CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION OF THE PROBLEM:

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography .

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

Steganography uses in electronic communication include steganographic coding inside of a transport layer, such as an MP3 file, or a protocol, such as IP.

The project 'Steganography' provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit.

Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

What is Steganography Used for?

Like many security tools, steganography can be used for a variety of reasons, some good, some not so good. Legitimate purposes can include things like watermarking images for reasons such as copyright protection. Digital watermarks (also known as fingerprinting, significant especially in copyrighting material) are similar to steganography in that they are overlaid in files, which appear to be part of the original file and are thus not easily detectable by the average person. Steganography can also be used as a way to make a substitute for a one-way hash value (where you take a variable length input and create a static length output string to verify that no changes have been made to the original variable length input)[4]. Further, steganography can be used to tag notes to online images (like post-it notes attached to paper files). Finally, steganography can be used to maintain the confidentiality of valuable information, to protect the data from possible sabotage, theft, or unauthorized viewing.

The most traditional image-based steganographic algorithms are as follows. A. Use all the least significant bits of a vessel image for the hiding space of the secret data B. Replace special components in the frequency domain of the vessel image with the secret data C. Utilize the quantization error of the vessel image for a place to hide secret data.

However, all these methods have a relatively small data hiding capacity. The capacity is 5-15 % of the vessel data. Therefore, the straightforward application of the steganography has been limited to “watermarking” because it does not need a large data hiding capacity.

BPCS-Steganography is absolutely different from traditional techniques. The most important feature is a large embedding capacity. In most cases it can embed 50% of the vessel data (a 24bit BMP image case) .

Unfortunately, steganography can also be used for illegitimate reasons. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer. Furthermore, a person with a hobby of saving pornography, or worse, to their hard drive, may choose to hide the evidence through the use of steganography

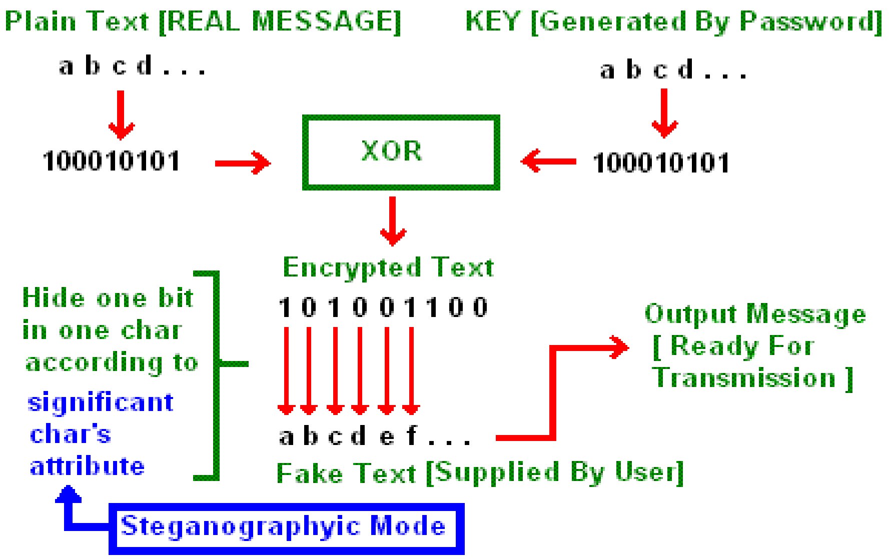
Steganography catagorises as-

1. Text steganography
2. Audio stegnography
3. Video steganography

1.1.1 Text steganography:

The goal of steganography is to transmit a message through some innocuous carrier i.e text, image, audio and video over a communication channel where the existence of the message is concealed. Based on Fig.1, steganography is one of the information hiding techniques and which can be categorized into linguistic steganography and technical steganography. Linguistic steganography defined by Chapman as "the art of using written natural language to conceal secret messages". A more specific definition by Krista Bennet in explaining linguistic steganography as a medium which required not only the steganographic cover that is composed of natural language text, but the text itself can be either generated to have a cohesive linguistic structure, or the cover text that begin with natural language

.


Plain Text [REAL MESSAGE]
KEY [Generated By Password]
a b c d . . .
a b c d . . .
100010101
XOR
100010101
Encrypted Text
1 0 1 0 0 1 1 0 0
Hide one bit in one char according to significant char's attribute
Output Message [Ready For Transmission]
a b c d e f . . .
Fake Text [Supplied By User]
Steganographyic Mode

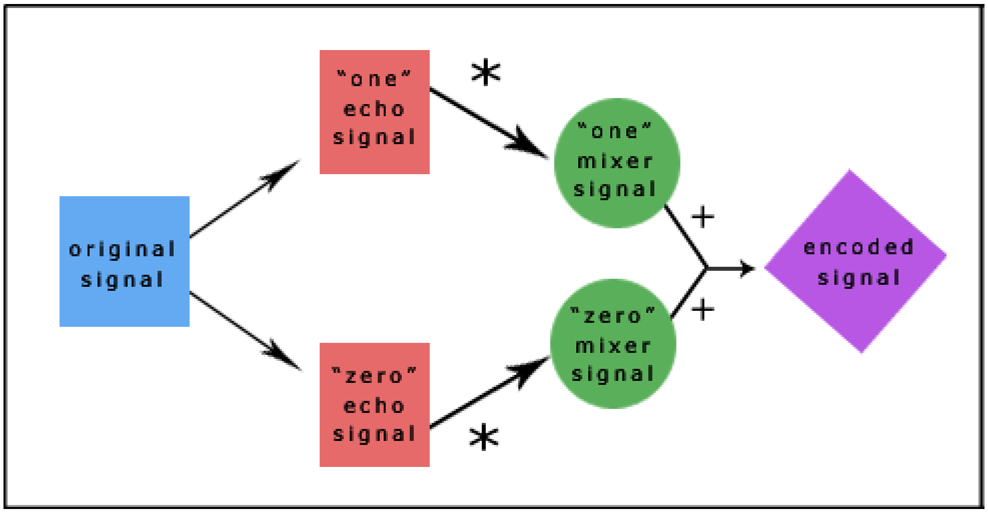
1. a Text steganography from [3]

1.1.2 Audio Steganography :

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.

The methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications.

For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented. On the other hand, a large corporation wishing to protect its intellectual property from "digital pirates" may consider a more sophisticated method such as phase coding, SS, or echo hiding



1. b Audio Steganography from [6]

1.1.3 Video Steganography :

Video Steganography is a technique to hide any kind of files in any extension into a carrrying Video file.This project is the application developed to embed any kind of data(File) in another file, which is called carrier file. The carrier file must be a video file. It is concerned with embedding information in an innocuous cover media in a secure and robust manner. This system makes the Files more secure by using the concepts Steganography and Cryptography.

1.2 OBJECTIVES:

The project has the following objectives:

1. The tool should be easy to use, and should use a graphical user interface.
2. To create a tool that can be used to hide data in a file system.
3. The tool should work cross-platform.
4. The tool should effectively hide a message using an image degradation approach, and should be able to retrieve this message afterwards.
5. The tool should take into account the original content, to theoretically more effectively hide the message.
6. The tool should be able to encrypt the message before embedding it.

1.3 Characteristics of Strong Steganography:

Though steganography's most obvious goal is to hide data, there are:

several other related goals used to judge a method's steganographic strength. These include

Capacity :- how much data can be hidden.

Invisibility: - inability for humans to detect a distortion in the

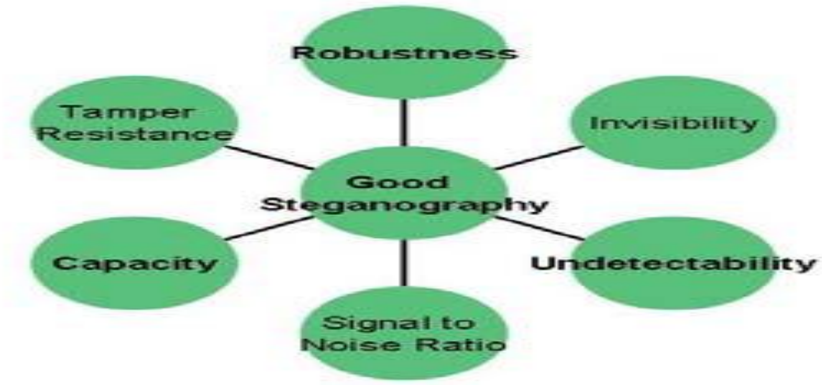
stego-object.

Undetectability :- inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects.

