Steganography in Multiple Data: Review

Preeti Hooda
Department of Computer Science and Application Engineering
Ganga Institute of Technology & Management (Jhajjar)

Kamal Ranga
Department of Computer Science and Application Engineering
Ganga Institute of Technology & Management (Jhajjar)

Abstract - The rapid development of multimedia and internet allows for wide distribution of digital media data which need a big security and privacy, hence to achieve it is necessary to find appropriate protection because of the significance, accuracy and sensitivity of the information.

The phenomenal growth of e-commerce applications in the World Wide Web requires the need to increase the security of data communications over the Internet, especially for highly sensitive document transfer. in this paper Steganography techniques were introduced and developed to increase security. We are implementing text, image ,audio and video steganography integrated in single steganography technique using RJ algorithm.

Keywords: steganography

I. INTRODUCTION

Steganography provides digital way to keep the data secure. The Steganography consists of techniques to allow the communication between two persons. It hides not only the contents but also the existence of the communication in the eyes of any observer. These techniques use a second perceptible message, with meaning disjoined by the secret message. This second message works as a "Trojan horse", and is a container of the first one. The new technologies and, in special way, the information networks require more and more sophisticated strategies in order to prevent the message privacy. Due to the high proliferation of digital images and the high degree of redundancy present in digital images, there is an increased interest in the usage of images as the cover object in steganography. So, in this context, digital images and audio is excellent candidate to turn into containers of the messages, since the bits of a secret text message can be Superimposed, as slight noise, to the bits employed for coding a digital image.

1.1 Steganography

The modern formulation of steganography is often given in terms of the prisoner's problem where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examined by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication. Specifically, in the general model for steganography, illustrated in Fig. 1.1, we have Alice wishing to send a secret message m to Bob. In order to do so, she "embeds" m into a cover-object c, and obtains a stego-objects. The stego-object*s* is then sent through the public channel. Thus we have the following definitions:

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-object: refers to the object which is carrying a hidden message. So given a cover object, and a messages the goal of the steganographer is to produce a stego object which would carry the message. In a pure steganography framework, the technique for embedding the message is unknown to Wendy and shared as a secret between Alice and Bob. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties

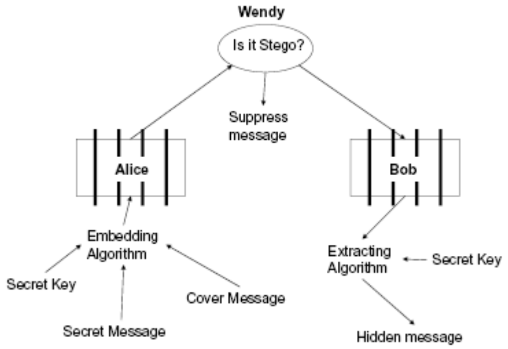


Fig.1.1 General model for steganography.

The secret key, for example, can be a password used to seed a pseudo-random number generator to select pixel locations in an image cover-object for embedding the secret message (possibly encrypted). Wendy has no knowledge about the secret key that Alice and Bob share, although she is aware of the algorithm that they could be employing for embedding messages.

The warden Wendy who is free to examine all messages exchanged between Alice and Bob can be passive or active Wendy should not be able to distinguish in any sense between cover-objects (objects not containing any secret message) and stego-objects (objects containing a secret message).

1.2 *Steganographic Security*

In steganography, unlike other forms of communications, one's awareness of the underlying communication between the sender and receiver defeats the whole purpose.

Therefore, the first requirement of a steganographic system is its undetectability. In other words, a steganographic system is considered to be insecure, if the warden Wendy is able to differentiate between cover- objects and stego-objects.

1.3. Steganographic Capacity

Steganographic capacity refers to the maximum amount (rate) of information that can be embedded into a cover-object and then can be reliably recovered from the stego-object (or a distorted version), under the constraints of undetectability, perceptual intactness and robustness, depending on whether Wendy is active or passive. Compared to data hiding systems, stego-systems have the added core requirement of undetectability. Therefore, the steganographic embedding operation needs to preserve the statistical properties of the cover-object, in addition to its perceptual quality. On the other hand, if Wendy suspects of a covert communication but cannot reliably make a decision, she may choose to modify the stego-object before delivering it. This setting of steganography very much resembles to data hiding problem, and corresponding results on data hiding capacity can be adapted to steganography.

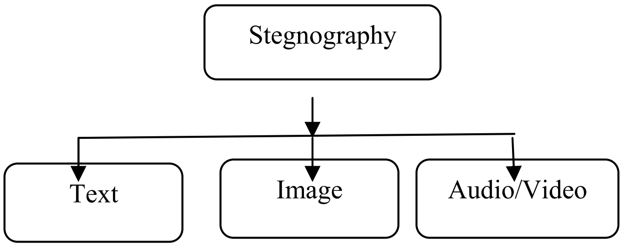


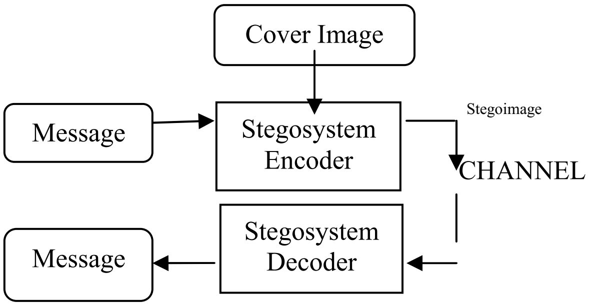
Figure 2.2 Categories of Steganography

1.4 Text Steganography

Hiding information in text is historically the most important method of Steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. It is only since the beginning of the internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data**.**

1.5 Image Steganography

Given the large amount of redundant bits present digital representation of an image, images are the most popular cover objects for steganography. This dissertation will focus on hiding information in images in the next sections.



