International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A Innovative Records Embedding Technique for Hiding Text in Video File using Steganography

[1]Jambukesh H J ,[2]Harisha K S, [3]Prashanthi H J
[1,2,3]Assistant Professor, Dept. of E&CE, Government Engineering College, Haveri, Karnataka, India
jambu6995@gmail.com,harishaks2008@gmail.com,prashanthi.hj@gmail.com

Abstract
The Internet is continuously susceptible to capture by unauthorized people over the world. The standing of dropping a accidental of the valid data being noticed during the communication is being an subject now days. Some resolution to overcome these subjects is cryptography, but once it is decrypted the information secrecy will not exits any more. Hiding data for privacy, this approach of information hiding can be extended to copyright protection for digital media. The importance as well as the technique used in implementing data hiding is trying to discuss in particulars here. The out-dated LSB modification technique by randomly dissolving the bits of the message in the image and thus making it harder for illegal people to extract the original message, is vulnerable to lose of valuable hidden secrete information. Here, the proposed a data hiding and extraction procedure for AVI (Audio Video Interleave) videos embedding the secret message bits in DCT higher order coefficients. The secret information taken here is an grayscale image pixel values. The grayscale pixel values are converted to binary values and embedded those values in higher order coefficient value of DCT of AVI video frames. Data Hiding and Extraction procedure are experimented successfully. Various experiment results are show here. All experiments are done using Matlab 2018a simulation software.

Keywords: Steganography, Data hiding, Least Significant Bit Method (LSB), Compression, De-compression, Encryption, Decryption, Embedding, De-embedding.

1. Introduction

As the Internet and digital media are getting more and more popular requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Data Hiding, 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. The purpose of hiding such information depends on the application and it can be a secret message or a company logo that represents

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

significant information. Nevertheless, the Internet is an open environment, so information security has becoming increasingly important.

Today information security technology has two main branches, cryptography and information hiding. Cryptography process data into unintelligible form, reversibly, without data loss. It aims to prevent unauthorized receivers from decoding the programs by scrambling them. Information hiding is divided into Steganography and digital watermarking. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. Steganography and Cryptology 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. Nowadays the term "Information Hiding" relates to both watermarking and steganography. Watermarking is the technique used to hide information in a digital object (video, audio or image) so that information is robust to adjustments or alterations. By watermarking, the mark itself is invisible or unnoticeable for the human vision system. In addition, it should be impossible to remove a watermark without degrading the quality of the data of the digital object. On the other hand, the main goal of steganography is to hide secret information in the other cover media (video, audio or image) so that other persons will not notice the presence of the information. Although steganography is separate and different from cryptography, but they are related in the way that they both are used to protect valuable information. In steganography carrier medium is defined as the object that carries the hidden information. Stego-object is the resultant production of steganography that is transmitted to the destination. Stego-key is defined as the key used to extract the hidden data from the stego-object. Data may be embedded in various possible carriers like audio file, document, file headers, digital image and video.

The paper is organized as follows, in introductionwe have an overview of the terms compressionand decompression of video. The existing methodexplains the problem definition along with theevaluation criteria that is used in the paper. Theproposed method describes the technique which weused in this paper. It is followed by the results andanalyses in. Finally, the paper is concluded withadvantages of the existing methods.Design of a steganographic system can be categorized into spatial domain methods and transform domain methods. In spatial domain, the processing is applied on the image pixel values . In the transform domain method, the first step is to transform the cover image into frequency domain. Then the transformed coefficients are processed for hiding the secret information. However, methods of this type are computationally complex. Steganography methods using DCT , DWT, DFT come under this category.

Three different aspects in information-hiding systemscontend with each other: capacity, security, and robustness.Capacity refers to the amount of information thatcan

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

be hidden in the cover medium, security to an eavesdropper'sinability to detect hidden information, and robustnessto the amount of modification the stegomedium can withstand before an adversary can destroyhidden information.

