Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Improved Security Mechanisam of text in Video by using Steganographic Technique: A Review

Manpreet Kaur
Research Scholar, CSE Dept
Chandigarh University, Gharuan, Punjab, India

Er. Amandeep Kaur
Assistant Professor, CSE Dept.
Chandigarh University, Gharuan, Punjab, India

Abstract- Steganography is an art of hiding the secret message in a cover object without leaving a remarkable track on the original message. It is used to increase the security of message sent over the internet. In contrast to cryptography, it is not used to scramble the data but it is used to conceal the data in digital media. This review paper will deal with video steganography, cryptography, hash-LSB and a new encryption algorithm. At the end, we will discuss the goal of this paper and what types of techniques worked on video steganography.

Keywords- Steganography, Cryptography, Hash-LSB, Encryption algorithm.

I. Introduction

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of Steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all [11]. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file [5]. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in Steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it.

Steganography and cryptography are closely related. Cryptography scrambles messages so it can’t be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message [12]. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In Steganography Comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in Steganography is the stego-media. The message in Steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

There are four types of Steganography methodology:

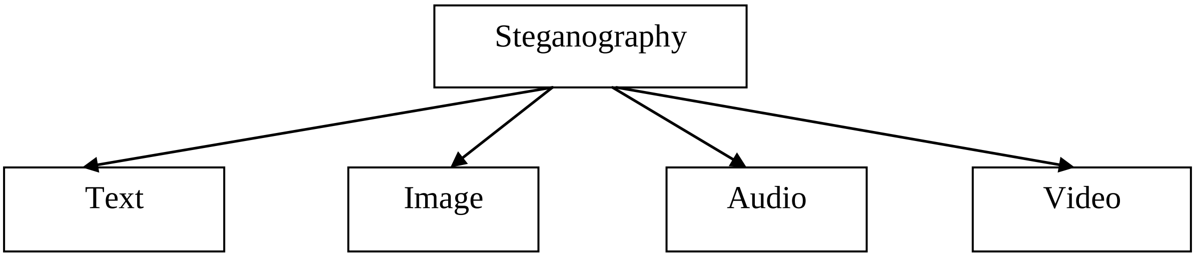

Figure1:- Types of Steganography

The use of video as a carrier cover for the secure message is overcame the capacity problem and added small enhancement to the security aspects [8]. The integration of Steganography and cryptography techniques provided powerful systems for sharing secure messages. This integration especially within video cover carrier is a good stage of such systems, but the capacity of the produced message from the cryptography technique which is called cipher-text is larger than the original message (plaintext) [5].

The cryptography techniques increase the size of message after the encryption to be greater than the size of the original message, on another hand shown that the cipher-text size is much larger than the plaintext size by using the cryptography techniques. While found out the cipher-text size is usually long, at least twice that of the original plaintext [12].

Video Steganography techniques:

Several new approaches are studied in video data Steganography literature. In this section, some of the most well-known approaches have been discussed.

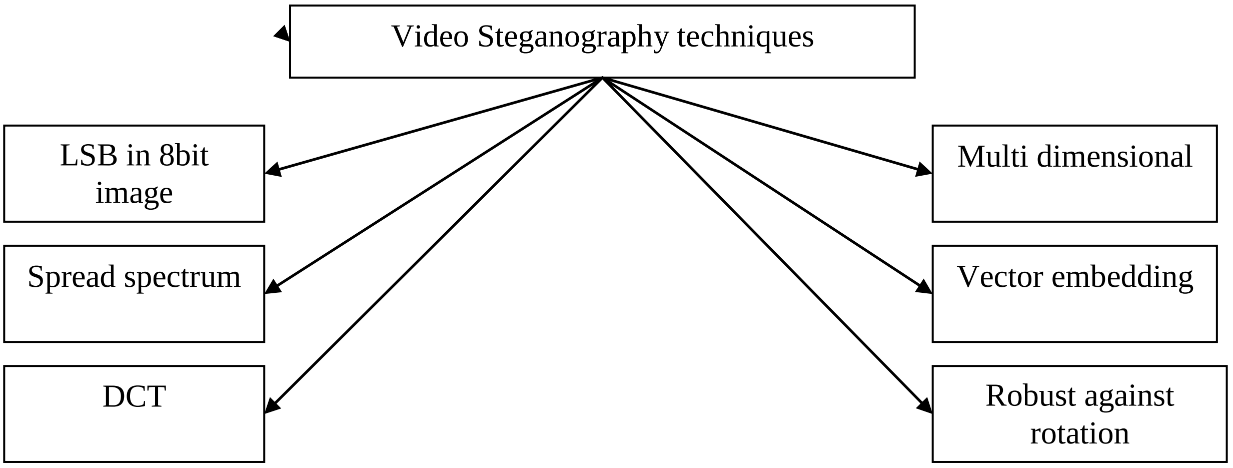

Figure2: Techniques of video steganography

First of all, the most common method is Least Significant Bit method (LBS) which hide secret data into the least significant bits of the host video. This method is simple and can hide large data [14].

