ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENHANCING VISUAL DATA SECURITY WITH USER AUTHENTICATION

Jayshree D. Kularkar*[1] & Bhakti Kurhade[2]

*[1,2]Department Of Computer Science and Engineering, Abha Gaikwad Patil College Of Engineering, Nagpur, India.

ABSTRACT

The critical issue in the world is the manner in which to safely transmit the secret information and prevent the detection of information. Steganography is a system that hides information in an application cover carrier like image, text, audio, and video. In this paper we use the video steganography. In this technique first convert the video into frames, then out of that frames select one frame, that frame is called as cover image. Then take a secrete image which has to be transmitted. This secrete image is convert into gray image and encrypt that image with the help of secrete key. Thus, we get the encrypted image. This encrypted image is embed into the cover image by using improved LSB technique. The output is called the stego image. This stego image is then add to that video at the place of cover image and rebuilt the video. This rebuilt video is then send to the receiver side where the receiver receives the original image by decrypting that image. Video Steganography is a technique to hide any image into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. The improved least significant bit is an important technique for embedding information in a carrier file. In this technique, the cover image divided into three different channels i.e. RGB then hide the secrete image into these channels by inserting specific bits in red, specific bits in green and specific bits in blue channels.

Keywords- *Steganography, Video Steganography, cover video, cover frame, secret message, LSB.*

I. INTRODUCTION

Currently, internet and digital media are getting more and more popularity. So, requirement of secure transmission of data also increased. For this reason various good techniques are proposed and already taken into practice. In this project, we use the steganography process for the secure data transmission from the sender to receiver through the internet. Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word ***steganos*** which literally means "covered" and ***graphia*** which means "writing", i.e. covered writing. The most common use of steganography is to hide a file inside another file. Generally, in data hiding, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia files like images, video or audio. Which in turn is being hidden within another object. The medium where the secret data is hidden is called as cover medium, this can be image, video or an audio file. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Higher the quality of video or sound more redundant bits are available for hiding. Application of Steganography varies from military, industrial applications to copyright and Intellectual Property Rights (IPR). By using lossless steganography techniques messages can be sent and received securely [2]. Traditionally, steganography was based on hiding secret information in image files. But modern work suggests that there has been growing interest among research fraternity in applying steganographic techniques to video files as well [3], [4]. The advantage of using video files in hiding information is the added security against the attack of hacker due to the relative complexity of the structure of video compared to image files. An application of the algorithm is illustrated with AVI (Audio Video Interleave) file as a cover medium. The results obtained are significant and encouraging. Effort has also been taken to study the steganalysis.

In network technology, secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many secure transmission methods require a type of encryption. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done. Many infrastructures such as banks rely on secure transmission protocols to prevent a catastrophic breach of security. Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. While transferring secret images, various image secret sharing schemes have been developed.

Steganography (literally meaning *covered writing*) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shared messenger's head, letting his hair grow back, then sharing it again when he arrived at his contact point. Steganography mechanism is used to hide data like secret images and any other files within another file. Steganography and the cryptography mechanisms are combined together to send a secret data with full security. The best steganographic method that works in this domain is the LSB (Least Significant Bits), which replaces the least significant bits of pixels selected to hide the information.

In this project, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame. First divide the video into frames then take a secrete image and encrypt that image with

ISSN 2348 – 8034
Impact Factor- 3.155

the help of secrete key. It gives the encrypted image then this encrypted image is hide with that of the selected frame. The output is called the stego image in which the message image inside it, is hidden after that this stego image is rebuilt into the video. Thus, this video is send to the receiver where the receiver retrieves the secrete image by applying desteganography that means the reverse process.

II. LITERATURE SURVEY

For studying the concepts of video steganography, we have surveyed many research papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography.

In [1] Author has proposed a scheme is that variation of plain LSB algorithm. The stego image quality is improve by using bit inversion technique. In this technique certain least significant bits of cover image is inverted after LSB steganography that co-occur with some pattern of other bits and that reduces the number of modified LSBs. It used RC4 on plain LSB.