A classical steganography system's security relies onthe encoding system's secrecy. An example of this type ofsystem is a Roman general who shaved a slave's head andtattooed a message on it. After the hair grew back, theslave was sent to deliver the now hidden message. Althoughsuch a system might work for a time, once it isknown, it is simple enough to shave the heads of all thepeople passing by to check for hidden messages ultimately,such a steganographic system fails.Modern steganography attempts to be detectableonly if secret information is known namely, a secret key. This is similar to Kerckhoffs'Principle in cryptography, whichholds that a cryptographic system'ssecurity should rely solely on the key material. For steganography to remainundetected, the unmodifiedcover medium must be kept secret,because if it is exposed, a comparisonbetween the cover and stego mediaimmediately reveals the changes.

2. Literature Survey

A.A.Zaidan, B.B.Zaidan, Fazidah Othman, presented on strength of the combination between hiding and encryption science is due to the non-existence of standard algorithms to be used in hiding and encrypting secret messages. Also there are many ways in hiding methods such as combining several media (covers) with different methods to pass a secret message. Furthermore, there is no formal method to be followed to discover a hidden data. For this reason, the task of this paper becomes difficult. In this paper proposed a new system of information hiding is presented. The proposed system aim to hide information (data file) in unused area 1 of any execution file (exe.file), to make sure changes made to the exe.file will not be detected by anti-virus and the functionality of the exe.file is still functioning. The system includes two main functions, first is the hiding of the information in the unused area 1 of PE-file (exe.file), through the execution of four process (specify the cover file, specify the information file, encryption of the information, and hiding the information) and the second function is the extraction of the hiding information through three process (specify the steno file, extract the information, and decryption of the information). The testing result shows the result file does not make any conflict with anti-virus software and the exe.file still function as usual after the hiding process.

A.W.Naji, Shihab A.Hameed, B.B.Zaidanimplemented on the hurried development of multimedia and internet allows for wide distribution of digital media data. It becomes much easier to edit, modify and duplicate digital information. In additional, digital document is also easy to copy and distribute, therefore it may face many threats. It became necessary to find an appropriate protection due to the significance, accuracy and sensitivity of the information. Furthermore, there is no formal method to be followed to discover a hidden data. In this paper, a new information hiding framework is presented. The proposed framework aim is

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

implementation of framework computation between advance encryption standard (AES) and distortion technique (DT) which embeds information in image page within executable file (exe. file) to find a secure solution to cover file without change the size of cover file. The framework includes two main functions; first is the hiding of the information in the image page of exe.file, through the execution of four process (specify the cover file, specify the information file, encryption of the information, and hiding the information) and the second function is the extraction of the hiding information through three process (specify the stego file, extract the information, and decryption of the information).

G. Sahoo and R. K. Tiwari, discussed aboutthe growing possibilities of modern communication need the special means of security especially on computer network. Data security in the last few years has gained a wider audience. In this paper we have discussed a new steganographic technique based on the file hybridization. In contrast to other methods of steganography where data embedding in image work on the principle of only one image file, the proposed method works on more than one image. The effectiveness of the proposed method is described pictorially and also has been shown that a multi-level of security of data can be achieved.

S. Katzenbeisser, F. Petitcolas**,**designed about Steganography, a means by which two or more parties may communicate using "invisible" or "subliminal" communication, and watermarking, a means of hiding copyright data in images, are becoming necessary components of commercial multimedia applications that are subject to illegal use. This new book is the first comprehensive survey of steganography and watermarking and their application to modern communications and multimedia. Handbook of Information Hiding: Steganography and Watermarking helps you understand steganography, the history of this previously neglected element of cryptography.

3. Problem Statement

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguist. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly. Many different carrier file formats can be used to hide the images or any other files, but digital images are the most popular because of their frequency on the internet.

4. Methodology of the work

- Selection of video: Video should be in .AVI(audio video interleave) format.Here the system will load the header of .AVI file. The Audio/Video Interleaved (AVI) file format is used with application that capture, edit and playback audio/video sequences. .AVI files contain multiple streams of different types of data. Most AVI sequences use both audio and video streams. A simple variation

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

for an AVI sequence uses video data and does not require an audio stream.