Another well-known method which has been still researching is called Spread Spectrum. This method satisfies the robustness criterion. The amount of hidden data lost after applying some geometric transformations is very little. The amount of hidden lost is also little even though the file is compressed with low bit-rate. This method satisfies another criterion is security.

A technique for high capacity data hiding using the Discrete Cosine Transform (DCT) transformation. Its main objective is to maximize the payload while keeping robustness. Here, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of frames [4].

A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2) .This method embeds audio information to pixels of frames in host video [9].

II. Related work

This paper 2009 Mozo A.J.[13] "Video Steganography using Flash Video (FLV)"successfully deals with the demands of using video steganography on FLV. The project focused on FLV files because of their relatively small size compared to other video file formats, their simplicity in structure, and their popularity in video-hosting websites. This allow doctors and medical personnel to embed multiple medical records such aselectrocardiogram signals, ultrasound files, medical prescriptions, urinalysis, and may more medical files into single video file (FLV)

In this paper 2010 swathi A. [17]"Video Steganography by LSB Substitution Using Different Polynomial Equations" Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. A data hiding scheme is developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation.

This paper 2011 Hussein A. [9] "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error "deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis. There is new method to hide the data in motion vectors of MPEG-2 compressed video. The results of this paper are evaluated on two metrics: quality distortion to reconstructed video and data size increase of the compressed video.

In this paper 2012 Poonam V. [4] "Improved Protection in Video Steganography Using DCT & LSB" 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 system is based on the research findings developed an application which is able to hide the data with high security in AVI videos. Also this is an independent platform application with high probability and high consistency. This is used to embed text files into video files.

This paper 2012 Attallah M. AI- shatnawi, [3] "A new method in image steganography with improved image quality" presents an efficient, simple, robust method to attack and improve the image quality and it obtained an accuracy ratio of 83%. The results of this work and LSB hiding techniques were discussed and analyzed based on the ration between the number of identical and non identical bits between the pixel color values and the secret message values.

The paper 2013 Jue W. et al. [21] "Video Steganography Using Motion Vector Components" based on the H.264/AVC Video coding standard, a new video steganography algorithm is proposed and realized. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier. This work presents a video Steganography algorithm based on motion vector component's differences. It obtains the higher carrier utilization and embedding capacity with good visual invisibility and statistical invisibility.

This paper 2013 sunil. K. Moon. [20] "Analysis of secured video steganography using computer forensics techniques for enhances data security" deals with the idea of video steganography, cryptography and the use of 4LSB to embed the secret data in true color image. In this computer forensics technique is used for extracting the secret data and used to find the parameters like frame numbers, height, width and histogram of secret message before and after hiding to video.

In this paper 2013 kumar A, Sharma R.[12] "A secure image steganography based on RSA algorithm and Hash-LSB technique" mentioned that a new technique of image steganography with hash LSB and RSA algorithm for providing more security of data into RGB pixel values of the cover image. This paper also tells about a LSB method for true color image by enhancing the security level of hidden information. The Hash-LSB technique have been applied to .tiff images. As well as it can work with any other formats.

This paper 2013 vipul Sharma, sunny kumar, [18] "A new approach to hide text in image using Steganography" proposed a new steganographic algorithm for hiding text files in images to increase the capacity of secret data. A compression algorithm is used with maximum compression ratio of 8bit/pixels. A system developed in java based on the proposed algorithm. This work found that .bmp images are efficient for this algorithm.

The paper 2013 k.steffy Jenifer, G. yogaraj, [19] "LSB approach for video Steganography to embed images" based on LSB approach is used along with the masking filtering and transformation techniques to hide the secret images or any other files. This technique is used to convert the color image into gray scale image. This method improves the visual quality of the share images. There are different advantages like: user friendliness, simple process of embedding secret image with more security.

III. Present work with existing techniques used

There are two types of techniques which are used in this paper:

A. RSA algorithm

The algorithm was given by three MIT's Rivest, Shamir & Adleman and published in year 1977. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above.

B. LSB insertion method

One of the most common techniques used in steganography today is called least significant bit (LSB) insertion. Also called LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system. The Least Significant Bit insertion varies according to number of bits in an image [16]. For an 8-bit image, the least significant bit i.e. the 8th bit of each byte of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each component like RGB (red, green and blue) will be changed. LSB steganography involves the operation on least significant bits of cover image, audio or video.

IV. Need and Significant

The problem statement consists of embedding the secret information in LSB of each RGB pixel values of the cover video. To enhance the security of message, the secret message have to be converted in the cipher text using RSA algorithm. In this approach we have a new technique called Hash-LSB derived from LSB insertion on images and videos. In Hash–LSB, the hash function is used to evaluate the positions where to hide the data. This technique provide a solution for transferring and sharing the important data without any compromise in security. We have used Hash-LSB and RSA algorithm to create a secure steganography algorithm which is more secure than many algorithms being used for purposes of hiding the important data.