[2]In this paper the author focus on Secret sharing technique is used to hide information. Secret sharing is a technique for splitting a message into several parts so that all parts are sufficient to recover the message. Video Fragmentation is used to extract frames (convert video into images) from video for carrier. The secret color image pixels will be converted to m-ary notational system. The (t-1) digits of secret color image pixels are generated using reversible polynomial function.

[3] The author developed a data hiding scheme to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation

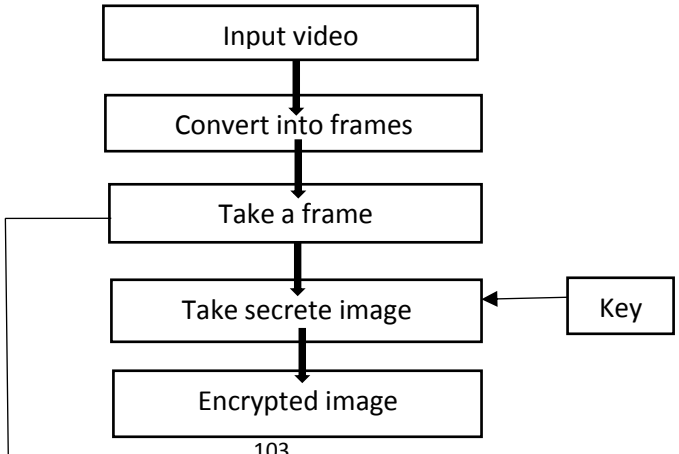
[4] In this work the author proposed a novel type of digital video encryption that has several advantages over other available digital video encryption schemes. They also present an extended classification of digital video encryption algorithms in order to clarify these advantages. They analyze both security and performance aspects of the proposed method, and show that the method was efficient and secure from a cryptographic point of view.

In [5] author proposed a hash based least significant bit (LSB) technique. A spatial domain technique where the secret information is embedded in the LSB of the cover frames. Eight bits of the secret information is divided into 3, 3, and 2 and embedded into the RGB pixel values of the cover frames respectively. A hash function is used to select the position of insertion in LSB bits.

In [6] the author has proposed a novel non-expanded visual cryptography scheme with authentication using block encoding. It combines the feature of authentication with the block encoding scheme to transmit the secret information and prevent the detection of information, regardless of whether the original image is changed. In other words, the block encoding method with the extra ability of hiding confidential data is combined with the scheme to prevent the detection of information.

In [7] author proposed an advance approach for dynamic data protection using LSB and hybrid approach. The method for replacing one or two or three LSB of each pixel in video frame and apply Advance encryption standard (AES). It becomes very difficult for intruder to guess that an image is hidden in the video as individual frames are very difficult to analyze in a video.

III. PROPOSED WORK



ISSN 2348 – 8034
Impact Factor- 3.155

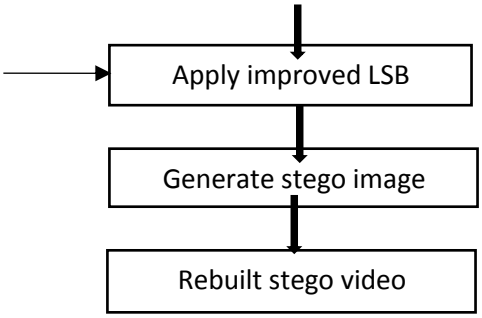


Fig 1. Flow of proposed scheme

The above figure show that the flow of proposed scheme. The crucial issue is that to transmit the important data from sender to receiver. Thus it is the confidential data, therefore it is important to transmit the data in secure way. In this project, we transmit the secrete image from sender to receiver by applying improved LSB to the secrete image. First, we take the video, in this video it has many frames. Thus select the one frame of that video. That is the cover image, which is used to cover the secrete image. Then take a secrete image which has to be transmitted. This secrete image is encrypted with the help of the secrete key, thus we get the encrypted image. This encrypted image is to be hide with the cover image by applying improved LSB technique. The improved LSB is the technique, to divide the colored cover image into three different channels i.e. RGB. Hide the secrete image into these channels by inserting specific bits in red, specific bits in green and specific bits in blue channels. The output is called the stego image, where the message image inside it, hidden. This stego image is rebuilt into that video and this video is then send to the receiver. Until now we do the work on sender side. The remaining work that means the receiver portion will done in the next paper.

