International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 4, Issue 2

A Real Time Approach for Secure Image Transmission Using Video Steganography

Metaliya Viral G. Anurag Rishishwar Manish Trivedi

Abstract— **Text, Image and video are the three most basic forms of transmitting information. With the help of text and image encryption methods, any particular set of words or images can be transmitted without worrying about security. With the help of pixel mapping algorithm, we can securely transmit the image inside the frames of video which are the basic building blocks of any video file. In the proposed research paper the video is distributed into the photo frames using a matlab code and all the frames are sequentially stored. Each such frame contains a combination of red, blue and green layers. Same way each image can be converted into red, green and blue layer. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. In the proposed work, top layer of each frames, get from video, are modified so as to insert single line of each layer from image. After the completion of the pixel value modification, all the images is placed in a sequential manner and than all the frames are cascaded for generation of the original video file with encryption. This new video is almost similar to the original video file with no changes visible to the naked eye.**

Index Terms— **Video Encryption, Cryptography, Pixel Mapping, Steganography.**

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 pixels 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 frames are modified. So by the changes made in the smaller number of pixels in a sequence of images all the movements are described perfectly in a video file. This is very simple and easy 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 showcasing the movements happening in the particular video.
For persistence of vision, any video should be constructed by taking atleast 25 frames per second as our eye can detect 16 frames per second with minor flickering. So that any video is basically a combination of different frames and all the frames constituting a video has a fixed frame rate. Practically, the frame rate is 25 so we can say that 25 frames are captured within one second time. For the efficient and successful implementation of this particular algorithm, first of all video segmentation is performed. For a particular case, if video is of 10 minutes duration than this video majorly contains 15000 frames in it. These frames are vital building blocks for the video as well as for video encryption process. We can insert and send the image 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 lossless 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 stenography method can be used for the encryption of the video files. Stenography 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 Steganography technique can be generated by using a pixel mapping algorithm. Also the Steganography technique is faster and efficient in terms of time required for marking the particular set of images.

II. SECURE IMAGE TRANSMISSION USING CRYPTOGRAPHY

Figure 1 describes the flowchart showing the sequence of steps to be executed for generating the encrypted video file for secured image transmission. The algorithm is briefly described in terms of flowchart for the better understanding of the complete process. The complete algorithm is coded in a Matlab showing the detailed process involved in the video encryption and the image insertion in the video file for secured transmission. As shown in the algorithm in figure 1 the complete video is segmented into number of frames 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 image which is to be transmitted is partitioned into the group of pixel line. As we need to modify only one line of each frame of video, we need to segment image in lines of pixels only. Each pixel in the image segment can be represented by a specific value of red, green and blue layer. So each of the pixels occupies 1 byte or 8 bits in the image. In this particular algorithm each of the frame has to be modified by pixel value of image that to be transmitted in different layers of video frame. After this each of the pixels is subdivided into three different layers, namely red, green and blue layer. So now we have three value for each of the pixel from image data to be inserted into the

