuous frames and audio, that moves in a fixed time. Videos are getting popular as a cover object in steganography due to high embedding payload than a digital image [5] and temporal features of video also provide perpetual redundancy which is not available in digital images [4].

This paper presents a brief description of video steganography. Section II discusses about different video steganographic techniques. Section III discusses about the related works done in video steganography.

II. VIDEO STEGANOGRAPHY

Due to the advancement of Internet and multimedia technologies, digital videos have become a popular choice for data hiding [3].In video steganography the secret data is hiding in the video. The video contains continuous frames, so redundancy is high and this can be utilized for embedding secret data. Recently, there are many useful applications of video steganography techniques such as video error checking, military services, bandwidth saving, video surveillance and medical video security [3].

Video steganography techniques can be classified into various techniques like Spatial or Substitution based techniques [6], Transform based techniques [7, 8] and based on Classification i.e. Format based and Video Codec methods [9].

A. Spatial Domain Based Method

A spatial domain method basically deals with hiding information in pixels of video frames [4]. There are many methods for hiding data by using a spatial steganography technique; all of them are changing some bits in the video frame for data hiding. Some methods used for video steganography using the spatial domain method are described as follows.

The most popular method of steganography is Least Significant Bit method (LSB) [10] due to its high embedding capacity, less embedding complexity and ease in implementation. In the spatial domain, cover image and secret data modified by using LSB and level encoding [11]. Let px [i] represents a pixel in an image, the binary form of that pixel can be px [i] = {$p_{7,}$ p_6, p_5, p_4, p_3, p_2, p_1, p_0} .Here LSB is $p_{7.}$ In this approach the LSB pixels of the carrier image are replaced with the secret data so that it can’t be recognized by the human visual system. Changing of LSB pixels in the image does not create a large difference in the original image, so this method is an efficient way to hide data. According to the number of bits in an image, the method of embedding data will differ.

Another method in spatial domain steganography is Most Significant Bit (MSB) method. Here the most significant pixel will be replaced instead of least significant bit. In the pixel px [i] described above, the most significant bit is p_0.Changing most significant bit also does not make any large difference in the original image.

Pixel Value Differencing (PVD) is another method. In this, difference between pixel value is considered for embedding process. The difference between a pixel and its neighbour will gives the number of embedded bits. If the difference is larger then secret bits can be embedded. This method has high imperceptibility and low embedding payload [12].

RGB based Steganography is another method. In this method a digital image is an array of numbers that represent light intensities at various points or pixels [12].Images can be stored in 8- bit i.e. grayscale image and 24-bit i.e. RGB image. In RGB images red, blue and green colours are combined. These are the primary colours and these colours are represented by one byte. Each pixel is represented as a combination of these primary colours.RGB steganography method attempts to overcome the problem of the sequential fashion and the use of stego-key for the selection of pixels [13].

B. Transform Domain Video Steganography

Transforming pixel from time domain to frequency domain is the basic idea of Transform domain video steganograpgy. The digital image is a collection of pixels which are present in high and low frequency components of the image [13].There are different Transform domain video steganography techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier transform (DFT), Integer Wavelet Transform (IWT), Haar Transform and discrete Curvelet Transform (DCVT).Among these techniques DCT and DWT are most used techniques for steganography.

Embedding process is depending on the DCT coefficients in DCT method. Any DCT coefficient value above the proper threshold is a potential place for insertion of secret information [12]. If the DCT coefficient value difference of pixels in a cover video is greater than a certain threshold value, then the MSB of secret message can be hidden in LSB of cover video. Yanquing et al. [14] had achieved high security and high visual quality by using DCT coefficients based on generic algorithm. Difference of non-zero DCT coefficients had been chosen to achieve PSNR of 38.26 at a high embedding rate with high security [15].

