ISSN (e): 2250 – 3005 || Volume, 05 || Issue, 10 ||October – 2015 ||
International Journal of Computational Engineering Research (IJCER)

A Study on Video Steganographic Techniques

Syeda Musfia Nasreen , Gaurav Jalewal, Saurabh Sutradhar

Abstract

Data hiding techniques have taken important role with the rapid growth of intensive transfer of multimedia content and secret communications. The method of Steganography is used to share the data secretly and securely. It is the science of embedding secret information into the cover media with the modification to the cover image, which cannot be easily identified by human eyes. Steganography algorithms can be applied in audio, video and image file. Hiding secret information in video file is known as video steganography. Video Steganography means hiding a secret message that can be either a secret text message or an image within a larger one in such a way that just by looking at it, an unwanted person cannot detect the presence of any hidden message. For hiding secret information in the video, there are many Steganography techniques which are further explained in this paper along with some of the research works done in some fields under video steganography by some authors. The paper describes the progress in the field of video Steganography and intends to give the comparison between its different uses and techniques.

Keywords: *video steganography, LSB method, data hiding, embed, stego video, AVI, PSNR.*

I. Introduction

The premise from which to measure a secure video steganography system is to assume that the opponent knows the system being employed, yet still cannot find any evidence of the hidden message. Video steganography algorithm tries to replace the redundant bits of the cover medium by the bits of the secret medium. Now the availability of those redundant bits to be inserted in the cover media depends on the quality of video or sound. Military, industrial applications, copyright, intellectual property rights etc. are some of the most commonly used applications of video steganography.

The advantages of using video stream as the cover file are to get extra security against the attacker because the video file is much more complex that the image file. One more advantage of embedding the secret data to the video is that the secret data is not recognized by the human eye as the change of a pixel color is negligible. In video steganography, we can also very secretly hide data in audio files as it contains unused bits. We can store secret data up to about four least significant bits in the audio file. So it is more beneficial to use video steganography rather than other steganography methods when we need to store more amounts of secret data. [1]

1.1. Techniques of video steganography

There are various techniques of video steganography. The best technique is to hide the secret data without reducing the quality of the cover video, so that it cannot be detected by naked eyes. The embedded video is known as the "stego" video which is sent to the receiver side by the sender.[2]

Variety of video steganography techniques are used now days, to secure important information. Some much known techniques are explained briefly in the following:

1.2. LSB (Least Significant Bit) method

LSB is said to be the best method for data protection because of its simplicity and commonly used approach. It is the most easiest and effective way of embedding data. In LSB, the cover video's pixel values are extracted which are in bytes, then its LSB are substituted by the bits of the secret message that we will embed. Now since we change only the lsb bits of the host video, it doesn't gets distorted and almost looks alike as the original video.[3]

1.3. Non-uniform rectangular partition

This method is for uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. But we have to make sure that both the secret as well as the cover file should be of almost the same size. Each of the frames of both the secret as well as cover videos is applied with image steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video. [3]

1.4. Compressed video steganography

This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency. [3]

1.5. Anti-forensics technique

Anti-forensic techniques are actions taken to destroy, hide and/or manipulate the data to attack the computer forensics. Anti-forensic provides security by preventing unauthorized access, but can also be used for criminal use also. Steganography is a kind of anti- forensic where we try to hide data under some host file. Steganography along with anti- forensics makes the system more secure. [3]

1.6. Masking and filtering

Masking and filtering are used on 24 bits/pixel images and are applicable for both colored and gray scale images. It is like watermarking over an image and doesn't affect the quality of that image. Unlike other steganography techniques, in data masking the secret message is so processed such that it appears similar to a multimedia file. Data masking cannot easily be detected by traditional steganalysis.[3]

