International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 12 6847 - 6850

An Efficient Approach to Secure Versatile Data File in Video using Forbidden Zone Data Hiding Technique

Richa Sharma[1]
Student, M.Tech(Computer Engineering)
Marudhar Engineering College
richa.sharma014@gmail.com

Ms. Deepika Gupta[2]
Assistant Professor
Marudhar Engineering College
deepika.gupta1218@gmail.com

***Abstract*:-**Video Steganography is a technique in which we can hide all types of files with any extension into a carrying Video file. In this dissertation, we are using two main terminology that is host file and carrier file where host file is a hidden file (any kind of file like text file, image file, and audio/video file) and carrier file must be a video file. The main motivation of this dissertation is to secure transferring of data by using steganography and cryptography technique. It is concerned with embedding information in an innocuous cover media in a secure and robust manner. In this dissertation we are using Forbidden Zone Data Hiding technique where no alteration is required in host signal range during data hiding process.To securely transferring the data file, we use video data hiding and making use of correction capacity of repeat accumulate code with superiority of forbidden zone data hiding. Using this approach we can also hide and transfer the large video file whose size is larger than cover file in secure manner. The main advantage of using video file in hiding information is the added security against of the third party or unintended receiver due to the relative complexity of video compared to image and audio file.

***Keywords*-** *Cryptography, Steganography, Forbidden zone data hiding*

*****

I. INTRODUCTION

Security and privacy plays a main role in data transformation. For secret communication , cryptography is a technique that scrambles original text or convert original message into non-readable format while steganography deals with hiding a secret data in some carrier file which may be text , image , audio and video file that cannot be viewed by unauthorised person. The video steganography uses a some frames of video files to embed a secret message and file. Most of the latest work in data hiding is about copyright protection and authentication of multimedia data. The advantage of steganography over cryptography is that messages do not attract attention to themselves. Data hiding in which some data is conveyed within a host medium and transmitted to the receivers end. There are main requirements of a data hiding system:

Imperceptibility: There should not be perceptual squalor due to data hiding. Ideally one could not be able to differentiate host signal and marked signal.

Robustness: This is the ability and strength of a data hiding system after certain attacks, in terms of correctly decoding the hidden data.

Capacity: It refers to the possible number of message bits that can be hidden in the host signal.

Security: some security applications may be crucial. In that case, secure the hidden data so that adversary cannot interfere or interfere by any means.

II. FORBIDDEN ZONE DATA HIDING

Forbidden Zone (FZ) [8] is defined as the host signal range, where alteration is not allowed during data hiding process. Let s (bold denoting a vector) be the host signal in RN and m ∈ {0, 1} be the data to be hidden. Then the marked signal x is obtained as given in (1).

$$X = \begin{cases} \boldsymbol{s}, & \boldsymbol{s} \in \boldsymbol{FZm} \\ \boldsymbol{Mm}(\boldsymbol{s}), & \boldsymbol{s} \in \boldsymbol{AZm} \end{cases}$$

where FZm, Allowed Zone (AZm) pair defines the host signal zones where modification is allowed or not and Mm(.) is a mapping from RN to a suitable partition of RN. The requisite on these zones and partitions is simply based on the restraint that they should be mutually exclusive for different m.

FZm and AZm are defined using the control parameter and the difference vector:

$$FZm = \{ s \mid \| em \| \leq r \}, \quad AZm = \{ s \mid \| em \| > r \}$$

Masking is applied to data hiding and watermarking in a number of efforts, as in order to incorporate perceptual analysis, so that perceptually usable host signal samples and permissible distortion limits are determined. However, FZ does not involve any perceptual analysis and adaptive coefficient selection process. The main motivation of FZ is decreasing the embedding distortion at a certain decoding error level. Similar to QIM, FZ should be applied, when the embedding distortion is within perceptually feasible margins. This requirement is generally satisfied as a result of the host signal power constraint, which states that the host

 ISSN: 2321-8169
6847 - 6850

signal power is significantly greater than embedding distortion. FZDH involves a set partitioning to determine the range of host signal where alteration is allowed. FZDH employs a mapping in the AZ, for which quantizers are not the only choice. In FZDH, initially all regions are forbidden and one decreases these zones according to the desired level of decoding error with respect to a channel noise. FZDH keeps some of the host signal unaltered. FZDH approaches to the data hiding problem from a different perspective than coding techniques: there exists uncoded portions of the host signal range. The main motivation is to keep the host signal unaltered for some ranges, which should be determined according to the desired level of robustness, embedding distortion amount and channel noise level.

