International Organization of Research & Development (IORD)
ISSN: 2348-0831
Vol 02 Issue 02 | 2015

ENHANCING VISUAL DATA SECURITY WITH USER AUTHENTICATION

Jayshree D. Kularkar1, Sonal Honale2
Department Of Computer Science and Engineering,
AbhaGaikwad Patil College Of Engineering,Nagpur,India.

ABSTRACT

Crucial issue is the manner in which to safely transmit the secret information and prevent the detection of information. An extended visual cryptography with authentication technology for the original image was proposed in previous studies. 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. The video is divide into frames secrete image embed into one of the frame by using LSB replacement technique. Least Significant Bit (LSB) insertion method was more suspicious and low robustness against attacks. Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video basedSteganography can be more eligible than other multimedia files, because of its size and memory requirements. The least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. 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.

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 ofdata 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. Themost common email encryption is called PKI. In order toopen 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.

The secret image and the cover image is embedded together to construct a stego image. All stegoimages are embedded to construct video. The reversible image sharing process is used to reconstruct the secret image and cover video. The video is divide into frames secrete image embed into one of the frame by using LSB replacement technique. Least Significant Bit (LSB) insertion method was more suspicious and low robustness against attacks. Video Steganography is a technique to hide any kind of files 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 least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. 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. Video Fragmentation is used to extract frames (convert video into images) from video for carrier. The secret color image pixels will be converted to mary notational system. The (t-1) digits of secret color image pixels are generated using reversible polynomial function. A reversible polynomial function and the participant's numerical key are used to generate secret shares. Because of rapid network structures and computer technology development, it is convenient to transmit various data through the Internet, such as text, images, voice, and video. The transmitted data may include military secrets, commercial secrets, or private information of individuals. Therefore, it is crucial to determine methods to safely transmit the secret information and prevent the detection of information. Visual cryptography was introduced by Naor and Shamir[1], which is an approach used to decrypt secret images by using human visual system without any cryptography computations. In the domain of visual cryptography, a secret image can be revealed by stacking two share images. Therefore, the secret image cannot be obtained with only one of the images. The (k, n)-threshold indicates that a secret owner generates n share images for n participants for the original secret image to be visible when least k (2 …k) them are stacked together. The proposition by Naor and Shamir was succeeded by (2, 2)-VC scheme, which indicates that the scheme constructs two share images, and the secret image is recovered by stacking two share images together. In traditional approaches, share images were expanded two or four times large size, that is, each secret pixel is encoded into1 ~2 pixels or 2 ~2 pixels. Six fundamental blocks are defined to generate two share images.

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 which is very important to us for studying the basic concept of steganography. The author deals which steganography using video file as a cover carrier. Video based steganography can be used as one video file having separate images in frames. Since that the use of the video based steganography can be more eligible than other multimedia files. This author is mainly concerned with how to embed data in a video file in from of bmp images and how we can make use of the internal structure of the video to hide data to be secured. The basic concept of this author which we have used in my research work and the second concept which has been implemented in our research work is how to use steganography using video file as a cover carrier.

[2] Based on similar concept with stenography, is the art of communicating a message embedded it into multimedia data. It is desired to maximize the amount of hidden information while preserving security against detection by unauthorized parties. The image based stenography issues has been illustrated to hide secret information in images and the possibility of using the image as a cover carrier for hiding secure data.

In [3] an image encryption algorithm combining the image encryption based on S-boxes scrambling with error correcting code was developed. The error correcting code could effectively improve the security of image encryption algorithm based on S-boxes scrambling. The basic concept of this author which we have used in my work focuses on maximizing security, capacity factor of data hiding and secures the data through AES.

In [4] author uses an algorithm based on AES expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the 128 bit key, which changes for every set of pixel. The keys to be used are generated independently at the sender and receiver side based on AES key expansion process. Hence the initial key is shared rather than scaring the whole set of keys. The author gives the information about AES. The AES is provides high encryption quality with minimum memory requirement and computational time.

In [5] the author has proposed an AES technique which presents fundamental mathematics behind the algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. AES provides better security and has less implementation complexity. It has emerged as one of the strongest and the most efficient algorithm.

In [6] author used a method for hiding of information on the billboard display is presented. It is well known that encryption provides secure channels for communicating entities. However, due to lack of covertness on these channels, an eavesdropper can identify encrypted streams through statistical tests and capture them for further cryptanalysis. The author propose a new form of steganography, on-line hiding of information on the output screens of the instrument. This method can be used for announcing a secret message in public place. It can be extended to other means such as electronic advertising board around sports stadium, railway station or airport. This method of steganography is very similar to image steganography and video steganography. Private marking system using symmetric key steganography technique and LSB technique is used here for hiding the secret information.

In [7] 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.

In [8] author focuses on the data security approach when combined with encryption and stenographic techniques for secret communication by hiding it inside the multimedia files. The high results are achieved by providing the security to data before transmitting it over the internet. The files such as images, audio, video contains collection of bits that can be further translated into images, audio and video. The files composed of insignificant bits or unused areas which can be used for overwriting of other data author explains the algorithm using video steganography for enhancing data security.

In[9] author designs software to develop a stenographic application to hide data containing text in a computer video file and to retrieve the hidden information. This can be designed by embedding the text file in a video file in such a way that the video does not lose its functionality using DCT & LSB Modification method. This method applies imperceptible modification. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

In[10] 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. The current study presents the design and implementation of a stenographic procedure that can automatically analyze a video and hide images efficiently and effectively inside it for application in a digital records environment. 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. Reversible polynomial function and the participant's numerical key are used to generate secret shares. The secret image and the cover image is embedded together to construct a stego image. All stego images are embedded to construct video. The reversible image sharing process is used to reconstruct the secret image and cover video. The secret is obtained by the Lagrange's formula generated from the sufficient secret shares. Quantization process is applied to enhance the nature of the cover video.

III. Conclusion

A secured LSB technique for video steganography has been presented in this paper. This technique utilizes cover video files in spatial domain to conceal the presence of sensitive data regardless of its format. Performance analysis of the proposed technique after comparison with LSB technique is quite encouraging.

References

1. Yi-Jing Huang1 and Jun-Dong Chang2"Non-expanded Visual Cryptography Schemewith Authentication" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25- 26 , Kaohsiung , Taiwan.
2. Hemant Gupta " 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.
3. J.K. Mandal "hash based least significant bit techniquefor video steganography(hlsb)"International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.
4. A. Swathi **"**Video Steganography by LSB Substitution Using Different Polynomial Equations"International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.
5. VipulaMadhukarWajgade, "Enhancing Data Security Using Video Steganography"International Journal of Emerging Technology and Advanced EngineeringWebsite: www.ijetae.com (ISSN 2250- 2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013).
6. K. Steffy Jenifer **"**LSB Approach for Video Steganography to Embed Images"K. Steffy Jenifer et al,
7. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 319-

322.

8. Poonam V Bodhak“Improved Protection In Video Steganography Using DCT & LSB”International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue4, April 2012.
9. Rohit G Bal“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.

10. MarghnyMohamed”Data hiding by LSB substitution using genetic optimal key permutation ” in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.

11. [10]P.Karthigaikumar “Simulation of image encryption using AES algorithm”IJCA special issue on computer science New dimensions &perspectives, 166-172, 2011.

12. [11]P.Mohan Kumar and K.L.Shunmuganathan “A New approach for hiding data in images using image domain method” in International Journal of computer and internet security ISSN 0974-2247 volume 3 number PP 69-80, 2011.