II. Related works

In 2009, Eltahir, L. M. Kiah, and B. B. Zaidan presented a high rate video streaming steganography system based on least significant bit method.[22] The results of using this method on instant images saves up to 33.3% of the image for data hiding which is an enhancement for LSB. The idea of the suggested method is by using 3-3-2 approach, which uses the LSB of RGB (red, blue, green) colors in 24 bits image. The method here takes the least 3 bits of red color, 3 bits of green color and only 2 bits from blue color because human vision system is more sensitive to blue than red and green, to come up with 1 byte which is used for data hiding. So to make the outcome image look almost the same as the original, the 3-3-2 approach is very efficient.
The result was found to be good and the size of data was substantial i.e. about 33.3% from the size of image. They didn't found any difference between two frames and their histograms, especially for human vision system. [4]

In the year 2011 ShengDun Hu, KinTak U presented a video steganography system based on non-uniform rectangular partition. This technique is used in uncompressed videos. In this method a secret video is hidden in a cover video, both should be of almost the same size. In each frame of both the videos, a mechanism is applied for hiding the video stream. The frame length of the cover video should be greater than or equal to the frame length of the secret video, in order to hide the secret video in to the cover or host video. Each frame of secret video is portioned in to non-uniform rectangular part which is encoded. The secret video stream is hidden in the leftmost four least significant bits of each frame of the host video stream.
Results of using this technique showed no distortion, so no one will think that any kind of data is being hidden in the frames. All the PSNR values of the frames were larger than 28db. [5]

In 2014, R. Shanthakumari and Dr.S. Malliga presented a paper on Video Steganography using LSB matching revisited algorithm, where they have taken a video stream of AVI format. In the paper they have initially splitted the cover video into frames. Now, the message can be embedded in multiple frames, therefore size of a message does not matter in video steganography. After embedding the secret data in multiple frames of the cover video stream, all the frames are then grouped together to form the stego video, which is then again will be splitted into frames and data will be extracted in the receiver side.
The proposed method in this paper was found to have two problems which were low embedding rate and lack of security. LSBMR algorithm has a low replacement rate and hence the Mean Square Error (MSE) is low, as a result of which LSBMR is more secured than the LSB algorithm for data hiding. The PSNR value decreases on increase of the embedding unit.[6]

In 2015, Vivek Kapoor and Akbar Mirza presented a paper on Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission. At first, they have divided the host video into frames, then the text file to be embedded is compressed using the ZIP compressor and the bytes are generated. The advantage of sending compressed data over the network is to minimize the payload and reduce extra burden of the network. Then the color of each color pixels is calculated in RGB 24 bit format. Then chunks of bits are created from the extracted bytes of the secret message. Then these chunks are embedded in the video frames. Text files are then combined with video frames and the file is sent. The proposed method is designed for MPEG format; however it can work with other video file formats also like AVI, 3GP by doing some modification in it. They have calculated the Data Quality, Mean Squared Error(MSE) and Peak Signal to noise ratio(PSNR) of both the original and the stego video and it was found that Mean Square Error and Peak Signal to Noise Ratio is low enough that it cannot be noticed easily in the Steganalysis process. Then they have also compared their method with LSB method and they found that the proposed method gives better MSE and PSNR values than the LSB method. [7]

In 2013, Hemant Gupta, Dr. Setu Chaturvedi presented a video steganography through LSB based hybrid approach. This method is used in AVI videos. The video is converted into 20 equal gray scale images. Data hiding is done is done in the host video by using Single bit, two bit, three bit LSB substitution and after that Advanced Encryption Standard Algorithm is applied. After processing the source video by using the data hiding procedures, the encrypted AVI Video is sent by the sender and decryption is performed by the receiver. They have found the PSNR and correlation factor between Original and embedded image for 1 bit LSB & 2 bit LSB & 3 bit LSB Substitution and AES method. It is observed that PSNR value decreases and security increases with the increase of LSB substitution bit. In this paper they have found no correlation relation between original image and encrypted image for different frames.[8]