In DWT, digital image or frame is decomposed into four sub bands, with the lower sub band having relevant information and high sub band having finer details [10]. Sub bands are represented as LL, HL, LH and HH. Here the LL sub band is the low frequency portion and so it looks like the original image. The temporal resolution is the main advantage of this technique. It transforms a discrete time signal to discrete wavelet representation [11]. Ghasemi et al. [16] had proposed embedding in 4X4 block of DWT coefficients using generic algorithms based functions and then OPAP is applied to achieve PSNR of 35.27 dB.

C. Format Based Method

For a particular video format, there are various techniques. H.264/AVC is latest video compression standard with high efficiency in compression and well adapted for network transmission [10]. Flash video (. FLV) format has simple structure and small size, so video files in this format are considered to be very popular in the internet. Mason et al [17] has described a technique based on its simple structure to embed secret messages in video tags to achieve good visual quality without any distortion.

III. RELATED WORKS

Most of the research work in video steganography is the extension of image steganography because video is the combination of continuous images or frames and audio in a constant time interval. One of the most common methods of image steganography is least significant bit (MSB) method which can be applied in video steganography. Mohamed Elsadig et al. [18], described the 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. The concept used in this method is that, video contains several images and hiding data on each video frame does not visually change the frames in the video. With this technique hide data efficiently than other steganography media. The results successfully extracted the embedded data from stego file and also more data can be successfully stored in one image. The video contains approximately 27 frames, so that can store lots of data in a secure manner. Hiding data using other methods of image steganography in output frame are considered as future works.

In 2010, Sherly A.P and Amritha P.P presented a paper titled “Compressed video steganography using TPVD” [19].In this method data is hidden in a compressed video. For embedding data, I frame with maximum scene change blocks are used. Tri-way pixel-value differencing (TPVD) is used for embedding so that, the capacity of the hidden secret information can enlarge and provide an imperceptible stego-image for human vision. The proposed architecture consists of four functions such as, I, P and B frame extraction, the scene change detector, motion vector calculation and the data embedder and steganalysis. Decompression is not required for this method because all processes are defined and executed in a compressed domain. Increase the payload without affecting the quality of the video is the main advantage of this method.

In 2011, Constantinos Patsakis and Nikolaos Aroukatos [20] presented a paper which concentrated on an effective steganographic classifier having very good properties. This work, addresses to the problem of identifying a clean image from a set where other instances of the same image exist, but data have been embedded in DCT. This work presents a classifier for steganographic content when DCT is used. Any previous training is not needed by the classifier. Input for this is just the set of images to be classified. The disadvantage of this method is that, if DCT coefficients altered the performance decreases. DWT steganalysis is considered as the future work for this paper.

In 2012, Xikai Xu, Jing Dong and Tieniu Tan [21] presented a paper, which deals with a universal spatial feature set for video steganalysis. The proposed method provides a generalized and effective way of constructing feature set for video steganalysis. They developed a new approach to extract inter-frame features also. The experiments done by the team shows that, the proposed method is more effective than SPAM. This method is not applicable for Motion Vector based video steganography, because the modification of motion vector changes the correlation of adjacent pixels. This paper suggests future works can be done to solve the high dimensionality problem of the feature space and also use the correlation of more than three adjacent pixels to improve the performance of the proposed method.

In 2012, Lakshmi Narayan K, Prabakaran G and Bhavani R presented a paper titled “A High Capacity Video Steganography Based on Integer Wavelet Transform” [2]. In this paper Integer wavelet transformation in cover image is utilized to get the stego-image. In this method, IWT is applied to cover image and secret image and then fused together into cover image. After this apply inverse IWT to that cover image, then stego image is generated. In the extraction process reverse of embedding process is done. Experimental results of this paper show that, the stego-image retrieved is a high capacity and security with certain robustness. This method will also provide the secret image recovered from the stego image with minimum distortion. Applying this method into multiple wavelet transform and extended to colour images are the future works.

In 2013, Prajna Vasudev and Kumar Saurabh suggested a novel “Video Steganography using 32x32 vector quantization of DCT” [22].In this method first video frames or images are extracted from the video and then find 32x32 vector quantization of DCT for each frame. After this apply LSB quantization method. As a result, some vacant space will form in the frames and these vacant spaces are filled with information bits.

