# STEGANOGRAPHY USING MATLAB

D.Bhavana[1], D.Ravi Tej[2], M.Puneeth[3], A.Harini[3], Y.Mani Shankar[3], T.Sai Madhuri[3]

Asst.Professor, KLUniversity1, Asst.Professor, SRK Institute Technology[2], Graduating Students of KLUniversity[3].

***Abstract-****Steganography is a process in which a secret message is covered with a file that may be an audio, image, video the main advantage in steganography is file will be as usual after the encryption. Steganography can be used as a weapon if u have any negative intention. Research and analysis is the only way to detect the steganographed message. In this paper we are going to explain how to hide a message in an audio file and image using matlab software*

***Keywords:*** *Cryptography, steganography, stegano-message, steganalysis encoding, decoding*

## I. INTRODUCTION

1.1Cryptography:

Cryptography is a process of transmitting data in a particular so that only the receiver can read and process it. The plain text is scrambled using key and converted into a cipher text. Key contains mathematical logics to scramble the plain text, key is used at encryption of plain text and decryption of cipher text .The arts and science of developing the cryptosystem is called as cryptography, various techniques and algorithms are used to transfer cipher text to plain text and plain text.

1.2Cryptographer:

The person who deals with the cryptography is known as cryptographer. Cryptographers are the persons who deal with all the mathematical logics on plane text to convert it as cipher text .These people are experts in cryptography.

1.3Crypt analysis:

Crypt analysis is nothing but studying the cipher text to obtain the plane text without knowing the key. This is process of decoding the message by an intruder to obtain the plane text without key.

1.4Cryptanalyst:

The person who decrypts the plain text without knowing the key is called as cryptanalyst or the person who deals with the crypt analysis is called as cryptanalyst.

1.5Cryptology:

The combination of cryptography and cryptanalysis is called as cryptology.

## II.CRYPTOGRRAPHY TERMS

The following are the cryptography terms

2.1Plaintext:
plain text is a text that which is an original message that can be readable by any one.This is not a coded message

2.2 Cipher text:

This cipher text is a coded message that which is encrypted by using the mathematical algorithms

2.3 Key:

It is used to control the behavior and operation of cryptographic algorithm.‘

2.4 Key space:

All possible key values in a cypto algorithm is called as key space

2.5 Crypto system services:

The following are the crypto system services

Confidentiality, integrity, Authenticity, Non-repudiation, Access control

## *III.CRYPTOGRAPHY ISSUES*

3.1Confidentiality:

The message should understand by the sender and receiver only. sender should encrypt the message and receiver should decrypt the message

3.2 End-point Authentication:

Identity should be confirmed by sender and receiver

3.3 MESSAGE INTEGRITY:

The sender and receiver should check that message is not changed without any detection

3.4 Encryption systems:

3.5 Substitution cipher: substitution cipher converts one letter to another

3.6 Transposition cipher:

It changes position of the letter in text or it jumbles the text

## IV.CRYPTOGRAPHIC METHODS

The following are the different types of cryptographic methods

4.1 Symmetric:

Same key is used by the sender and receiver for encrypting and decrypting the data

4.2 Asymmetric:

It has key pairs related mathematically for encryption and decryption these key pairs are called as public key and private key

4.3 Symmetric algorithms:

4.3.1 DES MODES: CFB , OFB, CM ,ECB, CBC

3DES, IDEA, Blowfish, CAST, SAFER, TWO FISH, RC4 ,RC5, CAST, AES

4.4 Asymmetric algorithms:

The following are the asymmetric algorithms

Diffie-Hellman, RSA, EL Gamal, Eleptic curve cryptography(ECC)

4.4.1 Hashing Algorithms:

4.4.1.1 MD5:

128 bits of hash value is computed, file integrity checking is done by using MD5 algorithm.

4.4.1.2 SHA-1:

160 bits of hash values are computed, message digest algorithm is approved by NIST

4.4.1.3 HAVAL:

Computation takes place from 128 to 256 bit hash, it is between 3 and 5 rounds

4.4.1.4 RIPEMD-1601:

It is developed by Europe ,published in 1996

## V. STEGANOGRAPHY

Steganography is originated from the Greek word ,the word stegno means “covered” and the word graphine means “writing”. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated[1].Stegnography is a process in which a secret information is covered with images and the the message is decoded, when it reaches to the receiver .If anyone tries to view the message he will not see the covered data
Steganography is used in the corporate world to face corporate intelligence attempts .The terrorist organizations are using this steganography mainly to communicate secret information

The rumor is that some of terrorist organizations uses steganography by uploading the images on some websites and the information is shared among them secretly. Steganography key schemes are dependent on kirckhoffs principle.

Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information.[2]

One of the most widely used applications is for socalled *digital watermarking*. The entertainment industry is particularly very nervous due to the ease at which exact copies of digital music and video can be made. A solution using steganography can be done by hiding notices or serial numbers or other copyright details inside the media which can later be made use of.[3]
Steganography is an old technique that has existed since antiquity. Herodotus, a Greek historian who lived in the 5th century B.C.,relates how the Greeks sent and received warnings of enemy movements using a message underneath the wax of a writing tablet.

ISSN: 2349-6495

Others can be found in the use of secret ink to hide information on a white paper or the use of micro-dot by intelligence agencies in
World War 2.[7]

Steganaography idea was first introduced by Johannes Trithemius in 1499 to share secret information for example hidden information was written on wood then information is covered with wax an unknown message was written on that wood ,invisible inks are also used in those days to implement steganography. This steganography idea has been started in ancient Greece the same hidden idea is taking place in our modern days also to hide the secret information. In ancient ages the information is dependent upon the physical bodies (physical steganography) the medium used here are wood, skin, wax etc .This steganography method went on developing during the world wars to share the information more secretly a new carrier was introduced with electromagnetic waves at present digital images audio and video files are the most popular carriers .In a social relations exchange of information is involved which requires the protection so cryptography and steganography techniques came into pictures In steganography the sender and receiver are invisible ,it provides not only security but also privacy .steganography is the most efficient technique forPrivacy and it is a tool for the modern so File formats that are used to cover messages are

Bmp,Jpeg,Gif.Wav,Mp3.

5.1 Audio Steganography: A steganography technique that uses audio as the cover media is called an audio steganography. It is the most challenging task in steganography. This is because the human auditory system (HAS) has a large dynamic range that it can listen over. Thus, even a minute change in audio quality also can be detected by the human ears.

5.2 Image Steganography*:* A steganography technique that uses images as the cover media is called an image steganography. Hiding secret messages in digital images is the most widely used method as it can take advantage of the limited power of the human visual system (HVS) and also because images have a large amount of redundant information that can be used to hide a secret message. [4]
To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy”
areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.[6]

5.3 Encryption:

The process of converting the original message to cipher text is called as encryption

5.4 Decryption:

The process of converting the cipher text to plain text (or) original messsage is called as decryption

5.5 Steganalysis:

Steganalysis is an art and science of detecting message hidden by steganography ,It is an analysation of recognizing pattern to test which format does image belong to the key issue for steganalysis is just like the patterns of recognition and feature extraction.

The features should be different for the image without hidden image and for stego-image

With the extensive application of steganography, it is challenged by ste-ganalysis. The most notable steganalysis algorithm is the RS attack which detects the steg-message by the statistic analysis of pixel values.[5]

5.6SteganographyTechniques:
Line Shift coding, word shift coding, feature coding ,Least Significant Bit insertion(LSB),Low Bit Encoding(LBE),Masking and filtering

Steganography Usage in Modern Devices:

For every page addition of yellow dots takes place, on these yellow dots time stamps and printed serial numbers are encoded

For example color laser printers

5.7 Steganography concepts:

5 .7.1 Multi Level steganography(MLS):

Combination of two or more steganographic methods leads to MLS .There are two methods one is upper layer and the other is lower level upper level is a carrier for the another method that is a lower level, some of the interesting benefits to hide the information are binding the information into a file they are as follows

Undetectability in upper level methods increases,total steganographic band width increases ,verification ability of steganogram's integrity, steganogram extraction and analisation has a limit of successful identification.The concept of network steganography is extended and it is redefined for making it generalfew useful MLS applications are presented to improve secrete communications on telecommunication networks

## VI HICCUPS(HIDDEN COMMUNICATION SYSTEM FOR CORRUPTED NETWORKS )

HICCUPS is one of the intra protocol steganography system which is used to modify the frames of protocol fields and content .wireless lans are suitable for "hiccups".The innovation in this system is the usage of the frames which are wrong checksums that are made intentionally for the establishment of covert communications this was first stegnography methods for wireless lans

6.1 LACK (Lost Audio Packets Steganography ):

This lack is one of the protocol steganography technique that which modifies the voice packets and time related to their content some audio packets are selected and delayed intentionally before the transmission at transmitter if delay is excessive at receiver of such packets then packets will be discarded by that receiver , the intentionally delayed packets of pay load used for transmitting secrete information for receivers which are aware of this procedure so extra packets are not generated .

