A METHODOLOGY FOR SECURE CONTENT TRANSMISSION USING VIDEO CRYPTOGRAPHY

[1]Prof. Somnath R.Wateganokar, [2] Shraddha Pandey, [3] Dattakumar Malkhede, [4]Saurabhi Shingade, [5]Shivanjali Sangale
[1]Professor, [2]Student, [3]Student, [4] Student, [5] Student

[1]Electronics And Telecommunication,
[1]Bharati Vidyapeeth College Of Engineering,, Navi Mumbai, India

Abstract : The rapid advancement in the field of computer network and Internet has increased the easiness of Data Communication. This kind of advancement has expanded the dread of sneaking the information while sending information from the sender to the receiver. Picture and video are two of the most essential types of transmitting data. With the assistance of Image and video encryption techniques, a specific arrangement of pictures or recordings can be transmitted without stressing over security. In the proposed paper an extremely straightforward and constant calculation, utilizing pixel mapping, is utilized for the encryption of the pictures which are the fundamental building squares of any video record. In the proposed research paper, the video is divided into number of frames utilizing a MATLAB code and every one of the frames are sequentially stored. Each such frame contains a mix of red, blue and green layers. If we consider a pixel equivalent to 8 bit than every pixel has the value in the scope of 0 to 255. In the proposed work for each casing, two pixels arranged at the upper left and the base right corner are changed in order to embed a message in each picture.The encryption of data to be transmitted is done using RSA cryptographic algorithm. For encryption of the images of a video file (i.e for steganography) we use DCT to overwrite text data into pixel. After the fulfillment of the pixel value changing every one of the pictures is set in a sequential way and afterward, every one of the picture is cascaded for generation of original video file with encryption. This new video is relatively like the first video record without no changes visible to the naked eye

IndexTerms **- Video Encryption, Lossless Watermarking, Pixel Mapping, Steganography**

I. INTRODUCTION

For typical person the capacity to see the movements of other invigorate casings or video has been widely considered and it has appeared for the developments made in the running video just the little measure of the pixels is adjusted and rest every one of the pixels stay static in the event that we think about the pixels of any back to back edges in a video. So, by the progressions made in the more modest number of pixels in a grouping of pictures every one of the developments is portrayed splendidly in a video document. This is an exceptionally straightforward and simple strategy for imagining any procedure under examination. Research demonstrates that among the back to back pictures having a million quantities of pixels just a couple of hundred pixels are changed for displaying the developments occurring in the specific video.

Any video is essentially a blend of various casings and every one of the edges establishing a video has a settled edge rate. For the most part, the edge rate is 25 so we can say that 25 outlines are caught inside one moment time. For the productive and fruitful usage of this specific calculation, there is a prerequisite that the video should be segmented. For a specific case on the off chance that we guess that the video is of 5 minutes longer than this video significantly contains 7500 casings in it. These edges are indispensable building hinder for the video and in addition for the video encryption process. We can embed and send the content alongside the edge by utilizing different accessible watermarking strategies. There are different diverse watermarking systems accessible like visual watermarking, discrete cosine change, discrete Fourier change, and lossless watermarking strategy. All the watermarking strategies as of late accessible have certain disadvantages and furthermore, these techniques are a smidgen tedious. Likewise, the watermarking strategies can be adjusted utilizing further developed methods for picture preparing. To get over the downsides of the watermarking procedures stenography technique can be utilized for the encryption of the video documents. Stenography is primarily valuable regarding proficient and precise information preparing for the instance of the constant applications. In the proposed work likewise, the stenography strategy can be produced by utilizing a pixel mapping calculation. Likewise, the stenography system is quicker and proficient as far as time required for denoting the specific arrangement of pictures

II. RESEARCH METHODOLOGY

1.1Cryptography

Cryptography is the technique in which information is converted into unintelligible form called cipher text. By this technique one can send and share the information securely. Cryptography technique can be used for the information like image file, audio file and video file. In video cryptography process, video is segmented and converted into the frames. Each frame is consisting of many pixels, each pixel is of byte or 8 bits. In cryptography process information is converted into the unreadable and untraceable format by encryption process using encryptor key. This encrypted information is then transmitted to the particular receiver. At the receiver side encrypted information is decrypted by cryptography decryptor. At the receiver site using decryptor retrieve the original information. Cryptography encryption is done by the public key which is also available at the receiver key. In cryptography technique public key play important role. For the cryptography technique we have three algorithms namely Hash algorithm, Asymmetric Encryption algorithm, Symmetric Encryption algorithm. Out of which we used

Asymmetric Encryption algorithm in which public key is used at transmitter site and private key is used at receiver site. By using Asymmetric Encryption algorithm all people able to access the video but not decrypted by them. It is only decrypted by receiver's private key.