1.6 Audio/Video Steganography

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganography potential, the larger size of meaningful audio files makes them less popular to use than images [17].

1.7 Steganography Attacks

Steganographic attacks consist of detecting, extracting and destroying hidden object of the stego media [49]. Steganography attack is followed by steganalysis. There are several types of attacks based on the information available for analysis. Some of them are as follows: -

- **Stego-only**, where the attacker has access only to the stego-image,
- **Known cover**, where the attacker has access only to the carrier,
- **Known message**, where the attacker has access only to the message,
- **Chosen stego**, where the attacker has access to both the stego-image and stego-algorithm, and
- **Chosen message**, where the attacker generates a stego-image from a message using an algorithm, looking for signatures that will enable him to detect other stego-images.

Steganography has applications in whenrever there is an intention to hide a message in a cover in a fashion that the existence of the message is not noticeable. The counter job of steganography is steganalysis where tries to find or estimate the hidden message communication. There are three conflicting conditions in steganography, i.e. imperceptibility, robustness, and capacity, with a compromising interrelation. A simple interpretation of this phenomenon is that the higher the volume of embedding data, the more vulnerability of stegomessage against different attack strategies will result in.

So two major steganography methods are spatial and transform domain based.

In spatial domain based steganography, there is one major approach is least significant bit (LSB).

- In the LSB method, the LSB of the cover message is replaced either one by one or randomly with next bit of the hidden message.
- The most popular transform-based steganography method is discrete cosine transform (DCT).In transform domain based steganography, the payload bits are hidden in the DCT coefficients.

1. *Techniques for Image Steganography*

Given the proliferation of digital images, and given the high degree of redundancy present in a digital representation of an image (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. There have been a number of image steganography algorithm proposed, these algorithm could be categorized in a number of ways. The different types of steganography techniques are substitution, transform domain, spread spectrum, statistical and distortion techniques and cover generation techniques.

2.1 *Substitution* techniques replace the least significant bits of each pixel in the cover file with bits from the secret document.

2.2 *Transform domain technique hides* secret information in the transform space (like frequency domain) by modifying the least significant coefficients of the cover file.

2.3 *Spread spectrum techniques* spread hidden information over different bandwidths. Even if parts of the message are removed from several bands, there would still be enough information present in other bands to recover the message.

2.4 *Statistical techniques* change several statistics of the cover file and then split it into blocks where each block is used to hide one message bit. The cover block is modified when message bit is ‘1’.

2.5 *Distortion techniques* exploit signal distortion to hide information. For example the sender applies a sequence of modifications to the cover file which corresponds to the secret information. Then the receiver measures the differences between the original cover and the distorted cover images to detect the sequence of modifications and consequently recover the secret message.

II. Proposed Algorithm

A. Existing Techniques

Various techniques for All Steganography are:

- ⦿ High Capacity LSB Coding (Least Substitution Bit) for data hiding.
- ⦿ Phase Coding.
- ⦿ Highly Robust Spread Spectrum Technique.
- ⦿ Echo Coding.

A.1 STEGANOGRAPHY TECHNIQUES

There are three techniques used for embedding information in a cover object (Weiss 2009:1): insertion, substitution and generation. Data insertion techniques hide data in sections of the file that are ignored by the processing application and the technique does not modify bits that are relevant to the end user.

Substitution-based techniques replace data from the cover medium with data from the secret mess This does not result in a larger cover file; however, depending on the cover medium and steganographic algorithm used, substitution may result in degrading the cover object (Fridrich 2010:55).

- ⦿ Generation techniques create a cover object specifically for the purpose of hiding the secret message. The properties of the generated cover object are usually dependent on secret message structure (Fridrich 2010:55).While insertion and substitution techniques can be discovered by comparing the stego object with the original object, generation techniques are immune to comparison tests since the result of a generation algorithm is the original object.