Robustness:- message's ability to persist despite compression or other common modifications.

Tamper Resistance:-message's ability to persist despite active measures to destroy it.

Signal To Noise Ratio:- how much data is encoded versus how much unrelated data is encoded.



1.c Properties of Good Steganography from [3]

1.4 PROJECT SCOPE:

1.4.1 Applications

Usage in modern printers: Printer steganography

Steganography is used by some modern printers, including HP and Xerox brand color laser printers. 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.

1.4.2 Rumored usage in terrorism

When one considers that messages could be encrypted steganographically in e-mail messages, particularly e-mail spam, the notion of junk e-mail takes on a whole new light. Coupled with the "chaffing and winnowing" technique, a sender could get messages out and cover their tracks all at once.

Rumors about terrorists using steganography started first in the daily newspaper USA Today on February 5, 2001 in two articles titled "Terrorist instructions hidden online" and "Terror groups hide behind Web encryption". In July of the same year, the information looked even more precise: "Militants wire Web with links to jihad".

A citation from the USA Today article: "Lately, al-Qaeda operatives have been sending hundreds of encrypted messages that have been hidden in files on digital photographs on the auction site eBay.com". These rumors were cited many times—without ever showing any actual proof—by other media worldwide, especially after the terrorist attack of 9/11.

The USA Today articles were written by veteran foreign correspondent Jack Kelley, who in 2004 was fired after allegations emerged that he had fabricated stories and invented sources.

In October 2001, the New York Times published an article claiming that al-Qaeda had used steganographic techniques to encode messages into images, and then transported these via e-mail and possibly via USENET to prepare and execute the September 11, 2001 Terrorist Attack.

To date, over 725 digital steganography applications have been identified by the Steganography Analysis and Research Center.

Over the past couple of years, steganography has been the source of a lot of discussion, particularly as it was suspected that terrorists connected with the September 11 attacks might have used it for covert communications. While no such connection has been proven, the concern points out the effectiveness of steganography as a means of obscuring data. Indeed, along with encryption, steganography is one of the fundamental ways by which data can be kept confidential. This article will offer a brief introductory discussion of steganography: what it is, how it can be used, and the true implications it can have on information security.

CHAPTER 2
LITERATURE REVIEW

2.1 INFORMATION SECURITY

In general, security denotes “the quality or state of being secure to be free from danger” **.** Security is classified into different layers depending on the type of content intended to be secured: Physical security: Defines the required issues that are needed to protect the physical data or objects from unauthorized intrusion. Personal security: It is defined as the security of the individuals who are officially authorized to access information about the company and its operations

Operational security: It mainly relies on the protection of the information of a particular operation of the chain of activities.

Communication‟s security: The communication‟s security encompasses the security issues regarding the organisation‟s communication media, technology and content.

Network security: The network security is responsible for safeguarding the information regarding the „networking components‟, „connections‟ and contents.

Information security:

Information security is the protection of information and the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized use or modification of use of data or capabilities.

The main objective of the project is to propose the method and critically discuss the properties which help to transmit the data or information over a network without any modifications. The critical characteristics of information are

1. Availability

2. Accuracy

3. Authenticity

4. Confidentiality

5. Integrity

Availability: prevention of unauthorised disclosure of information. It enables users who need access the information to do so without any interference or obstruction and to receive it in the required format. The availability of information requires the verification of the user as one with authorized access to information

In other words the availability can be defined as “Ensuring timely and reliable access to make use of information. A loss of availability is the disruption of access to or use of information or an information system”

Accuracy: The information is deemed accurate if it does not contain any mistakes / errors and possesses the value that end user expects. If the information holds a value different from that of the end user‟s expectations because of intentional or unintentional modifications of its content it becomes no longer accurate **.**

Authenticity: Authenticity refers to the quality or state of being genuine or original. It should not be a reproduction or fabrication of any previously known data. The Information is considered authentic when it is originally created, placed, stored or transferred. In general, authenticity is ensuring that all the data remains in its original state by stopping any ways of the unauthorised modification of information **.**

Confidentiality: “The confidentiality is the quality or state of preventing disclosure or exposure to unauthorized individuals or system”. Confidentiality is basically privacy and secrecy which means protection of personal data or that of data belonging to an organisation. Confidentiality of information ensures that only those with the rights and privileges access a particular set of information and prevent from unauthorized access **.** It is the prevention of unauthenticated modification of data. “The quality or state of being whole, complete and uncorrupted is the integrity of information”. The integrity of any data is lost when it is subjected to corruption, damage (external / internal), destruction or other disruption of its authentic state by intended or unintended sources **.**

2.1.1 Security attacks:

The data is transmitted from source to destination which is known as its normal flow as shown in the figure. But the hackers might hack the network in order to access or modify the original data. These types of attacks are formally known as security attacks.There are different types of approaches for preventing the security attacks. The most useful approaches are 1. Cryptography

2. Steganography

3. Digital watermarking

2.2 CRYPTOGRAPHY

The word cryptography is derived from two Greek words which mean “secret writing”. Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. Cryptography is an effective way to protect the information that is transmitting through the network communication paths .

Cryptology is the science that deals about cryptography and cryptanalysis. Cryptography is the approach of sending the messages secretly and securely to the destination. Cryptanalysis is the method of obtaining the embedded messages into original texts **.**

In general, cryptography is transferring data from source to destination by altering it through a secret code. The cryptosystems uses a plaintext as an input and generate a cipher text using encryption algorithm taking secret key as input.

The important elements in cryptosystems are

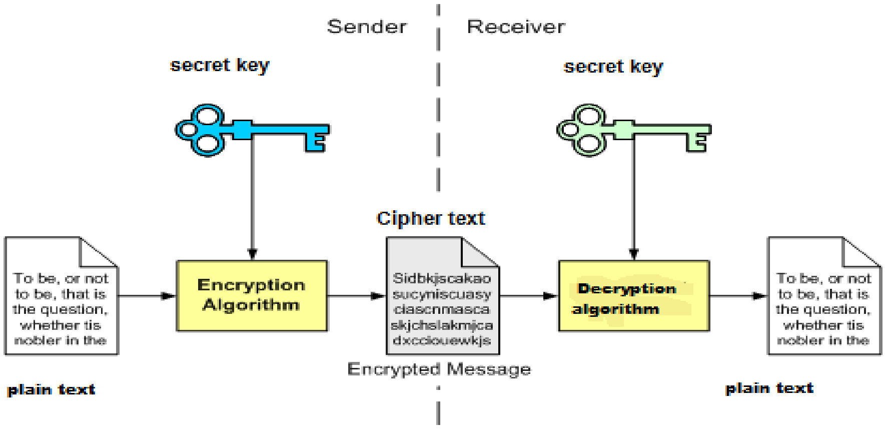
1. Plain text (input)

2. Encryption algorithm

3. Secret key

4. Cipher text

5. Decryption algorithm


Sender
Receiver
secret key
secret key
Cipher text
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxccioueswkjs
Decryption algorithm
To be, or not to be, that is the question, whether tis nobler in the
Encrypted Message
plain text
plain text

2. a General model of cryptographic system from [8]

2.3 STEGANOGRAPHY

Steganography in Greek means „covered writing‟. Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganographic techniques available to hide the data depending upon the carriers we use.

Steganography and cryptography both are used for the purpose of sending the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption and secret key. In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption.

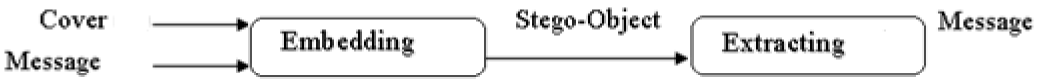
Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object the suitable formats are used. „Redundancy‟ is the process of providing better accuracy for the object that is used for display by the bits of object. he main file formats that are used for steganography are Text, images, audio, video, protocol The different types of steganographic techniques that is available are

1. Pure steganography

2. Public key steganography

3. Secret key steganography

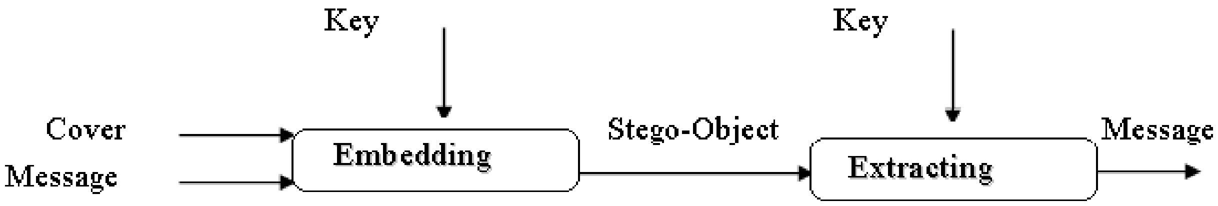
2.3.1 Pure steganography: Pure steganography is the process of embedding the data into the object without using any private keys. This type of steganography entirely depends upon the secrecy. This type of steganography uses a cover image in which data is to be embedded, personal information to be transmitted, and encryption decryption algorithms to embed the message into image.



