A Persistent Approach For Secure Text Transmission Utilizing Video Cryptography

Sudhakar Putheti
Vasireddy Venkatadri Institute of Technology

K.Anupriya
Vasireddy Venkatadri Institute of Technology

G. Harshitha
Vasireddy Venkatadri Institute of Technology

K.Saritha
Vasireddy Venkatadri Institute of Technology

K.Kamal Kethura
Vasireddy Venkatadri Institute of Technology

Abstract: Image and video are the two most basic forms of transmitting information. With the help of Image and video encryption methods any particular set of images or videos can be transmitted without worrying about security. LSB based steganography method is used for the encryption of the images which are the basic building blocks of any video file. 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. If we consider a pixel as an 8 bit value than each pixel has the value in the range of 0 to 255. For each frame two pixels situated at the top left and the bottom right corner of red and blue layers are modified so as to insert text in each image. After the completion of the pixel value changing all the images are placed in a sequential manner and then 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.

Keywords - *Cryptography, steganography, LSB.*

1.INTRODUCTION

For normal human being the ability to perceive the motions of other animated frames or video has been extensively studied and it is shown that for the movements created in the running video only small amount of pixels are modified and rest all the pixels remain static if we compare the pixels of any consecutive frame. 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.

Any Video is basically a combination of frames and all the frames of a video constitutes a fixed frame rate. Generally, the frame rate is 25 i.e. 25 frames are captured within in a second of time. For in a particular case if the duration of video is 4 minutes then number of frames we will get is 4*60*25=6,000. All these frames are vital for the video encryption process. The changes that we made on pixels are not visible to our naked eye[1].

There are various watermarking techniques which are used to send the text along with the frame like visible watermarking, discrete cosine transforms, discrete Fourier transform, loss-less watermarking, not-visible watermarking method etc. All these watermarking techniques have certain drawbacks and also these methods are little bit time consuming. To get over the drawbacks of these watermarking methods stenography method can be used which is very efficient and accurate data processing in case of real time applications[2][3][4].

In the proposed LSB based stenography method is used which is faster and efficient in terms of time required.

2.EXISTING SYSTEM

The user has to select any type of video i.e. mp4, avi etc. Then divide the video into frames and store all those frames in the sequential order.

The Following are the steps followed by the sender:

Step 1: Convert the selected input video is into frames.

Step 2: The input text is convert into ASCII format and represent in 8-bit format.

Step 3: Text bits are subdivided into group of 2 bits which means four group of 2 bits is equal to one character of text.

Step 4: One character is embedded in one frame i.e. change the 2 lsb bits of top and bottom pixel values of red and blue layer[5].

Step 5: After embedding the bits into the frames[10] then we need to reconstruct the video by using the extension .avi.

Step 6: The reconstructed video is sent to the receiver in the network.

The following is the process performed by the receiver:

At the receiver end, he first selects the video then divided it into frames and extract the bits. After extracting bits, he from a group of 8-bits which represents one character.

2.1 CRYPTOGAPHY

Cryptography is the art of protecting data by transmitting it into an unreadable and untraceable format known as cipher text. The Only Person Who possess the secret key can decipher it. By using encryption key, the information need to send is converted into cipher text. The encrypted information is then transmitted to a particular receiver. At the receiver, by using the secret key decrypts the received information (encrypted information). So, the by use of cryptography method only the receiver who has the knowledge of secret key can retrieve the information content from the video file. There a number of encryption algorithms like DES, AES, IDEA, SHA-512 among all these algorithms here in this particular paper we are using RSA algorithm for encryption. The reason for using RSA algorithm is it is simple and secure.

2.1.1 RIVEST SHAMIR ALDEMAN FOR PUBLIC KEY ENCRYPTION

The RSA algorithm is base for all network secured public key crypto system algorithm. RSA is asymmetric algorithm and it is useful for security, identification and authorization[13].

Keys to maintained for every user:

Public key- key is disclosed.

Private Key- secretly maintained by user.

At the sender's the information is encrypted with receiver's public key and at the receiver end the received information is decrypted by using the receiver's private key.

The following are steps involved in the RSA algorithm:

Step 1: choose any two prime numbers say p and q

Step 2: calculate n=p*q.

Step 3: calculate $\varphi(n)= (p-1) * (q-1)$

Where $\varphi(n)$ is Euler's Totient function.

