iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: V Month of publication: May 2017

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Video Steganography Used for Hiding Video Data

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

[1] M.E(Computer Engineering), Sant Gadge Baba University, Amravati, Maharashtra.

[2] Computer Science & Technology, Sant Gadge Baba University, Amravati, Maharashtra.

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

Johannes Trithemius (1462-1516) was a German Abbot. His writing, “Steganography: hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa” is ostensibly a work describing methods to communicate with spirits[2]. 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.

The standard and concept of “What You See Is What You Get (WYSIWYG)” which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a Steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS) hence, they can convey more than merely 1000 words[8].For decades people strove to develop innovative methods for secret communication The remainder of this introduction highlights briefly some historical facts and attacks on methods (also known as Steganalysis).

Steganography or Stego as it is often referred to in the IT community literally means, "covered writing" which is derived from the Greek language. Steganography is defined by "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography,[11] where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present"[1].

A. History of Steganography

Through out history Steganography has been used to secretly communicate information between people.

Some examples of use of Steganography is past times are:

1) During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.

2) In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message,the recipient would shave off the messengers hair to see the secrete message.

3) Another method used in Greece was where someone would peel wax off a tablet.

II. LITERATURE REVIEW

Johannes Trithemius was a German Abbot. His writing, “Steganographia: Hoe Est Ars PerOccultamScripturam Animi Sui VoluntatemAbsentibusAperiendiCerta” 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.

III. RELATED WORK

Steganography is important topics in information hiding. Steganography refers to the technology of hiding data into digital media without drawing any suspicion. This paper provides a survey on Steganography for digital images and video, mainly covering the fundamental concepts, the progress of stenographic methods for images in spatial representation and in JPEG format, and the development of the corresponding Steganalytic schemes. Some commonly used strategies for improving stenographic security and enhancing Steganalytic capability are summarized and possible research trends are discussed.

Three common requirements, security, capacity, and imperceptibility, may be used to rate the performance of Steganography techniques.

A. Security

Steganography may sure from many active or passive attacks, correspondingly in the prisoner's problem when Wendy acts as an active or passive warden.

B. Capacity

To be useful in conveying secret message, the hiding capacity provided by Steganography should be as high as possible, which may be given in absolute measurement (such as the size of secret message), or in relative value.

C. Imperceptibility

Stegno images should not have severe visual artifacts under the same level of security and capacity, the higher the deity of the Stegno image, the better.

D. Steganography Techniques

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that alteration made to the image is perceptually indiscernible.

E. 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 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].

IV. ANALYSIS OF PROBLEM

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 linguistry. 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

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet.

V. IMPLEMENTATION

A. *Data Embedding Technique*

We are explain in very simple way how actual data encrypt and hide behind the image Select image file as a master file which user want hide data behind this then the message will convert into character array of byte. Convert 32 bit size of input file into byte array. Create byte array same as length of input file and read all bytes in byte array then it writes byte in given output file from their offset value i.e embed message. Above it is method of embedding and when user type message or select data file after press Go button above procedure implements. User's data will embedded successfully.

Now this byte data compress by using the java.util.zip.*. You can compress data as your wish by using slider compression scale when you are using it that time slider compresion are used it's work on compression ratio.

Formula is used for compression ratio:

CompressionRatio=(short)((double)fileArray.length/(double)message.length()×100.0)

B. *Retrieving Technique*

Retrieves an embedded message from a Master file. Click on retrieve message. Select master file image, video, which you had been use for hiding secret message click on go button. import javax.crypto.* and import javax.crypto.spec.* are used for encryption and decryption. In order to create a Cipher object, the application calls the Cipher's getInstance method, and passes the name of the requested *transformation* to it.

C. *Video in another Video Technique : Encoding Process*

In video steganography, we can hide the video in another video. Encoding method for video in another video is shown in Fig. 7. In this, first we will read cover file and segment that secret video streams into frames. After finding frames, find the size of cover video. Simultaneously segment video streams into frames then split the secret message bit stream into R × C group size then each group of messages are rearranged to specific pattern for hiding. Encrypt small message into a byte of data bit on LSB and check whether all small messages are completed or not. If completed then check in all frames hidden messages are included or not. If hidden messages are included then create the rule list for receiver and generate stego video.

