Comparison of Various Video Steganography Techniques

Ritej Gaba[#1], Gaurav Deep[*2]

[#]*University College of Engineering, Punjabi University Patiala Jalalabad(w), Punjab, India*

[1]ritejgaba@gmail.com

[*] *University College of Engineering, Punjabi University Patiala Patiala, Punjab, India*

[2]deepgaurav48@gmail.com

Abstract— **The aim of this study is to compare the various video steganography techniques and to find which technique is better. Which technique can be used for hiding more amount of data and which technique is less prone to attacks from the third party other than the authorized sender and receiver. This paper gives the brief knowledge of various video steganography techniques.**

Keywords—**Bit-plane Complexity Segmentation(BPCS), Least Significant Bit(LSB), Human Visual System(HVS), Set Partitioning in Hierarchical Trees(SPIHT).**

I. INTRODUCTION

Steganography is a technique of hiding secret data within any media. The objective of the steganography is to hide the secret data within a cover media in such a way that others cannot recognize the presence of secret data. Modern steganography techniques uses the digital multimedia files to hide secret data also at the network packet level[1].

Video steganography is to hide secret data in video cover media. Video steganography techniques are classified into temporal or frequency domain and spatial domain. In frequency domain, first of all frames are extracted from a video file that we are using as cover media and then a particular frame is to be selected for hiding the secret data, after that this frame is transformed into frequency components by using FFT,DWT or DCT and in the end messages are embedded in some or all of the transformed coefficients. This embedding can be bit level or block level[2]. In spatial domain the bits of message can be inserted in intensity pixels of the video in LSB positions. Video cover media for hiding the secret data is famous these days as it has attracted a lot of attention because they can hide a large amount of secret data. The hidden data can be embedded into image or the sound file of the video[3]. The main advantage of hiding data into video file is the added security against the attack of the third party due to relative complexity of the structure of video file as compared to image file. In fact video steganography is much similar to image steganography the difference is, video is a stream of frames which are also a type of images. When fourteen images per second are played it becomes a video. If thirty images per second are used then it becomes a good quality video.

II. VARIOUS VIDEO STEGANOGRAPHY TECHNIQUES

A. Bit-plane complexity segmentation(BPCS) steganography

This method is based on wavelet compression for video data and bit-plane complexity segmentation steganography. This method uses the lossy compressed video which provides a natural way to hide large amount of data. it makes use of BPCS decomposition and characteristics of the human vision system where noise like regions in bit-plane of an image which is extracted from a video are replaced with secret data without damaging the image quality because if the image quality is damaged then it would effect the video in which it has to embed[4].

In wavelet based video compression methods such as 3-D set partitioning in hierarchical trees(SPIHT) algorithm and motion-jpeg2000, wavelet coefficients in DWT is quantized into bit-plane structure and so BPCS steganography can be applied in wavelet domain. 3-D SPIHT-BPCS steganography and Motion-JPEG2000-BPCS steganography are implemented and tested, which are the combination of 3-D SPIHT video coding and BPCS steganography, and that of Motion-JPEG2000 and BPCS steganography, respectively. Final results show that 3-D SPIHT-BPCS is better than Motion-JPEG2000-BPCS in case of embedding secret data in video file i.e embedding performance of this is better. In 3-D SPIHT-BPCS steganography, near about 28% of embedding rates of the compressed video size are achieved for twelve bit representation of wavelet coefficients with no noticeable degradation in video quality.

B. Least significant bit(LSB) based video steganography

This technique is a simple and common approach to hide data in video cover file. First of all video is converted into frames and then the least significant bit of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue color components can be used, since they are each represented by a byte. We can say, one can store 3 bits in one pixel. An image of size 800*600 can store total amount of 1440000 bits of secret data[5].

For example a grid of 3 pixels of 24 bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

If we want to hide character A which has ASCII code as 01000001 into least significant bit of this part of the image then the resulting grid will be as:-

(00101100 00011101 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

The LSB's has been changed in the final grid as shown.