In 2014, Mritha Ramalingam and Nor Ashidi Mat Isa [23] presented a paper which describes a steganographic approach for sequential data encoding and decoding in video images. In most of the methods, after hiding data there may be some loss in the quality of video. This paper proposes an effective method for transmitting maximum hidden data without losing video quality. To achieve this goal, for sequential data encoding and decoding an encryption key is used. The performance of this method is evaluated using video images in bit mapped (bmp) format with red, green and blue (RGB) components. In encoding read required details in bmp image and process every pixel values of the RGB components. Then read secret data and convert it into integer values. For embedding encryption key is used, that means encrypt secret data using a symmetric XOR encryption key. Encoding function hides the data along the columns moving from left to right through the target image in RGBBGRRG order. After this write stego-video image. Decoding has been just the reverse of embedding procedure. The experimental results show the proposed system is simple and produces imperceptible distortions in resulting bmp images. Drawback of the proposed method is less security. The future works are focused on embedding different data of different file formats and tries to improve security, capacity and robustness.

In 2015, R.J Mstafa and K.M.Elleithy [24] proposes a high payload video steganographic algorithm in DWT domain based on BCH codes. A secret message is first encoded by BCH (n, k, t) coding to improve the security of the algorithm. Then it is embedded into the middle DWT coefficients of video frames because, DWT middle and high frequency regions are considered to be less sensitive data. BCH is a powerful random cyclic code method used for detecting and correcting errors in a block of data. In hamming code only one bit can correct, but in BCH more than one bit can correct. In the embedding phase using first key, change the positions of the whole secret message and convert into a one dimensional array. Using BCH (15,11) encoder, encode the message and XOR it with the second key. Cover video is split into video frames in YUV colour space. Then apply two dimensional DWT separately in Y,U and V frame component. The message is embedded in middle and high frequency coefficients of each Y,U and V components and apply inverse two dimensional DWT on the frame components. Rebuild the stego frames from YUV stego components and output the stego videos which are reconstructed from all embedded frames. Extraction is reversing the embedding process and use inverse IDWT. The proposed method can be applied in slow and fast motion objects and proved as more efficient than other methods. Various attacks are done to prove the robustness of the proposed algorithm and the results were consistent.

In 2016, Ammad Ul Islam et al [1] proposes an improved steganographic technique based on MSB using Bit Differencing. In this method bit no 5 is used to store the secret bits based on the difference in 5th and 6th bits of the cover image. If the difference between 5th and 6th bits is not equal to the data bit, then replace the 5th bit with the data bit. Generally attacker focus on the LSB bits for finding secret data, but the proposed method uses MSB bits so this makes more security for hidden data. Comparative analysis shows that the proposed technique has greater PSNR and higher payload capacity, so that can hide more than one data in a single cover image.

IV. Conclusions

In today's world, security of information is an important fact to be considered in communication. Steganographic techniques become essential tool for securing information. This paper presents a review of different video steganography techniques. Various video steganography techniques such as spatial domain, transform domain and other classifications are discussed. This paper also gives a brief description about steganography. In this paper different video steganography techniques are compared and analyzed.

References

[1] Ammad Ul Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnan Khan, Usman Ali and Muhammad Naeem "An Improved Image Steganography Technique based on MSB using Bit Differencing". The sixth International Conference on Innovative Computing Technology(INTECH 2016).978-1-5090-2000-3/16/$31.00 ©2016 IEEE

[2] Lakshmi Narayan K, Prabakaran G, Bhavani R " A High Capacity Video Steganography Based on Integer Wavelet Transform". Journal of Computer Applications ISSN: 0974 – 1925,Volume-5,Issue EICA2012-4,February 10,2012.

[3] Ramadhan.J.Mstafa,Khaled.M.Elleithy,Eman Abdelfattah "Video Steganographic Techniques:Taxonomy,Challenges and Future Directions".78.1-4799.6776.6115/$31.00 © 2017 IEEE.