- Kipper (2003:39) identified a further six categories, namely substitution, transform domain, spread spectrum, statistical method, distortion and cover generation techniques. These six categories, can also fall within the three broader categories of steganography techniques. Kipper's six techniques can be merged with the original three categories resulting in Table

Table 2.1. Steganography technique categories

Technique	General categorisation	Explanation
Substitution system techniques	Substitution	Redundant bits from the cover object are replaced with bits from the secret message
Transform domain techniques	Substitution	Changes made to the cover object during compression, are used to hide information
Spread spectrum techniques	Substitution	The secret message is embedded in noise and then combined with the cover object
Statistical method techniques	Substitution	Only one bit is embedded in the cover object resulting in a statistical change
Distortion techniques	Insertion	A change in the cover object is created to hide information that can be recovered when comparing the changed object with the original
Cover generation techniques	Generation	A cover object is created for the purpose of hiding information

As illustrated in the table, substitution is the most popular technique. Substitution techniques do not add information to the cover object and thus do not increase the size of the object – a process that is easily detectable. However, the disadvantage of substitution is that the amount of data of the original object to replace needs to be carefully selected.If not carefully selected, the changes might become perceivable to someone looking for hidden information. Most steganographic algorithms implement substitution techniques. This dissertation thus focuses on substitution techniques in the discussion of image steganography algorithms done in chapter 5 since substitution techniques are the most studied steganography techniquestoday (Fridrich 2010:53).

- Categorising steganography based on the techniques used, is one approach. An alternative approach is to categorise steganography based on the types of digital files that are used as carriers for the embedded information. This approach to categorisation is examined next

B. Comparison of various techniques

Audio Steganographic algorithms are characterized by a few defining properties like Capacity, Transparency and Robustness. These properties are desirable to be achieved from any of the techniques used for information hiding.A few approaches provide capacity and lacks in robustness. Other provide high robustness and lacks capacity. Plus, imperceptibility is the desired feature expected from all[4]. These are discussed as:

Approach	Summary	Advantage & Disadvantage
LSB Coding	LSB is considered as the easiest technique in implemented in information hiding of digital audio. LSB Coding can be done by simply replacing the LSB of each sampling point by hidden data.	Advantages: 1. Low computational complexity of the algorithm compared with others techniques. 2. High payload And disadvantage: 1. Low robustness, due to the fact that the random changes of the LSB degrades the audio quality.
Phase Coding	Phase Coding works by substituting the phase of an initial audio segment with a reference phase , this phase represents the hidden data.	Advantage: 1.Basic technique And disadvantages: 1.Phase coding method is a low payload 2.The message is not dispersed over the entire data set available, but is implicitly localized and can thus be removed easily by the attackers.
Spread Spectrum Technique	Spread spectrum (SS) is technique designed to encode any stream of information via spreading the encoded data across as much of the frequency spectrum as possible. even though, there is interference on some frequencies, SS allows the signal reception.	Advantage: 1.Difficult to detect and/or remove a signal. 2.Provide a considerable level of robustness And disadvantage: Spread spectrum technique used transform functions with appropriated inverse transform function, which can cause a delay.

Echo Coding	Echo technique embeds data into a host audio signal by introducing an echo; the hidden data can be adjusted by the two parameters: amplitude and offset, the two parameters represent the magnitude and time delay for the embedded echo, respectively.	Advantage: The main advantage of echo hiding is that the echo detection technique is easy to implement. And disadvantage: Echo hiding is also prone to inevitable mistakes, such as the echo from the host signal itself may be treated as the embedded echo.

Table 2.1. Comparision of various techniques for All Steganography

3.4 Ri JANDEAL ALGORITHM APPROACH

Design Goals

A major design-objective of all the operations in AES is performance. High performance was the main, distinguishing reason for Rijndael to be chosen by the NIST. Additionally to performance, a lot of other properties were considered for the various parts of the encryption process. The design goals where described by Rijmen and Daemen in [13].

General Design Goals

As a matter of fact, performance should only be a secondary feature of a cipher, in other words it should be as fast as possible, but no faster. Other general design goals are resistance against (all) known cryptanalytic attacks in such a way, that any such attack is not faster than a brute-force attack on the cipher.

Rijmen and Daemen name the following design goals:

- Security
- Efficiency
- Key Agility
- Versatility
- Simplicity
- Symmetry

Security and efficiency are self-explaining. Usually they are opposing each other and it is the primary task to find a balance between them. Versatility is the notion of not depending on a single kind of hardware. A versatile cipher can be implemented on many different platforms, on 8 Bit systems as well as on 32 Bit hardware, in such a way that it can use as many features of powerful hardware, but also works efficiently on weak hardware. Key Agility is an untypical term, it refers to the fast creation of expanded key material from the key, so that the cipher also works well in systems with fast-changing keys.

The notion of simplicity refers to the ease of understanding and implementing the cipher. AES uses a very limited number of operations, of which only one is influenced by the key material. The rounds of AES are equal except for the final round, and most operations can be implemented using pre-calculated lookup-tables (as shown in the public-domain implementation by Rijmen and Daemen, the SubBytes, ShiftRows and MixColumns operations can be combined by using several lookup-tables).

The symmetry appears in several parts of the design of AES. Aside of the final round, all rounds are equal. All bits are treated equal during each round as well, in difference to Feistel Ciphers [O1]. One of the few points that contradict this philosophy is that AES is not self-inverse. Contrary to Feistel Ciphers, applying the AES encryption with the reverse key schedule does not result in decryption of the ciphertext.

