**PROJECT REPORT**

**on**

**Designing, Testing and Implementation of Audio Steganography on a Network**

**Submitted by**

500061524 R-134217045 Ayush Sharma

500060114 R-134217083 Mehul Aggarwal

**Under the guidance of**

Dr. Adarsh Kumar

#### Associate Professor

Department of Systemics



**SCHOOL OF COMPUTER SCIENCE**

UNIVERSITY OF PETROLEUM & ENERGY STUDIES

Bidholi Campus, Energy Acres, Dehradun – 248007.

**January- 2020**

C:\Users\aktomar\Desktop\logo.png

**CANDIDATE’S DECLARATION**

We here by certify that the project work entitled **“Designing, Testing and Implementation of Audio Steganography on a Network”** in partial fulfillment of the requirements for the award of the Degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING with specialization in Cyber Security And Forensics submitted to the School of Computer Science, Department of Systemic, University of Petroleum & Energy Studies, Dehradun, is an authentic record of our work carried out during a period from **January 2020** to, **May 2020** under the supervision of **Dr. Adarsh Kumar,** Associate Professor.

The matter presented in this project has not been submitted by us for the award of any other degree of this or any other University.

**(Ayush Sharma, Mehul Aggrawal )**

**(R134217045, R134217083)**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_2020

**Dr. Adarsh Kumar**

School of Computer Science

University of Petroleum & Energy Studies

Dehradun - 248001 (Uttrakhand)

**Acknowledgement**

We wish to express our deep gratitude to our guide Dr. Adarsh Kumar, for all advice, encouragement and constant support he has given us throughout our project work. This work would not have been possible without his support and valuable suggestions.

We are also grateful to **Dr. Manish prateek, Director** SoCS, UPES for giving us the necessary facilities to carry out our project work successfully.

We would like to thank all our **friends** for their help and constructive criticism during our project work. Finally we have no words to express our sincere gratitude to our **parents** who have shown us this world and for every support they have given us.

|  |  |  |
| --- | --- | --- |
| **Name** | **Ayush Sharma** | **Mehul Aggrawal** |
| **Roll No.** | **R134217045** | **R134217083** |

**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 audio steganography is applied on audio which is transfer from sender side to receiver side. Nowadays, the use of a audio based steganography is common and numbers of steganalysis tools are available to check whether the audio is stego-video or not. Most of the tools are checking for information hided by LSB, DCT, etc.

**Keywords:** Steganography, LSB technique , LSB Transformation, Discrete cosine Transform.

**Table of Content**

**Sr. No. Topic Page No.**

1. Introduction 1

2. Problem Statement 2

3. Literature Review 2

4. Objectives 3

5. Methodology 4

5.1 LSB Algorithm 7

5.2 AES Encryption of Audio 8

6. Outputs 8

7. Applications 9

8. System Requirements 10

9. Schedule 11

10. Summary 12

11. References 12

**INTRODUCTION**

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 audio form is the most popular because of their frequency on the Internet. For hiding secret information in audio files, there exists a large variety of stenographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project intends to give an overview of audio steganography, its uses, and techniques. The project encodes secret message in audio files and then sends it to the receiver. The receiver then decrypts the message to get the original one.

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. 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.

Steganography derives from the Greek word steganos, meaning covered or secret, and graph (writing or drawing). On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio or image file.

Where cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography’s role is gaining prominence.

What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.)

Steganography hides the secreted message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis.

When information is hidden inside video in program or person hiding the information will usually use the discrete cosine transform (DCT) method. DCT works by slightly changing the each of the images in the video, only so much though so it is not noticeable by the human eye. To be more precise about how DCT works, DCT alters values of certain parts of the images, it is usually rounds them up. DCT makes use of Least Significant Bit (LSB) steganography technique. For example if part of an image has a value of 6.667 it will round up to 7.

Steganography in videos is similar to that of steganography in images, apart from information is hidden in each frame of video. White space and tabs occur naturally in documents, so there is not really any possible way using method of steganography would cause someone to be suspicious.

