IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Video data hiding using Video Steganography

Ms.Prachi P. Sadawarte[1], Prof. P. A. Tijare[2]

M.E. Computer Engineering, SantGadge Baba University, Amravati, Maharashtra, India[1]

Computer Science & Technology, SantGadge Baba University, Amravati, Maharashtra, India[2]

Abstract: Internet is behaved as a backbone for the current modern technologies; it is globally connected, unsecure network. We can transfer the data through internet for data accurate and faster to the destination. Besides this, anyone can modify and misuse the valuable information through hacking at the time. Steganography is an art of hiding the secret data or information inside the digitally covered information. The hidden message can be text, image, speech or even video and the cover scan be chosen accordingly from either a text, an image, an audio or video. Steganography is a type of cryptography in which the secret message is hidden in a digital picture but here in this project video steganography is applied on video which is transfer from sender side to receiver side. Nowadays, the use of a video based steganography is common and numbers of steganalysis tools are available to check whether the video is stego-video or not. Most of the tools are checking for information hided by LSB, DCT, Frequency Domain Analysis etc. Here consider video as set of frames or images and any changes in the output image by hidden data is not visually recognizable.

Keywords: Steganography, LSB technique, Discrete Wavelet Transform, Discrete cosine Transform.

I. INTRODUCTION

Data security means to protect a database from destructive forces and the unwanted actions of unauthorized users. Huge amount of confidential information is being exchanged over the Internet (publicly open medium) as this is the most cost-effective and widely available way. Steganography is the art or practice of concealing a file, image, or message within another a file, image, or message[8]. The word steganography is of Greek origin and means "covered writing" or "concealed writing". Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it.[3] On the other side steganoalysis is the science of detecting hidden message. The objective of steganalysis is to break steganography system and that condition is met if an algorithm can judge whether a given image contains a secret message. To reduce the possibility of attack, security needs to be kept secret i.e. invisible security[7].

Steganography is a type of cryptography in which the secret message is hidden in a digital picture. Steganography differs from Cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, whereas steganography focuses on keeping the very existence of the message secret[9]. Various image based steganography method namely LSB (least-significant-bit), PVD (pixel-value differencing), etc. The main objective of steganography is to hide a secret message inside harmless cover media in such a way that the secret message is not visible to the observer. Thus the stego_image should not diverge much from original cover image[4]. In this generation, steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

1.1 Steganography

Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it. The following formula provides a very generic description of the pieces of the steganography process:

cover_medium + hidden data + stego_key = stego_medium

In this context, the cover_medium is the file in which is used to hide the hidden_data, which may be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_mediumIn text, hiding information is historically the most important method of steganography. This method was to hide a secret message in every nth letter of every word of a text message. In video steganography, a digital video consists of a set of frames (images) that are played back at certain frame rates based on the video standards[10]. Video steganography hides the message in any one of the frames/images, after hiding, it is very difficult to examine in which the data/message is hidden.

1.1.1 Least Significant Bit(LSB)

The most popular and common techniques is based on manipulating the least-significant-bit (LSB) and planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression. Least significant bit (LSB) insertion is a simple approach for embedding information in a cover image. The least significant bit (i.e. the 8th bit) of some or

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

all of the bytes inside an image is changed to a bit of the secret message. In this 24-bit image, a bit of each of red, green and blue colour components can be used, and they are each represented by a byte[5].

II. LITERATURE REVIEW

Johannes Trithemius was a German Abbot. His writing, "Steganographia: Hoe EstArsPerOccultamScripturam Animi Sui Voluntatem Absentibus AperiendiCerta" is ostensibly a work describing methods to communicate with spirits. A rough translation of the Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men." Although people have hidden secrets in plain sight—now called steganography—throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques[5]. Anti-Forensics with steganography data embedding in digital images: Digital images are used to communicate visual information.