S-Box Design

The SubBytes operation that represents a Substitution Box (S-Box) was designed with the following considerations:

- Non-Linearity
  - The correlation between input- and output-data should be as small as possible
  - The difference propagation probability should be as small as possible (helps against differential attacks)
- High Algebraic Complexity

The S-Box used in AES is depends only on the values of the individual 8 Bit cells in the state. It does not depend on the key, nor is it position-dependent. The non-linearity and the high algebraic complexity are introduced to defend linear and differential cryptanalysis and should make prevent interpolation attacks in general.

The ShiftRows Design

The ShiftRows transformation (especially in combination with the MixColumns operation) introduces the necessary diffusion. Therefore it was designed to provide optimal diffusion by using different shifting offsets for all rows. The second design goal was to reduce the efficiency of saturation- and truncated differential attacks.

The Mix Columns Design

As this step in one of the two steps used to introduce diffusion, the diffusion power is a main design goal of this step. As the S-Box already introduces the necessary non-linearity, the MixColumns operation should be linear. The efficiency, especially on 8 Bit systems, is another important design goal.

The diffusion is achieved in combination with the ShiftRows step. In AES, full diffusion (every input bit influences every output bit with a probability of 1/2) is achieved every two rounds.

The operation is linear, which makes it easy to understand and implement. It also makes it efficient without giving up on security, because one non-linear step during each round should be sufficient.

The MixColumns step is based on several multiplications and additions of 8 Bit numbers. Therefore, implementing it on 8 Bit systems poses no problem.

The Key Schedule and Add Round Key Design

The key schedule consists of two steps, the key expansion and the key selection. The key expansion step was built with performance and low memory consumption in mind, as the AES should be compatible with 8 Bit hardware (e.g. for Smart Cards). It should eliminate symmetries in the key, which is achieved by the round constants Rcon. The other two design-criteria are to introduce a high level of diffusion into the key and to apply non-linear tranformations (the S-Box) on the key material. The last two properties of the key-schedule provide some resistance against analysis of key-differences (related key attacks).

The key schedule has the purpose of providing enough key material for all rounds in such a way, that attacks based on the round key become difficult. Aside from increasing the difficulty of related-key- and slide-attacks, it should also provide enough security in systems where the full key or parts of it are known to the attacker, which is the case in hash functions.

Key expansion is realised as a recursive function based on the previous round-key. This means the amount of memory for storing the round-key (if it is computet on-the-fly) is N_b * 4 + 4 bytes, where the last 4 bytes represent the next round-key word calculated out of the corresponding word from the previous round-key.

3.5 Encryption Steps Overview

The Rijndael algorithm N_r consecutive rounds, each operating on the intermediate result (the state) of the previous round). Before the first round, The round-key is added to the state. The last round is different in that it skips the column mixing step.

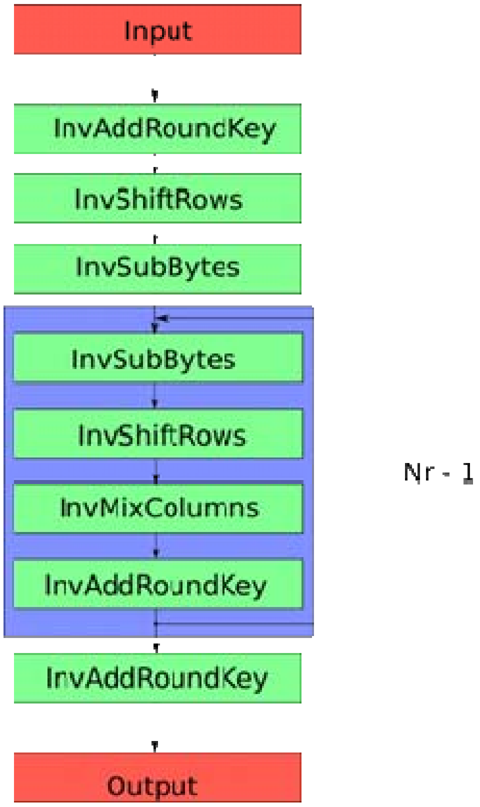
Rijndael Encryption Round	
01	Byte Substitution (SubBytes)]]
02	Row Shifting (ShiftRows)]]
03	Column Mixing (MixColumns)]]
04	Adding Round Key (AddRoundKeys)]]

3.2 Data Encryption Table

Since the number of rounds is N_r ($N_r - 1$ rounds plus the final round) and round-key addition is done during each round, as well as before the first round, N_r blocks of expanded key data are necessary. Creation of the expanded key material is explained in the section about the Key Schedule.

3.6 Decryption Steps Overview

The decryption consists of the inverse application of the inverted encryption steps (InvSubBytes, InvShiftRows, InvMixColumns, InvAddRoundKey):



3.1 Diagram For Data Decryption

The inverse function of AddRoundKey and ShiftRows are trivial, since the + operator in $GF(2^8)$ is self-inverting and the inverse of a left-rotation by N elements is the right-rotation by N elements.