**Where does this secret data hide?**

It is possible to alter graphic or sound files slightly without losing their overall viability for the viewer and listener. With **audio**, you can use bits of the file that contain sound not audible to the human ear. With graphic **images**, you can remove redundant bits of color from the image and still produce a picture that looks intact to the human eye and is difficult to discern from its original.

**It is in those bits that stego hides its data. A stego program uses an algorithm, to embed data in an image or sound file, and a password scheme to allow you to retrieve information.**

**PROBLEM STATEMENT**

To protect important information we use cryptography. Steganography is different from cryptography, where the existence of the message itself is not disguised, but the content is obscured. Steganogrpahy could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy. For e.g.: Sending of encrypted credit card details over the internet is well known to a malicious user. But, the actual content is randomized or confused and hence not revealed. But, in Steganography the fact that the credit card details is being sent is kept secretly (as the message or the image appears innocent). The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal.

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 audio files are the most popular because of their frequency on the internet. For hiding secret information in audio, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points.

**LITERATURE REVIEW**

The constraints of embedding in LSB domain are equal to zero and changing too many zeros to non-zero values will have an effect on the compression rate. 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. proposed a video steganography algorithm based on LSB, 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 DCT with DCT .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 DCT based on texture feature, it has little impact on the video quality and bit rate, but it has little capacity to embed.

**OBJECTIVES**

The main objective of this project is to design, implement and test audio steganography techniques in a network. The system will use LSB techniques for embedding secret data in audio. Then this audio with secret data will be transferres over a network. The goal of stenography is to hide the data from a third party through the process of transmission and also at the receiving end, allowing both the parties to keep a check on security.

The goal of steganography is to covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings.

The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. This approach of information hiding technique has recently became important in a number of application area.

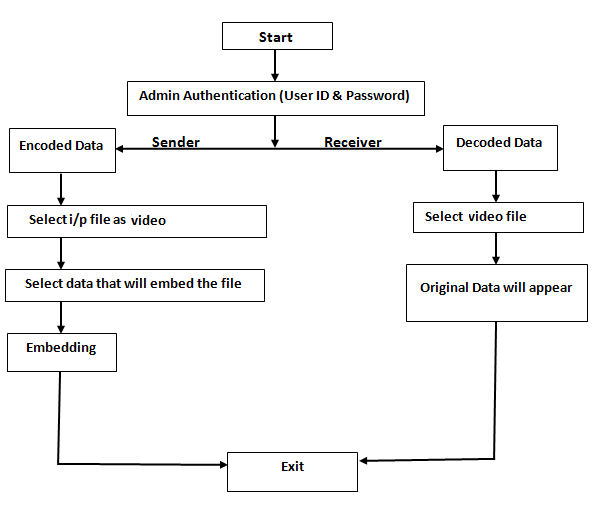
This project has following objectives:

* To product security tool based on steganography techniques.
* To explore techniques of hiding data using encryption module of this project
* To extract techniques of getting secret data using decryption module.

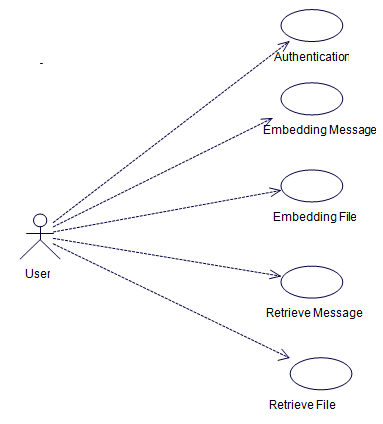
Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

**METHODOLOGY**

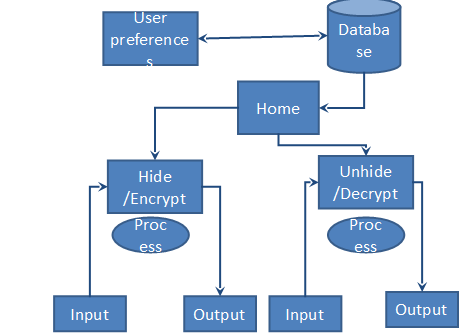
Then user have to select a particular image and video to hide the image. In this application we can also provide a dual security by using authentication verification. The general process of Steganography is that a data message is embedded within a cover signal. The output of the embedder is called a 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. 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.



