Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Video Data Hiding

Kumbhar Shraddha, Rokade Varsha, Sukre Mayuri
Department of Computer Science and Engineering,

***Abstract*— The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. Besides this, anyone can modify and misuse the valuable information through hacking at the same time.**

Secure Video Data Hiding is an important research topic due to design complexities involved. We propose a new video data hiding method that links two sets of data, a set of embedded data & another set of cover media data. In this project, we are using compression, decompression, DCT to provide security. By these techniques, the proposed method can achieve better confidentiality & data recovery.

***Keywords*— Discrete Cosine Transform(DCT), Steganography, Lempel-Ziv-Welch(LZW).**

I. INTRODUCTION

The Steganography is of Greek source and means "enclosed or hidden writing". Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Steganography is implemented in different fields such as military and Industrial applications. By using lossless steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files .Lately, there has been growing interest in implementing steganographic techniques to video files as well as audio files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files and audio files. Image-based and video-based steganography techniques are mainly classified into spatial domain and frequency domain based methods. The main aim of steganography is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major distinction between this method and the other methods of secret exchange of information because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Most steganography jobs have been carried out on images, video clips, texts, music and sounds. For video stream usually being accessible in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression. This is an unnecessary saddle best avoided. If the requirement of strict compressed domain steganography is to be met, the steganography needs to be embedded in the compressed domain. Nowadays, there are large amount of video watermarking algorithms been proposed. Some of them are applied for compressed video. To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid. Similar to cryptography and steganography may suffer from the attack method (steganalysis). Much of the research work in the field of steganalysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding. Another major stream is based on the concept of blind steganalysis, which is formed by blind classifiers. The classifier should be trained to learn the differences between cover and stego-image features at first. In this paper, we propose a secure compressed video steganography architecture taking account of steganalysis module, operated in a closed-loop manner to enhance the anti-steganalysis capability of the stegovideo with data embedded steganography.

A. STEGANOGRAPHY-

This paper focuses on the utilization of digital video/images as cover to hide data. The proposed steganography algorithm based where each pixel in each video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel. This algorithm is characterized by the ability of hiding larger size of data and the ability of extracting the written text without errors, besides it gives a high level of authentication to guarantee integrity of the video/ images before being extracted. Furthermore, the data were embedded inside the video/ images randomly which gave the video/ images a higher security and resistance against extraction by attackers.

II. EXISTING SYSTEM

Existing system for video data hiding is based on LSB(Least Significant Bit) replacement. LSB is the simplest form of Steganography. LSB is based on inserting data in the least significant bit of pixels, which leads to a slight change on the cover images that is not noticeable to human eye. since this method can be easily cracked and it is more vulnerable to

attacks. LSB method has intense affect on the statistical information of image like histogram. Attackers could be aware of a hidden communication by just checking the histogram if an image.

III. PROPOSED SYSTEM

The main aim of the project is to provide software that usually works by sending a text message behind a video which makes unable for a human eye or ear to detect. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial differences.

The architecture of the our system is :

