A SURVEY ON DIGITAL VIDEO STEGANOGRAPHY TECHNIQUES USED FOR SECURE TRANSMISSION OF DATA

[1] Mansi Dave, [2] Hinal Somani

[1]*Student of Gujarat Technological University, Department of Computer Engineering, L. J. Institute of Engineering and Technology, Gujarat Technological University, Ahmedabad, Gujarat, India*
[2]*Assistant Professor at L. J. Institute Of Engineering & Technology, Ahmedabad, Gujarat, India*

ABSTRACT

Recent advances in information technology have made quick delivery and sharing of multimedia information possible. But these advances in technology are leading breaches to information security and personal information. Now days, it is very risky to handle the data in internet against intruders. Data is generally in the form of text, audio, video and image. With the development of the technology, people have tend to figure out methods which are not only capable in hiding a message, but also capable of hiding the existence of a message. Steganography was introduced as a result of such research work. Steganography is the process of hiding secret information inside a data source which is referred as cover medium. Steganography has applications in different fields such as defence, medical, online transactions etc. It is mainly used in situations where the confidentiality of information is of prime importance in communication. Based on type of cover medium there is different type of steganography i.e. audio, video, text, image etc. Video Steganography is the process in which message is embedded inside the video type of cover medium in such manner that is existence. In this paper we analyze different video steganography techniques and their comparative study. To improve embedding process in terms of robustness and visual quality advance LSB (Least Significant Bit) method is used in proposed model.

Keywords: *Video Steganography, Least Significant Bit (LSB), Robustness, Visual quality*

1. INTRODUCTION

In our day to day life demand of internet applications are more vurnable to various kinds of security attacks. For protecting the system mainly two fields are widely used that is steganography and cryptography. That approaches are maintained data confidentiality and data integrity during data transmission. Steganography is a process that involves hiding important information (message) inside other carrier (cover) data to protect the message from unauthorized users [1]. Steganography is defined as the art and science of secret communications, primarily concealing the existence of the communication. [2]. Even without them having any suspicion of the data's existence. Human Visual System (HVS) can't recognize a slight change that happens in the media cover such as audio, image and video [3].Cryptography is a process that involves encryption of message form protecting message unauthorized users.

Video Steganography the message is embedded inside the video for protecting message from unauthorized users. Any successful steganography mainly considered two important factors that is embedding payload and embedding efficiency. The embedding payload defined as amount of secret information which is embedding inside the cover medium. This should be high [1].Embedding efficiency includes the stego video security, visual quality, robustness against attackers [2]. Increasing efficiency will cause the capacity of embedding to have a low payload. Changing the balance between these two factors mainly depends on the users and the type of steganography scheme [3]. In steganography at sender side embedding process is done in which the message is

embedded using key into original data is known as stego medium. On the other hand receiver side extracting process is done in which message is extracted using symmetric or same key which is used in sender side from stego medium as seen in fig 1. The symmetric key should be predefined between sender and receiver. Generally the video steganography is used for confidential applications like as military, defence, video watermarking, tamper detection etc. In our proposed model we use the advance LSB method for improving embedding process for video steganography in terms of robustness and visual quality.

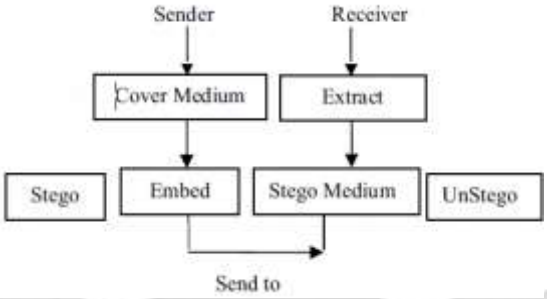

Fig -1: Steganography System [17]

In this paper, Section 2 describes parameters that need to be satisfied by video steganography technique and various techniques used for video steganography. Section 3 describes related work for Least Significant Bit (LSB) method. Section 4 describes comparative study of techniques which have been used to hide secret data in video file. Proposed work and Conclusion is presented in Section 5 and 6 respectively.