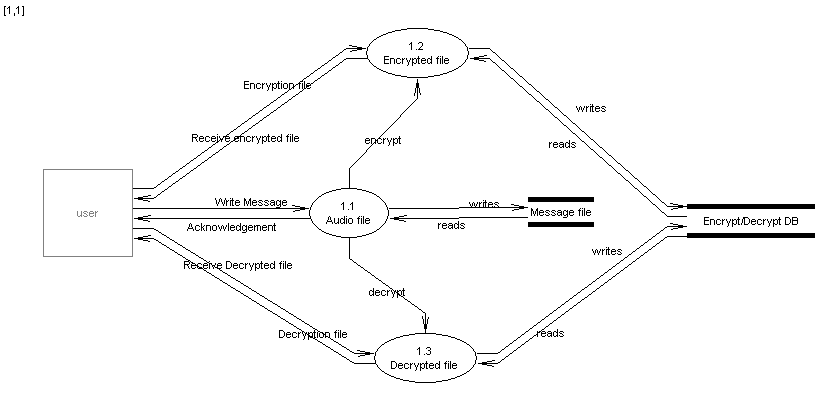
Fig[1]. Flow chart for proposed system.

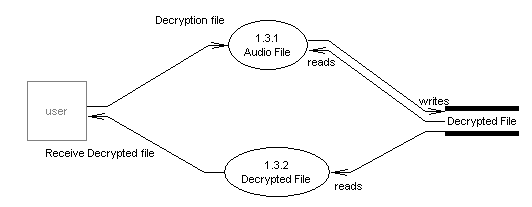


Fig[2]. ER diagram for proposed system.



Fig[3]. Data Flow Diagram

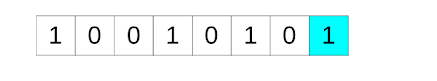




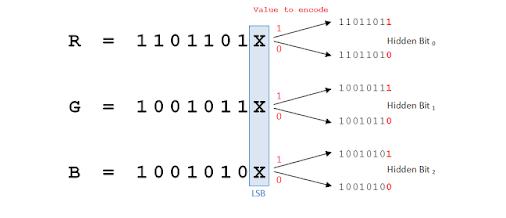
Fig[4,5] Behavioral Diagram

**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.



Fig[6]. Here the highlighted ‘1’ is the least significant bit. We can alter this value to hidden message.