III. EXISTING SYSTEM

Steganography Techniques	**Cover Media**	**Embedding Technique**	**Advantages**	**Limitation**
Binary File Technique	Binary file	The watermark can be embedded by making changes to the binary code that does not affect the execution of the file	Simple to implement	Only binary file can be hidden
Text Technique	Document	To embed information inside a document we can simply alter some of its characteristic	Alteration not visible to human eyes	Text file can be hidden
Image Hiding Technique LSB (Least significant bit)	Image	It works by using the least significant bits of each pixel in one image to hide the most significant bits	Simple & easiest way to secure data hiding	Text and image can be hidden
DCT (Direct cosine transform)		Embeds the information by altering the transformed DCT coefficient	Hidden data can be distributed more evenly in image. This method is more robust	
Wavelet transform		This method works by taking many wavelets to encode a whole image	Coefficients of the wavelets are altered with the noise within tolerable levels	
Sounds Technique	MP3 files	Data can be encoded in binary sequence which sound like noise but which can be recognised by receiver	Using watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium	Text File can be hidden
Video hiding technique	Video file	Forbidden zone data hiding technique used to hide data without any alteration	Secure and unaltered data can be extracted easily	Hide only text file by this method

IV. PROPOSED SYSTEM

In this proposed work, message, text file, image and video file will be hide behind the video file. Using this approach we can also hide and transfer the large video file whose size is larger than cover file in secure manner. The main advantage of using video file in hiding information is the added security against of the third party or unintended receiver due to the relative complexity of video compared to image and audio file. This technique is also useful to provide robustness against unauthorized attack.

 ISSN: 2321-8169
6847 - 6850

V. GRAPHICAL DESCRIPTION OF RESULT

1. Hidden Various Size Text File Output: As table shown that efficiently hiding text with the help of cover video file. It is a very basic step to hide text in a video file.

Cover Video File Size	Hidden Text File Size	Remark
1.43 MB	650 KB	Properly hide
1.43 MB	900 KB	Properly hide
1.43 MB	1.06 MB	Properly hide
1.43 MB	2.43 MB	Properly hide and easily hide lager text file

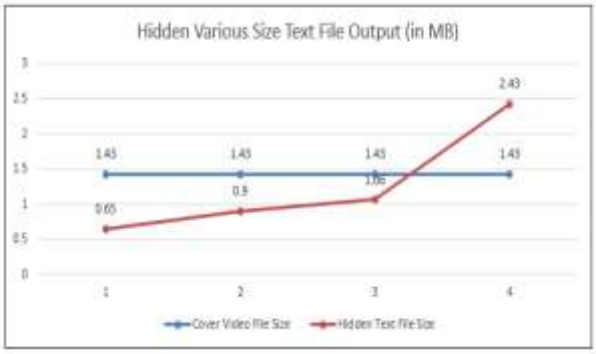

Fig 1 Graph between Cover Video File and Hidden Various Size Text File

2. Hidden Various Size Audio File Output: As table showing that with the help of proposed technique. We can hide different size of audio or larger size than cover file can be hidden very efficiently.

Cover Video File Size	Hidden Audio File Size	Remark
1.43 MB	525 KB	Properly hide
1.43 MB	700 KB	Properly hide
1.43 MB	1.50 MB	Properly hide
1.43 MB	3.25 MB	Properly hide

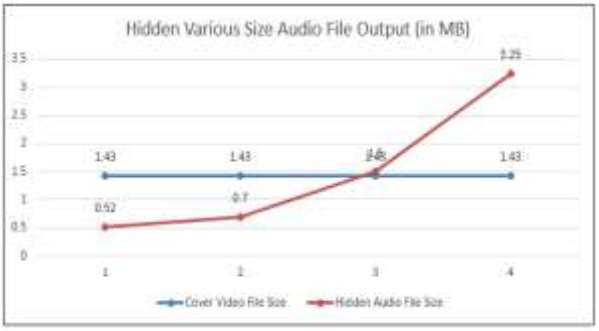

Fig 2 Graph between Cover Video File and Hidden Various Size Audio File

3. Hidden Various Size Images File Output: As table showing that with the help of proposed technique. We can hide different size of images or larger size than cover file can be hidden very efficiently.