Module Description:-

Module 1: Video to Frame conversion-

In this project first we take a video then this video is converted into frames using video reader function in matlab. Here video is taken as input and frames are obtained as output. For video data, file format refers to container format or codec. Video reader function is used to read the video files. It recognizes the container format such as avi, mpeg etc and access codec associated with particular file.

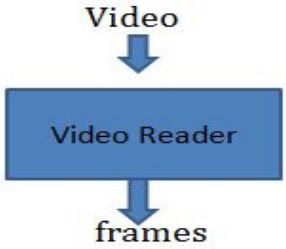


Fig.2. Conversion of video into frames

ISSN 2348 – 8034
Impact Factor- 3.155

Fig.3. Frames obtained from video file

Module 2: Encryption of secrete image-
In this module, take a secrete image convert the secrete image into gray which has to be transmitted from one to another. Then convert the secrete image into gray scale and encrypt that image with the help of secrete key which is share to receiver that means only receiver knows that key. No other person knows that key. This image is called encrypted image.

Fig.4. encrypted image

Module 3: Steganography-
In this module, the encrypted image is hide with the cover image. The cover image is the frame which has to be selected from the video. The steganography is done with the help of improved least significant bit (LSB) technique. The output is called the stego image in which the secrete image is hide with the stego image. This stego image is then add to the video at the place of cover image which we have to select and then rebuilt that video. This rebuilt video is send to the receiver.

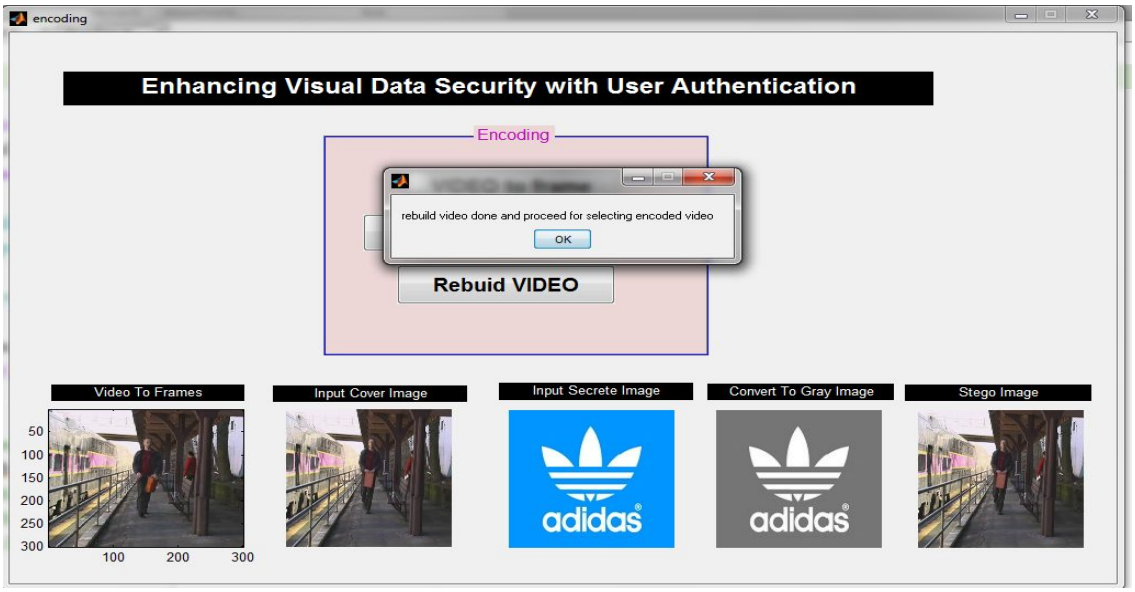


Fig.5. Encoding at sender side

ISSN 2348 – 8034
Impact Factor- 3.155

Module 4: Decryption-
When the receiver receives the video, the receiver convert that video into frames. Select the stego image and decrypt that image with the help of same secrete key which has to be used for at the time of encryption of the image. Thus, the receiver get original image that is the secrete image.