The inverse function to the SubBytes operation can be found by applying the inverse affine transformation and finding the multiplicative inverse. The inverse transformation is represented by the following matrix multiplication:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \text{X} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

3.3 Decryption Table

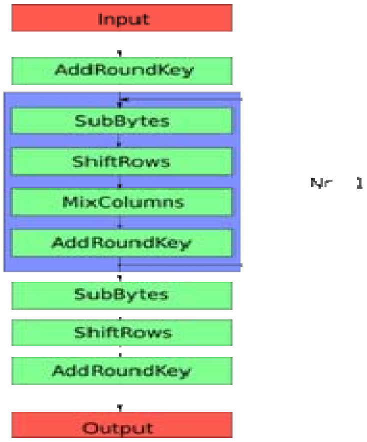
The multiplicative inverse can be found as explained in $GF(2^8)$. A much faster and easier way is to use a lookup-table here as well. The table can be initialised at the same time when the forward substitution table is created, as the substitution table values are $S_i = SubByte(i)$ and the inverse substitution values are $S_{S_i}^{-1} = i$.

The last operation that needs to be inverted is the MixColumn operation. It can be represented as multiplying each individual column with the inverse polynomial or inverse matrix. The inverse polynomial is $d(x) = 11 * x^3 + 13 * x^2 + 9 * x^1 + 4 * x^0$ and results in the following matrix multiplication:

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 09 \\ 09 & 14 & 11 & 13 \\ 13 & 09 & 14 & 11 \\ 11 & 13 & 09 & 14 \end{bmatrix} \text{X} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

3.4 Multiplication Inverse Table

3.7 OUTLINE OF RI JANDEAL ALGORITHM



3.2 Ri Jandeal Steps Diagram

3.8 Conclusion from Review of Literature & Problem Formulation

From the literature review, it can be summarized as although only some of the steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in audio. All the major steganographic techniques have their own different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the Spread Spectrum Steganography approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. On the other hand, LSB approach towards data hiding in audio provides a least robust method but at the same time it also provides a large capacity.
It is not achievable to get a high robust and high payload technique at the same time in the steganography. Hence, if it is desirable to get a robust one then its payload will be low and vice versa, a steganographic algorithm with high payload will be fragile. Plus, not all the applications require for the same robust feature to be supported. Such algorithms are called as fragile algorithms.
So, as to go for a robust technique, a modification can be done in the LSB approach of Audio Steganography and going for the Genetic Based Approach Toward Steganography Substitution Technique. Plus, the quality is measured by psnr As such by increasing psnr, quality would be better. In another sensible view, the quality is measured by imperceptibility. Thus getting noise more imperceptible, quality would be better.

5.3. OBJECTIVES:

1) Study the various steganography techniques.
2) we are implementing RSA algorithm to hide multiple data with multiple steganography
3) Verifying with already existing techniques.

5.4. Steganography Applications

Steganography is employed in various useful applications, e.g.

1. copyright control of materials,
2. Enhancing robustness of image search engines.
3. Smart IDs (identity cards) where individuals' details are embedded in their photographs.

Other applications are:

- video-audio synchronization,
- companies' safe circulation of secret data, TV broadcasting,
- TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network

Traffic of particular users, and checksum embedding.

A. Object/Project Snapshot

This is the first screen which has three tab options – is Image, Audio & Video for steganography. In right – top panel is displays the information about the image for encrypt & decrypt the data.

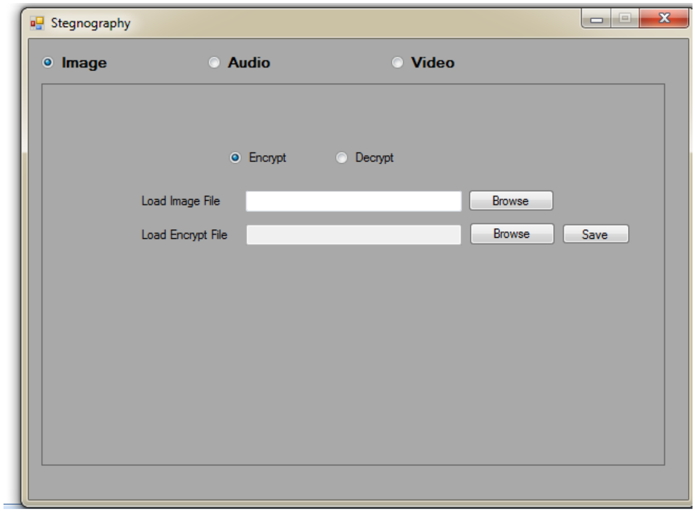


Fig 7.1 Steganography in Image

This is the second screen for Audio Steganography. In the mid we choose the audio steganography for data hiding. The image shows the option for audio file and encrypt it and decrypt it and the data to be hide into the audio file.

