RESEARCH ARTICLE OPEN ACCESS

Hiding Data in Video Stenography by Using Different Algorithm: A Review

Simaranjit Kaur
Sri Guru Granth Sahib World University
Fatehgarh Sahib
Punjab – India

ABSTRACT
Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner and is an art of hiding information in ways that avert the revealing of hiding messages. Video files are generally a collection of images. so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of image. The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Cryptography, on the other hand obscures the content of the message. We propose a high capacity data embedding approach by the combination of Steganography and cryptography.

Keywords:- Data hiding, Steganography, File Security, Data Sharing, Frame Extraction, Consumer Videos.

I. INTRODUCTION

Text, image, audio, and video can be represented as digital data. The explosion of Internet applications leads people into the digital world, and communication via digital data becomes recurrent. However, new issues also arise and have been explored, such as data security in digital communications, copyright protection of digitized properties, invisible communication via digital media, etc. but rapid development of the Internet and the digital information revolution caused significant changes in the global society, ranging from the influence on the world economy to the way people nowadays communicate. Versatile and simple-to-use software and decreasing prices of digital devices (e.g. digital photo cameras, camcorders, portable CD and mp3 players, DVD players, CD and DVD recorders, laptops, PDAs) have made it possible for consumers from all over the world to create, edit and exchange multimedia data. In steganography, the object of communication is the hidden message and the cover data are only the means of sending it. Secret information as well as cover data can be any multimedia data like text, image, audio, video etc The objective of this work is to develop a Compressed Video Steganography Scheme that can provide provable security with high computing speed, that embed secret messages into images without producing noticeable changes.

II. ALGORITHM

a. Random Byte Hiding Technique

In this technique, the information is hiding in each line of the video frame at the different place. For example, if the line begins with the pixel value of 'zz', the information is stored over the 'zz'+x location, where x is only known to the authorized receiver. So, when unknown person view the video, he sees it as normal video, while the person knowing the steganography can detect the hidden message.

The same kind of technique can be implemented by using 'y-zz' where y must be taken above the 256 (a bit higher than logical high level) so that 'y-zz' does not go negative. The similar technique can be implemented over the column line also. The lossless steganography requires storing the hidden information in a specific location and will requires some time to run the algorithm and to find the specific location where hidden information will be stored. Thus, in real time application, the lossless algorithm is becoming tougher to implement, and that depends on the system specifications. The lossy steganography requires store the data at some LSB location or at specific pixel locations. This is easy to implement and it can be apply in real time application with any normal system specifications. The video steganography is achieved by embedding the video files with the secret data that is to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end.

III. AES (ADVANCED ENCRYPTION STANDARD)

The AES algorithm is most secure and robust cryptographic algorithm against attacks. Unlike the DES which is far slow and is already broken and also produce inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds. AES has symmetric block cipher and hence uses same key for encryption and decryption. The block size of AES varies from 128, 192, and 256 bits, the substitution and permutation are performed in AES. The number of rounds depends upon the key length i.e. 10 rounds for 128 bit key, 12 for 192 bit key and 14 for 256 bit key. We have also used SHA-1 for providing more restricted approach as it generates the hash function with key which helps to make the secret data secure if it is being identified without key it can never be altered. The next stage is to perform actual steganography where this secret data is given to hide inside the video carrier the stego video is generated as a result of video steganography as shown in fig.1

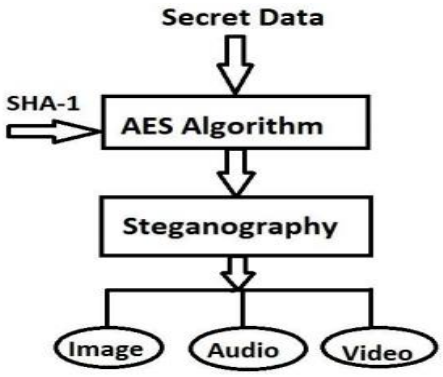

Figure 1: The Proposed Steganography

B. Extraction Of Video File (at Sender Side)

The video steganography composed of two main phases namely extraction of video files and embedding of secret message, as the secret message is already encrypted using AES and SHA-1 it can be easily embedded into carrier video. The extraction of video results in frames as video generally composed of still images and audio, the audio and image frames from the file video is extracted. From this extracted audio the stego file is generated as a secret data is hided in the audio not in the image frames.Audio contains unused bits or free bits of information in which secret data can be very easily hided.