2.b pure steganography process

This type of steganography can‟t provide the better security because it is easy for extracting the message if the unauthorised person knows the embedding method. It has one advantage that it reduces the difficulty in key sharing **.**

2.3.2 Secret key steganography: Secret key steganography is another process of steganography which uses the same procedure other than using secure keys. It uses the individual key for embedding the data into the object which is similar to symmetric key. For decryption it uses the same key which is used for encryption.

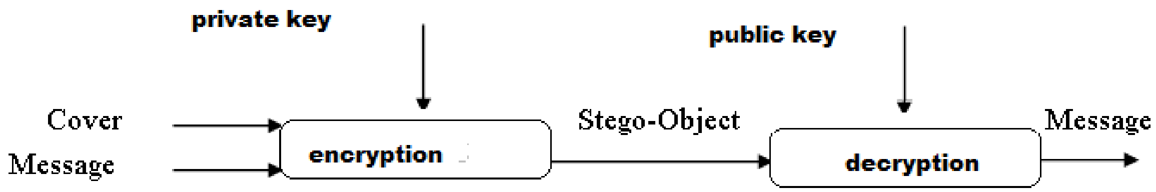


2.c secret key steganography

This type of steganography provides better security compared to pure steganography. The main problem of using this type of steganographic system is sharing the secret key. If the attacker knows the key it will be easier to decrypt and access original information **.**

2.3.3 Public key steganography:

Public key steganography uses two types of keys: one for encryption and another for decryption. The key used for encryption is a private key and for decryption, it is a „public key" and is stored in a public database .



2.d Public key steganography

2.4 ALGORITHM USED

For encryption and decryption of text messages using the secret keys steganographic system uses algorithms known as steganographic algorithms. The mostly used algorithms for embedding data into images are

1. LSB (Least Significant Bit) Algorithm

2. JSteg Algorithm

3. F5 Algorithm

2.4.1 LSB algorithm

LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using BMP images since the compression in BMP is lossless. But for hiding the secret message inside an image of BMP file using LSB algorithm it requires a large image which is used as a cover. LSB substitution is also possible for GIF formats.

problem with the GIF image is whenever the least significant bit is changed the whole colour palette will be changed. The problem can be avoided by only using the gray scale GIF images since the gray scale image contains 256 shades and the changes will be done gradually so that it will be very hard to detect. For JPEG, the direct substitution of steganographic techniques is not possible since it will use lossy compression. So it uses LSB substitution for embedding the data into images. There are many approaches available for hiding the data within an image: one of the simple least significant bit submission approaches is „Optimum Pixel Adjustment Procedure‟. The simple algorithm for OPA explains the procedure of hiding the sample text in an image.

Step1: A few least significant bits (LSB) are substituted with in data to be hidden.

Step2: The pixels are arranged in a manner of placing the hidden bits before the pixel of each cover image to minimize the errors.

Step3: Let n LSBs be substituted in each pixel.

Step4: Let d= decimal value of the pixel after the substitution.

d1 = decimal value of last n bits of the pixel.

d2 = decimal value of n bits hidden in that pixel.

Step5: If (d1~d2)<=(2^n)/2

then no adjustment is made in that pixel.

Else

Step6: If(d1<d2)

d = d – 2^n.

If(d1>d2)

d = d + 2^n.

This„d‟ is converted to binary and written back to pixel **(Amirtharajan et al., 2010).**

This method of substitution is simple and easy to retrieve the data and the image quality better so that it provides good security.

2.4.2 Jsteg Algorithm

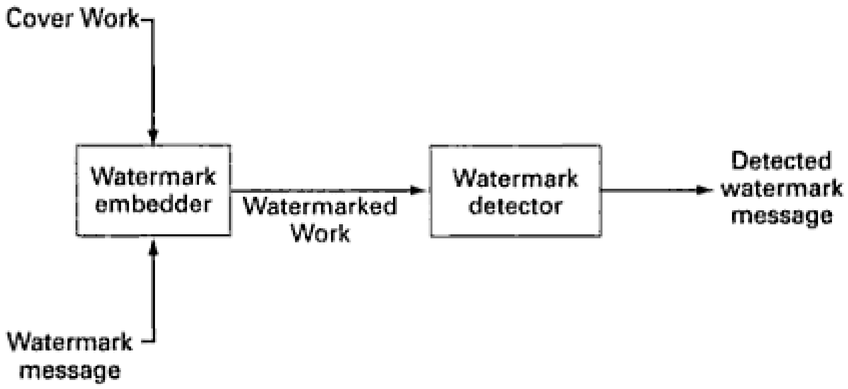
JSteg algorithm is one of the steganographic techniques for embedding data into JPEG images. The hiding process will be done by replacing Least Significant Bits (LSB). JSteg algorithm replaces LSBs of quantized Discrete Courier Transform (DCT) coefficients. In this process the hiding mechanism skips all coefficients with the values of 0 or 1. This algorithm is resistant to visual attacks and offers an admirable capacity for steganographic messages. Generally, JSteg steganographic algorithm embedded the messages in lossy compressed JPEG images. It has high capacity and had a compression ratio of 12%. JSteg algorithm is restricted for visual attacks and it is less immune for statistical attacks. Normally, JSteg embeds only in JPEG images. In these JPEG images, the content of the image is transformed into „frequency coefficients‟ so as to achieve storage in a very compressed format. There is no visual attack in the sense presented here, due to the influence of one steganographic bit up to 256 pixels.

2.4.3 F5 algorithm

F5 algorithm was introduced by German researchers Pfitzmann and Westfeld in order to avoid the security problem when embedding the data into the JPEG images. The F5 algorithm embeds the message into randomly chosen Discrete Courier Transform (DCT) coefficients. It utilizes matrix embedding which minimises the changes to be made to the length of certain message. The F5 Algorithm provides high steganographic capacity, and can prevent visual attacks. F5 algorithm is also resistant to statistical attacks. This algorithm uses matrix encoding such that it reduces the number of changes needed to embed a message of certain length. This algorithm avoids the chi-square attack since it doesn‟t replace or exchange the bits. The resistance is high for both visual and statistical attacks. It has high embedding capacity that is greater than 13%.This algorithm supports TIFF, BMP, JPEG and GIF formats.

2.5 DIGITAL WATERMARKING

“Watermarking is the practice of imperceptibly altering work to embed a secret message”**.** „Digital watermarking‟ is the process of inserting information into a digital signal. The main aim of digital watermarking is to protect the integrity and authenticity of digital media. Digital watermarking directly embeds a watermark containing owner identification into the host signal in such a way that the hacker can‟t remove the watermark without reducing the quality of the signal or an image. Digital watermarks can be used as proof of authorization and can be used as a signature which shows the ownership of particular asset like images, video and audio files.



2.e General watermarking system

CHAPTER 3

PROPOSED MATHODOLOGY

3.1 FEATURE OF PROPOSED MATHODOLOGY

In this project, the proposed method should provide better security when transmitting or transferring the data or messages from one end to another. The main objective of the project is to hide the message or a secret data into an image which further act as a carrier of secret data and to transmit to the destination securely without any modification. If there are any perceivable changes when we are inserting or embedding the information into the image or if any distortions occur in the image or on its resolution there may be a chance for an unauthorised person to modify the data. So, the data encryption into an image and decryption and steganography plays a major role in the project.

The three important sections in the project are:

Encryption: In this section for encryption, I have used LSB (Least Significant bit) algorithm which helped me to build a steganographic application to provide better security. The LSB algorithm provides better security compared to JSteg algorithm with improved data compression and data hiding capacities.

Steganography: I have used the image as carrier for transmission of data and by using the „Least Significant bit Algorithm‟ I have inserted the message bits in to the least significant pixels of an image.

Decryption: The decryption process is similar but opposite to the encryption process. When the receiver wants to decrypt the data from the image, it uses same „least significant bit algorithm‟ for extracting the data from the image by taking password or key as reference.