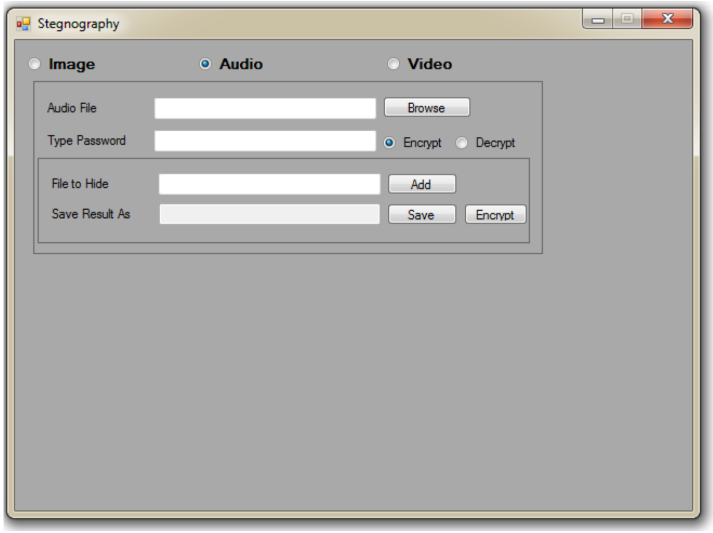
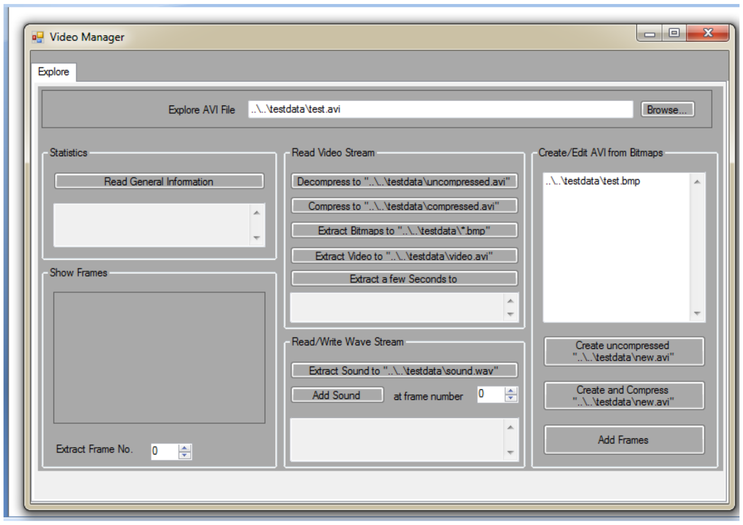


Fig 7.2 Steganography in Audio


Video Manager
Explore
Browse...
Statistics
Read General Information
Show Frames
Read Video Stream
Decompress to "..\..\testdata\uncompressed.avi"
Compress to "..\..\testdata\compressed.avi"
Extract Bitmaps to "..\..\testdata*.bmp"
Extract Video to "..\..\testdata\video.avi"
Extract a few Seconds to
Read/Write Wave Stream
Extract Sound to "..\..\testdata\sound.wav"
Add Sound
Create/Edit AVI from Bitmaps
Create uncompressed "..\..\testdata\new.avi"
Create and Compress "..\..\testdata\new.avi"
Add Frames

Explore AVI File ..\..\testdata\test.avi

..\..\testdata\test.bmp

at frame number 0

Extract Frame No. 0

Fig 7.3 Steganography in Video

At first, the cover image of any format is chosen because we can hide our message in any image formats.