6.2 PADSTEG:

Padsteg is called as padding steganography it is one of the interprotocal steganographic technique which is utilized for the relation between two or more number of protocals from TCP/IP for enabling of covered communications

6.3 RSTEG:-

RSTEG is called as "retransmission steganography ,it is one of the intraprotocal hybrid network steganography technique the main advantage in this rsteg is the acknowledgement not send for a received packet

## VII SCTP STEGANOGRAPHY

SCTP is a multi streaming based method ,it is also one of the intraprotocal steganographic method the main advantage of this method is subsequent checksum will transmit in streams which are determined by the bits of steganogram .

7.1 Steganalysis meets cryptanalysis:

As we have seen right now the encrypted message are present in the source file(e.g image)so to get the message we have to do cryptanalysis crypt algorithms are used for hiding the data.hence it is required to recover the message

7.2 Password guessing:

Try to get the password using social engineering technique and brute force attact

7.3 Stego_message:

The message after hiding into a desired file then the hidden message is called as stegano-message

7.4 Image Steganography:

Image steganography is one of the steganographical method in which a secret message is covered with an image and that will be uploaded directly to online websites and the image will be downloaded by a particular person and the information will be shared among them secretly .Image file formats

used to hide information are bmp,jpg

7.5 Audio Steganography:

This is the another type of steganographical method in which the secret information is hidden into an audio file and that will be uploaded directly into the websites randomly and then it will be downloaded and decrypted by a particular person and the information will be shared among them secretly.

Audio file formats to hide the information are wav,mp3

## VIII RESULTS

**8.1 Audio steganography**

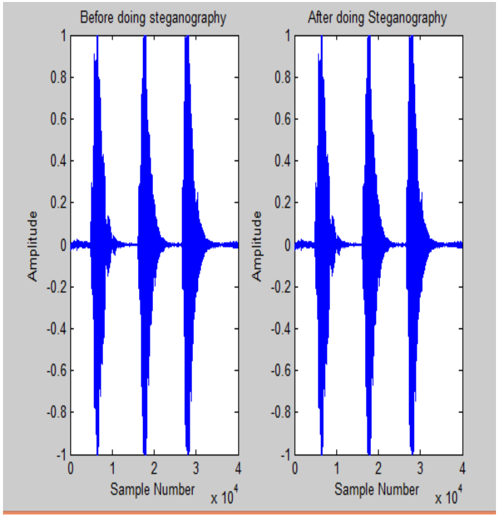


Fig 1:Image steganography at sender:

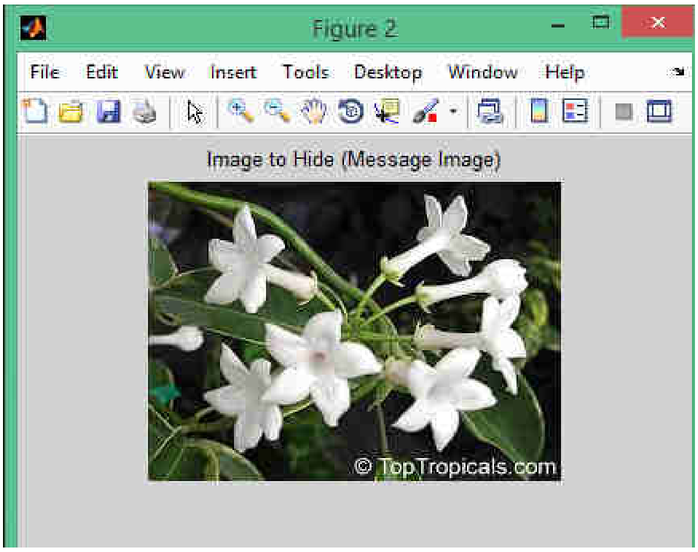


Fig 3: Image to hide

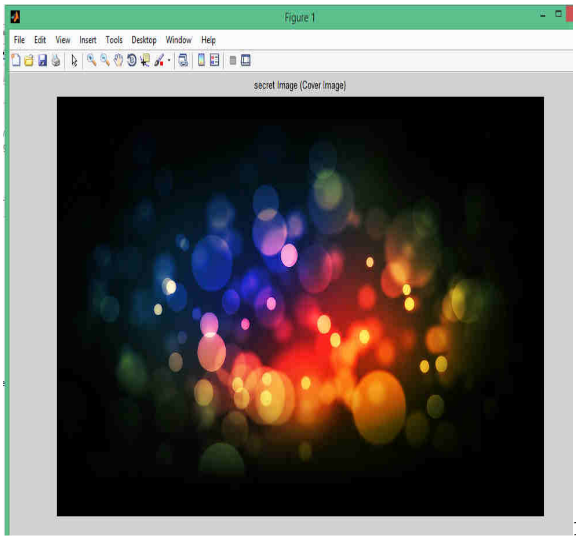


fig 2:

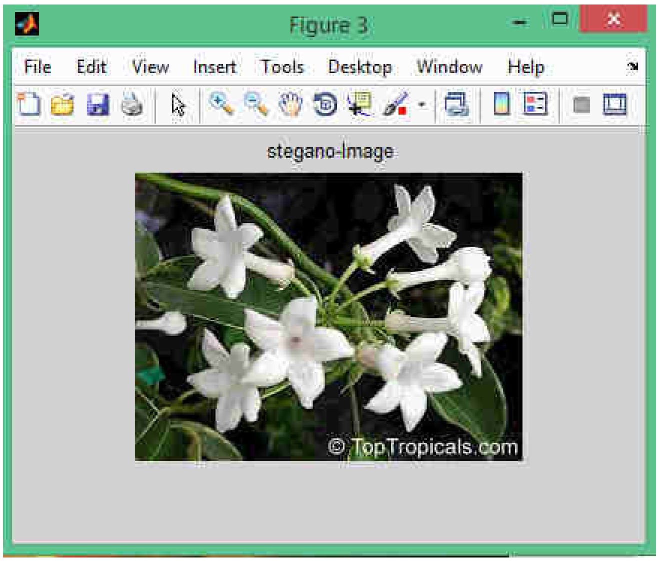


fig 4: Stegno image

ISSN: 2349-6495

# IMAGE STEGANOGRAPHY AT RECIEVER:

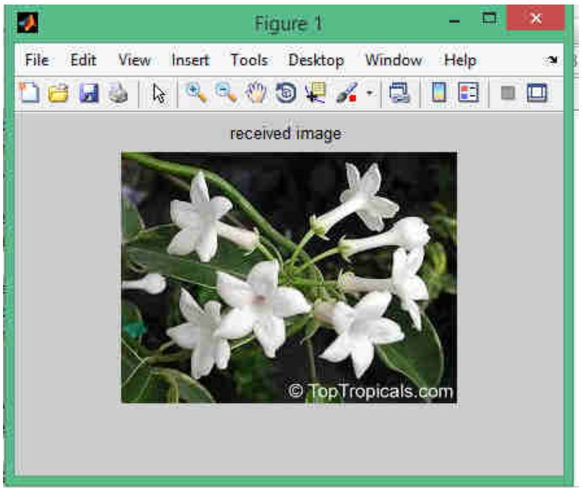


**Fig 5:Received figure**

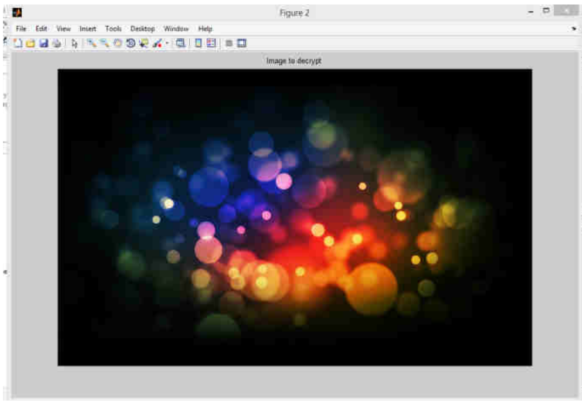

**Fig 6:**

## CONCLUSION:

Based on the project Steganography we hidden the message and audio files in an image and encoded it and decoded it and observed the required results in the form of image –image and audio –audio message ..

## REFERENCES:

[1]. Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information", IEEE Information Technology Conference, Syracuse, New York, USA, September 1st - 3rd, 1998.

[2]. Deepali, ,"Steganography With Data integrity" *International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 7,* November| 2012.

*[3].R. Udayakumar, K.P. Kaliyamurthie, Khanaa and A.V.Allin Geo"* Modeling of Steganography with Audio Files Using Matlab", World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 111-114, 2014.

[4]. Shikha, Vidhu Kiran Dutt,"Steganography: The Art of Hiding Text in Image using Matlab", Volume 4, Issue 9, September 2014.

[5]. Shen Wang, Bian Yang and Xiamu Niu," A Secure Steganography Method based on Genetic Algorithm", Volume 1, Number 1, January 2010.

[6]. Masoud Nosrati , Ronak Karimi, Mehdi Hariri," An introduction to steganography methods", *World Applied Programming, Vol (1), No (3), August 2011. 191-195.*

[7]. A H M Kamal" Steganography: Securing Message in wireless network", International Journal of Computers & Technology Volume 4 No. 3, March-April, 2013.