Here we are selecting the video of size 8.94MB and length 10s.

- Extraction of frames from video and selection of one frame:Here video is converted into much number of frames and any one frame is selected.

- Applying DCT: 8*8 DCT (discretecosine transforms) is applied to any one channel(R-channel) of the frame. DCT expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering such as lossy compression of audio and images where small high frequency components can be discarded.Use of cosine rather than sine is critical for compression. Since it turns out that fewer cosine functions are needed to approximate a typical signal.
- Selection of secret image:Select any of the secret images. Here we are selecting image with resolution of 630*420 and size 27.1 kb.

  Here our secret message is an imageGray level image. Pixel values of first 8x8 of 128x128 sized images are taken. Each pixel intensity is then converted into equivalent binary values. As the size of the secret image is 128x128 we got 128x128x8=131072 bit the secret messagebits to be hidden, and converting the Gray scale image into bit or binary values.
- Bit operation:As our eyes are sensitive to higher frequency components they are removed by performing DCT. These higher frequency component values are replaced by binary values of secret image by performing bitwise OR(addition) operation.
- Perform IDCT: Inverse DCT is applied to frame which is embedded with the secret image. IDCT reconstructs a sequence from its discrete cosine transforms ie decoding of the image(R-channel) takes place and is added to the remaining input frames, thus formation of reconstructed video takes place. This reconstructed video will be of same size as the input video.

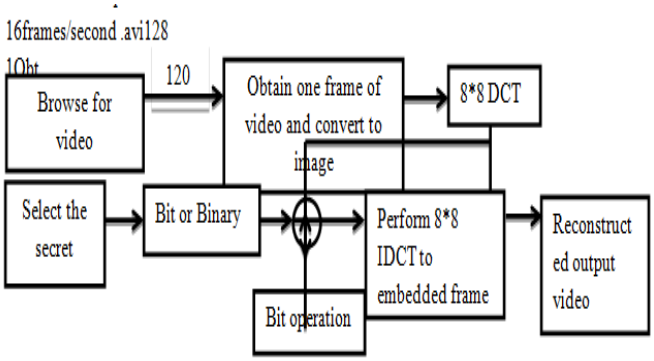

Figure 1: block diagram for encoding.

Decoding is done in reverse process of encoding. First each frame is extracted from just created AVI. Perform 8*8 DCT block processing on the channel where secret information was embedded earlier i.e, in R-channel and secret bit information are extracted by subtracting from original DCT block processed values.

Decryption 16frames/sec

avi16frames/s

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

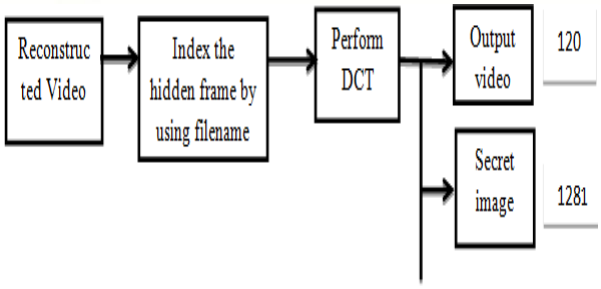

Figure 2: Block diagram for decoding.

Algorithm

Algorithm for embedding secret image in video.

Step 1: Select the input video.

Step 2: Check if video file not equal to zero. If 'no' repeat step1, if 'yes' goto step3.

Step3: Separate the frames from input video.

Step4: Select any one frame.

Step5: Apply DCT to any one channel of the selected frame.

Step6: Select the secret image and convert into binary values.

Step7: Embed the secret image into selected frame.

Step8: Obtain the reconstructed video.

Step9: Separation of secret image and output video.

