Improved Data Security Using Video Steganography

Anmol D Kulkarni, Esti Bansal, Hole Rajashree B, Jadhav Rasika R, Lakshmi Madhuri

Abstract— **Data security is a crucial issue now a days. Many techniques are available to protect confidential data from unauthorized users. Steganography is one of them. Many algorithms are available for steganography but these algorithms suffer from issues like less security, less data hiding capacity, etc. This paper aims to improve data security, to maintain the quality of the cover image and to reduce the size of the cover video before transmission. So, this paper proposes a two stage process to conceal secret text data into a video clip. In the first stage image steganography will be done using improved LSB and in the second stage video steganography will be done using DCT algorithm. The size of the video increases after embedding the data so lossless compression technique will be applied. The results of improved LSB and DCT were studied and compared with various techniques.**

***Index Terms*— Cover Object, Image Steganography, Video Steganography, Video Quality.**

I. INTRODUCTION

Now a days internet has become a popular medium for communication. The confidential data can be transmitted very easily but it provides vast opportunities for hackers to filch this data. Thus, the security of confidential data has become a very crucial issue. One of the ways of securing the secret or confidential data is Steganography.

Steganography is the technique of concealing secret data like message, image, audio or video in another message, image, audio or video to secure the secret information from unauthorized users [2].

Image steganography is a technique to hide any data into an image and **video steganography** is a technique to hide any data into a video. The container image or video which hides the secret data is called **cover object**. The resultant obtained after hiding is known as **stego object**. (Object could be image or video.) Steganography hides the information as well as keep the existence of message secret whereas other techniques only hides the information, so an individual may notice that some information is hidden. It is a safe and efficient way of communication between sender and receiver. Many steganographic methods have been proposed in the recent years [1]-[6]. But these techniques often lack in security, and may degrade the quality of a cover object. So, this paper aims at providing three goals:

- Enhanced data security
- Visual quality of stego video must remain unchanged
- The size of the final stego video must be reduced for fast transmission.

To achieve these goals a two stage process is proposed. In the first stage image steganography will be done and in the second stage video steganography will be done. To reduce the size of the video before transmission compression will be done.

II. LITERATURE SURVEY

An algorithm based on color histogram was proposed for video steganography [1]. The video is divided into frames and the histogram value of each frame is calculated. These values are compared with threshold value. Based on this, secret data is hidden into the frames by dividing each pixel in two parts, the number of bits embedded in the right part are counted in the left part. This algorithm provides ability to hide large amount of data and extraction of written text without errors.

Using improved LSB (Least significant bit) method the secret image is hidden in the cover image [2]. BITMAP images are used as they are lossless. Then by using bit plane slicing the cover image is divided into three planes namely Red, Green and Blue. Then, the bits of the secret data is replaced by least significant bits Red, Green and Blue in the order 2, 2 and 4 i.e., 2 bits in Red, 2 bits in Green and 4 bits in Blue. More data hiding is provided.

Using LSB technique the secret data is embedded in the cover video [3]. The cover video is divided into frames and the secret data is extracted from the cover video. The complexity and security is increased by embedding the data in multiple frames of the video. The frames of the video are divided and are converted as .bmp images. The pixel values of the cover video are converted to binary values and the secret data is also converted into binary values. Then the bits of secret data are replaced by the order 2, 3, 3 into Red, Green and Blue respectively, 2 Least Significant Bits of Red, 3 Least Significant Bits of Green and 3 Least Significant Bits of Blue.

Manuscript received Nov, 2015.
Anmol D Kulkarni, *Computer Department, Dr D Y Patil School Of Engineering, Lohegaon, Pune.*
Esti Bansal , *Computer Engineering Department, Dr D Y Patil School Of Engineering, Lohegaon, Pune.*
Hole Rajashree B, *Computer Departmant, Dr D Y Patil School Of Engineering, Lohegaon , Pune.*
Jadhav Rasika R, *Computer Departmant, Dr D Y Patil School Of Engineering, Lohegaon , Pune.*
Lakshmi Madhuri,*Computer Department, Dr D Y Patil School Of Engineering, Lohegaon, Pune.*

An algorithm was proposed based on the principle of linear block code [4]. They used a sequence of nine uncompressed video sequence as cover data. The secret message was a binary image. First the pixel position of both cover video and a secret image was reordered using a private key. Even the secret message was encoded using Hamming code (7, 4) to make the message more secure before embedding.

In [5], a secret video stream is hidden into a cover video stream. The secret video is first divided into individual components then they are converted into 8-bit binary value. Then it is encrypted using XOR transmission with secret key. While embedding the secret frames are stored in cover frames in a pattern BGRRGBCR. This provided enhanced security to the secret frames.

Video Steganography implemented by changing the least significant bit of the visual file bite stream into a message file [8]. The message was then converted into byte code and encrypted before embedding to a carrier file. The functions of avifill32.dll were used with C# wrapper files. Even though this approach is successful, the issue faced in this method is that the carrier file should be an uncompressed AVI file.

III. PROPOSED SYSTEM

We are using a two stage process as shown in Fig. 1 for secure transmission of data to enhance the security of the secret data which is to be sent. In the first stage the text data is concealed into an image using improved LSB (Least Significant Bit) technique [2] to get a stego image. In the second stage the stego image is concealed into the video using DCT (Discrete Cosine Transform) [7] technique to maintain the quality of the stego video obtained after hiding the stego image. Since the stego video is large in size which will take more time for transmission so before transmission it will be compressed.