B. Encryption Process As Image As a Cover

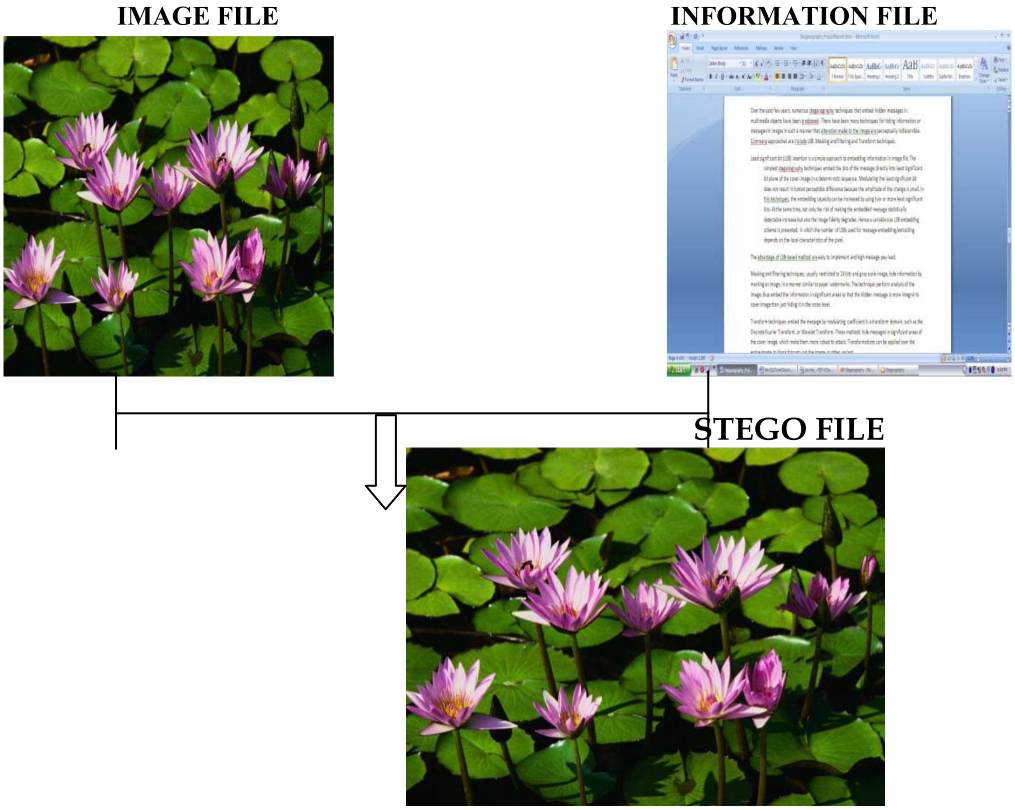
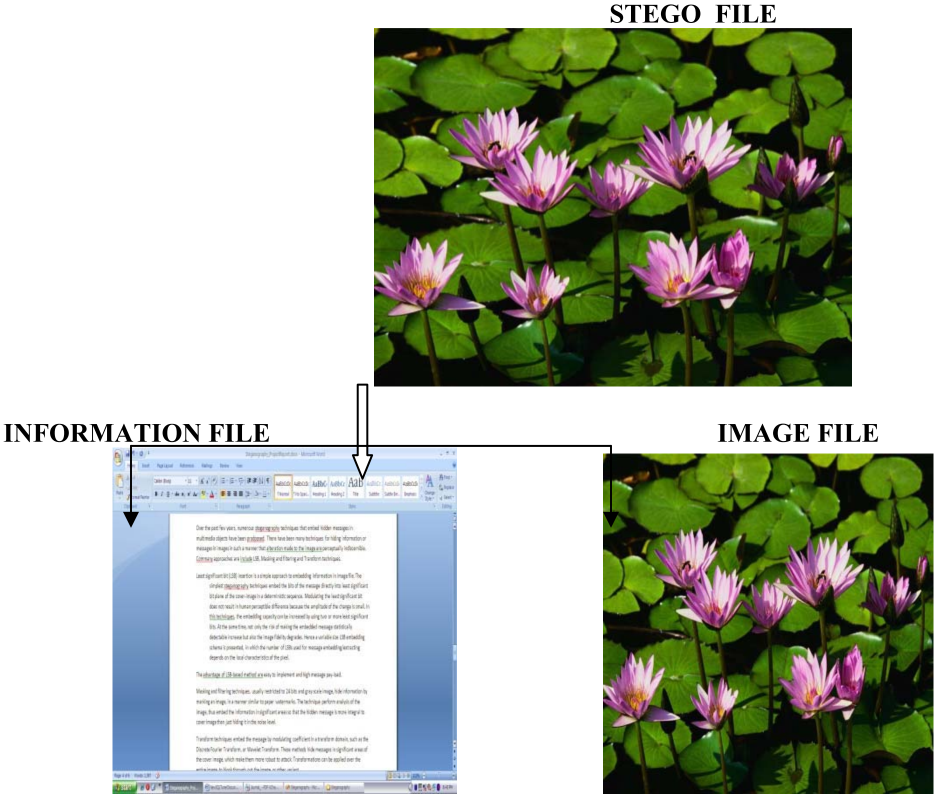


Fig 7.4 Encryption in Image Steganography

This diagram shows how information is hide into the image file. After providing the image as a cover file we obtained a new image into which our information is hide which is called stego file. This is done with the help of data encryption.

C. Decryption Process In Image Steganography



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 are perceptually indiscernible. Commany approaches are include LSB, Masking and filtering and Transform techniques.

Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this techniques, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel.

The advantage of LSB-based method are easy to implement and high message pay-load.

Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block through out the image, or other variant.

Fig 7.5 Dcryption in Image Steganography

At the receiver side we decrypt the imge. With the help of steganalysis we seprate the cover image and the information file.

D. Steganography In Audio

At first, the cover audio file format that is chosen is WAVE audio file format because this format is original of all the formats.

Figure 7.6 Wave Audio

Now,initially the cover audio file is played.

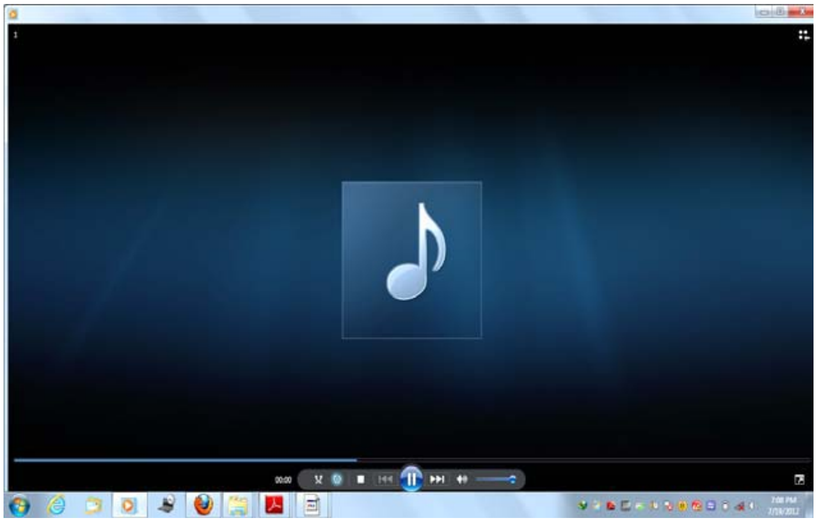
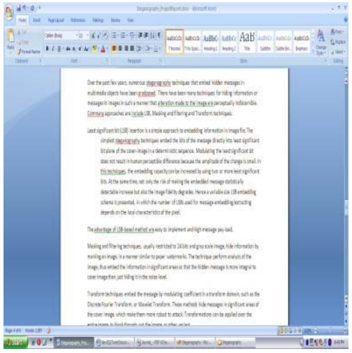