The Modules of the system are:

1) Tiny Algorithm Implementation Module

2) Stegnography Module

3) GUI Module

3.1 TINY ENCRYPTION ALGORITHM:

The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm designed to minimize memory footprint and maximize speed. It is a Feistel type cipher that uses operations from mixed (orthogonal) algebraic groups. This research presents the cryptanalysis of the Tiny Encryption Algorithm. In this research we inspected the most common methods in the cryptanalysis of a block cipher algorithm. TEA seems to be highly resistant to differential cryptanalysis, and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text) after only six rounds. Time performance on a modern desktop computer or workstation is very impressive.

As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and store data. The security of such systems greatly depends on the methods used to manage, establish, and distribute the keys employed by the cryptographic techniques. Even if a cryptographic algorithm is ideal in both theory and implementation, the strength of the algorithm will be rendered useless if the relevant keys are poorly managed.

The following notation is necessary for our discussion.

Hexadecimal numbers will be subscripted with "*h*," e.g., 10 = 16. *h*

Bitwise Shifts: The logical shift of x by y bits is denoted by $x << y$. The logical right shift of x by y bits is denoted by $x >> y$.

Bitwise Rotations: A left rotation of x by y bits is denoted by $x <<< y$. A right rotation of x by y bits is denoted by $x >>> y$.

Exclusive-OR: The operation of addition of n-tuples over the field (also known as 2F exclusive-or) is denoted by $x \oplus y$.

The Tiny Encryption Algorithm is a Feistel type cipher that uses operations from mixed (orthogonal) algebraic groups. A dual shift causes all bits of the data and key to be mixed repeatedly. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). TEA seems to be highly resistant to differential cryptanalysis and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text). Time performance on a workstation is very impressive.

Block ciphers where the cipher text is calculated from the plain text by repeated application of the same transformation or round function. In a Feistel cipher, the text being encrypted is split into two halves. The round function, F, is applied to one half using a sub key and the output of F is (exclusive-or-ed (XORed)) with the other half. The two halves are then swapped. Each round follows the same pattern except for the last round where there is often no swap. The focus of this thesis is the TEA Feistel Cipher.

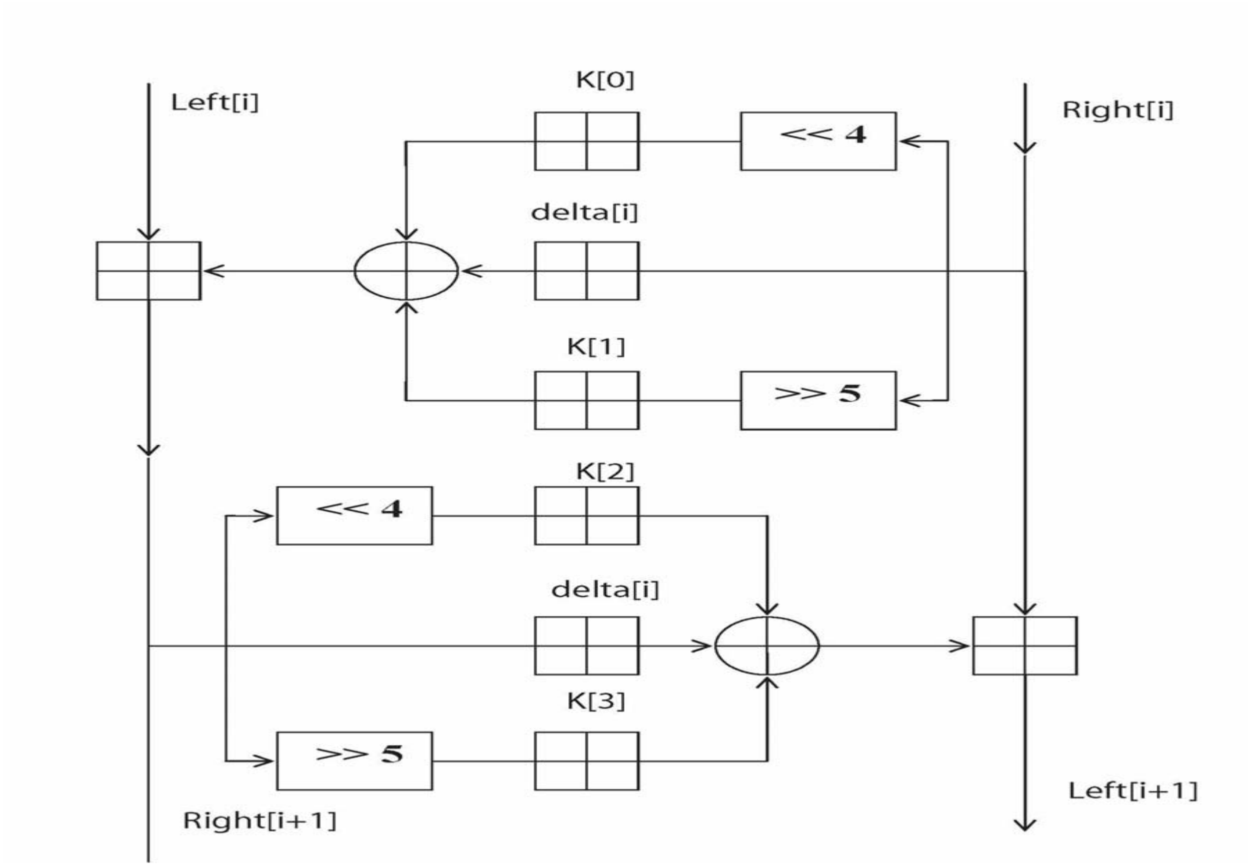
The inputs to the encryption algorithm are a plaintext block and a key K .The plaintext is P = (Left[0], Right[0]) and the cipher text is C = (Left[64], Right[64]). The plaintext block is split into two halves, Left[0] and Right[0]. Each half is used to encrypt the other half over 64 rounds of processing and then combine to produce the cipher text block.

- Each round *i* has inputs Left[*i*-1] and Right[*i*-1], derived from the previous round, as well as a sub key K[*i*] derived from the 128 bit overall K.

- The sub keys K[*i*] are different from K and from each other.

- The constant delta =$(5^{1/2}-1)*2^{31}$ =9E3779B h , is derived from the golden number ratio to ensure that the sub keys are distinct and its precise value has no cryptographic significance.

- The round function differs slightly from a classical Fiestel cipher structure in that integer addition modulo 2^{32} is used instead of exclusive-or as the combining operator.



Above Figure presents the internal details of the *i*th cycle of TEA. The round function, F, consists of the key addition, bitwise XOR and left and right shift operation. We can describe the output (Left[*i* +1] , Right[*i* +1]) of the *i*th cycle of TEA with the input (Left[*i*] ,Right[*i*]) as follows

Left [*i*+1] = Left[*i*] F (Right[*i*], K [0, 1], delta[*i*]),

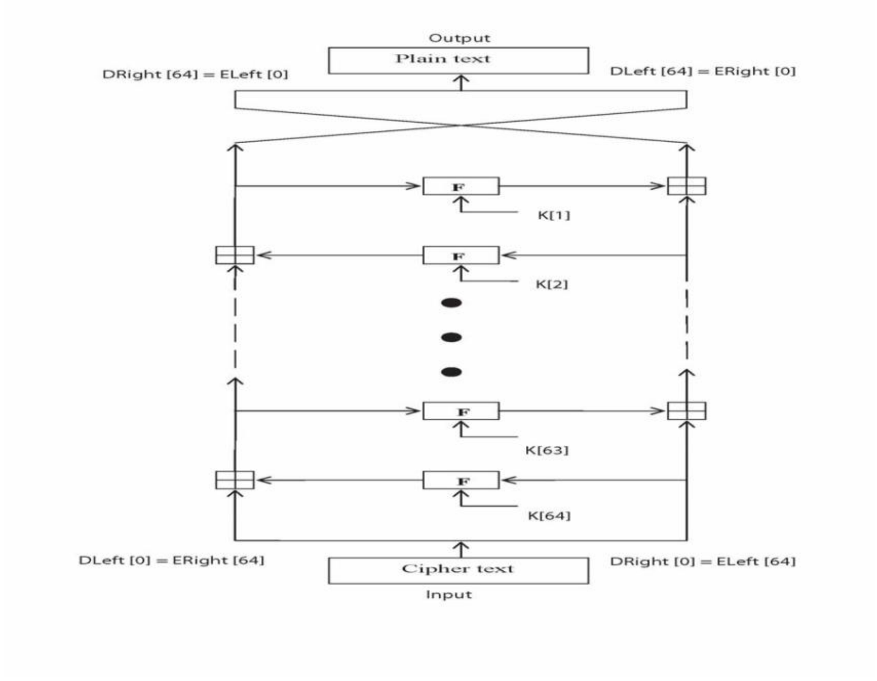
Right [*i* +1] = Right[*i*] F (Right[*i* +1], K [2, 3], delta[*i*]),

delta[*i*] = (*i* +1)/2 * delta,

The round function, F, is defined by

F(M, K[*j*,*k*], delta[*i*]) = ((M << 4) K[*j*]) ⊕ (M delta[*i*]) ⊕ ((M >> 5) K[*k*]).