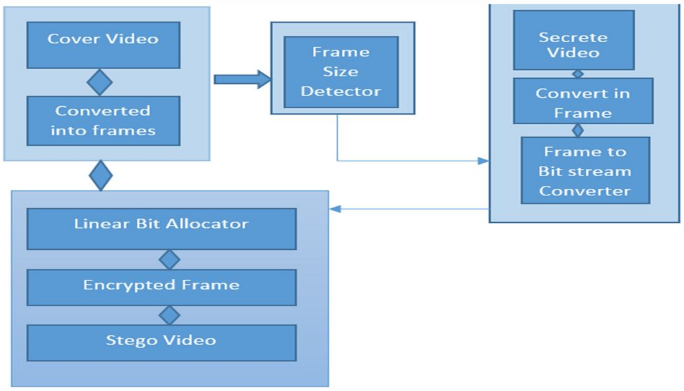


Fig Proposed Framework for Video in another Video (Encoding)

1) *Decoding process*: First read the stego video then segment video strems into frames. As we know that video is made up with combining all frames of images. Read rule list from first frame and seprate out frames which contain the hidden information. Decrypt small message from the frame for each column, row and extract LSB.

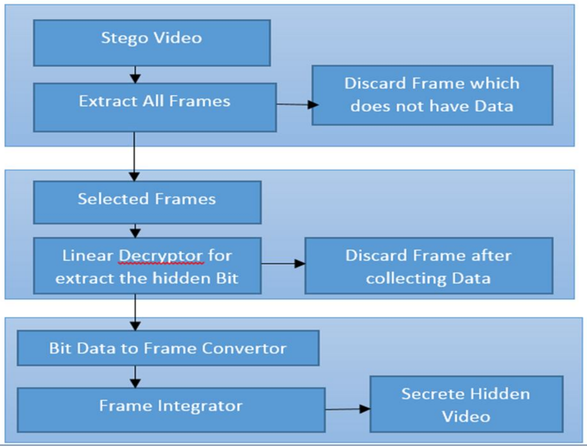

Stego Video
Extract All Frames
Discard Frame which does not have Data
Selected Frames
Linear Decryptor for extract the hidden Bit
Discard Frame after collecting Data
Bit Data to Frame Convertor
Frame Integrator
Secrete Hidden Video

Fig Proposed Framework for Video in another Video (Decoding)

D. LSB Algorithm

LSB:

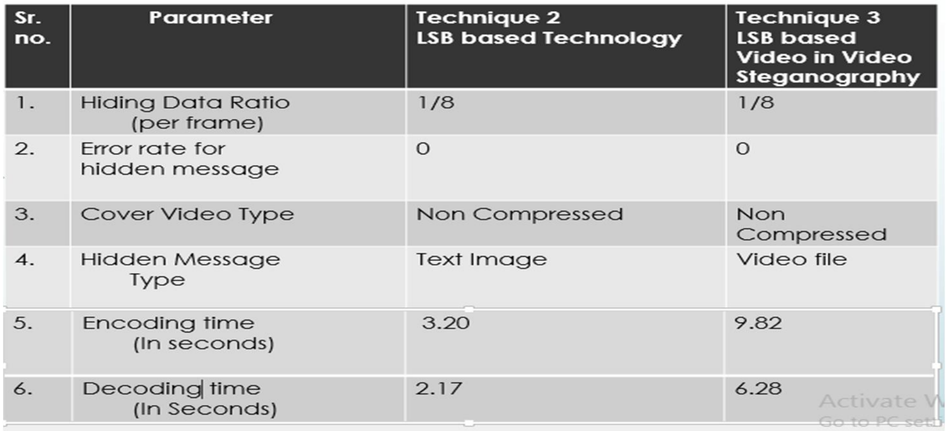
1) Algorithm to embed video message:

Step 1: Read the cover video and video message which is to be hidden in the cover video.
Step 2: Convert video message in binary.
Step 3: Calculate LSB of each pixels of cover video.
Step 4: Replace LSB of cover video with each bit of secret video message one by one.
Step 5: Write stego video.

2) Algorithm to retrieve secret video message:

Step 1: Read the stego video.
Step 2: Calculate LSB of each pixels of stego video.
Step 3: Retrieve bits and convert each 8 bit into character.