5. Results and discussions

When the system is executed (Graphical User Interface) is displayed. First select the secret message (Here secret message is a text message) then encrypt it with a secret key; this key can be created by the sender. Select the encrypted message and cover file (video file) to embed the encrypted message into video file. In the de-embed process select the embedded video file, click on de-embed button then the deembed process completed. Select the de-embedded file decrypt it with the same key which was used in the encryption. Finally the original secret message can be displayed without any changes.

Figure (A) 3: GUI Window

Figure (B) 4: Select input video.

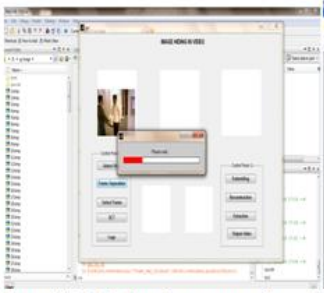

Figure (C) 5: Perform frame separation

Figure (D) 6: Frame separation completed

Figure (E) 7: Selection of frame

Figure (F) 8: Selection of input image

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

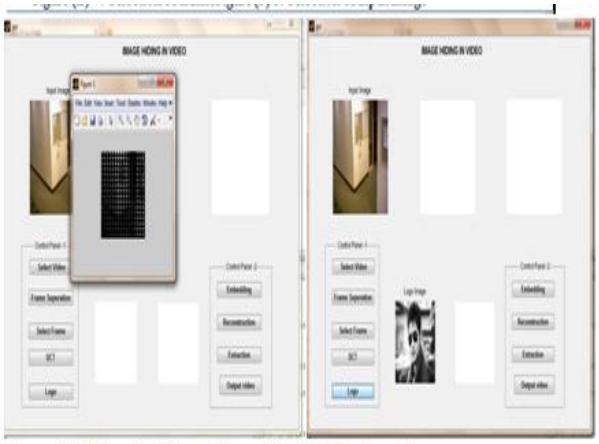

Figure (G) 9: Apply DCT Figure (H) 10: Select logo image

Figure (I) 11: Embedding process Figure (J) 12: Reconstructed video

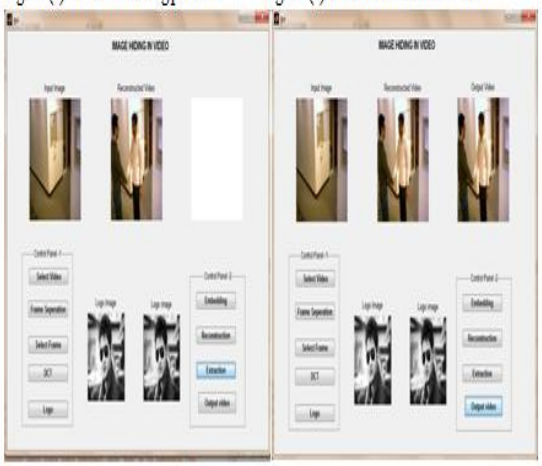

Figure (K) 13: Extraction of logo image Figure (L) 14: Output video obtained

Conclusion

The proposed system advanced an application which would be able to hide data into a video file that provides a robust and secure way of data transmission. This Stego system implements Steganography in video and reveals process without restarting the application or starting a different application. Also this system is a Platform-independent application with high portability and high Consistency. In the future secret message can be hiding inside the mobile images.

References

1) 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.
2) 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.
3) Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb, "A Secure Covert Communication Model Based On Video Steganography", Military Communications Conference .(MILCOM), pp. 1-6, 16-19 November IEEE 2008.
4) R.Kavitha, A. Murugan, "Lossless Steganography on AVI File using Swapping Algorithm", International conference on Computational Intelligence and Multimedia Applications, pp. 83-88, 2007 IEEE.
5) AshishT.Bhole Rachna Patel, "Design and Implementation of Steganography Over Video File", the Indian Journal of Technical Education, Special Issue for NCEVT' 12, pp. 69-72, April 2012.
6) F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, \Attacks on

copyright marking systems." In Aucsmith , pp. 218{238, ISBN 3-540-65386-4.