2. VIDEO STEGANOGRAPHY

For any successful video steganography system following measures should be considered:

A. Imperceptibility

Imperceptibility refers to the visibility of modification inside the cover media. High Imperceptibility means increasing the invisibility of slight modifications in cover object. Modern day steganalysis approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganalysis resistant video steganography methods [6] [7].

B. Payload

Payload or capacity refers to the amount of secret message that can be concealed inside cover media [8]. Video are gaining popularity as highly used cover media object due to their high embedding capacity and embedding efficiency.

C. Statistical Attacks

The attacks or methods applied on stego object to extract hidden or secret information are known as statistical attack [9].Steganography algorithm must be robust against statistical attacks It describes robustness feature.

D. Security

The most important feature of any steganographic algorithm is security. The embedding process should have high security with minimum vulnerability to attacks. Several approaches) have been proposed to secure message in steganography [10].

E. Computational Cost

Data hiding and Data retrieval are the two parameters used to calculate computational cost of any steganography approach [11] .Data hiding time refers to the time required to embed data inside a cover video frame and data retrieval refers to extraction time of secret message from the stego frame.

F. Perceptual Quality

Increment in embedding capacity may also lead to degradation of video quality or degradation of original contents of video. Video steganography approach must handle control degradation of video quality.

Generally the video steganography technique classified based on compressed domain (compressed , uncompressed video) , Embedding domain (spatial domain , transform domain) , classification based method(format based , video codec based).The message embedding process based on two techniques i.e. spatial domain based and transform domain based.

2.1 Spatial Domain Video Steganography

There are many methods of spatial steganography, all directly change some bits in the image of frame pixel values in hiding data. Some methods which are widely used for video steganography based on spatial domain are as follow:

A. Least significant bit (LSB): It is one of the most common and easiest method for message hiding. In this method, message is hidden in the least significant bits of image pixels. Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image. The hiding capacity can be increased by using up to 4 least significant bits in each pixel which is also quite hard to detect [13, 14, 15]. This method has high embedding payload, high visual quality, high dtectability.

B. Most Significant Bit (MSB): In this method the messages are embedded into cover image by replacing the most significant bits of the image directly. The visual quality is decreased.

C. Pixel Value Differencing (PVD): In this method the pixel value difference is considered for embedding process. The number of embedded bits is determined by the difference between the pixel and its neighbour. The larger the difference amount is, the more secret bits can be embedded. This method has high imperceptibility and low embedding payload.

D. RGB based Steganography: In this method a digital image is an array of numbers that represent light intensities at various points or pixels. Digital computer images can be normally stored as 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit file can be quite large however it provides more space for hiding information. As we know all colors are essentially combinations of three primary colors: red, green, and blue. Every primary color is represented by one byte ie every pixel represents a combination of (R, G, B). The parity bit patterns can correspond to the message being hidden. RGB Steganography method attempts to overcome the problem of the sequential fashion and the use of stego-key for the selection of pixels. [16].

2.2 Transform Domain Video Steganography

Transform domain technique is basically used for transforming pixel from time domain to frequency domain. Digital image is collection of pixels which are present in high and low frequency components of image. The edge pixels are high frequency pixels and non edge pixels are low frequency pixels. Generally there are different transformation techniques i.e. Discrete Cosine Transform(DCT) , Discrete Wavelet Transform(DWT) , Discrete Fourier Transform(DFT), Integer Wavelet Transform(IWT), Haar Transform, Discrete Curvelet Transform(DCVT). But DCT and DWT are widely used for steganography.

A. Discrete Cosine Transform (DCT): In this technique embedding process is depended on DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information. Here the MSB of secret message are hidden in LSB of only those pixels of cover video whose DCT coefficient value is greater than a certain threshold value. It separates the image into spectral sub-bands with respect to its visual quality, i.e. high, middle and low frequency components. It is more suitable for low subband of frequency.

B. Discrete Wavelet Transform (DWT): This technique main advantage is temporal resolution. In it wavelets are discretely sampled. There are two operations one is horizontal and second is vertical. At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right .Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part denoted as symbol L while the pixel differences represent the high frequency part of the original image denoted as symbol H. Secondly; scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

3. RELATED WORK

3.1 A High Payload Video Steganography algorithm in DWT Domain based on BCH (15, 11)

In this paper the proposed approach uses BCH (15, 11) code for encoding message before embedding message into video file for providing more security. Then they used 2D DWT transformation for embedding message into DWT coefficients of video frames. As DWT middle and high frequency regions considered less sensitive data the secret message is embedded only into middle and high frequency regions. The proposed approach improves hidden ration i.e. 28% and high embedding efficiency.

