Secure Text Transmission Using Video Stegnography

A .Jyothirmai
Andhra Loyola Institute of engineering and Technology.
Vijayawada.

Ch. Manju Sri
Andhra Loyola Institute of engineering and Technology.
Vijayawada

***Abstract*—Text, Image and video are the three most basic forms of transmitting information. With the help of Image and video encryption methods any particular set of images or videos or text can be transmitted without worrying about security. The video stegnography is the process of hiding some secret information inside a video like military information. In the proposed paper a very simple and it provides an efficient output, using pixel mapping, is used for the encryption of the images. The addition of information to the video is not recognizable by the human eye, because this process the change of a pixel is negligible. In the proposed paper the video is divided into the photo frames using a mat lab code and all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. After the completion of the video stegnography encryption all the images is placed in a sequential manner and then all the frames are cascaded for generation of the original video file. This new video is almost similar to the original video file with no changes visible to the human eye. When use of stegnography, the probability of finding the hidden information by an attacker is less compared to other methods. And less processing time**

Index Terms: Pixel Mapping, Video Encryption, Cryptography, Stegnography.

I. INTRODUCTION

For normal human being the ability to perceive the motions of other animate frames or video has been extensively studied and if we compare the pixel of any consecutive frames in a video, it is shown that for the movements created in the running video only the small amount of the pixels are modified and rest all the pixels remain static if we compare the pixels of any consecutive frames in a video. So by the changes made in the smaller number of pixels in a sequence of images in a video file. This is very simple and effective method for visualizing any process under study. Research shows that among the consecutive images having million numbers of pixels only few hundred pixels are modified for the particular video.

For continuous work of vision, any video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. Generally the frame rate is 25 so we can say that 25 frames are captured within one second time. Our eye can detect 16 frames per second. For the efficient and successful implementation of this particular algorithm there is a requirement that the video needs to be segmented. For a particular case if we suppose that the video is of
1 minutes duration than this video majorly contains 1500 frames in it. These frames are vital building block for the video as well as for video encryption process.

We can send the text along with the frame by using various available watermarking techniques. There are various different watermarking techniques available like visual watermarking, discrete cosine transform, discrete Fourier transform and loss-less watermarking method. All the watermarking techniques recently available have certain drawbacks and also these methods are a little bit time consuming. Also the watermarking techniques can be modified using more advanced techniques for image processing. To get over the drawbacks of the watermarking techniques stegnography method can be used for the encryption of the video files. Stegnography is mainly useful in terms of efficient and accurate data processing for the case of the real time applications. In the proposed work also the stenography technique can be generated by using a pixel mapping algorithm. Also the stenography technique is faster and efficient in terms of time required for marking the particular set of images.

II. SECURE TEXT TRANSMISSION USING CRYPTOGRAPHY

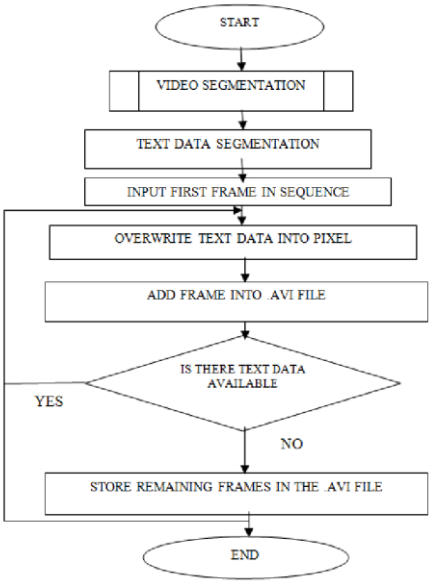

Figure 1 - Algorithm for Video generation for secured text data transmission

Figure 1 describes the flowchart showing the sequence of steps to be executed for generating the encrypted video file for secured text data transmission. The algorithm is briefly described in terms of flowchart for the better understanding of the whole process. The complete algorithm is coded in a Mat lab code showing the detailed involved in the video encryption and the text insertion in the video file for secured transmission. As shown in the algorithm in figure 1 the complete video is segmented into number of images using a small Matlab code module and after the processing of the video by the Matlab code module the video gets divided into different frames of same size. Then the text string which is to be inserted among the images is partitioned into the group of two bits each. As we need to modify only two pixels per image so we divide the text data into the group of two bits. Each character in the text data can be represented by a specific ASCI value so each of the character occupies 1 byte or 8 bits in an image. In this particular algorithm each of the image has to be modified by two pixel value and that also only the last two bits so each of the character in the text data to be inserted is represented by its ASCI value in line. After this each of the characters represented into the group of 8 bits is subdivided into the groups of 2 bits only. So now we have four groups for each of the character in the text data to be inserted into the images. In this algorithm to represent one particular character we require four pixels to store one particular character. As per the Glassman law importance of three basic colors which are red, blue and green are different. As per Glassman law the importance of the green layer is the most because it contains 59% weightage to generate any color in a particular pixel as per the requirement. Due to this in this particular algorithm only the value of the red and the blue layers are changed for processing the image so as to retain the original shade in the frame. The green layer in each of the images is unchanged. Only the blue and red layers pixels are modified in each of the image frames.