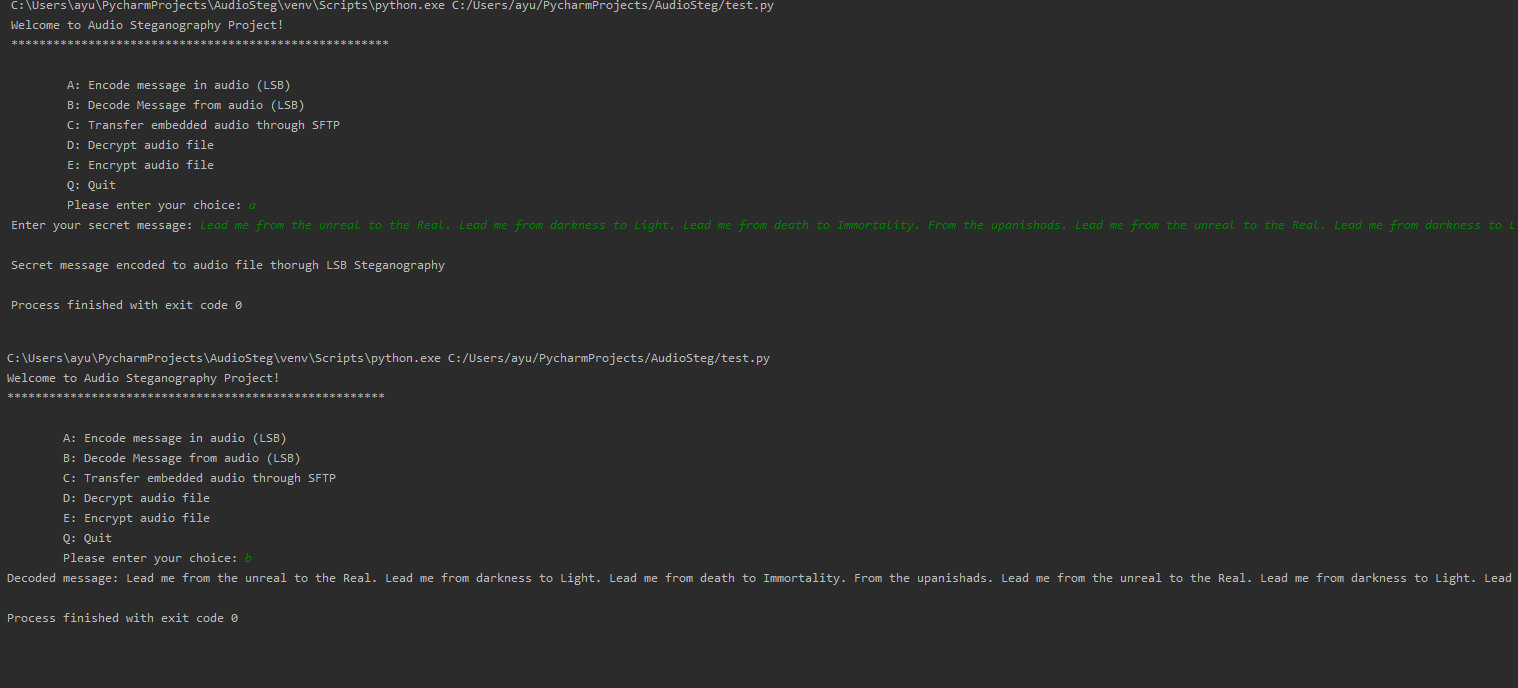


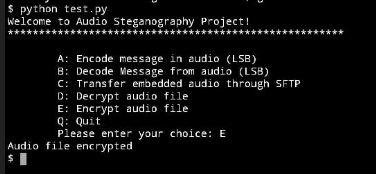
Fig[7]. Demonstration of LSB steganography.

**AES Encryption of audio**

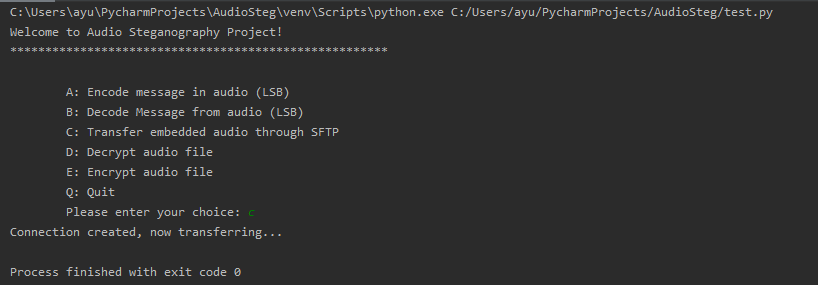
* Generate key and IV using random functions.
* open the file and read it. This will return bytes as the algorithm requires the data to be in the form of bytes.
* Encrypt it using the encrypt function of the pycrypto library.
* Write the encrypted bytes into a file.
* Take the encrypted bytes data and pass it to the decrypt function
* The resulting decrypted bytes data can be written to another file as a decrypted audio file.