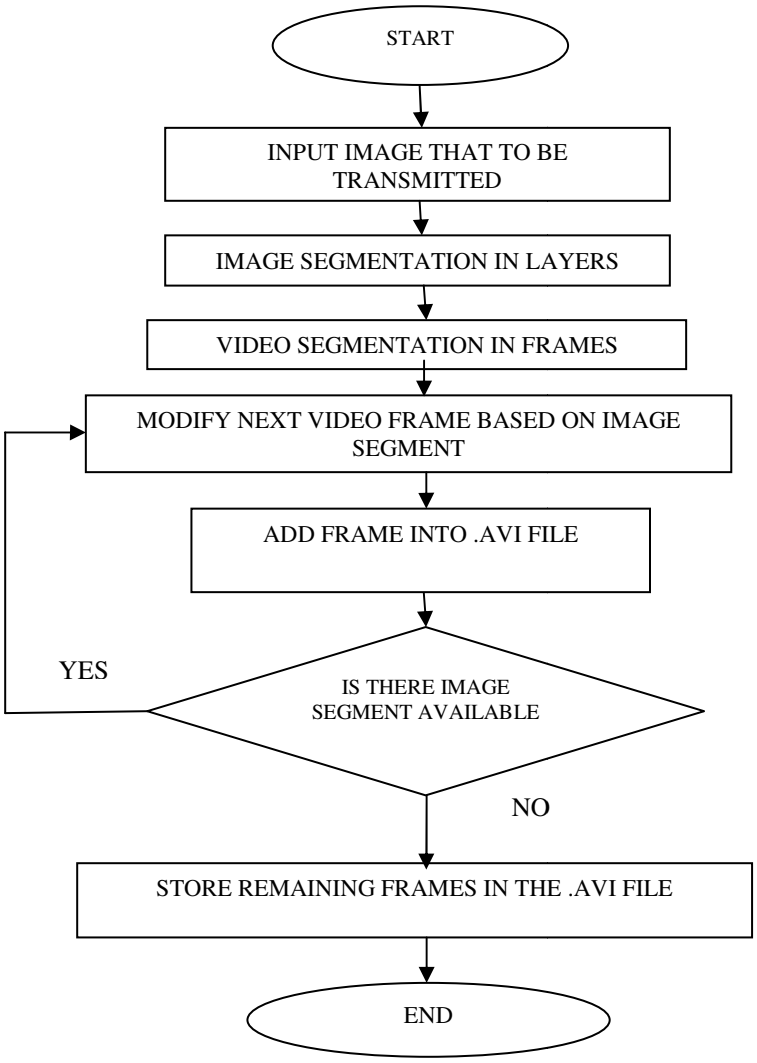

Figure 1 - Algorithm for Video generation for secured image transmission

Frame of video. In this algorithm to represent one particular pixel, we require to modify three layer of pixel of video frame to store one particular pixel of image. As per the grassman law importance of three basic colors which are red, blue and green are different. As per grassman 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 pixel data available so the next step to be followed is to encode or map the pixel data into the pixels of individual frames till the end of image segment. In the proposed work we are going to store one pixel into one frame so there is a requirement of n number of frames in video for storing n number of pixels from image. For a particular image frame by modifying only two pixels at top and bottom of the frame of video file does not make any significant changes in the visual effects of the video 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 of video and identify the red layer of the first pixel of it and overwrite it by value of red layer pixel of image. Similarly also over write the blue layer pixel of frame by the corresponding blue layer of first pixel of image. Same process is to be done for the pixels present in the bottom section of the image for green layer of first pixel of image. By this way we can impose one pixel into one frame and the same process is to be followed for all the pixels present in the image segment with consecutive different frames.

As mentioned earlier we can impose m number of pixels of image 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 image we can group the pixel value 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 but provides high security.

Case 2: The pixel value insertion can be done into the alternate frames for increasing high security.

Case 3: One can transmit the details of the frames modified in form of an array in a frame. After that pixel value 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 red, green and blue layer of the image 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.

Case 5: One can change or encrypt the scale of pixel value before substituting it into frames, so even anyone, decrypt the algorithm, can't get the original pixel value, means without knowledge of encryption algorithm, he may not able to detect or reconstruct original image.

III. CRYPTOGRAPHY

Cryptography is an art of protecting the information by transforming it into an unreadable and untraceable format known as cipher key. 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 like text, image, and video 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. The information looks like hidden inside the image or the video file. A very simplest and well known

algorithm for cryptography 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.

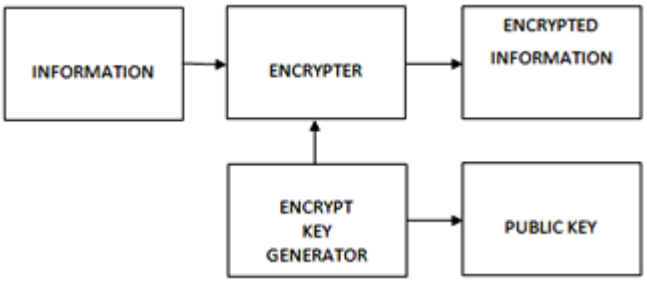

Figure 2 – Cryptography Encryptor

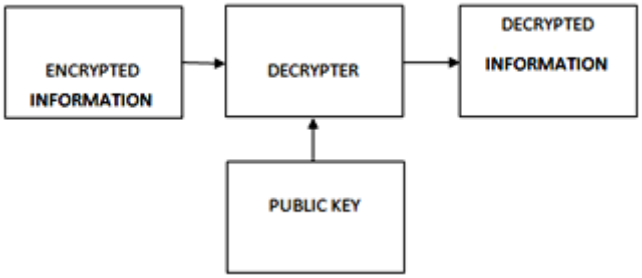

Figure 3 – Cryptography Decryptor

At the receiver end the Cryptography Decryptor is used which extracts the original information content mapped onto the 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 or a source gets the video file with image content hidden in it, it cannot be extracted without proper public key. So public key plays a vital role in the whole cryptography process.