C. Hash-Based least significant bit LSB video steganography

This technique is inspired from simple LSB video steganography technique. This technique was proposed because of the simplicity of the LSB technique and the chances of attacks from third party were more. So hash based LSB technique is different from LSB technique as it takes eight bits of secret data at a time and hide them in LSB of RGB pixel value of carrier frame in 3,3,2 order respectively and in such a way that first 6 bits of the 8 bit secret data are inserted into R and G pixels and other 2 bits are inserted into B pixel. This distribution pattern is taken because chromatic influence of the blue color is more to the human eye than the red and green color[2]. The embedding positions of the eight bits out of four available bits of LSB is obtained using a hash function like:-

$$a=b\%c$$

where a is calculated LSB position within a pixel, b represents the position of each hidden image pixel and c is number of bits of LSB which is 4 for the present case. The robustness of this technique is enhanced as compared to the other LSB techniques because of the random distribution of the bits. After hiding data in multiple frames of a video file, these frames are combined together to make a stego video and this video now can be used as a normal streaming video.

On the receiver side the authorized user has to perform the reverse process to decode the hidden message or data. First of all, stego video will be broken into frames after reading the header information and then using the same hash function on various frames can be applied to get the data.

D. Polynomial equation based LSB video steganography technique

This technique is also based on the LSB technique but with some enhancement of using polynomial equation to calculate the LSB bit positions to hide data same as the hash based technique but instead of using a hash method it uses a polynomial equation to determine the LSB positions. First of all it reads the original video signal and text to hide. Then it embeds this text into video signal. For this it converts the text into binary format, this binary conversion is done by taking the ASCII value of the character and then this ASCII value is converted into binary format. After performing this it takes the binary representation of the sample video signal and insert the binary representation of the text into the cover signal[5].

The LSB bits of the video signals are replaced by the binary bits of the data and this encoded signal is called stego signal. The message we want to hide is converted into the ASCII format then into the binary representation with each word of length 8 bits. These bits are substituted in the LSB of binary representation of each frame sample. Example of polynomial equation for calculating the LSB position in available 4 LSB's is as such:-

$$5x+1=0 \text{ or } 3x+3=0$$

On receiver side the authorized user can only decode or receive the hidden data if it knows the polynomial equation used to hide the data.

E. A Blind Video-Steganography Technique Based on Visible Light Wavelength for Raw Video Streams

In this in this technique they have developed a new data hiding method in video cover media based on the HVS(human visual system). This method uses visible light wavelength approach to find the most appropriate pixel location, in which the secret data are stored, in the cover video file. They have utilized the imperceptible light wavelengths(ultraviolet and infrared) for this purpose[3].

In this technique, the data hiding procedures are implemented by utilizing the imperfection of the color vision. It is based on finding the appropriate pixels in the video with the help of visible light spectrum data perceived by the HVS. The pixels having the boundary values (380nm to 750 nm) of visible light spectrum in the cover video frames, in which secret data has to be stored is determined. It can also be said that the pixels having a wavelength in the range of infrared or ultraviolet colors are searched for hiding the secret data in the video cover file. It is a known fact that human eye cannot detect the minute change in the visible light spectrum.

The hiding procedure is initiated by segmentation of the video file into frames. The wavelength value of each pixel in frames of cover media are calculated. As we know each pixel has mainly three components Red, Green and Blue, each color compound is individually recorded into a table. However only a particular wavelength range of each color is significant for pixel selection. These values are as listed below in the table[3]:-

Wavelength	R-intensity	G-intensity	B- intensity
Violet: 380-400	97-130	0-30	97-175
Red: 730-750	161-200	0-30	0-50

So according to this table RGB pixel having (100,0,105) code is appropriate for data hiding procedure. After determining the appropriate pixels for hiding the in video frames, the secret data is embedded into those pixels. After hiding these pixels are further checked to see whether their current wavelength is within the acceptable limits. If so, then each acceptable pixel is labeled as 1 otherwise labeled 0. In

this technique wavelength deviation is the crucial criteria for pixel selection so the wavelength deviation should be kept to minimum for the perceptiveness.