Now we have frames as well as very well distributed text data available so the next step to be followed is to encode or map the text data into the pixels of individual frames till the end of the text data. In the proposed work we are going to store one character into one frame so there is a requirement of n number of frames for storing n number of characters in the text data. For a particular image frame by modifying only two pixels at top and bottom of the image file does not make any significant changes in the visual effects of the frame so they are not visible to the human eye.

Next step to be followed as per the flowchart is to select the first frame from the sequence of the frames and identify the red layer of the first pixel and overwrite the last two bits with the first two bits of the character in the text data. Similarly also over write the last two bits of the blue layer pixel by the corresponding next two bits of the character. Same process is to be done for the pixels present in the bottom section of the image. By this way we can impose One character into one frame and the same process is to be followed for all the characters present in the text data with consecutive different frames.

As mentioned earlier we can impose m number of characters in a text data into n number of frames but the only condition is m should be less or equal to n. Different variants of the video encoding can be generated as described below :

Case 1: By modifying the segmentation pattern of the text data we can group the character bits into the group of 2, 4 or 8 bits. By this the number of frames to be modified can be increased or decreased according to the requirements.

Case 2: The text data insertion can be done into the alternate frames for boosting the data transmission security.

Case 3: One can transmit the details of the frames modified in form of an array in a frame. After that text data insertion can be done for providing the highest data security and safety.

Case 4 : One more modification can be done by changing the algorithm in a sense that the consecutive characters in the text data are encoded into all the three color layers in a particular fashion so that only the person who knows this pattern can decrypt the original text data.

III. CRYPTOGRAPHY

Cryptography is an art of protecting the information by transforming it into an unreadable and untraceable format known as cipher text. Only the person who possess the secret key can decipher or we can say decrypt the message into the original form. Cryptography is the technique by which one can send and share the information in a secret manner. Due the cryptography the information seems to be appearing like a garbage value and it is always almost impossible to find the information content lying under the image or a video file. A very simplest block diagram of cryptography encrypter is as shown in figure 2.

The encryption key generator is used to generate the encryption key as well as the public key as shown in the block diagram below. By using the encryption key the information content to be sent gets encrypted by the encryptor. The encrypted information is then transmitted to the particular receiver.

At the receiver end the Cryptography Decryptor is used as shown in figure-3. Which detect the original information content mapped onto the image or a video file with the help of a public key provided by the transmitter section. So by the use of the cryptography method only the receiver which has the knowledge of the public key can retrieve the original information content from the image or a video file. So even if any unwanted person gets the image or a video file with information content hidden in it, it cannot be extracted without proper public key. So public key plays a vital role in the whole cryptography process.

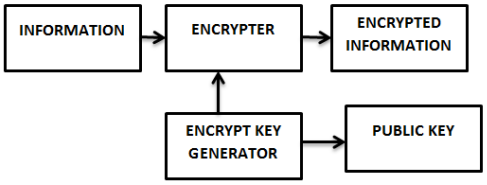

Figure 2 – Cryptography Encryptor

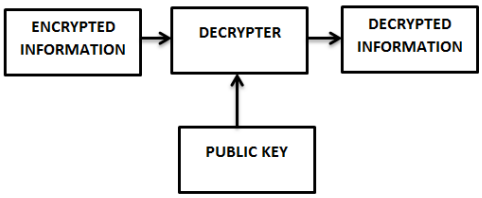

Figure 3– Cryptography Decryptor

IV. STEGNOGRAPHY

Stenography is the proposed method for secure the data more effectively. It is an art of hiding information by embedding message within each other. It works by replacing the very useless bits by the information content to be transmitted. It works by hiding information inside a cover. The cover may be an image file or a video file as per the user requirement. Even though the cover looks very simple and unchanged but it has information contained in it. Figure 4 describes the simplified process of stegnography.