The round function has the same general structure for each round but is parameterized by the round sub key K[*i*]. The key schedule algorithm is simple; the 128-bit key K is split into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). The keys K[0] and K[1] are used in the odd rounds and the keys K[2] and K[3] are used in even rounds.



3.1.b Tiny Encryption Algorithm:

Decryption is essentially the same as the encryption process; in the decode routine the cipher text is used as input to the algorithm, but the sub keys K[*i*] are used in the reverse order.

Figure presents the structure of the TEA decryption routine. The intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves of the value swapped. For example, if the output of the nth encryption round is

ELeft[*i*] || ERight[*i*] (ELeft[*i*] concatenated with ERight[*i*]).

Then the corresponding input to the (64-*i*)th decryption round is

DRight[*i*] || DLeft[*i*] (DRight[*i*] concatenated with DLeft[*i*]).

After the last iteration of the encryption process, the two halves of the output are swapped, so that the cipher text is ERight[64] || ELeft[64], the output of that round is the final cipher text C. Now this cipher text is used as the input to the decryption algorithm. The input to the first round is ERight[64] || ELeft[64], which is equal to the 32-bit swap of the output of the 64th round of the encryption process.

3.2 Steganography:

Stegnography is art of hiding information in ways that prevent the detection of hidden messages. Stegnography derived from Greek, literally means “Covered Writing”. It includes a vast array of secret communications methods that conceal the message’s very existence. Theses methods are including invisible inks, microdots, character arrangement, digital signature, and covert channels and spread spectrum communications.

In this technology, the end user identifies an video file, which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and video file are sent. Prior to this the data is embedded into the video and then sent. The image if hacked or interpreted by a third party user will open up in any video player but not displaying the data. This protects the data from being invisible and hence is secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the video file.

The module deals with identifying the hidden data in the video file. The module receives the video file that is then browsed to remove the associated data.

3.2 BPCS –STEGANOGRAPHY

Merits of BPCS-Steganography

We made an experimental system to investigate this technique in depth. The merits of BPCS-Steganography found by the experiments are as follows.

1. The information hiding capacity of a true color image is around 50%.

2. A sharpening operation on the dummy image increases the embedding capacity quite a bit.

3. Canonical Gray coded bit planes are more suitable for BPCS-Steganography than the standard binary bit planes.

4. Randomization of the secret data by a compression operation makes the embedded data more intangible.

5. Customization of a BPCS-Steganography program for each user is easy. It further protects against eavesdropping on the embedded information.

Method and principle of steganography :

The method of steganography outlined in this paper makes use of the more complex regions of an image to embed data.

There is no standard definition of image complexity. Kawaguchi discussed this problem in connection with the image thresholding problem, and proposed three types of complexity measures [4][5][6]. In the present paper we adopted a blackand-white border image complexity. The definition of image complexity

The length of the black-and-white border in a binary image is a good measure for image complexity. If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4. We will define the image complexity α by the following.

$$\alpha = \frac{k}{\text{The max. possible B - W changes in the image}}$$

Where, k is the total length of black-and-white border in the image. So, the value ranges over

$$0 \leq \alpha \leq 1. \qquad (2)$$

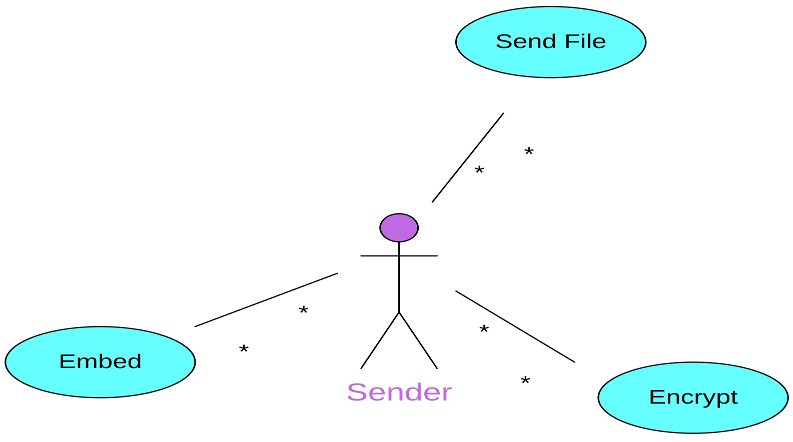
(1) is defined globally, i.e., α is calculated over the whole image area. It gives us the global complexity of a binary image.

However, we can also use α for a local image complexity (e.g., an 8 × 8 pixel-size area). We will use such α as our local complexity measure in this paper.

3.2.1 Graphical User Interface:

This project is developed using graphics in java swings. The options available are displayed in a menu format, like in an online editor. Clicking on any particular menu item through mouse or through keyboard a dropdown menu is displayed, listing all the options available under that menu item and the user can select the needed actions according to their wish.

USE CASE DIAGRAM



3.2.1 a USE CASE DIAGRAM

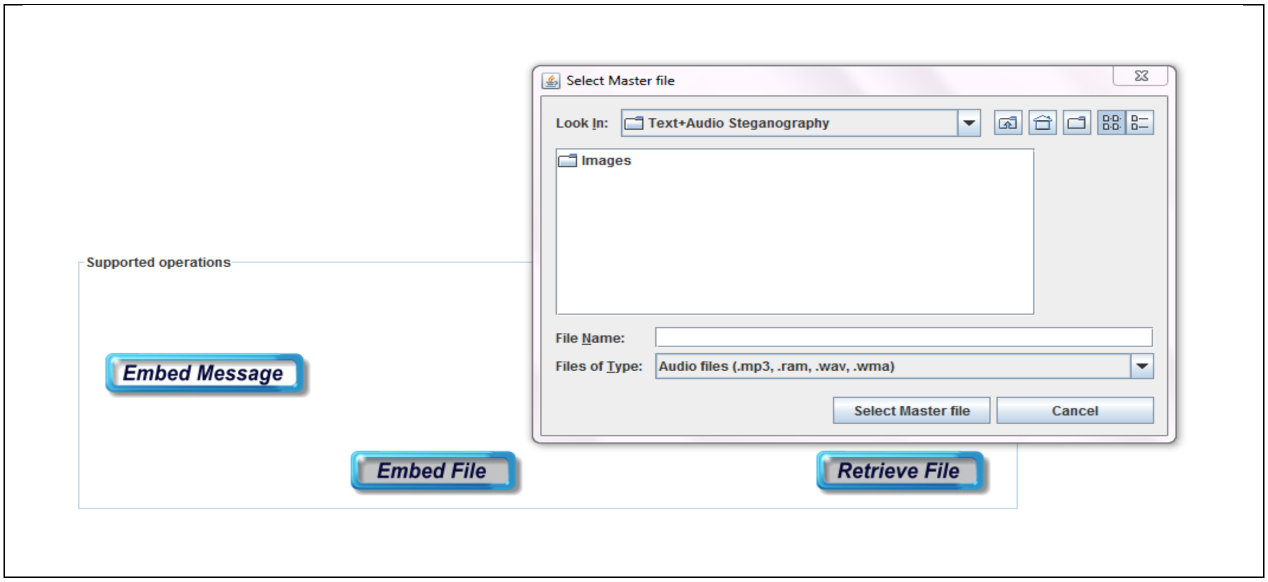
CHAPTER 4

RESULT AND DISCUSSION

All of the approaches to steganography have one thing in common that they hide the Secret message in physical object which is sent. The following figure shows the steganography processof the cover image being passed into the embedding function with the message to incode resulting in a steganography image containing the hidden massege .a keys often used to protect the hidden massege .this keys is usually a password ,so this keys also used to encrypt and decrypt the message before and after the embedding.

