International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 776 - 780

Video Steganography: A Method for Providing Improved Security

Miss. Rushvi Rajkumar Jaiswal
Dept. of Computer Sci. & Engineering, P.R.Pote COEM, Amravati
rushvijaiswal4@gmail.com

Prof. Vijay B. Gadicha
HOD Comp. Sci. Dept., P. R. Pote COEM, Amravati
vbgadicha@gmail.com

Abstract:- As the data traffic is growing day-by-day, it is very risky to handle the data in internet against intruders or hacker. The data that is transferring is mainly unstructured data and is generally in the form of text, image, audio and video. So for that in this paper, we have propose the technique called Steganography. This steganography serve as one of the best method to share the data secretly and securely. As the data is available in unstructured and in large format, there are different Steganography methods and algorithm that can be applied to audio, video and image file. Secret data may in the form of text, image or even in the form of video and audio. Hiding large secret information can be possible in the video file and is known as video steganography. In this paper, a review on some video steganography techniques has been presented and we have proposed the method of Advanced Video Steganography. Our proposed method is the combination of Compression, Encryption and then Embedding the secret information, which provide more secure data transfer.

Keywords: *Steganography, Cover Medium, Compression, Encryption, stego Video.*

*****

I. INTRODUCTION

Steganography is the practice of concealing a file, message, and important information of any format as text, image, audio or video within another file, message, of any format. Steganography is the art of hiding the information in some other host object. In ancient time this technique is used as, secret information is hidden in the back of wax, scalp of the slaves, in rabbits etc. The word *steganography* used from the past combines the Greek words *steganos*, meaning "covered, concealed, or protected", and *graphein* meaning "writing" [1]

Steganography is the act of changing the digital media as only sender and the recipient to whom one has to send the message is able to detect the message sent through it.

The following formula provides the description of the pieces of the steganography process [2]:

Cover Medium + Hidden Data + Stego Key = Stego Medium

In above formula, the Cover Medium is the file which is used to hide the secret data, which may be encrypted using the Stego Key. The resultant file we get from here is the stego medium which will, the same type of file as the Cover Medium. The block diagram showing the mechanism of Steganography is shown in Figure 1 [3] below.

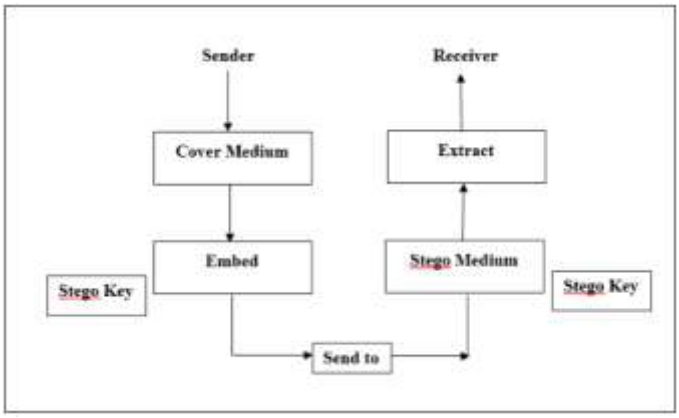

Figure 1. Block diagram of Steganography mechanism

In the above diagram, the secret data is being embedded inside a cover image to produce the stego image medium. In this embedding technique, a key is often needed. The proper stego key is used by the sender for the embedding procedure. The same key is needed by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

The Steganography method is different from the traditional cryptography method in following ways. Cryptography is the practice and study of secure communication. Steganography is the art and science of covert communication. Cryptography protect the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. In digital

steganography, electronic communications include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. As the Media files are of large size, they are ideal for steganographic transmission.

In the steganography, the cover can be image, text, audio and video. In this, the Image is the most familiar cover, but the limited size of image will restrict the capacity of embedding important data [4]. Whenever it is required to transmit large amount of secret messages, steganography in image will become insufficient. So steganographic method that has higher embedding capacity needs to be used. Because digital video is composed of series of frames and has greater signal space, steganography in video will have larger capacity for embedding useful information. Besides this, the degradation of video quality cannot be observed easily by eyes, it may be occur by video compression of lower quality. These reasons make it possible to securely hide data in video.