V. Proposed Methodology

The technique Hash-LSB improves the security of data. As well as this technique also increase the capacity of data to embed into the cover video. There is also comparison of result with existing techniques. The steps of methodology are following:

1. Preprocessing:- Select cover video(.avi file) and split into frames.
2. Frame Selection:- Cover frame from cover video will be selected as per pass key.
3. Conversion:- convert secret message into cipher text using RSA algorithm.
4. Embedding Process:- Hide the secret message (.text) into the cover frame using Hash-LSB to get stego frame. Hide the authentication key.
5. Replacement:- Replace the original frame with stego frame.
6. Recombination:- Recombine the frame to form into a stego video and transfer it using communication.

VI. Conclusion

In the steganography, Hash-LSB method is an efficient steganographic method for embedding the secret message into cover video without producing any changes of quality of video. In this work, this is a new way of hiding the information in a video with more security. This technique also applies a cryptographic method i.e RSA algorithm to secure a secret message which is not easy to break. A specific technique uses Hash function and RSA algorithm, is very much usable and truthworthy to send data over any unsecure channel. This technique can also be used in audio.

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to Er. Amandeep Kaur for his guidance and expert contributions to this paper. Without her support it would be impossible to complete this paper. I would also have to appreciate the guidance given by other supervisor as well as the panels especially in my project presentation that has improved a lot. Thanks for their comments and advices.

REFERENCES

[1] Avudainayagam A., Dapeng Wu, *"*Hyper-Trellis Decoding of Pixel-Domain Wyner–Ziv Video Coding*" IEEE transactions on circuits and systems for video technology,* vol. 18, no. 5, may 2008.

[2] Sharp A. and Sharif H., "A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform" *IEEE International Conference on Signal and Image Processing Applications (ICSIPA)* 2013.

[3] Attallah M. and AI- shatnawi, "A new method in image steganography with improved image quality" *Applied mathematics sciences,* vol.6, 2012.

[4] Bodhak V. and Gunjal L., "Improved protection in video Steganography using DCT & LSB" *international journal of engineering and innovative technology (IJEIT)* vol. 1, issue 4, April 2012.

[5] Bhowal K. and Jyoti Pal A., "Audio Steganography using GA", *IEEE International Conference on Computational Intelligence and Communication Networks CICN 2010, pp 449-453,* Nov 2010.

[6] Debiprashad B. and dasgupta K. "A novel secure image Steganography method based on chaos theory in spatial domain" *International of security, privacy and trust management (IJSPTM)* vol. 3, no 1, February 2014.

[7] Gupta H. and Dr. Chaturvedi D., "Video Data Hiding Through LSB Substitution Technique" *Research Inventy: International Journal Of Engineering And Science* Vol.2, Issue 10 2013,

[8] Gupta S. and Gujral G., "Enhanced least bit algorithm for image Steganography" *IJCEM international journal of computational engineering & management,* vol.15 issue4, July 2012.

[9] Hussein A. Aly *",* Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error*" IEEE transactions on information forensics and security,* vol. 6, no. 1, march 2011.

[10] Jiang H. and Joshi A., "Scene change detection techniques for video database systems*" Multimedia systems@* Springer-verlag 1998.

[11] Kapoor D. and Bajpai N., "A new horizon in data security by Cryptography & Steganography," *International Journal of Computer Science and Information Technologies, vol. 1, no. 4, pp.212-220, 2010.*

[12] Kumar A, Sharma R, "A secure image Steganography based on RSA algorithm and Hash-LSB technique " *International journal of kumar advanced research in computer science and software engineering vol.3,issue 4,* 2013vol.3, issue 7, July 2013.

[13] Mozo AJ., and Obien M.E., C.J. Rigor, "Video Steganography using Flash Video (FLV)" *I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore,* 5-7 May 2009.

[14] Mr tyagi V., "Data hiding in image using LSB with cryptography*" International journal of advanced research in computer science and software engineering* . vol.2, issue 4, april 2012.

[15] Olivia N., Anastasios D., "Scene change detection for H.264 using dynamic threshold techniques" *copyright 2005EURASIP. Published in proceeding of conference on speech and image processing, multimedia communications and services,* June 29-july2 2005.

[16] Patel K. and Kauwid Rora K., "Lazy Wavelet Transform Based Steganography in Video" *International Conference on Communication Systems and Network Technologies* 2013.

[17] Qin c., Ying-Hsuan Huang, "An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism*" IEEE transactions on circuits and systems for video technology,* vol. 23, no. 7, July 2013.

[18] Sharma V. and kumar S. "A new approach to hide text in image using Steganography*" International journal of kumar advanced research in computer science and software engineering* vol.3, issue 4, 2013.

[19] Steffy jenifer K. and Yogaraj G., "LSB approach for video Steganography to embed images" *International journal of computer science and information technology* vol.5 (1), 2014.

[20] Sunil. K. Moon, “Analysis of secured video Steganography using computer forensics techniques for enhances data security” *IEEE second international conference on image information processing* (ICIIP-2013).

[21] Tasdemir K. and Kurugollu F., “Video steganalysis of LSB based motion vector steganography” *International Conference on Communication Systems and Network Technologies* 2010.