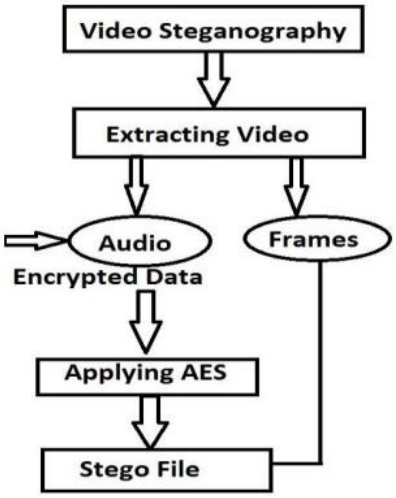

Figure 3: Extraction Of Video at Sender Side

IV. RELATED WORK

This section gives a brief overview on the related work done on the video compression using adaptive block based compression and Motion vector based on the MPEG-2 video Steganography. Moreover, the encryption algorithm used for text encryption is discussed. In the year 2000 Fridrich[10] had developed (t, n) threshold scheme, where a sender hides and splits the secret into n number of shadows. The sender then gives a share of the shadows to the approved participants. The secret data can be revealed if any t out of n authorized participants with their corresponding shadows is present. in 2012 Saurabh Singh [6] developed the Visual secret sharing from the (t, n) – threshold oncept. Random images called shadows are generated from secret image. During transmission the shadow is send out instead of shadows Chen et al [11] and Wang [10] describes the problems like pixel expansion, contrast, and meaninglessness which are more attracted by the attackers. Embedded image called stego image which is meaningful is used to hide the shadow from attackers. Wu, Y.S., Then,Balaji R in 2011 [5] recommended t-1 polynomial to generate shadows in secret sharing technique. To hide secretcover image and secret image are incorporate. The reconstruction of image has distortions because of truncation of gray value pixels (greater than 250). These kinds of small distortions are not tolerable in medical images and other sensitive images Poonam V Bodhak in 2012 [4] overcome these problems by using two pixels to describe the grey values that are greater than 250. This result in expansion of secret image therefore alters the quality of the stego image. To increase the volume of the embedded secret stream, in early 2009, instead of embedding one secret pixel into the (t -1) degree polynomial F(x) (t-3) secret digits into polynomial F(x). There has been a rapid growth of interest in this subject over the last ten years and for two main causes. Firstly, the publishing and broadcasting industries have become highly involved in techniques for concealing encrypted copyright marks and serial numbers in multimedia products such as digital films, audio recordings, e-books, etc; an appreciation of new market chances generated by digital distribution is linked with a fear that digital works could be too easy to copy. Secondly, directions by various governments to keep under control of the handiness of encryption services have inspired people to study methods by which private messages can be attached in apparently not harmful cover messages.

V. CONCLUSION

The construction of video steganography was realized by embedding the secret image into the meaningful cover image of any type of video file using random byte hiding technique. Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Enhancement of the image steganography system is printed out using LSN approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. The embedded video steganography has many specific advantages such as user friendliness, simple and effective process of embedding secret image with more security.

REFRENCES

[1] Mamta Juneja, Parvinder Singh Sandhu, " Information Hiding using Improved LSB Steganography and Feature Detection Technique" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[2] Mamta.Juneja and Parvinder S. Sandhu, "An improved LSB based Steganography with enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong-Kong (China).

[3] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[4] Poonam V Bodhak, Baisa L Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", ISSN: 2277-3754 International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[5] Balaji R, Naveen G, "Secure data transmission using video Steganography", 2011 IEEE International Conference on Electro/Information Technology (EIT), pp. 1-5, 15-17 May 2011.

[6] Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB Replacement", International Journal of Engineering Science and Technology, Vol. 2(12), pp. 6999-7003, 2010.

[7] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", University of Michigan, IEEE 2003.

[8] Cvejic N. and Sepp änen T. "Increasing the capacity of LSB based audio steganography ", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[9] Giuseppe Caccia, Rosa Lancini, "Data Hiding in MPEG2 Bit Stream Domain", Proceedings of International Conference on Trends in Communications, 2001, pp.363-364.

[10] Fridrich, Jessica and others. "Steganalysis of LSB Encoding in Color Images. " Proceedings of the IEEE International Conference on Multimedia and Expo. 1279 --1282. New York: IEEE Press, 2000.