Various forensic techniques have been developed to verify the authenticity of digital images. Set of digital image forensic techniques are proposed for detecting global and local contrast enhancement, identifying the use of histogram equalization, and detecting the global addition of noise to a JPEG compressed image[3].One of the most popular and easy to implement digital steganography technique is LSB embedding. In this method, the LSB position of each pixel in the cover image is substituted by one bit of secret data. We can improve the quality of the carried image obtained from LSB substitution method by applying optimal pixel adjustment. However, the simplicity of the LSB technique allows the embedded bits to be easily detected by applying the retrieval method of the scheme. To address such issue, an enhanced LSB method based on selecting specific bits from the host image and swapping them with secret data bits has been provided[11]. Further study has been introduced where the security level of the LSB method was increased by embedding secret data into different LSB positions based on a secret key.

An improved version of PVD, which combined the PVD technique with the well-known LSB substitution steganography, was proposed. The method embeds the secret data into the smooth areas of the host image using LSB replacement and into the edge areas using the PVD scheme[4].

Steganography in computer forensics: Computer forensic technique is used to find the parameter like height and width, frame number of data, PSNR, histogram of secrete message data before and after hiding to audio-video. If all these parameters are verified and found to be correct, then only it will send to receiver otherwise it stops the secrete message data in computer forensic block. Anti-Forensics with steganography data embedding in digital images: Digital images are used to communicate visual information. Various forensic techniques have been developed to verify the authenticity of digital images. Set of digital image forensic techniques are proposed for detecting global and local contrast enhancement, identifying the use of histogram equalization, and detecting the global addition of noise to a JPEG compressed image[3]. In this project we are embedding video inside another video using LSB technique.

The constraints of embedding in DCT domain are that many of the 64 coefficients are equal to zero and changing too many zeros to non-zero values will have an effect on the compression rate[5]. Nowadays, with the developing of network, the bandwidth has highly improved, so we can transmit video sequence as easy as a picture, it would not interest by attacker, so we can hide secret information on the cover media, it also satisfy the original intention of steganography that hide the truth that the secret information exist, so our algorithm will catch a highly security in network of protecting the information safety.

When embedding secrets in spatial domain, it is easy to detected by many steganalysis algorithms. G. L. Hua, Z. B. Li, B. Feng. [11] proposed a video steganography algorithm based on H.264/AVC, the algorithm can be implemented to achieve embedding and extracting, but the algorithm is weak in anti-attack. X. J. Ma.

The Research on Video Data Hiding Algorithms Based on H.264/AVC [7].Wuhan: HuazhongUnivercity of Science and Technology, 2010 has proposed a novel algorithm based on H.264, it improves the visual quality, but the embedding efficiency and embedding capacity needs to be improved. W. W. Zhang has proposed robust video watermarking algorithm for H.264/AVC based on texture feature, it has little impact on the video quality and bit rate, but it has little capacity to embed. C. H. Liu, O. T. Chen. Data Hiding in Intra Prediction Modes of H.264/AVC [9]. IEEE Press. 2008, 3025-3028 has proposed a method based on macro-block segmentation, the bit rate increase is very low, but it is weak in the anti-steganalysis detection.

3. PROPOSED WORK

This work is based on video steganography for hiding video file or data within a another video file.Generally, in data hiding, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia files like images, video or audio.

Message Hiding:
We give original content as input with watermak data embedding.
We view flipping an edge pixel in binary images as shifting the edge location one pixel horizontally and vertically. We can hide the message into the image. Data/text/message can be hide in pixels of image.[5]

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

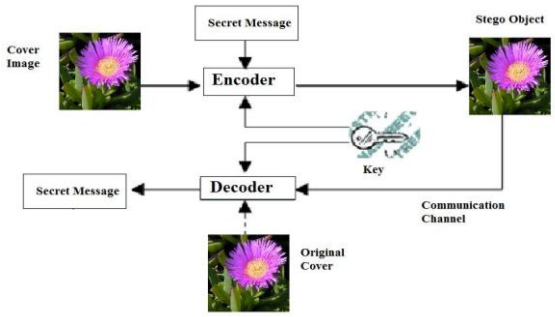

Fig 3.1 Steganography Process

Image/video/audio Hiding:
In video hiding; user wants to hide the video or data file in the video or image.