4.1 SNAPSHOT ON TEXT AND AUDIO STEGANOGRAPHY:

4.1.1 Embed massage:

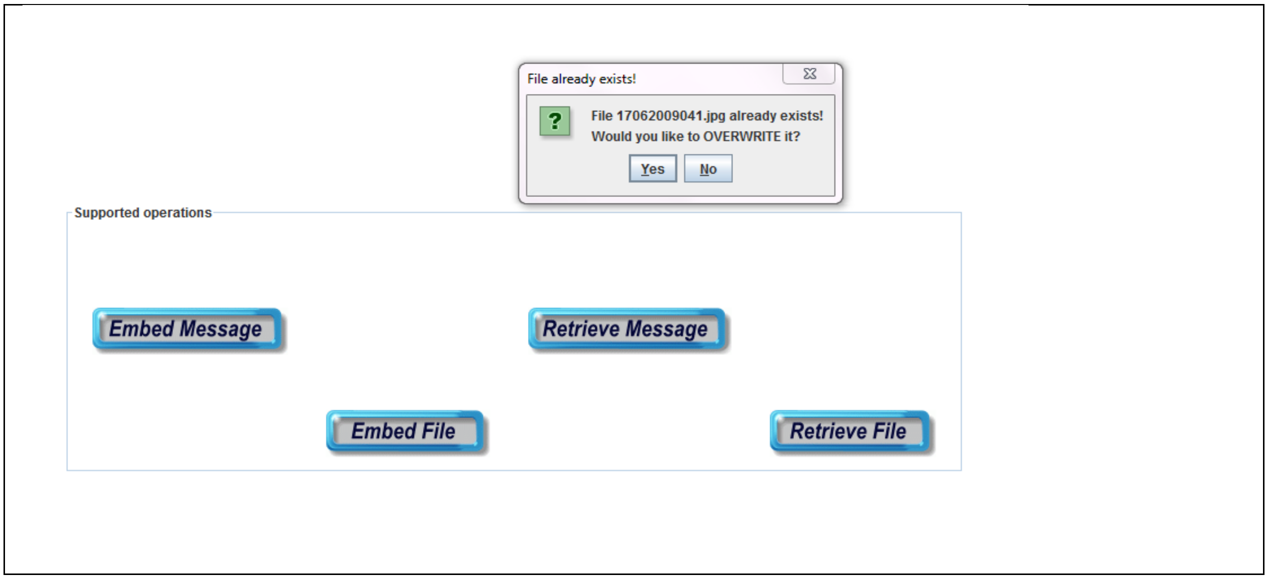


Look In: Text+Audio Steganography

File Name:

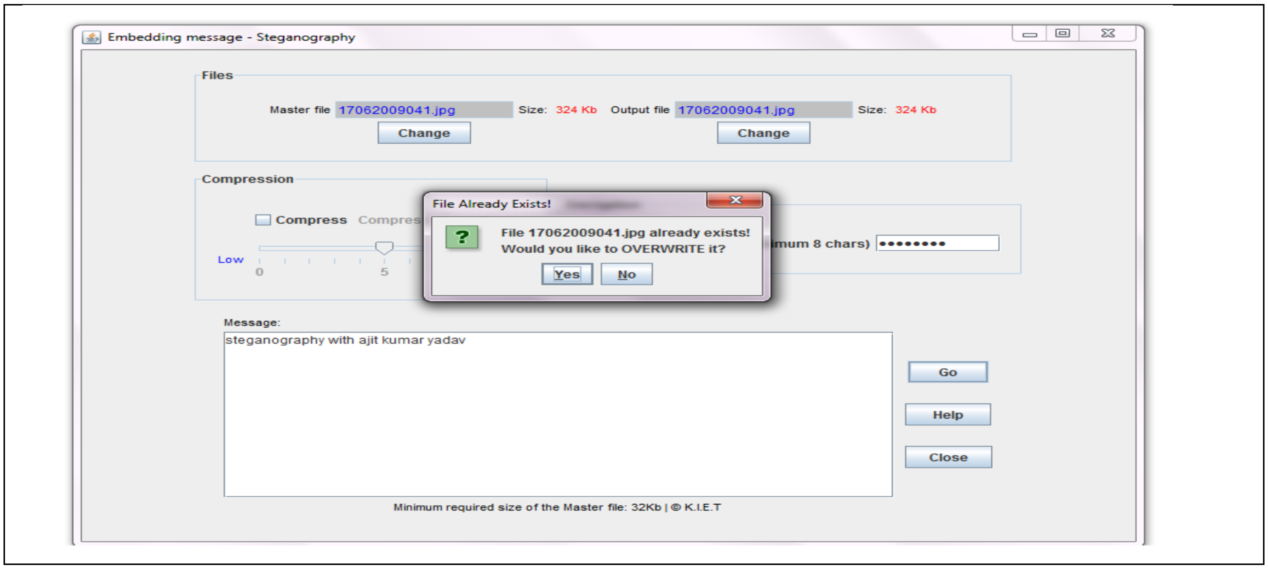
Files of Type: Audio files (.mp3, .ram, .wav, .wma)

4.1.2 Embed file :



File 17062009041.jpg already exists!
Would you like to OVERWRITE it?

4.1.3 Retrieve message



Master file 17062009041.jpg Size: 324 Kb Output file 17062009041.jpg Size: 324 Kb

□ Compress

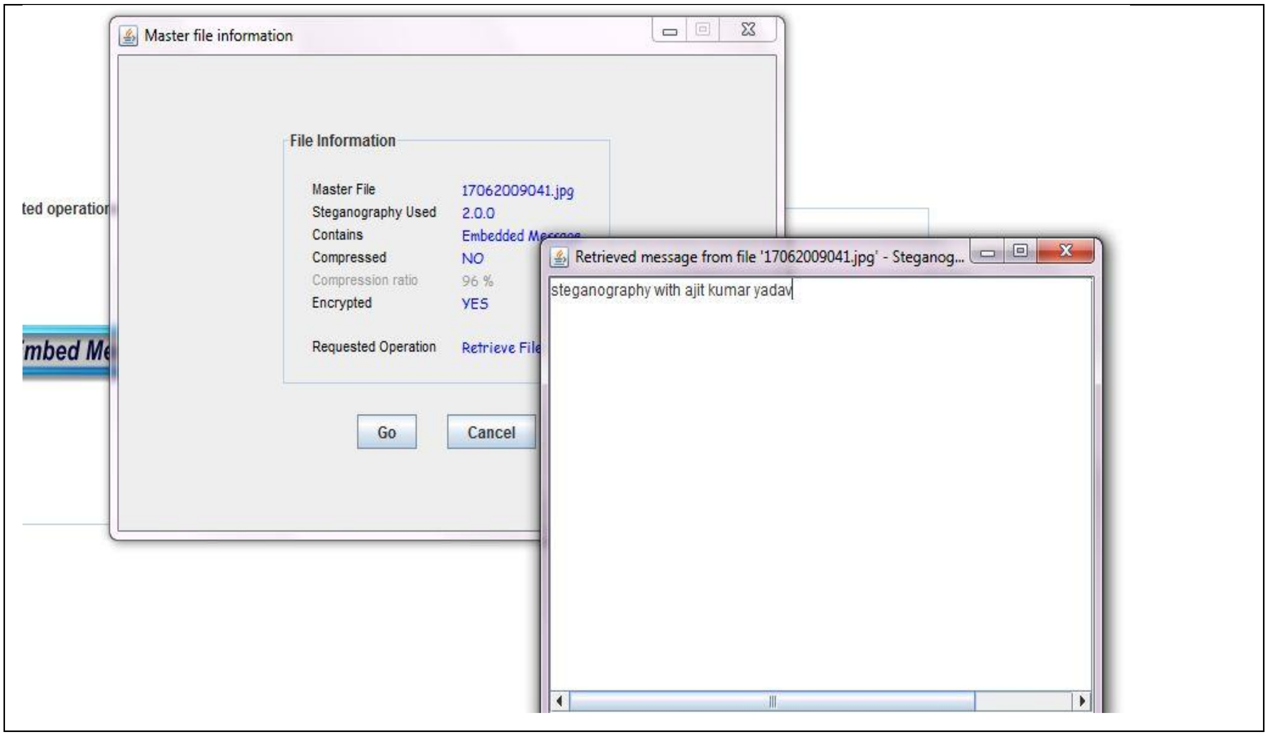
imum 8 chars) ●●●●●●●●●

File 17062009041.jpg already exists!
Would you like to OVERWRITE it?