Application of Steganography varies from different application industry as military, industrial applications to copyright and Intellectual Property Rights (IPR), data authentication. The problem with existing video steganography technique is, they have work only on .AVI files and only single data format i.e. text or image. The challenge is for developing an algorithm which will facilitate the usage of any video format(flv, mts, mpeg, mov) as the cover and versatile data format(text, image, audio, video) as secret message [5]. After studying the literature related to steganography it is observed that the techniques/methods available for Video Steganography lack support for versatility with respect to its cover file format and data file format. The amount of data the cover file can carry is also limited and security layers are not added effectively which results in insecure communication.

The best technique is to hide the secret data along with the quality of the cover video, is that it cannot be detected by naked eyes. The embedded video is known as the "stego" video which is sent to the receiver side by the sender [6]. Variety of video steganography techniques are used now days, out of which to secure important information we have use the combination of some methods as Advanced Video Steganography. In our advanced video steganography technique, we make use of combination of video Compression, video Encryption and finally embedding that video. This advanced video steganography technique is proposed in further section. The paper also consist of Literature Survey of some methods used by some authors and advantages of this advanced video steganography methods.

II. LITERATURE SURVEY

It is observed that the work done so far has limitation of single cover file format i.e. .avi files are mostly used, other formats are been neglected. The secret message which can be embedded in cover file is generally text or image, there is limitation of size the cover file can carry. Security is also one of the issue which is not taken into consideration while implementing steganography concept. The Work done by different authors are as below:

One of the most common and easy method of image steganography is least significant bit method (LSB). This method can be applied to the video steganography. In this method least significant bit of the frames of host video is used to carry the secret information [7]. This method is simple and requires least computational power but in this method the secret information can be destroyed easily by some file transformation. Moreover the security of this method is very poor and can be broken easily.

Bin Liu et al [8] "Secure Steganography in Compressed Video Bit-streams" it is one of the new compressed feature secure steganography (CVSS) calculation is proposed. In this calculation, implanting and discovery operations are executed completely in the compacted area, without any requirement for the decompression process. The new criteria that make use of factual imperceptibility of adjoining edges are utilized to modify the installing technique and limit that builds the security of proposed calculation. Along these lines, the plot safe properties are acquired. Trial results demonstrated this plan can be connected on packed feature steganography with high security properties.

In "Compressed video steganography using TPVD" the authors, Sherly A P and Amritha PP [9], proposed the method in which data is hidden in compressed video. In the previous method, Data is hidden in the macro block of Iframe that undergoes maximum scene change. The block of P frame and B frames are used for data hiding. P and B frame block having maximum motion of magnitude is chosen for data hiding. This method is modify using triway-pixel-value differencing method, for hiding the data.

In 2013, Liu in his paper [10] suggested a robust steganography scheme in H.264 compressed video. This method is able to prevent inter-frame distortion. In order to make the scheme more robust, message is encoded using BCH code and then embedding operation is performed. Coefficients of DCT of luminance I-frame component is used as host data. Simulation results show high quality and robustness.

The author Sheng Dun Hu, Kin Tak U [11] presented a video steganography system based on non-uniform rectangular partition. This technique is used in

uncompressed videos. In this method a secret video is hide in a cover video, both should be of almost the same size. In each frame of both the videos, some mechanism is applied for hiding the video stream. The frame length of the cover video should be greater than or equal to the frame length of the secret video, for hiding the secret video in to the cover or host video. Each frame of secret video is portioned in to non-uniform rectangular part which is encoded. The secret video stream is hidden in the leftmost four least significant bits of each frame of the host video stream. Results of using this technique showed no distortion, so no one will think that any kind of data is being hidden in the frames.

In the year 2009 [12], Cheng-Hung Chuang and his fellow researcher presented optical video crypto-system with adaptive steganography for encrypting and decrypting the video sequence. A double random phase encoding algorithm is applied in this method to encrypt and decrypt the video stream. Video signal is first converted to RGB model and then all the three channel i.e Red, Green and blue channel are separated. The Encryption operation is applied to each channel by two random phase mask. In this method, Session keys are used for generating these phase mask. These key in cipher text form is the embedded in the encrypted version of the video stream by adopting content dependent low data distortion embedding method. Zero-lsb sorting technique is used to hide ciphered data to encrypted video stream for key delivery. Experimental results shows that the performance of adaptive steganography is better than the traditional one.