Then user have to select a particular image and video to hide the image. In this application we can also provide a dual security by using authentication verification.

The general process of Steganography is that a data message is embedded within a cover signal. The output of the embedder is called a stego signal.

After transmission, recording and other signal processing which may contaminate and distort the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor.

The carrier of steganography can be an image, text, audio or a video file. Most of the steganography systems are developed in order to embed a text file, image or an audio file in a carrier file.

Only a few algorithms are developed to embed a video file in a video file. This research is mainly carried out in order to embed a video in a video.

The existing methods have several issues. The GOP method (group of picture), increases the size of the embedded video unusually.

Thus, it is easy to detect the existence of a hidden message. The constraints of embedding in DCT domain are that many of the 64 coefficients are equal to zero and changing too many zero to non-zero values will have an effect on the compression rate[5].

Nowadays, with the developing of network, the bandwidth has highly improved, so we can transmit video sequence as easy as a picture, it would not interest by attacker, so we can hide secret information on the cover media, it also satisfy the original intention of steganography that hide the truth that the secret information exist, so our algorithm will catch a highly security in network of protecting the information safety.

When embedding secrets in spatial domain, it is easy to detected by many steg analysis algorithms.

3.1 Data Flow Diagram

A **data flow diagram** (**DFD**) is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing (structured design).

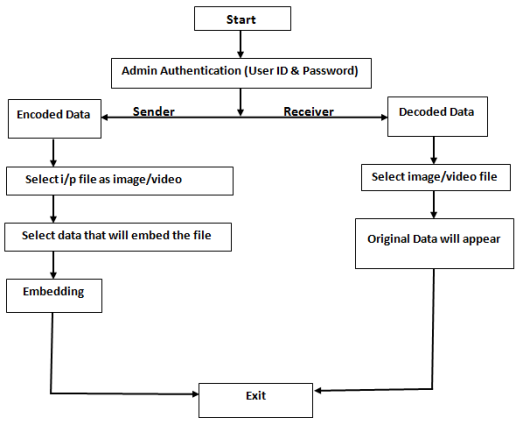

Fig 3.2: Data Flow Diagram

- Admin authentication provide security to access application by using User ID and Password. Then the application processing start.

3.2 UML Diagram of Application

From given diagram user get over view about application that they will compatible with it to access.

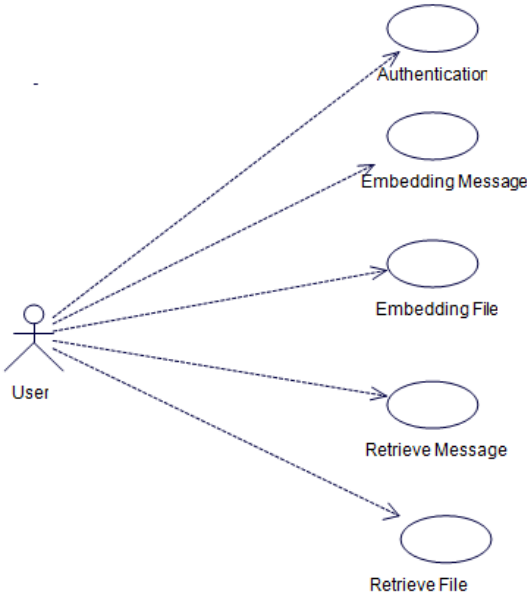

Fig 3.3: UML diagram of Application

IV. IMPLICATION

- To study the existing techniques for Video hide.
- To analyze different techniques proposed in literature for data security during message transmission.
- To apply the LSB techniques for hide the video over video.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

- To implement the hiding techniques for hidden information.

V. APPLICATION

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems
- Steganography provides us with :

1. Potential capability to hide the existence of confidential Data.
2. Hardness of detecting the hidden(i.e, embedded) data
3. Strengthening of the secrecy of the encrypted data

- Modern Printers

Steganography is used by leading manufacture in digital & laser printers, including HP and Xerox. Here, tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

VI. CONCLUSION

Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication. It is not necessary for the two parties to agree to a specific hiding format. If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information. In order to avoid this, the some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is delivered.