In 2013, Pooja Yadav, Nischol Mishra and Sanjeev Sarma presented a video steganography technique with encryption and LSB substitution. In their technique, they had 2 video streams called Host and the Secret video with same number of frames and equal frames per second (12 frames and 15 fps). A header of 8 bits is used for representing the frame size of the hidden video and was appended in the beginning of each frame. After this the appended header was encrypted along with the secret frames by using symmetric encryption. Using sequential encoding, the secret video frames are encoded to the host video frames and then from the encoded frames the secret video is generated. They used XOR transformation for encrypting the data with secret keys and decrypting the secret message to retrieve the original information. For sequential encoding they used a pattern of BGRRGBGR (Blue (B), green (G) and red (R)) to encode the message in the LSB. They used 2 AVI video files and found the PSNR value of the stego video as 35 dB which was the same as the host video.
To find the result they have calculated the PSNR value frame by frame and maximum, minimum and average PSNR value of total frames. Frame by frame comparison of the host and the embedded video stream shows that there was no distortion in the stego video. According to the calculated PSNR values, it was observed that there was much similarity between the host and the embedded video. The host video was found to be distortion less and also the recovered video stream had also an acceptable quality. [9]

Ramadhan J. Mstafa and Khaled M. Elleithy, Senior *Member, IEEE, Department* of Computer Science and Engineering, University of Bridgepor, proposed a highly secured method of video steganography by using Hamming Code (7, 4). In their project, they used 9 video files as cover and 1 secret image which were to be hidden. At first, they generated the frames from the video stream and then separated each frames into Y, U & V components. Then by the use of a special key, all pixel positions of video are randomly ordered. A binary image is used as the message which was converted to a 1-dimensional array and the position of the message is changed by a key. Now, 4 bits of the message is encoded using Hamming Code (7, 4) encoding technique. Now, the encoded data is XORed with the random values and the result is embedded in 1 pixel of Y, U and V components. The pixels are then reordered in their original position and the final stego video was rebuilt from the embedded frames. Similar steps are involved in the data extraction process.
The stego video has mostly the same quality as the original video because of the low modification on the host video stream. The visual quality is measured by the PSNR and all the obtained experimental results have a PSNR above 51 dBs. Using this method, attackers are not likely to be suspicious since they have a good visual quality for stego videos. The algorithm is much secured because security has been satisfied by having more than one key to embed and extract the secret message. [10]

In 2008, Bin Liu et al proposed a new steganography algorithm for compressed video Bit streams. In this technique, the embedding and detecting data is done only in compression domain and no decompression is needed here. The cover video was first compressed by eliminating temporal, spatial and statistical redundancies.

The video was then divided into several slow speed and single scene video sub-sequences. After the scene detection process, they embedded the secret message in the video file without any distortion. Finally the embedded video was tested for Steganalysis to check the presence of hidden data in the video. They constantly adjusted the scale factor for manipulating the hidden data strength until the analyzer was unable to detect the hidden message.

The PSNR value and the correlation value changes the magnitude of the stego-video, which says that the perception quality and intraframe correlation of test video is little changed. There is no noticeable change in the visual quality of the compressed video, also their system was found to highly secured as they were continuously testing the video for Steganalysis.[11]

III. Comparative Analysis

This paper presented a background of Steganography and a comparative study of some Steganographic techniques. There are two important parameters of evaluating all Steganography technique, first is imperceptibility and the second is capacity. Imperceptibility means the embedded data must be imperceptible to the observer and computer analysis. Capacity means maximum payload is required, *i.e.* maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. The results of surveying the papers in different techniques of video steganography showed that all the methods possess the ability to hide data without noticing changes in their properties.

It was found that in [4], they have used the 3-3-2 approach along with LSB and the result was found to be good and about 33.3% from the size of image can be used for data hiding. In other words, in the space of 5 images, 500 pages of data could be stored without resizing. Similarly, 1 second in certain video types contains approximately 27 frames, which in turn creates a lot of room for hiding data. In [5], Results of using this technique showed no visual distortion in the host file and even the quality of the new video generated can be accepted for practical use. In [6], it has been known that in the LSB algorithm due to high replacement rate, MSE value is high. So it lacks from security**.** In case of LSBMR algorithm due to low replacement rate, MSE value is low which makes it secure when compared to LSB algorithm. In their method, intruder may not be able to identify the presence of the secret message inside the frame. Also, the comparison with the original video never gives the original secret message, which ensures additional security.