Figure 7.7 Input played

And the signal is analyzed in .NET using the function Waveread and the plot is obtained as:



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 are perceptually indiscernible. Commany approaches are include LSB, Masking and filtering and Transform techniques.

Least significant bit (LSB) insertion is a simple approach to embedding information in image file. The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this techniques, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel.

The advantage of LSB-based method are easy to implement and high message pay-load.

Masking and filtering techniques, usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. The technique perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variant

Figure 7.8 Secret Message

Now, after embedding the secret message the Stego Audio is obtained in output and again the plot for the Audio, this time the Stego Audio is obtained.
And, the output i.e. the Stego Audio is played.

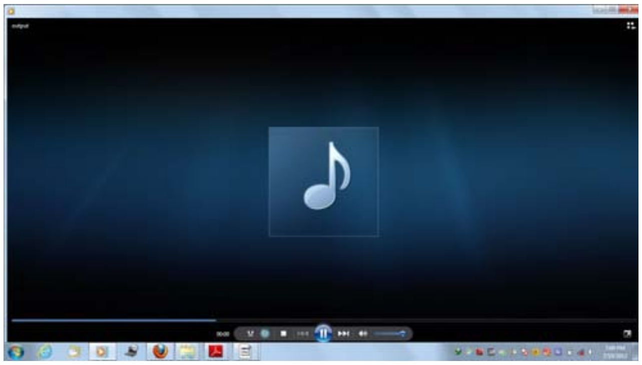


Figure 7.9 Stego Audio played

IV. Conclusion

In previous technique we are just using only Steganography in image or Steganography in audio. But here the challenge is that we used both Steganography and also Steganography in video integrated in single Steganography we can hide our text using image, audio & video using a single techniques.

A. Need for The Proposed Research Work:

The past few years have seen an increasing interest in using images as cover media for steganographic communication. There have been a multitude of public domain tools, many being ad-hoc and naive, available for image based steganography. Given this fact, detection of covert communications that utilize images has become an important issue. In this research work, some fundamental notions related to steganography are going to be reviewed.

As a number of security and capacity and robustness definitions are being covered, there has been no work successfully formulating the relationship between the two from the practical point of view. For example it is understood that as less information is embedded in a cover-object the more secure the system will be. But due to difficulties in statistical modeling of image features, the security versus capacity trade-off has not been theoretically explored and quantified within an analytical framework.

In previous technique we are just using only steganography in image or steganography in audio. But here the challenge is that we used both steganography integrated in single steganography.

B. Significance of the Proposed Research Work:

Steganography methods usually struggle with achieving a high embedding rate. As an alternative channel to images, video files have many excellent features for information hiding such as large capacity and good imperceptibility. The challenge, however, is to be able to embed into a group of multiple data which are highly intercorrelated and often manipulated in a compressed form. Steganography's ultimate objectives, which are undetectability, robustness and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Robustness of steganography is one of the three main goals to be achieved. Robustness is a kind of attack that would "destroy the embedded evidence" which is generally called image tampering. Robustness is a practical requirement for a steganography system. "Many steganography systems are designed to be robust against a specific class of mapping." It is also rational to create an undetectable steganography algorithm that is capable of resisting common image processing manipulations that might occur by accident and not necessarily via an attack.

REFERENCES

[1] Y. K. Lee and L. H. Chen, "High Capacity Image Steganographic Model," IEEE Proceedings – Vision, Image, and signal processing, vol.147, No. 3, June 2000, pp. 288-294.

[2] N. Rajpal, A. Kumar, S. Dudhani and P. R. Jindal, "Copyright Protection Using Non Linear Forward feedback Shift Register and Error correction technique," 7th Annual International conference Map India 2004, pp. , New Delhi, India, January 2004.

[3] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon, "Data masking: A secure covert channel paradigm," IEEE Multimedia Signal Processing, St Thomas, US Virgin Islands, 2002.

[4] L. Marvel, C. Boncelet and C. Retter, "Spread Spectrum Image Steganography",IEEE Trans on Image Processing, vol. 8, no. 8, pp.1075-1083, 1999.

[5] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis of Spread Spectrum Data Hiding Exploiting Cover the International Society for Optical Engineering, Electronic Imaging, San Jose, CA, USA, 2005.

[6] T. Sharp, "Hide 2.1, 2001," http://www.sharpthoughts.org.

[7] Steganography and Digital Watermarking http://www.jjtc.com/Steganography

[8] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "Digital Image Steganography: Survey and Analysis of Current Methods", 1992