III. PROBLEM DEFINITION

Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. We also have to consider the transfer of large amount of data through the network will give errors at the time of transferring and only the single level of security is present in the existing systems [13]. Now days, hacking activities are growing day-by-day and they easily hack important information and security mechanisms is not sufficient to stop it. Though security status increased at a higher level but the major drawback of new status of security is cost, and became so costly. For that we need better solutions with good security level with lower cost.

These can be avoided by making use of our proposed system. The mechanism, which is used to hide the information in the image files [14]. Here, to make the solution on the problems mentioned above, we have proposed the Advanced Video Steganography technique. This advance method consist of the combination of Compression, Encryption and embedding technique, which is mentioned in our proposed system.

IV. PROPOSED WORK

Video Steganography is the art of writing hidden messages inside videos, in such a way that no one instead of the sender and intended recipient realizes the existence of a hidden message. Steganography mostly uses repeating portions of the Video files to embed the secret message. There are many techniques for hiding data in Video, here we use one of those technique along with the encryption of the video and message. The proposed steganography system will take a plain text file, container file and a password, and then the system will encrypt and embed plaintext file in the container file. Steps below gives working of how the system is expected to embed and extract covert data.

A. Encryption and Decryption:

Encryption will be performed using an Advanced Encryption Standard (AES) algorithm. The use of AES encryption will add a high level of security to the data being embedded.

B. Embedding Algorithm:

During the embedding process, data needs to be encoded in the frames of the video stream. Since it is possible for a video frame to span multiple packets of a video file, the proposed system will need to read sequential packets of data from that file to avoid complications that could arise from seeking to random portions of the video file.

C. Extraction Algorithm

The extraction algorithm will work in a similar principle. Packets will be read sequentially from the container file, and the correct extraction method will be used depending on whether the packet contains a video frame and which method is used for embedding.

- Work flow of our proposed system:

The Advance Video Steganography technique uses video as the cover file, this video is divided into frames to find position of data insertion. As there are many frames in a video there is more chance of redundant bits to be found, where secret message can be embedded. This system is three times more secure than the existing system (LSB) as three levels of security is added. The first is using Compression technique which is Huffman coding for compressing the secret message which can be text, audio, image or video. Compression increases the embedding capacity of data and intruder cannot guess that compression is been used, if he detects compression he may not be able to know which compression technique is been used. Then next level of security is provided by the use of Encryption algorithm

 ISSN: 2321-8169
776 - 780

which is AES +256 shift. This again is enhanced by using a password as a key for AES. Next level of security is provided by embedding secret data in the stego video due to which it would be difficult to recognize message bits and secret data bits. Figure 2. [15] below shows the actual working of this system.

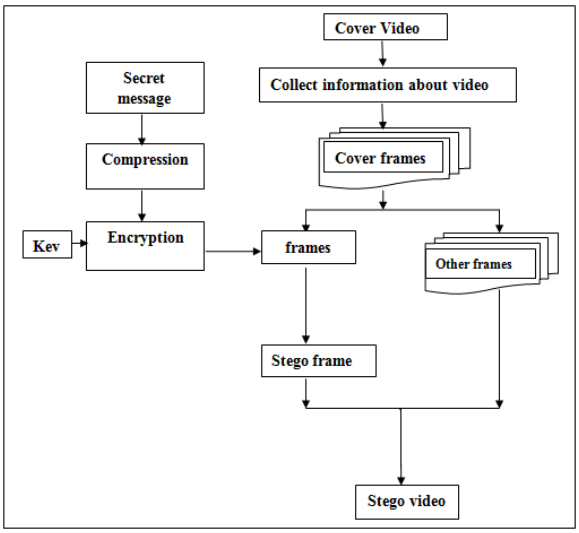

Figure 2. Actual working of system

The Step wise working of our Advanced Video Steganography is given below:

- Input Video file.
- Read required info from video & break it into frames.
- Input secret message in the form of text, or audio, or image, or video.
- If Compression of the secret message is required use Huffman encoding.
- Encrypt the secret message using AES algorithm+256 bits shift operation.
- Find position of insertion of bits. Combine frames and insert some secret data.
- Generate stego-video file for transmission.