Message:
steganography with ajit kumar yadav

Minimum required size of the Master file: 32Kb | © K.I.E.T

4.1.4 Retrieve file



Master file information

File Information

Master File 17062009041.jpg

Steganography Used 2.0.0

Contains Embedded Message

Compressed NO

Compression ratio 96 %

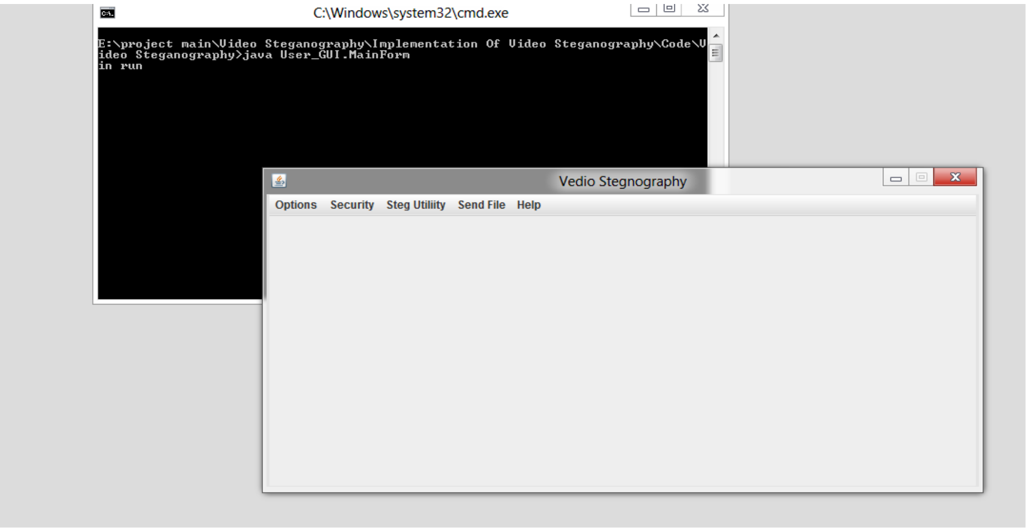
Encrypted YES

Requested Operation Retrieve File

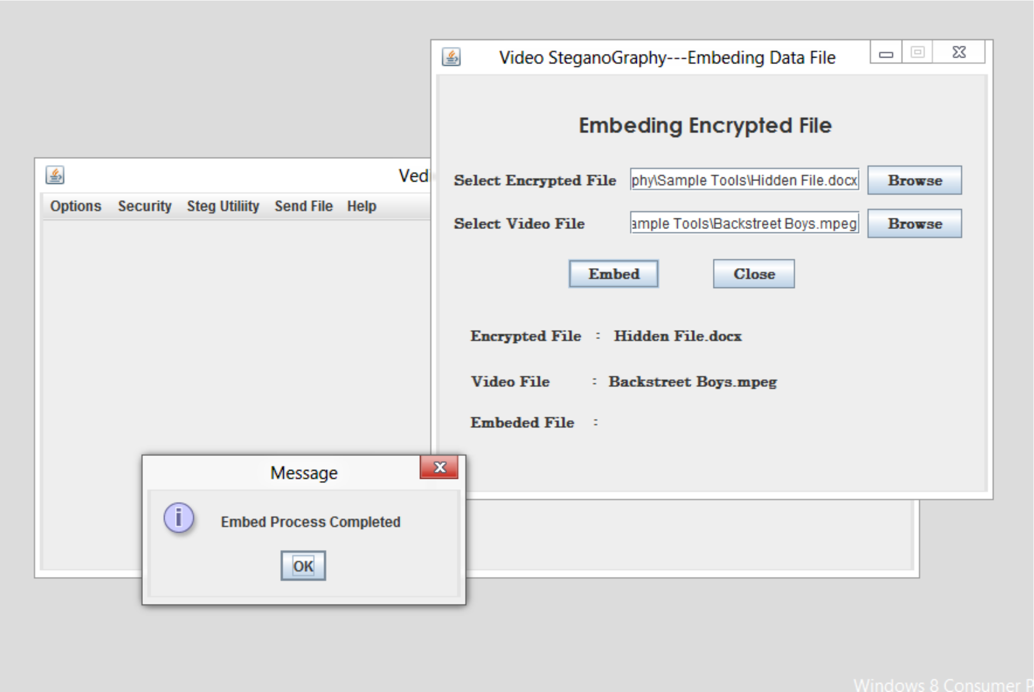
Retrieved message from file '17062009041.jpg' - Steganog...

steganography with ajit kumar yadav

4.2 Snapshot of video Steganography



```
E:\project main\Video Steganography\Implementation Of Video Steganography\Code\V
ideo Steganography>java User_GUI.MainForm
in run
```



Embeding Encrypted File

Select Encrypted File phy\Sample Tools\Hidden File.docx

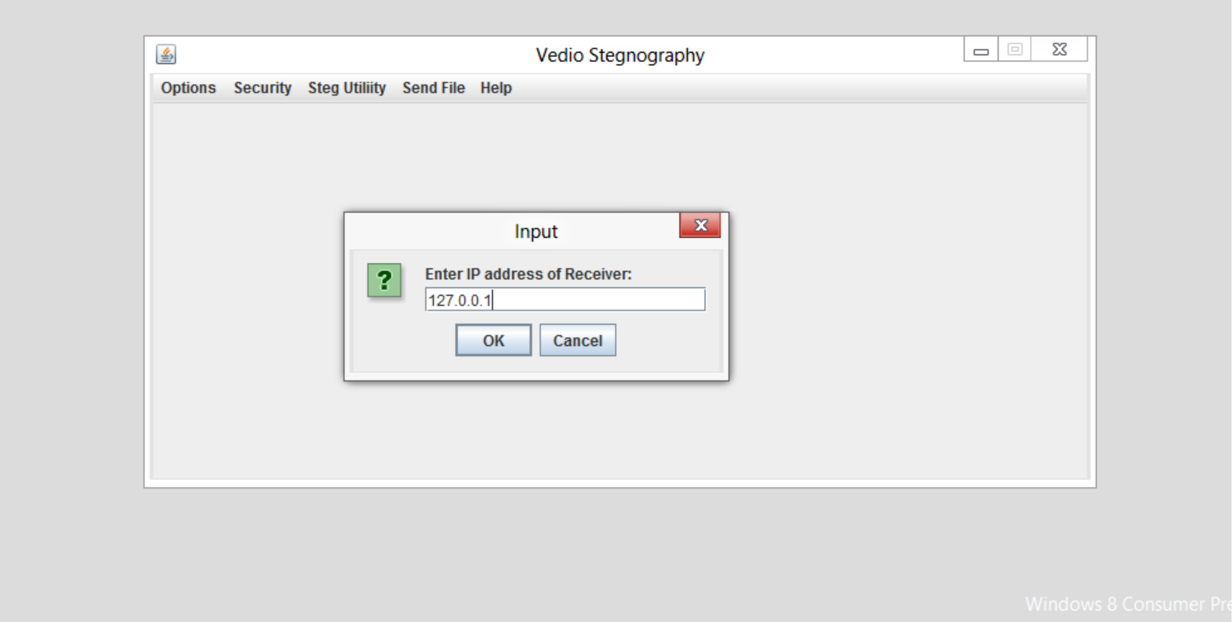
Select Video File ample Tools\Backstreet Boys.mpeg

Encrypted File : Hidden File.docx

Video File : Backstreet Boys.mpeg

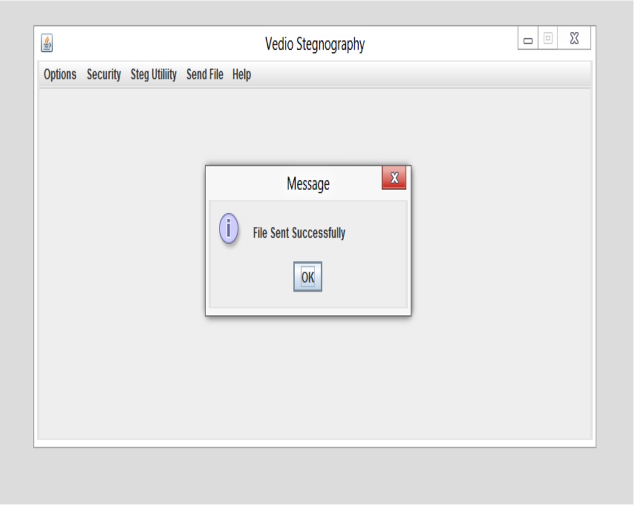
Embeded File :