1.2 Stegnography

Steganography is the technique in which information is hidden within same data. It can apply for the images file, video file and audio file. Steganography is an encryption technique that can be used along with cryptography as an extra secure method in which to protect data. Steganography protects from unauthorized viewing. By using Steganography data gets more secure and unauthorized from the unknowns. First video gets segmented into the series of frames of equal size. From each frame a smaller region is modified depending upon the private key used at receiver. Due to this it is not authorised by unknown. In pixel mapping selected pixels are then converted into the frequency domain with the help of DCT in which two to three pixels replaced by the spilled message part and then this pixel part is again converted back into the spatial domain. Conversion from the frequency domain to spatial domain is done by inverse DCT. Finally rearrange pixel again place at respective position until the whole information content to be finish. At the end these modify frames are arranged in sequential manner and video is constructed.

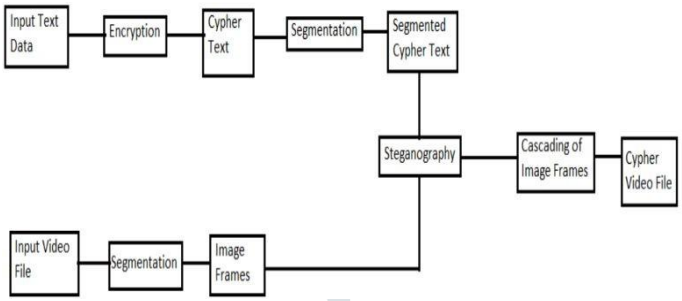

Fig 1.Block Diagram of the overall Process

The total input video is divided into number of pictures utilizing a little MATLAB code module and after the handling of the video by the MATLAB code module the video gets partitioned into distinctive edges of same size. At that point the content string which is to be embedded among the pictures is parceled into the gathering of two bits each. As we have to adjust just two pixels per picture so we isolate the content information into the gathering of two bits. Each character in the content information can be spoken to by a explicit ASCI esteem so every one of the character involves 1 byte or on the other hand 8 bits in a picture. In this specific calculation each of the picture must be adjusted by two-pixel esteem and that moreover just the last two bits so every one of the characters in the content information to be embedded is spoken to by its ASCI esteem in line. After this every one of the characters spoke to into the gathering of 8 bits is subdivided into the gatherings of 2 bits as it were. So now we have four gatherings for every one of the characters in the content information to be embedded into the pictures. In this calculation to speak to one specific character we require four pixels to store one specific character. According to the grassman law significance of three essential hues which are red, blue and green are unique. According to grassman law the significance of the green layer is the most in light of the fact that it contains 59% weightage to create any shading in a specific pixel according to the prerequisite. Due to this in this specific calculation just the estimation of the red and the blue layers are changed for handling the picture to hold the first shade in the edge. The green layer in every one of the pictures is unaltered. Just the blue and red layers pixels are altered in every one of the image frames.

Presently we have frames and exceptionally very much circulated content information accessible so the subsequent stage to be pursued is to encode or delineate content information into the pixels of individual frames till the end of the content information. In the proposed work we are going to store one character into one casing(frame) so there is a prerequisite of n number of casings(frames) for putting away n number of characters in the content information. For a specific picture outline by altering as it were two pixels at top and bottom of the image frame does not make any huge changes in the enhanced visualizations of the casing so they are not unmistakable to the human eye. Subsequent stage to be pursued is to choose the first frame from the arrangement of the casings and distinguish the red layer of the primary pixel and overwrite the last two bits with the initial two bits of the character in the content information. So also, likewise over compose the last two bits of the blue layer pixel by the relating next two bits of the character. Same process is to be improved the situation the pixels present in the bottom area of the picture. By along these lines we can force one character into one frame and a similar procedure is to be pursued for every one of the characters present in the content information with back to back various frames

III. RESULTS

The design and implementation is done on MATLAB (Version 2018) image toolbox. The results are shown below :-

1) INPUT AND OUTPUT OF RSA ALGORITHM:

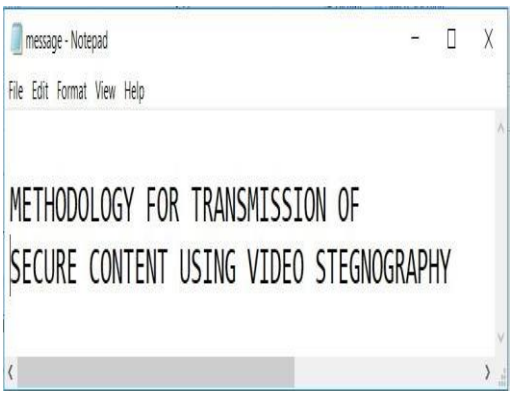

Fig.1a:Input text data

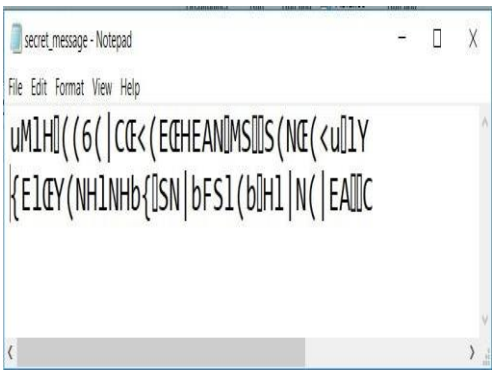

Fig.1b:Output text data after RSA Encryption

2) COMPARISON OF INPUT AND OUTPUT STEGO VIDEO:

There is no visually noticeable difference in the first frames of the original video and stego video.

Fig.2a: First frame of input video -sun.avi

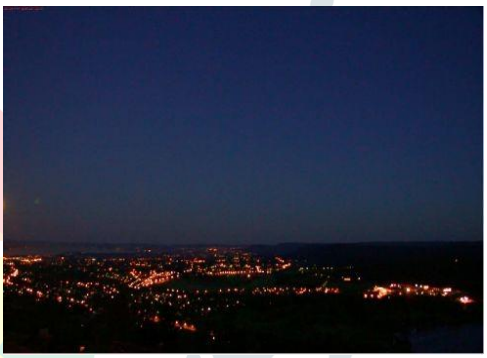

Fig.2b:First frame of Output stego video-output.avi

IV.APPLICATIONS

- Secure text transmission makes it possible to send news and information without being censored and without the fear of message being intercepted and tracked back to us.
- It can be used for private banking information, some military secrets, E-commerce.

V.ADVANTAGES

- It is user friendly.
- Simple and less complex technique.
- It is more successful process of embedding secret message with more security.
- The integrity of the hidden data is maintained after embedding it.
- Increases the security of the information

VI. CONCLUSION

Today, security of the information has become the most important concern. By using cryptography and steganography technique for encryption and decryption can be made more secure. Also, by using pixel mapping algorithm the text information is encrypted inside the image and at receiver, it is decrypted. The information lying under the video is not visible to naked eyes. This is how the information can be secured.

References

[1] Jyoti Uppar, Hemanth Kumar K S and Dr Siva Yellampalli, "A Real Time Approach for Secure Text Transmission Using Video Cryptography",INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY (IJIRT), ISSN: 2349-6002, Volume 4 Issue 3, August 2017.

[2] Viral, G.M. ; Jain, D.K. ; Ravin, S. "A Real Time Approach for Secure Text Transmission Using Video Cryptography",proceedings of 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), IEEE Conference Publications, pp 635-638, 2014.

[3] Fillatre. L, "A Real Time Approach for Secure Text Transmission by using Video Cryptography",in International Journal of Research and Development in Applied Science and Engineering (IJRDASE)ISSN: 2454-6844, Volume 9, Issue 2, April 2016

[4] Sudeepa K B, Raju K, Ranjan Kumar H S, Ganesh Aithal, "A New Approach for Video Steganography Based on Randomization and Parallelization", International Conference on Information Security and Privacy (ICISP2015),11-12 December 2015.

[5] "A Secured Text Transmission Through Video Using Modified Status Bit LSB along With RSA Cryptography" by Rajakumar Loni , Mrs. D.Kavitha in IJCSMC, ISSN 2320–088X Vol. 4, Issue. 5, May 2015.

[6] Kamred Udham Singh,"Video Steganography: Text Hiding In Video By LSB Substitution", in Kamred Udham Singh Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5(Version 1), May 2014

[7] Islam, M.R. ; Siddiqa, A. ; Uddin, M.P. ; Mandal, A.K. ; Hossain, M.D. "An efficient filtering based approach improving LSBimage steganography using status bit along with AES cryptography", proceedings of 2014 International Conference onInformatics, Electronics & Vision (ICIEV), IEEE Conference Publications, pp 1-6, 2014