[4] Bharti Chandel,Dr.Shaily Jain "Video Steganography:A Survey".IOSR Journal of Computer Engineering(IOSR-JCE).e-ISSN:2278-0661,p-i]ISSN:2278-8727,Volume 18,Issue 1,Ver.III(Jan-Feb.2016),PP 11-17.

[5] M.Jafar,K.Morteza "An adaptive scheme for compressed video steganography using temporal and spatial features of the video signal".International Journal of Imaging System and Technology,19,December 2009,306-315.

[6] S.Manish,K.Sushmita,R.Richa "Video Steganography using Pixel Intensity Value LSB Technique".International Journal on Recent and Innovation Trends in Computing and Communication,3(2),2015,287-290.

[7] K.Naveen,B.NagKishore,M.Vasujadevi "Image Hiding in a Video-based on DWT & LSB Algorithm".International Conference on Photonics,VLSI & Signal Processing,2014

[8] M.Ramadhan,E.Khaled "A High Payeload Video Stegnography Algorithm in DWT Domain Based on BCH Codes".Wirelss Telecommunications Symposium (WTS),New York,April 2015,1-8.

[9] M.M.Sadek,A.S.Khalifa,G.M.Mostafa"Video Steganography:A Comprehensive Review, Multimedia Tools Applications".74, March 2014,7063-7094.

[10] S.Mansi,M.Vijay "Current status and key issues in image steganography:A survey".Computer Science Review,13-14,Nov 2014,95-113.

[11] Ankita Patel,Ajay Barot "A Survey Paper on Video Steganography".IJSRD-International Journal for Scientific Research&Development,Vol.3,Issue-12,2016,ISSN(online): 2321-0613

[12] Mansi Dave,Hinal Somani "A Survey on Digital Video Steganography Techniques Used for Secure Transmission of Data".IJARIIE-ISSN(O)-2395-4396,Vol-2 Issue-6 2016.

[13] 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.

[14] G.Yanqing,K.Siangwi,Y.Xingang "Secure Steganography based o binary particle swarm optimization",Journal of Electronics(China),26(2),February 2009,285-288.

[15] L.Chiang,L.Shiang "High-Performance JPEG steganography using complementary embedding strategy",Pattern Recognition,41(9),September 2008,2945-2955.

[16] E.Ghasemi,J.Shanbehzadeh,B.ZahirAzami "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm",Communication and Signal Processing,February 2011,pp 42-45.

[17] A.J.Mozo,M.E Obien,C.J.Rigor,D.F Ravel "Video Steganography using Flash Video(FLV)", Instrumentation and Measurement Technology Conference,May 2009,822-827.

[18] Mohamed Elsadig,Miss Laiha Mat Kiah,Bilal Bahaa Zaidan,Aos Alaa Zaidan "High Rate Video Streaming Steganography",2009 International Conference on Future Computer and Comunication 978-0-7695-3591-3,09$25.00© 2009 IEEE.

[19] Sherly A P,Amritha P.P "A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2,No.3,August 2010.

[20] Constantinos Patsakis,Nikolaos Aroukatos "A DCT Steganographic Classifier based on Copressive sensing",2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing 978-0-7695-4517-2/11 $26.00 © 2011 IEEE.

[21] Xikai Xu,Jing Dong and Tieniu Tan "Universal Spatial Feature Set for Video Steganalysis",ICIP 2012,978-1-4673-2533-2/12/$26.00 © 2012 IEEE.

[22] Prajna Vasudev,Kumar Saurabh "Video Steganography Using 32x32 Vector Quantization of DCT",International Journal of Software&Hardware Research in Engineering, Vol.1,Issue.3,Nov 2013.

[23] 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 © 2014 IEEE.

[24] R.J Mstafa and K.M. Elleithy "A High payload video steganography algorithm in DWT domain based on BCH codes(15,11)", Wireless Telecommunications Symposium(WTS),2015,pp.1-8.