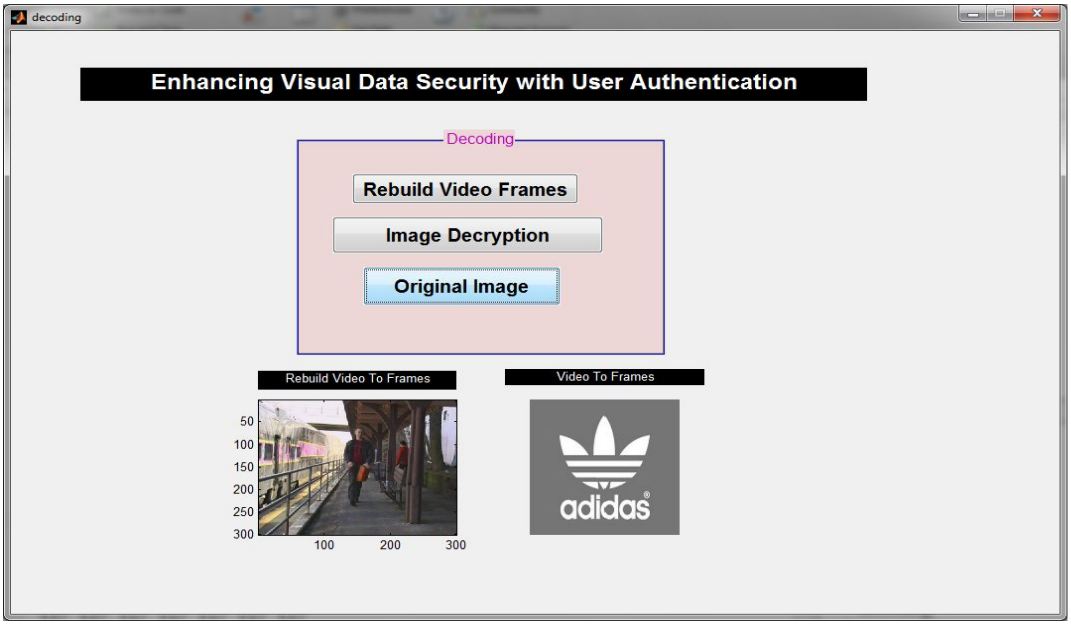


Fig.6. Decoding at receiver side

IV. CONCLUSION

After encrypt the secrete image divide the colored cover image into three different channels i.e. RGB. Hide the secrete image into these three channels by inserting specific bits in red, specific bits in green and specific bits in blue channels. This is called the improved LSB technique. The output is called the stego image, this stego image is rebuilt into the video.

REFERENCES

1. *Nadeem Akhtar, Pragati Johr " Enhancing the Security and Quality of LSB based Image Steganography" 2013 5th International Conference on Computational Intelligence and Communication Networks.*
2. *Rohit G Bal, Dr P Ezhilarasu "An Efficient Safe and Secured Video Steganography Using Shadow Derivation" International Journal of Innovative Research in Computer and Communication Engineering An ISO 3297: 2007 Certified Organization Vol. 2, Issue 3, March 2014.*
3. *A. Swathi, Dr. S.A.K Jilani, Ph.D, "Video Steganography by LSB Substitution Using Different Polynomial Equations" International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5*
4. *Daniel Socek, Hari Kalva, "New approaches to encryption and steganography for digital videos" Springer-Verlag 2007 Multimedia Systems DOI 10.1007/s00530-007-0083-z.*
5. *J.K. Mandal "hash based least significant bit technique for video steganography(hlsb)" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.*
6. *Yi-Jing Huang and Jun-Dong Chang, "Non-expanded Visual Cryptography Scheme with Authentication" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan.*
7. *Hemant Gupta, Dr. Setu Chaturvedi "Video Steganography through LSB Based Hybrid Approach" International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 6, Issue 12 (May 2013), PP. 32-42.*