Step 4: select e such that $1<e<n$ and e and $\varphi(n)$ are coprime i.e. GCD $(e, \varphi(n)) =1$.

Step 5: calculate value for d such that $(d*e) \% \varphi(n)=1$.

Step 6: Private key: (d, n).

Step 7: Public key: (e, n).

The encryption formula is: $c= me \bmod n$.

The decryption formula is: $m=cd \bmod n$.

2.2 STENOGRAPHY

Stenography is the art of hiding information in a cover such as digital image file[11][12]. The cover may be a video or image based on the user requirement.

The following are some of the basic terms used in stenography:

Embedding: It is the process of hiding information in text, image, audio and video.

Extraction: It is the reverse process of embedding i.e. getting the hidden information.

The most popular method of stenography is LSB (LEAST SIGNIFICANT BIT) method[7][8]. LSB replaces the least significant bit of pixel by the hidden message bits.

3.PROPOSED SYSTEM

The selected video and then divide it into frames and all these frames are stored in the local memory by using a small matlab code module in a sequential order.

The following flow chart depicts the implementation process for generating an encrypted video file for secured text data transmission.

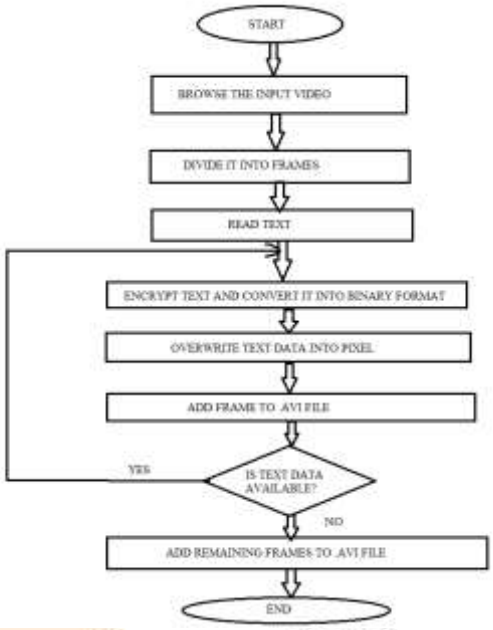

fig: implementation process for generating encrypted video for secured text data transmission.

Then the input text data is read from user. Each character in the input text data can be represented by ASCII value so each character occupies 1 byte or 8 bits. Then encrypt the text data and convert it into binary form.

As we need to modify only two pixels of red and blue layers per image or frame, here in the proposed work only the selected frames are changed i.e. let us say the kth frame is changed first and the next frame changed is (k+i) th frame. Selection of value of i is based on the number of bits in the encrypted input text data. Then LSB bit of selected frame is modified with the encrypted text bits.

As per the grassman law of importance of three basic colors which are green, blue and red are different. As per the grassman law the importance of green layer is the most because it contains 59% weightage to generate any color in a particular pixel as per the requirement[6]. Due to this, in this particular algorithm only the values of red and blue layers are changed for processing the image so as to retain the original shade in the frame.

Here for a particular selected frame we are modifying only two pixels[9] which are the top and bottom of image frame and the changes that we made are not visible to naked eye.

After overwriting the text data into frames those particular frames are stored to a AVI file. This process is continued till all the bits in the text data is embeded in the frames. After the completion of embedding process, the remaining frames are stored in to the AVI file.

Now we have the encrypted video file which is stored in the format .avi and is ready to transmit in the network.

The explanation of RSA algorithm with example is follows:

Let us say the prime numbers be p=11 and q=13.

- Then value of n=p*q=11*13=143.
- The value of φ(n)= (11-1) *(13-1) =10*12=120.
- Now select e such that 1<e<n and e and φ(n) are co-prime i.e. GCD (e, φ(n)) =1. Let us say e=7.
- calculate value for d such that (d*e) % φ(n)=1. Consider d=103 (i.e. (103*7) %120=1).
- Then Private key: (d, n) = (103,143) and Public key: (e, n) = (7,143).
- The encryption formula is: c= me mod n.
- The encryption of the character ‘h’ whose ASCII value is 104 is c= (104)7 mod 143=91.
- Therefore, cipher text c for letter h is 91.
- The decryption formula is: m=cd mod n.
- The decrypted message m=91103 mod 143=104 which is ASCII value of character ‘h’.
- Hence the decrypted information is letter ‘h’.