In [7], videos of different sizes and resolutions are tested for their method and they have got successful in keeping the MSE and PSNR value low enough that it cannot be noticed easily in the Steganalysis process. They have provided a comparison between the basic LSB method and their method gave better values of MSE and PSNR than the LSB method. The average PSNR of the proposed LSB embedding technique (per pixel, RGB) to the traditional layering technique in which embedding is done by layers of RGB. They found an improvement of about 1.5 dB in their PSNR value when compared to the traditional LSB technique and also a lesser MSE which means in detectability. In [8], the authors calculated PSNR value for different amount of LSB substitution. For 1 LSB substitution, the PSNR value was found between 45-50 for different no of frames. For 2 bit LSB substitution, PSNR was found to be in the range of 40-45. And for 3 bit LSB substitution, PSNR value was about 35. By the use of AES encryption, their method was more secured as compared to traditional LSB techniques. In [9], their results showed that no visual distortion is there in the host video stream and even the quality of the recovered secret video is also acceptable in practical. In [10], use of Hamming code makes the technique highly efficient and more secured. The authors used more than 1 key and thus have obtained a high level of security as compared to traditional steganographic methods like LSB substitution where only one XOR encryption is used. In [11], unlike other steganographic technique, the authors have implemented a closed loop feedback steganalysis to test their project's immunity towards steganalysis. The complete project was done in compressed domain hence avoiding decompression process.

With continuous advancements in technology it is expected that in the near future more efficient and advanced techniques in steganalysis will emerge that will help law enforcement to better detect illicit materials transmitted through the Internet.

IV. Conclusion

In the era of fast information interchange using internet and World Wide Web, video Steganography has become essential tool for information security. This paper gave an overview of different video steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years.

References

[1] https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/chakraborty.doc

[2] Arup Kumar Bhaumik, Minkya choi, "Data hiding in video" IEEE International journal of database application,vol.2no.2 June 2009.pp.9-15

[3] https://edupediapublications.org/journals/index.php/ijr/article/view/678/309

[4] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan, "High Rate Video Streaming Steganography," in Information Management and Engineering, 2009. ICIME '09. International Conference on, 2009, pp. 550-553.

[5] ShengDun Hu, KinTak U," A Novel Video Steganography based on Non-uniform Rectangular Partition ",IEEE International Conference on Computational Science and Engineering,pp 57-61, Aug.2011.

[6] R. Shanthakumari and Dr.S. Malliga," Video Steganography using LSB matching revisited algorithm", IOSR Journal of Computer Engineering ,Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01-06

[7] Vivek Kapoor and Akbar Mirza, "An Enhanced LSB based Video Steganographic System for Secure and Efficient Data Transmission", International Journal of Computer Applications (0975 – 8887) Volume 121 – No.10, July 2015

[8] Hemant Gupta and Dr. Setu Chaturvedi,"video steganography through LSB based hybrid approach", International Journal of Engineering Research and Development, Volume 6, Issue 12 (May 2013), PP. 32-42

[9] Pooja Yadav, Nischol Mishra and Sanjeev Sarma, "video steganography technique with encryption and LSB substitution", 2013, School Of Information Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India

[10] Ramadhan J. Mstafa and Khaled M. Elleithy, Senior Member, IEEE, Department of Computer Science and Engineering University of Bridgeport Bridgeport, CT 06604, USA, "A Highly Secure Video Steganography using Hamming Code (7, 4) "

[11] Bin Liu, Fenlin Liu, Chunfang Yang and Yifeng Sun , "Secure Steganography in Compressed Video Bitstreams",The Third International Conference on Availability, Reliability and Security