3.2 A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes

In this paper the proposed approach uses BCH (7, 4) code and DCT transformation. The secret message is encrypted using BCH (7,4) code for providing security the it is embedded into DCT coefficients of video

frames. The hidden message is embedded into DCT coefficients of each Y, U, and V planes excluding DC coefficients. The proposed approach provides hidden ration 27.53% as high hidden capacity.

3.3 A Highly Secure Video Steganography using Hamming Code (7, 4)

In this paper the proposed approach uses Hamming Code (7, 4) for encoding message before embedding it into video. The result of the encoded message will be added to random generated values by using XOR function. After these steps that make the message secure enough, it will be ready to be embedded into the cover video frames. In addition, the embedding area in each frame is randomly selected and it will be different from other frames to improve the steganography scheme's robustness. In it for more security purpose 3 keys are used. The first key is used to reposition pixels in Y, U, V, and the secret message into a random position, which makes the data chaotic. In order to select the locations for embedding the secret message into the host data, the second and third keys are used. So, this approach improve robustness , security , visual quality in terms of PSNR i.e. 51db.

3.4 Video Steganography Algorithm Based on Trailing Coefficients

In this paper the proposed approach uses concept of trailing coefficients and DCT transformation. The algorithm firstly conducts DCT transform on the frame, and then obtains the trailing coefficient for each quantized DCT blocks, last embedded by changing its values. First step is generated pseudo random code then DCT is applied then identified trailing coefficients based on that identify odd and even numbered block. Firstly the proposed algorithm based on trailing coefficient and we modify the value of trailing coefficient to make sure the secret information bit is 0 then the sum value –ve and when information bit is 1 then the sum is +ve ensure that DCT coefficients are changed. In it odd numbered block then hide and even numbered block then correct. It provides high hidden capacity and better robustness after noise addition.

3.5 Robust video steganography algorithm using adaptive skin tone detection

This approach is based on blind adaptive data hiding algorithm for video files where human skin regions are regarded as the Regions Of Interest (ROI) hosting the embedding process. A skin map is created for each frame using an adaptive skin detection algorithm with reduced number of false positives. Then the skin map is converted to a skin-block-map in order to eliminate the error-prone skin pixels that can result in inefficient retrieval of the hidden data. Moreover, the embedding process is done using a wavelet quantization technique over the red and blue channels of the host frames for increased robustness.

4. COMPARATIVE STUDY

Table -1: Comparison of Implemented Techniques For Video Steganography

Sr. No	Title	Method Used	Advantages	Disadvantages
1	A High Payload Video Stegnography algo in DWT Domain based on BCH (15, 11)	BCH(15,11) and 2D-DWT is used	Better performance in terms of high embedding payload and robustness	Security is less and improved embedding payload w.r.t. visual quality in frequency domain
2	A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes	BCH(7,4) and DCT is used	Provides high payload with minimal tradeoffs and high robustness	Improved embedding payload w.r.t. visual quality in frequency domain
3	A Highly Secure Video Steganography using Hamming Code (7, 4)	Hamming code(7,4) and Linear block code is used	Improved Visual quality, , Security	Increased Computational complexity because for providing more security 3 keys are used.

4	Video Steganography Algorithm Based on Trailing Coefficients	DCT and trailing coefficients is used	Provides large capacity of steganography due to trailing coefficients and high robustness	Improved visual quality in terms of PSNR
5	Robust video steganography algorithm using adaptive skin tone detection	Blind adaptive data hiding algorithm for video file	Provides high imperceptibility, high robustness against MPEG 4 compression	Increases hidden capacity by using RDWT

Here Table 1 provides the information about the method used and also include about the advantages and disadvantages of each and every methods.

5. PROPOSED WORK

As seen all the methods that are invented in LSB, most of the method suffers through about the capacity, robustness and distortion created by embedding bit into video file. In order to enhance the robustness with maintaining perceptual transparency and improve visual quality, a new video steganographic technique has been proposed and following are the steps.