IV. STEGANOGRAPHY

Stenography is the art of hiding information by embedding information like text, image video 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.

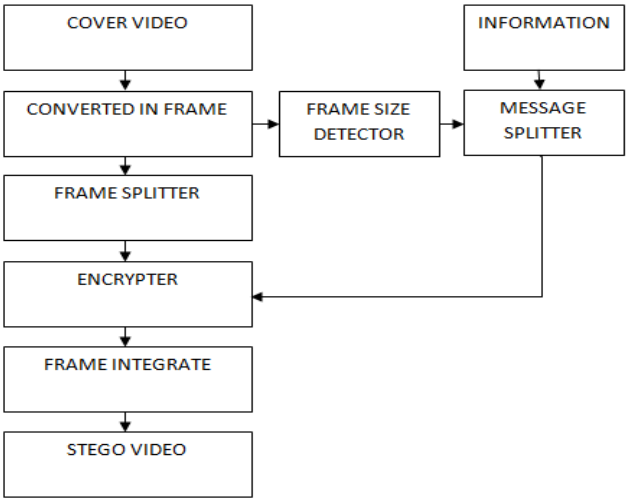

Figure 4 – Stegnography Encryptor

First of all the video file is converted into a series of frames of equal size. The image 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 portion of image 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 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.

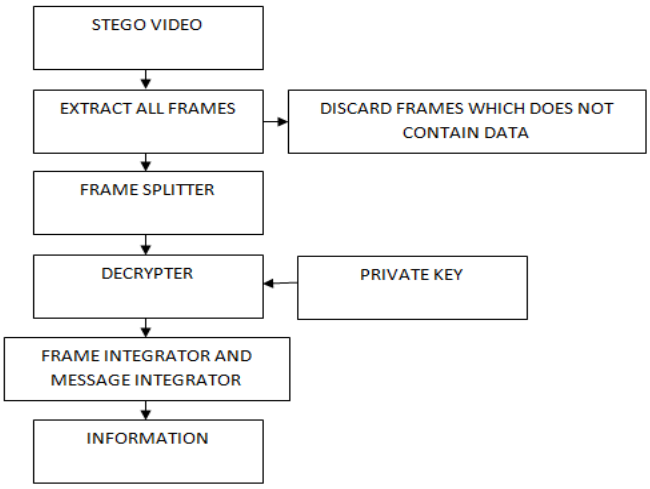

Figure 5 – Stegnography Decryptor

The main blocks in a Stegnography Decryptor is as shown in figure 6. From the figure 6 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.

V. CONCLUSION

One of the important features of the proposed work is it plays a vital role in transmitting the image on a video file very effectively and efficiently. The information underlying the image or a video is not visible to the naked eye. Only the person having the private key and the rule list can identify and decode the original image into its original form. This method simplifies the task of securing the vital information from the misuse and protects it from the unwanted user. With the use of the cryptography and stegnography combination the information security can be increased.

REFERENCES

[1] "A real time approach for secure text transmission using video cryptography" by Viral Metaliya, Dipak Jain and Ravin Sardhara in conference on Communication Systems and Network Technologies (CSNT), ISBN 978-1-4799-3069-2.
[2] http://en.wikipedia.org/wiki/Time-lapse
[3] Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1
[4] Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.
[5] R. Schaphorst, "Videoconferencing and video telephony," Boston, MA: Artech House Publishers, 1996.
[6]/www.mathworks.com/products/imaq/demos.html?file=/products/demos/shipping/imaq/demoimaq_timelapse1.html.
[7] /www.mathworks.com/matlabcentral/fileexchange/12262-datetime-stamp-in-a-plot
[8] Lossless Visible Watermarking- Shu-Kei Yip
[9] Adnan M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Trans. On Image Processing, vol. 13, no.8, Aug, 2004.
[10] Avcibas, N. Memon, and B. Sankur " Steganalysis using image quality metrics", IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003
[11] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani,"Dual layer data hiding using cryptography and steganography" in IJSET volume 1, issue 4, ISSN: 2277-1581