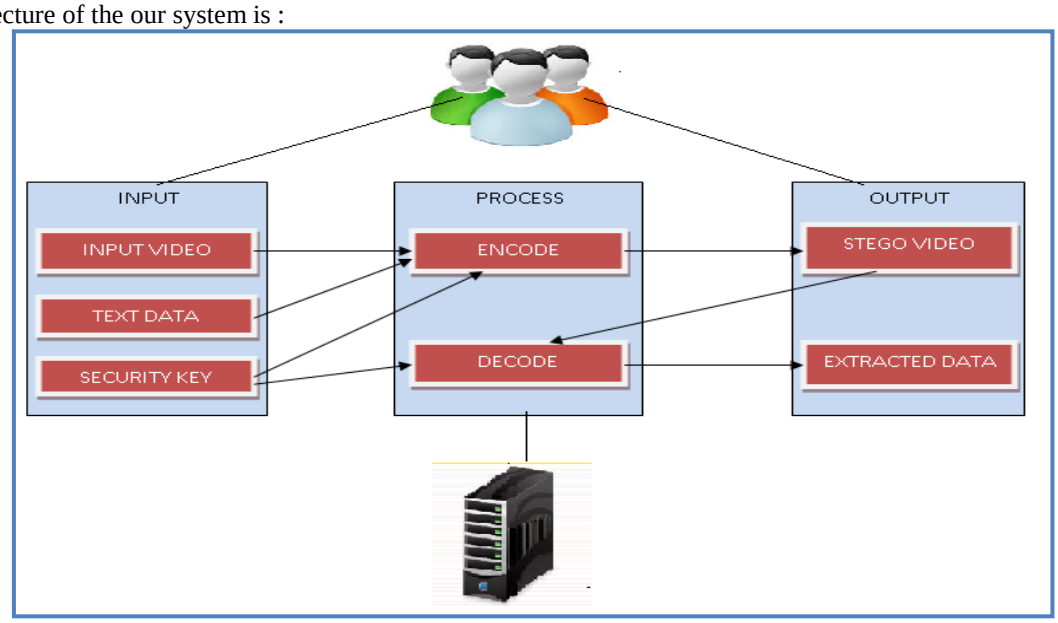

Fig 1 : System Architecture

In the Above architecture diagram describes user provide his input video file , text data and security key for hiding data into Video. The process of system is to collect necessary input from user and Encode the data into Video and Generate Stego Video Similar to Input Video. When user wants to decode it then user needs to provide stego video file and security key which is already used for encoding process. System validate stego video and security key of user and decode the message from the video which is called as extracted data from the video. It is more secure.

IV. CONCLUSION

In the Steganography, DCT 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. LZW algorithm to secure a secret message which is not easy to break, This project very much usable and trustworthy to send data over any unsecure channel.

ACKNOWLEDGMENT

We wish to avail this opportunity to acknowledge our profound indebtedness and extend our deep sense of gratitude to our guide **Prof. R B Thakur, IOKCOE** for his valuable guidance profound advice and encouragement that has feel to the successful completion of this project.

REFERENCES

[1] K.Mohan, S.E.Neelakandan, "*Secured Robust Video Data Hiding Using Symmetric Encryption Algorithms*" , International Journal of Innovative Research in Engineering & Science, December 2012, (issue 1 volume 6), ISSN 2319-5665.

[2] M. Suresh Kumar, G. MadhaviLatha, "*DCT Based Secret Image Hiding In Video Sequence*", Int. Journal of Engineering Research and Applications, August 2014, Vol. 4, Issue 8(Version 1), ISSN: 2248-9622.

[3] R. Ravi Kumar,V. Kesav Kumar, "*Selective Embedding & Forbidden Zone Data Hiding For Strong Video Data Thrashing*", International Journal Of Engineering and Technology,Sep-2013,Volume 4,issue 9,ISSN:2231-5381.

[4] V. Priya, "*Reversible Information Hiding In Videos*", International Journal Of Innovative Research in Computer and Communication Engineering, March-2014, vol 2, special issue 1, ISSN: 2320-9801

[5] Mr Sudheer Adepu, Mr P. Ashok , Dr. C.V.Guru Rao , "*A Security Mechanism for Video Data hiding* ", International Journal of Computer Trends and Technology (IJCTT) , August2013, vol4 , Issue8, ISSN: 2231-2803.

[6] Manpreet Kaur, Er. Amandeep Kaur, "*Improved Security Mechanisam of text in Video by using Steganographic Technique: A Review"* , International Journal of Advanced Research in Computer Science and Software Engineering , May 2014 ,Volume 4, Issue 5, ISSN: 2277 128X.

[7] Dr.K.Sathiyasekar, S.Karthick SwathyKrishna K S, "*A Research Review On Different Data Hiding Techniques*" Inter National Journal Of Engineering And Computer Science, Jan2014, Vol 3 ,Issue 1., ISSN:2319-7242.
[8] http://www.symantec.com/connect/articles/steganography-revealed
[9] http://www.garykessler.net/library/steganography.html
[10] http://www.chmag.in/article/may2012/steganography-over-converted-channels