A. Embedding Process:

Step 1: At Sender side, take secret message as input which is embedded in cover medium
Step 2: Encrypt the message using key.
Step 3: Apply advance LSB method on encrypted message
Step 4: Take video as input which act as cover medium
Step 5: Segmented video into N number of frames
Step 6: Divide each frame into YUV color space
Step 7: Apply 2 dimensional DWT (2D-DWT) individually on each Y, U, V frame component
Step 8: Embedding message into middle and High frequency coefficients (LH, HL, LL) of each of the Y, U, V components.
Step 9: Apply inverse 2D DWT on Y, U, V frame components
Step 10: Regenerate Stego frame from YUV stego components
Step 11: Reconstructed stego video as output by rearranging all embedded stego frames.

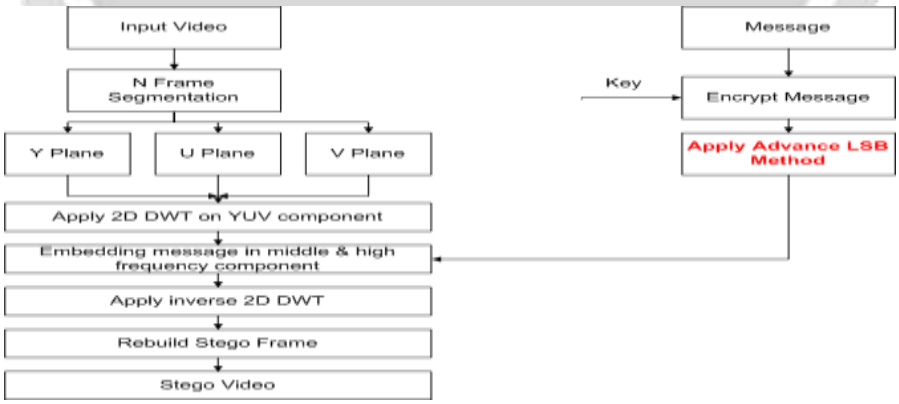

Fig -2: Proposed embedding approach

B. Extracting Process:

Step 1: At Receiver side , stego video is taken as input
Step 2: Segmented stego video into N number of stego frame
Step 3: Divide each stego frame into YUV color space
Step 4: Apply 2D-DWT individually to each Y, U, V component.

Step 5: Extract the message from middle and high frequency coefficients (LH, HL, HH) of each Y, U, V component
Step 6: Apply advance LSB method on extracted message
Step 7: Decrypt the message.
Step 8: Reposition of message again to original bit using same key as sender side
Step 9: Extracted secret message from stego video as output received.

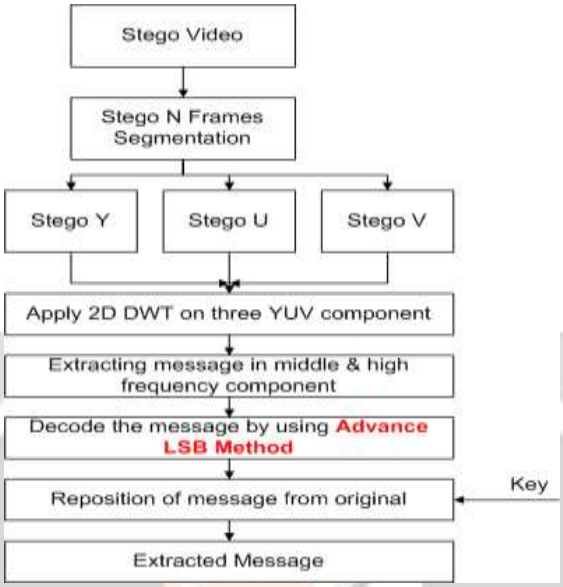

Fig -3: Proposed extracting approach

6. CONCLUSION

There are number of issues related to video steganography i.e. robustness, security, hiding capacity, compression and decompression etc. In proposed method we used advance LSB approach for embedding process i.e. improved performance of steganography system in terms of visual quality and robustness. Because unlike other methods, advance LSB doesn't directly embedded bit of message in video, in advance LSB the embedding process depends on the message bit and the parity generated by the LSB of each color components. Advance LSB works based on odd even parity rules so it is provided high robustness and high visual quality.