First of all the video file is converted into a series of

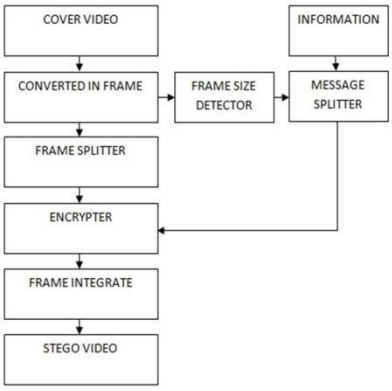

Figure 4 – Steganography Encryptor

frames of equal size. The information content which is to be transmitted by mapping onto the video file is distributed into small portion depending on the size of the frames in the video file. From each frame a smaller region is modified depending upon the private key. Due to this the selected groups looks very random to the third party who does not have the private key with them.

The selected pixels are then converted into the frequency domain with the help of the discrete cosine transform. Usually a predefined portion of the pixels like we say the last two or three bits are then replaced by the spilled message portion and then the pixel portion is again converted back into the spatial domain. The conversion from the frequency domain to the spatial domain is done with the help of inverse DCT. Then that group of pixels is placed back into the particular frame. This process is followed until the end of the whole information content. The frames are then arranged into a sequential manner and the video is constructed from it. Now this video contains the information which gets transmitted along with the transmission of the video file.

The Stegnography encoder has to keep some control message

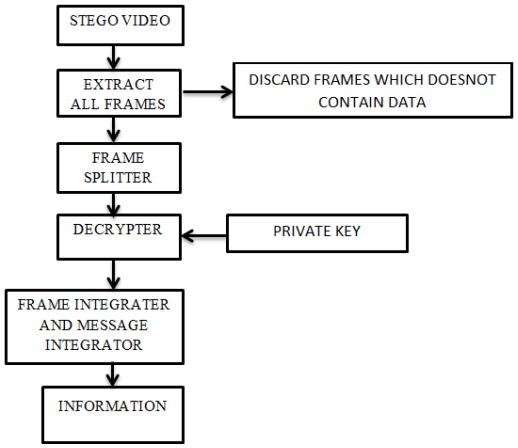

Figure 5: Steganography Decryptor

Into the video file by which the receiver can understand the data format, way of hiding the information content, type of encryption done etc. This is known as the rule list for a particular stegnography process. This rule list is generated and mostly it is placed in the first frame of the video file. This rule list acts as a reference for a particular desired receiver. Without rule list the receiver may not be able to understand and retrieve the original information content hidden within the received video file. So the rule list plays a vital role at the receiver side.

The main blocks in a Stegnography Decryptor is as shown in figure 5. From the figure 5 it is very clear that if the private key is not known than it is impossible to extract the original information content in the received video file. There are certain methods like some steganalysis tools by which the information can be detected without the use of the private key also. This seems to be the major drawback of the simple Stegnography technique. Stegnography method can be modified for improvements so that without private key the

Information may not get extracted easily. That means without private key the hidden information is doesn't recognize easily.

V. DATE & TIME STAMPING

The selected frames which have changes as per the algorithm are stored in the final video file. While capturing the frames for the video file, the date and time at which that particular frame has been captured becomes very much important in understanding the finer details of the subject. For these date and time stamping a lossless visual watermarking method is used. The stamping method results into the numeric characters that are represented with the help of the binary representation as shown in the figure 6.

Figure 6 -Time-stamping using Visual lossless Watermarking. With the help of the lossless watermarking algorithm the pattern for each character to be stamped if found. Algorithm also produces resultant pixel image of size 20x18. For each predefined location pixel to pixel mapping is done. In the numeric character if the pixel value is equal to 1, than the respective image pixel is kept as it is. If the pixel value is not equal to 1 than the pixel value is increased by a factor of 30 percent or reduced by same percentage depending on whether the pixel is bright or dark. Figure 6 shows the original, time stamped and recovered image. The numbers are stored

Figure 6 – Time & Date stamping Analysis

in the form of binary digits having array of 20x18 characters. The numbers which are denoted by 0 are highlighted and it represents the character to be displayed. With the help of a MATLAB based algorithm time stamping is done for the recorded images.

CONCLUSION

One of the important features of the proposed work is it plays a vital role in transmitting the information mapped on an either image or a video file very effectively and efficiently. The information in the image or a video is not visible to the human eye. Decode the original information, if and only if the person is having private key and identification of rule list. This method simplifies the task of securing the vital information from the misuse.

And original data protects from the unwanted user. With the use of the cryptography and stegnography combination the information security can be increased.

REFERENCES

[1] http://en.wikipedia.org/wiki/Time-lapse.
[2] Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.
[3] Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.
[4] R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.
[5] Avcibas, N. Memon, and B. Sankur Steganalysis using image quality metrics, IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003.