The LSB stenography method is explained as follows:

For example, let us the pixel value is 10, the binary representation for 10 is 00001010. LSB bit is ‘0’ it is replaced by the text bit which is say ‘1’. Then result is 00001011 which is equivalent to 11 in decimal notation. Now the pixel value is changed to 11.

The advantage of proposed system is that even though the intruder tries to hack the information he may not get the original information, because we store the information in the selective frames not in the contiguous.

4. SIMULATION RESULTS

We performed simulation on matlab R2014b under windows 10 64-bit operating system, 64-bit processor and 4GB RAM. From the simulation results it is clear that the proposed scheme is ideal for secret data communication and it meets key requirements including security and robustness.

fig: a screen shot of video frames stored in sequential order of some input video

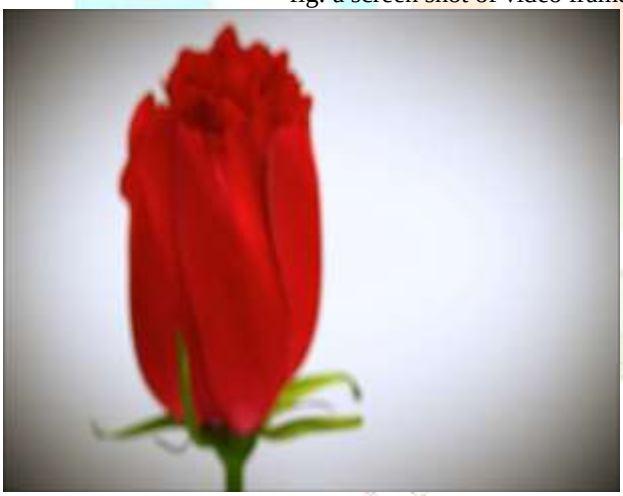

fig: an original video frame

fig: encrypted video frame

5.CONCLUSION

The most important feature of this proposed work is, a crucial role of transmitting information in a video file effectively and efficiently. Another important feature is not visible to human eye. The only who knows the private key and the rules listed can only decode the information into its original form. This method simplifies the task of securing the vital information from misuse and protect it from unwanted user. With the use of RSA, cryptography and stenography combination the information security can be increased.

6.REFERNCES

[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 978-14799-3069-2.

[2] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S.Sadasiva Rao, "Image Stenography combined with Cryptography", International Journal of Computers & Technology, ISSN:22773061, Vol.9, July 2013, pp.976-984.

[3] Neetu Settia. “Cryptanalysis of modern Cryptography Algorithms”. International Journal of Computer Science and Technology. December 2010.

[4] Lokesh Kumar, Novel Security Scheme for Image Stenography using Cryptography Technique", International Journal of advanced Research in computer Science and Software Engineering, ISSN:2277 128X Vol.2, April 2012, pp.143-146.

[5] Dipesh G Kamdar, Dolly Patira and Dr. C.H. Vithalani "Hiding using Cryptography and stenography" ISSN:2277-1581.
[6] A Joseph Raphael, Dr. V. Sundaram, "Cryptography and Stenography- A survey International Journal of Computer and Technology Applications" ISSN:2229-6093, Vol.2(3),2010, pp.626-630.
[7] B Dunbar A Detailed look at Stenographic techniques and their use in an open systems environment. Sans InfoSec reading Room,2002.
[8] Shristi Mishra, Prateeksha Pandey, "A review on Steganogaphy techniques using Cryptography", International Journal of Advanced Research in Science and Engineering", ISSN:2319-8354 Vol.4 March 2015.
[9] Dipesh G kamdar, Dolly Patira and Dr. C.H.Vithalani "Hiding using Cryptography and stenography", ISSN:2277-1581.
[10] S. Ashwin, J. Ramesh, K. Gunavathi, "Novel and Secure Encoding and Hiding Techniques using Image Stenography".
[11] W.Huaiqing and S.Wang, Cyber warfare:Steganography vs. steganalysis. Communications of the ACM, 47(10):76-82,2004.
[12] M. G. J. Fridrich, Pratical steganalysis of digital images-state of art. security and Watermarking of Multimedia contents IV,4675:1-13,2002.
[13] P Gayathri Devi, "Overview of RSA and its Enhancements", International Journal of Innovative research and Development, ISSN:2278-0211(Online) Vol.2 Issue 11, November 2013.