REFERENCES

[1] 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.

[2] Remah Alshinina, Khaled M.Elleithy et al."A DCT-based Robust Video Steganographic Method Using BCH Error Correcting Codes ". IEEE, 2015, doi : 10.1109/LISAT.2016.7494111.

[3] Ramadhan J. Mstafa, Khaled M.Elleithy et al."A Highly Secure Video Steganography using Hamming Code (7, 4)", IEEE, 2014 , doi : 10.1109/LISAT.2014.6845191.

[4] Yingnan Zhang , Minqing Zhang , Ke Niu , Jia Liu ,"Video Steganography algorithm based on trailing coefficients". At INTERNATIONAL CONFERENCE ON INTELLIGENT NETWORKING AND COLLABORATIVE SYSTEMS, IEEE, 2015, pp.360-364, doi: 10.1109/INCoS.2015.47.

[5] Mennatallah M. Sadek & Amal S. Khalifa, & Mostafa G. M. Mostafa "Robust video steganography algorithm using adaptive skin tone detection". Springer, 2016, doi: 10.1007/s11042-015-3170-8.

[6] Yi-Tu.Wu, F.Y. Shih, Genetic algorithm based methodology for breaking the steganalytic systems, Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 36(1), Feb 2006, pp.24-31, doi: 10.1109/TSMCB.2005.852474 .

[7] M. Kharrazi, H.T. Cover Selection for Steganographic Embedding, Image Processing, IEEE International Conference, Oct 2006, Atlanta, GA, ,doi: 10.1109/ICIP.2006.312386

[8] C.Abbas, C.Joan and C.kevin, Digital Image steganography: survey and analysis of current methods, Signal Processing, 90(3), March 2010, 727752, doi:10.1016/j.sigpro.2009.08.010

[9] W.Andreas, P.Andreas, Attacks on Steganographic Systems, Information Hiding, 1768, Oct 2000, pp.61-76, doi: 10.1007/10719724_5.

[10] V. Sathya, K. Balasubraminvam, N. Murali, M. RajaKumaran, Vigneswari, Data Hiding in audio signal, video signal text and JPEG images, IEEE INTERNATIONAL CONFERENCE ON ADVANCES IN ENGINEERING ,SCIENCE AND MANAGEMENT(ICAESM), March 2012, pp.30-31.

[11] T. Shanableh, Data Hiding in MPEG video files using multivariate regression and flexible macro block ordering, IEEE Transaction. Inf. Forensics, Security, 7(2), 2012, pp.455-464, doi: 10.1109/TIFS.2011.2177087 .

[12] S. Mansi, M.Vijay, Current status and key issues in image steganography: A survey, Computer Science Review, 13-14, Nov 2014, pp .95-113, doi: 10.1016/j.cosrev.2014.09.001 .

[13] Chen Ming, Zhang Ru, Niu Xinxin & Yang Yixian "Analysis of Current Steganography Tools: Classifications & Features", IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT INFORMATION HIDING AND MULTIMEDIA SIGNAL PROCESSING, pp.384 - 387, 2006, doi: 10.1109/IIH-MSP.2006.265023 .

[14]Tao Zhang, Wenxiang Li, Yan Zhang, & Xijian Ping "Detection of LSB Matching Steganography Based on Distribution of Pixel Differences in Natural Images" PROCEEDINGS OF INTERNATIONAL CONFERENCE ON IMAGE ANALYSIS AND SIGNAL PROCESSING, pp. 548-552, 2010, doi: 10.1109/IASP.2010.5476056.

[15] Mamta Juneja, and Dr. Parvinder S. Sandhu "An Improved LSB based Steganography Technique for RGB Color Images "2ND INTERNATIONAL CONFERENCE ON LATEST COMPUTATIONAL TECHNOLOGIES (ICLCT'2013), pp. 10-14, 2013 .

[16] 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 .

[17] Richa Khare, Rachana Mishra, Indrabhan Arya. "Video Steganography by LSB Technique Using Neural Network" PROCEEDINGS OF INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENCE AND COMMUNICATION NETWORKS, pp. 899-902, 2014, doi: 10.1109/CICN.2014.189.

.

.