Embed Process Completed

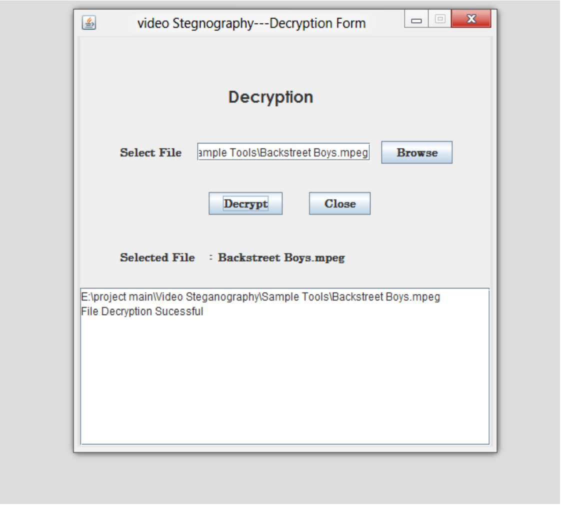


Enter IP address of Receiver:

127.0.0.1



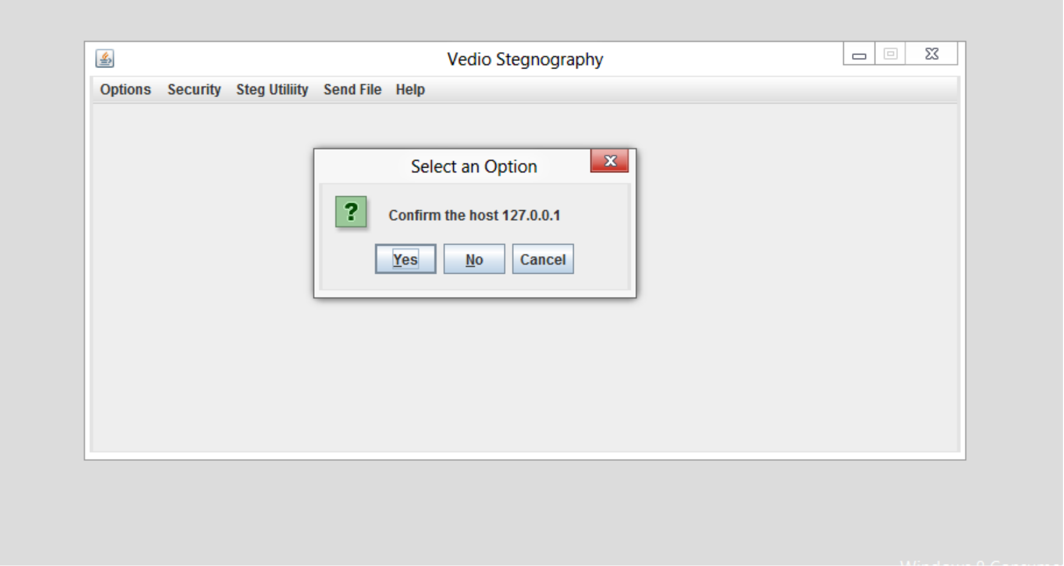
File Sent Successfully



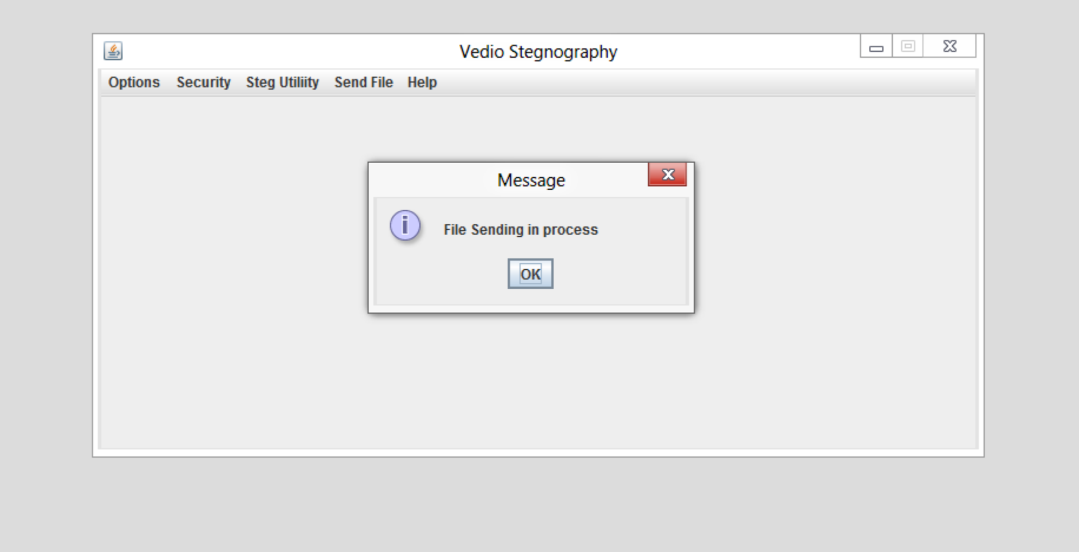
Select File ample Tools\Backstreet Boys.mpeg

Selected File : Backstreet Boys.mpeg

```
E:\project main\Video Steganography\Sample Tools\Backstreet Boys.mpeg
File Decryption Sucessful
```



Confirm the host 127.0.0.1



File Sending in process

CHAPTER 5

CONCLUSION AND FURTHER SCOPE

5.1 CONCLUSION :

The project **“Steganography** ***“which*** has been developed using Java meets the requirement of the organization. The main objective of the system developed is the protection of data resources and programs against accidental or intentional destruction or modification or disclosure to unauthorized persons. User friendliness is another feature of this system that offers enhanced convenience to the ser working with the system. The interactive interface provided by the software eases the data security process for the authorized user.

Developing this software has been a good experience for me. During the development of the project I had got enough to learn and got the chance to increase my knowledge in the field of software. I am satisfied that the system meets all the requirements

The entire project has been developed and deployed as per the requirements stated by the user, it is found to be bug free as per the testing standards that is implemented. Any specification untraced errors will be concentrated in the coming versions, which are planned to be developed in near future. The system at present does not take care of lower level check constraints in accessing the file types in distributed environments, which is to be considered in the future up gradations.

As per the present status the project developed is well equipped to handle the Central file system of an organization in a server and provide access to the users with various privileges as prescribed by the higher authorities in the password file.

5.2 MERIT

Accuracy is as per the expectations.

Techniques used are simple but yet efficient.

The number of parameters can be increased as and when required.

There is always a scope of improvement.

Automation will reduce the manual work greatly.

Ensure better handling and management of multimedia data.

5.3 LIMITATION

Computing speed is relatively slow.

Simultaneous classification of videos is not feasible.

Resource requirement is definitely high.

Processing is time taking.

5.4 TOOL AND PLATFORM USED

JCREATOR Version 5.00 (in beta)

JCREATOR is a IDE environment and fourth-generation programming language. Developed by MathWorks, JCREATOR allows matrix program compilation, applet generation and data implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including Java.

Although Jcreator is intended primarily for compilation. An additional package,its adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

5.5 FUTURE SCOPE

Hiding data on the network in case of a breach.

Peer-to-peer private communications.

Posting secret communications on the Web to avoid transmission.

Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

References

[1] Chan, C.K. Cheng, L.M., 2004. H*iding data in images by simple lsb substitution: pattern recognition.*vol 37. Pergamon.

[2] Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, *European Journal Of Scientific Research*, vol 39(1), pp 231-239

[3] Amirthanjan,R. Akila,R & Deepikachowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, *International Journal of Computer Application*, 2(3), pp.2-10.

[4] Arnold, M. 2000. Audio watermarking: Features, applications and algorithms, *Proceeding of the IEEE International Conference on Multimedia and Expo,* pp 1013-1016.

[5] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. *International Journal of Advancements in Technology*, 1(1), pp.05-11.

[6] Bloom,J. A. et al.,2008. *Digital watermarking and Steganography*. 2nd ed. Morgan Kaufmann.

[7] Bishop, M., 2005. *Introduction to computer security.* 1st ed. Pearson publications.
Cachin, C., 2004. Information: Theoretic model for steganography. *Work shop on information hiding, USA.*

[8] Cox, I. Miller, M. Bloom, J. Fridrich, J & Kalker, T. 2008. Digital watermarking and Steganography. 2nd Ed. Elsevier. David, W. (2004) Managing information: IT for Business purpose. 3rd edn, pg no. 215, Elsevier.

[9] Hellman, M.E., 2002. An overview of public key cryptography. IEEE communication magazine.

[10]Jeffrey A, Bloom et al., 2008. Digital watermarking and steganography, 2nd edn, Morgan Kaufmann publications.