**OUTPUTS**

Fig[8]. Encoding & Decoding of secret message through Audio Steganography



Fig[9]. Encryption of Audio file using AES



Fig[10]. Transmitting audio file through SFTP

**APPLICATIONS**

Steganography is applicable to, but not limited to, the following areas:

**1) Confidential communication and secret data storing**

The "secrecy" of the embedded data is essential in this area. Historically, steganography have been addressed in this area. Steganography provides us with:

(A) Potential capability to hide the existence of confidential data

(B) Hardness of detecting the hidden (i.e., embedded) data

(C) Enhancing the secrecy of the encrypted data

**2) Protection of data alteration**

We take advantage of the fragility of the embedded data in this application area.However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

**3) Access control system for digital content distribution**

In this area embedded data is "hidden", but is "explained" to publicize the content. Today, digital contents are getting more and more commonly distributed over Internet than before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who can make access to the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital contents to e-mail messages and send them to the customers.

**4) Media Database systems**

Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.

(1) The title of the picture and some physical object information

(2) The date and the time when the picture was taken

(3) The camera and the photographer's information

**SYSTEM REQUIREMENTS**

A set of programs associated with the operation of a computer is called software. Software is the part of the computer system which enables the user to interact with several physical hardware devices.

The minimum software requirement specifications for developing this project are as follows:

**Operating System : Windows 10**

**Language : Python**

**Office Suite : Microsoft Office**

**Additional Hardware : SSH enabled server**

The Collection of internal electronic circuits and external physical devices used in building a computer is called Hardware.

The minimum hardware requirement specification for developing this project is as follows:

**Processor : Intel Core 2 Duo**

**RAM : 2 GiB RAM**

**Hard Disk : 100 MB**

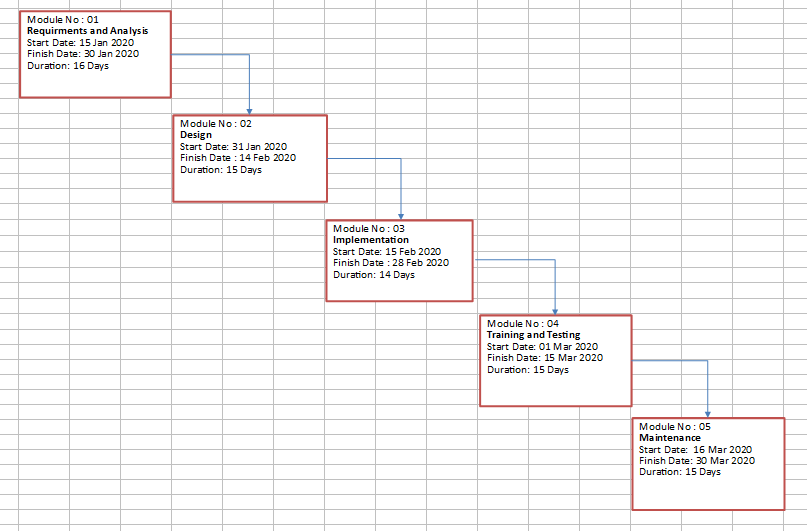
**SCHEDULE**

1. To study the existing techniques for audio hide.

2. To analyze different techniques proposed in literature for data security during message transmission.

3. To apply the LSB techniques for hide message over audio.

4. To implement the hiding techniques for hidden information.

 Fig[11]. PERT chart for the project

**SUMMARY**

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

**REFERENCES**

[1] Video data hiding using Video Steganography Ms.Prachi by P. Sadawarte1, Prof. P. A. Tijare International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 2, February 2017

[2] Data Hiding in Intra Prediction Modes of H.264/AVC using LSB. IEEE Press. 2008, 3025-3028

[3] A Review Paper on Video Steganography by [Arjun Nichal](https://www.researchgate.net/profile/Arjun_Nichal2), International Advanced Research

Journal in Science, Engineering and Technology, Vol. 3, Issue 12, December 201

[4]<https://www.academia.edu/41554175/KEY_BASED_LEAST_SIGNIFICANT_BIT_LSB_INSERTION_FOR_AUDIO_AND_VIDEO_STEGANOGRAPHY>

**Synopsis Draft verified by**

**Project Guide HOD**

**(Name & Sign) (Dept. of Systemics)**