After receiving the stego video the receiver will decompress it and extract the stego image. Then subsequently from the stego image the secret message will be extracted.

Following is a brief description of the proposed system.

Stage 1: Image Steganography

In this stage the secret text message is hidden into a cover image by using improved LSB technique. This stage ensures that the secret text message do not degrade the quality of the cover image. The cover image taken is a colored image represented by 24bits where 8 bits are of Red, 8 bits of Green and 8 bits of Blue.

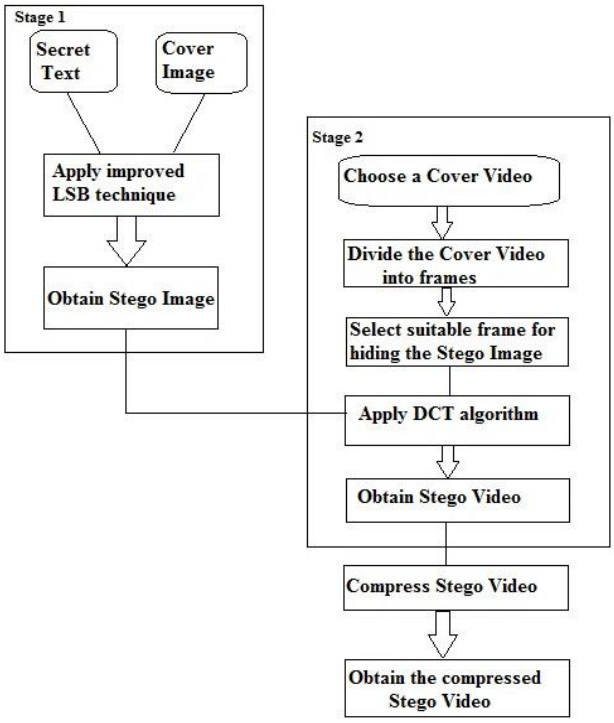

Fig. 1: Basic model for proposed system

Improved LSB technique

This technique involves following steps:

- Conversion of secret text message into bits.
- Bit plane slicing of the cover image into Red, Green and Blue Planes.
- Replacing the least significant bits of the cover image with the bits of secret text message such that more bits are replaced in Blue and fewer bits are replaced in Red and Green.

The reason of replacing more bits in Blue is to increase the quality of hiding. As stated in [2] [8] small changes in blue are not observed by human eyes since blue is less sensitive as compared to red and green. Thus more bits can be replaced in blue and fewer bits in red and green.

The output of this stage will be a stego image which will be given as input to the second stage.

Stage 2: Video Steganography

In this stage the cover video is taken of AVI (Audio Video Interleave) format and divided into frames. A suitable frame is selected. Frame selected will be such that it results less distortion after hiding the stego image into it. DCT algorithm is applied to the selected frame to conceal the stego image. The DCT algorithm separates the frame into parts of differing importance [7]. DCT transforms the time domain signal into its frequency components [9].

This stage maintains the visual quality of the video. The output of this stage is stego video. The two stages enhance the security of the secret text message by using steganography twice. Since the stego video obtained will be of large size which will take more time for transmission so the video will

be compressed further to obtain a compressed video. Compression can be classified into two types lossy and lossless. In our approach we will use lossless compression technique. The compressed video will be transmitted to the receiver through internet.

IV. CONCLUSION

The proposed method provides enhanced security to the secret message using the two stage process which doesn't let the hackers gain access to the secret message. All the mentioned goals can be achieved by the proposed system. This system is effective for covert communication between sender and receiver. In future even better techniques may be applied.

REFERENCES

[1] S. Deepa1, R. Umarani**, "**A Prototype for Secure Information using VideoSteganography", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 4, Issue 8, pp 442-444, August 2015..

[2] Amritpal Singh, Harpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", IEEE *International Conference on Electrical, Computer and Communication Technologies (ICECCT)* , DOI : 10.1109/ICECCT.2015.7226122, 2015.

[3] Mrudul Dixit, Nikita Bhide, Sanika Khankhoje, Rajashwini Ukarande, "Video Steganography", *International Conference on Pervasive Computing(ICPC)*, DOI: 10.1109/PERVASIVE.2015.7087159, 2015.

[4] Ramadhan J. Mstafa , Khaled M. Elleithy, "A Highly Secure Video Steganography using Hamming Code (7, 4)", *IEEE Long Island Systems, Applications and Technology Conference(LISAT)*, DOI: 10.1109/LISAT.2014.6845191, 2014

[5] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, "A Secure Video Steganography with Encryption Based on LSB Technique", *IEEE International Conference on Computational Intelligence and Computing Research*,, DOI: 10.1109/ICCIC.2013.6724212, 2013.

[6] A. Munasinghe, Anuja Dharmaratne, Kasun De Zoysa, "Video Steganography", *2013 International Conference on Advances in ICT for Emerging Regions (ICTer)*, pp- 056-059, DOI: 10.1109/ICTer.2013.6761155, 2013.

[7] Poonam V Bodhak, Baisa L Gunjal, " Improved Protection In Video Steganography Using DCT & LSB" *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume 1, Issue 4, pp 31- 37, April 2012

[8] http://www.abelard.org/colour/col-hi.htm

[9] D. Nithya Kalyani, Dr. K. Mahesh, "Safe Information Hiding Using Video Steganography", *International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 4, Issue. 7, pp. 502-512, July 2015.