F. Cluster based video steganography using pattern matching

This technique is different from other techniques, as it is not based on the LSB technique, it does not use any hash method or polynomial equation to calculate the LSB bits, it does not work as bit plane complexity segmentation video steganography technique, it also does not use the wavelength intensity of different colors of a video frame like Wavelength based technique. It is cluster based video steganography using pattern matching, it means, it uses the clusters to hide data and these clusters are determined by using the pattern matching algorithm[6].

It starts same as other techniques of extracting frames from a video file in which want to hide secret data, after extracting the frames, we have to choose particular frame to hide data, As we know there are three main colors Red, Green and Blue in any color image or frame extracted from a video. After selecting the frame we have applied an algorithm to match these colors pixels, with this algorithm we get clusters of these three colors Red, Green and Blue, with the number of pixels the each cluster have. From this number or count we get to know which cluster has more number of pixels or we can say which cluster is bigger in size. Then we chose this cluster to hide secret data, this could be Red, Green or Blue cluster based on the frame we have selected. Particular pixels after a fixed distance are selected for embedding the secret data in color cluster by setting the offset value it means the distance between the two pixels chosen for hiding data in a color cluster.

Same as this, all color clusters can be used to hide data in increasing order or decreasing order in number of pixels, as well as all the frames can be used if we want to hide large amount of data but it is not recommended because it can degrade the quality of the video file.

III. COMPARISON OF VARIOUS TECHNIQUES

Sr. No.	Video steganography techniques	Amount of data we can hide	Security	Complexity
1	BPCS	Medium	Low	Medium
2	LSB	Medium	Low	Low
3	Hash Based LSB.	Medium	Medium	Medium
4	Polynomial equation based LSB.	Medium	Medium	Medium
5	Visible light wavelength based.	Small	Medium	High
6	Cluster based using pattern matching.	Large	High	Medium

Various attributes used with values are as such:

I. Amount of data we can hide: small, Medium and Large.

II. Security: Low, Medium and high.

III. Complexity: Low, Medium and High.

IV. CONCLUSION

In the above study and comparison of various video steganography techniques we found that among all these techniques Cluster based video steganography using pattern matching is best to use because of many reasons where first one is the amount of data that we can hide is large by using all different color clusters like Red, Green, Blue, Black, White etc in increasing or decreasing order in the number of pixels each cluster contain. Second one is the security feature, for unauthorized user it is really very difficult to decode the secret message until or unless he/she knows about the algorithm used to create clusters, algorithm used to give offset in the cluster and the frame in which data is hidden. Third one is the complexity to implement this technique which is also not high as other available techniques. This technique can be implemented in MATLAB.

REFERENCES

[1] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, "Steganography and Steganalysis: Different Approaches"

[2] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Stagenography(HLSB)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol. 1, No 2, April 2012.

[3] Ozdemir Cetin and Ahmet Turan Ozcerit, " A Blind Video-Steganography Technique Based on Visible Light Wavelength for Raw Video Streams", *1st International Syposium on Sustainable Development*, June 9-10 2009, Sarajevo.

[4] "Video steganography based on bit-plane decomposition of wavelet transformaed video" http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=837722

[5] A Swathi and Dr. S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", *International Journal Of Computational Engineering Research (ijceronline.com)*, Vol. 2 Issue. 5.

[6] Ritej gaba and Er. Gaurav deep, "Cluster based video steganography using pattern matching", *International journal of advanced and innovative research*, Vol 2 issue 5, may 2013.

[7] http://www.irongeek.com/i.php?page=videos/steganography-intro)

[8] Niels provos and Peter Honeyman, "Hide and seek- an introduction to Steganography".