VI. RESULTS



Sr. no.	Parameter	Technique 2 LSB based Technology	Technique 3 LSB based Video in Video Steganography
1.	Hiding Data Ratio (per frame)	1/8	1/8
2.	Error rate for hidden message	0	0
3.	Cover Video Type	Non Compressed	Non Compressed
4.	Hidden Message Type	Text Image	Video file
5.	Encoding time (In seconds)	3.20	9.82
6.	Decoding time (In Seconds)	2.17	6.28

VII. APPLICATION

A. Confidential communication and secret data storing
B. Protection of data alteration
C. Access control system for digital content distribution
D. Media Database systems
E. 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

F. 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.

VIII. CONCLUSION

We would like to used discuss the appropriateness of Steganography as a tool to conceal highly sensitive information. Secret data should be undetectable without secret knowledge. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should become more common and a more standard definition of robustness is required to help overcome this. This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties.

The project "Steganography" after being tested and was found to be achieving what is meant for. But this system never provides a full proof solution for all their problems in the user point of view. The system is found to be 100% error free and ready for implementation. The system has been found to work efficiently and effectively. Due to its higher user friendliness, others may use these documents as a prototype for developing similar application.This application is used only in a security firms and national, multinational companies etc., Use a reputable steganography tool that you know does not leave a well signature behind in the object.

IX. FUTURE SCOPE

A. Future Scope

1) *Corporate Espionage:* The Corporate Espionage is the trade in which all support to the business is depending or the information. Information is like the trade sequence which valuable or extremely important assets of corporate. This corporate espionage released that information which should be extremely damaging to the company profit.
2) *Watermarking:* It is the form of Steganography. Digital watermarking process the copyright we hide the data behind the Image/Video without knowing the end user. It is used to identify the image pattern that appears as various shaded of lightness/darkness when view by transmitted light caused by thickness or density variations paper.
3) *Pervasive Computing:* The goal Pervasive computing which a current network technology with wireless computing. Pervasive Computing is the result of computer technology advantage at exponential speed a trend towards all manmade and some natural product having Hardware and Software.

REFERENCES

[1] Steganography over Video File by Hiding Video in another Video File, Random Byte Hiding and LSB Technique Rachna Patel, Asst. Prof., Computer Engineering Department, CGPIT, Uka Tarsadia University (UTU), Maliba Campus, Bardoli, Gujarat, India. Mukesh Patel, Asst. Prof., B.V. Patel Inst. of Business Management, Computer & Information Technology, BVPBMC&IT, Uka Tarsadia University (UTU), Maliba Campus, Bardoli, Gujarat. 2014 IEEE International Conference on Computational Intelligence and Computing Research.

[2] Steganography over Video File using Random Byte Hiding and LSB Technique Ashish T. Bhole, Rachna Patel, Department of Computer Engineering, SSBT‟s COE & T, Bambhori, Jalgaon, India 2012 IEEE International Conference on Computational Intelligence and Computing Research.

[3] Audio-Video steganography Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, Rajiv Gandhi College of Engineering & Research RTMNU Nagpur University Nagpur, India IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS‟15

[4] Arvind kumar, km. Pooja (2010) "Steganography – A Data Hiding Technique" IJCAvolume 9, issue 7.

[5] Video Steganography by LSB Technique using Neural Network Richa Khare, Rachana Mishra, Indrabhan Arya CSE Dept, Oriental College of Tech Bhopal, India 2014 Sixth International Conference on Computational Intelligence and Communication Networks.

[6] Video Steganography A. Munasinghe, Anuja Dharmaratne, Kasun De Zoysa University of Colombo School of Computing Colombo, Sri Lanka. 2013 International Conference on Advances in ICT for Emerging Regions (ICTer)

[7] Video Steganography Algorithm Based on Trailing Coefficients Yingnan Zhang, Minqing Zhang ,Ke Niu, Jia Liu Key Laboratory of Network&Information Security of PAPF, Engineering University of the PAPF Xi‟an, China. 2015 International Conference on Intelligent Networking and Collaborative System.

[8] A Novel Video Steganography based on Non-uniform Rectangular Partition ShengDun Hu, KinTak U Faculty of Information Technology Macau University of Science and Technology Macau, China. IEEE International Conference on Computational Science and Engineering-2011

[9] Hamdy M. Kelash , Osama F. Abdel Wahab ,Osama A. Elshakankiry ,Hala S. El-sayed (2013) "Hiding Data in Video Sequences Using Steganography Algorithms" IEEE.

[10] Sunil. K. Moon , Rajeshree. D. Raut (2013) "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security" IEEE

[11] Rini T Paul (2011) "Review of Robust Video Watermarking Techniques" IJCA.