V. FEATURES OF OUR ADVANCED VIDEO STEGANOGRAPHY

The features of Our Proposed Advanced Video Steganography which makes it favorable for data hiding are as follows:

A. Accuracy:

The extraction of the hidden information from the medium should have to be accurate and reliable.

B. Improves Capacity:

Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50%, but there is limitation on how much information can be hidden into an image. Video Steganography has overcome this problem.

C. Less Imperceptibility:

It is less imperceptible because of quick display of the frames in the video. And becomes harder to be detected by human perception system.

D. Correction of Errors:

Since the transmission of any data is always subject to corruption due to errors, then the video transmission must deal with these errors without retransmission of corrupted data.

E. Robustness:

The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.

F. More Privacy:

Extraction of hidden information from the video is not possible without prior permission of intended user having password. Since random data are placed in unused frames in video, the attacker is does not know the real secret data hidden in the video. That helps to highly confidential data in military and bank application can be transmitted over internet even in unsecured connection.

VI. CONCLUSION

The Advanced Video Steganography technique has been presented in this paper. With the aim of solving the problems like versatility, low embedding rate, security issues, to this our proposed technique has proved to be a better solution for Video Steganography. In HLSB only .avi files were used as cover whereas in the proposed technique different cover file formats can use versatile data file format as text, image, audio and video. Although any type (text, image, audio, and video) of data was embedded in the cover there is only slight change in size of stego video. The video quality is not compromised in steganography process and consist of some drawbacks. Thus our proposed Advanced Video Steganography method outperformed than existing techniques with many useful features.

REFERENCES

[1] Patrick Philippe Meier, *"Steganography 2.0: Digital Resistance against Repressive Regimes", irevolution.* Wordpress.com. *Retrieved 17 June 2010.*

[2] Shivani Khosla, Paramjeet Kaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking" International Journal of Computer Applications (0975 – 8887) Volume 95 – No.20, June 2014.

[3] Richa Khare, Dr. Kuldeep Raghuwanshi, "A REVIEW OF VIDEO STEGANOGRAPHY METHODS", *International Journal of Research in Advent Technology*, Volume 2, Issue 1, January 2014.

[4] Ko-Chin Chang, Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia, VOL. 3, NO. 2, JUNE 2008.

[5] Sherly A P, Amritha P P, "A Compressed Video Steganography using TPVD", *International Journal of Database Management Systems (IJDMS)*, Vol.2, No.3, August 2010.

[6] Arup Kumar Bhaumik, Minkya choi, "Data hiding in video" IEEE International journal of database application, vol.2 no.2 June 2009.pp.9-15

[7] Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).

[8] Bin Liu "Secure Steganography in Compressed Video Bit-streams", IEEE Conf. on Pervasive Computing (JCPC), 2009, pp 185 – 190

[9] Sherly A P and Amritha P P, "*A Compressed Video Steganography using TPVD* ",International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010

[10] Y. Liu, Z. Li, X. Ma, and J. Liu, "A Robust Data Hiding Algorithm for H. 264/AVC Video Streams," *Journal of Systems and Software*, 2013.

[11] ShengDun Hu, KinTak U," A Novel Video Steganography based on Non-uniform Rectangular Partition ", IEEE International Conference on Computational Science and Engineering,pp 57-61, Aug.2011.

[12] Cheng-Hung Chuang and Guo-Shiang Lin, "An Optical Video Cryptosystem with Adaptive Steganography", Proceedings of International Association for Pattern Recognition (IAPR) Conference on Machine Vision Applications (MVA'09), pp. 439- 442, Keio University, Yokohama, Japan, May 20-22, 2009. (NSC97- 2221-E-468-006 International Conference on Computational Intelligence and Multimedia Applications, 2007.

[13] Marghny Mohamed, "Data hiding by LSB substitution using genetic optimal key permutation", in International arab journal of e-technology, vol.2, no 1 January 2011.

[14] P. Mohan Kumar, "A new approach for hiding data in image using image domain methods" in International journal of computer and internet security volume 2, 69-80, 2011.

[15] Pooja Shinde, Tasneem Bano Rehman, "A Novel Video Steganography Technique", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 12, December 2015.