Cover Video File Size	Hidden Images File Size	Remark
1.43 MB	525 KB	Properly hide
1.43 MB	700 KB	Properly hide
1.43 MB	1.75 MB	Properly hide
1.43 MB	3.00 MB	Properly hide

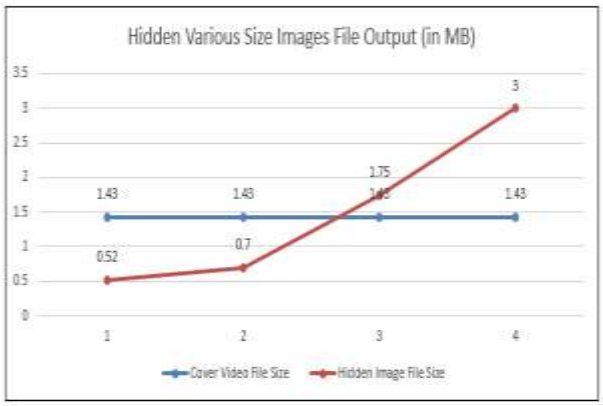

Fig 3 Graph between Cover Video File and Hidden Various Size Image File

4. Hidden Various Size Video File Output: As table showing that with the help of proposed technique. We can hide different size of video or larger size than cover file can be hidden very efficiently.

 ISSN: 2321-8169
6847 - 6850

Cover Video File Size	Hidden Video File Size	Remark
1.43 MB	1.79 MB	Properly hide
1.43 MB	1.90 MB	Properly hide
1.43 MB	2.61 MB	Properly hide
1.43 MB	3.24 MB	Properly hide

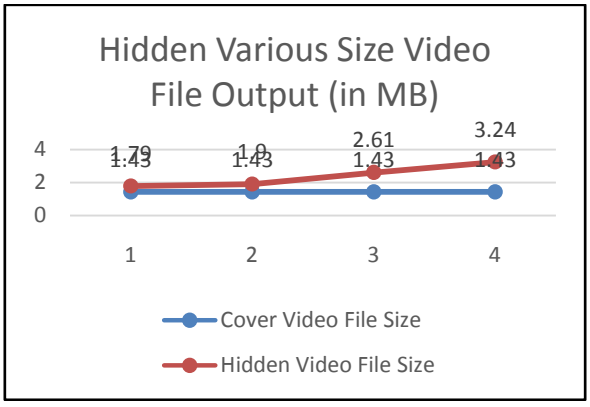

Fig 4 Graph between Cover Video File and Hidden Various Size Video File

VI. CONCLUSION

This proposed work is very useful to hide the all type of information while sending the important and confidential documents in cover video file; it will be invisible for unauthorized person. To securely transferring the data file, we use video data hiding and making use of correction capacity of repeat accumulate code with superiority of forbidden zone data hiding. Mainly we focusing on large video file that size larger than a cover file is also securely hidden without any data loss. The main advantage of using video file in hiding information is the added security against of the third party or unintended receiver due to the relative complexity of video compared to image and audio file. This system is helpful for the defence and security departments sending and receiving the confidential matters in emergency situations.This framework for video data hiding is also superior to water marking method in terms of performance. This is an innovative method to secure data with achievement of lossless cover video. The proposed method can take advantage of all traditional data hiding techniques and achieve excellent performance without loss of perfect secrecy.

REFERENCES

[1] J. J. Chae , B. S. Manjunath," Data Hiding in Video", Department of Electrical and Computer Engineering University of California, Santa Barbara CA 93106-9560 .
[2] Min Wu , Bede Liu ," Data Hiding in Image and Video: Part I—Fundamental Issues and Solutions" IEEE Transactions On Image Processing, Vol. 12 (6), 2003.
[3] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Application, Vol. 9, No.7, November 2010.
[4] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa
[5] Hafiz Malik , K. P. Subbalakshmi ,R. Chandramouli ," Nonparametric Steganalysis of QIM Steganography using Approximate Entropy", Electrical and Computer Engineering Department, Stevens Institute of Technology, Hoboken, NJ 07030
[6] Brian Chen, Gregory W. Wornell," Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Trans. Inform. Theory, Submitted June 1999 Revised September 2000
[7] Chintan Mahant, " Steganography and Stega Different Approaches for Information Hiding "International Journal of Engineering Research & Technology (IJERT)Vol. 1 Issue 10, December- 2012
[8] Snehal Satpute ,Sunayana Shahane, Shivani Singh, Manisha Sharma ," An Approach towards Video Steganography Using FZDH (Forbidden Zone Data Hiding) ", International Journal of Innovations & Advancement in Computer Science IJIACS Volume 4, Issue 1, January 2015 ISSN 2347 – 8616.