CHAPTER 1

1. INTRODUCTION

Image hiding techniques embed a secret image into another image. The combination of the secret image and the cover image is the resultant stego image. Using the image hiding techniques, existence of the secret image in the final image will be unaware by an unintended observer, so that it can be transferred carefully. Internet has become more popular and common now-a-days. Sending important data through the net has become a serious threat. Moreover sending the data in an encrypted format is very common and embedding the secret message in an image is a challenge. To safeguard the images from the illegal prevention or interference, techniques such as image hiding is used for the safe transmission of images.

Steganography is one of the strategies utilized for the concealed trade of data and it can be characterized as the analysis of undetectable communication that normally manages the method for concealing the presence of the communicated message. Steganography is the art and science of invisible communication by hiding secret information into other sources of information like text, video, audio, image etc. In image steganography the digital image is used as cover image in which we hide data and the message implanted image is called stego-image.

This part is talking about the history of Steganography and how it was developed subsequent to its ordinary early stages. Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties. After that, examine what sorts of Steganography are being used today, and where and how they are continuously utilized.

The conquest of this framework was the path in which to recover the masked message. With a specific end goal to read the message, all you needed to do was hold it up to a light and the ink shined. Along these lines, if the adversary blocked the letter and simply so happened to read the letter with a light behind it, would effectively see the secret message. There is no report on exactly how fruitful this method truly was amid that war.

An alternate wartime procedure utilized was the fence framework. This strategy included deliberately setting letters inside an apparently common content. The secret message was sent

and afterward the recipient was just ready to see the secret message by utilizing a unique fence. The fence was simply a chunk of wood that would fit over the message.

1.1 Motivation

In this modern era computers and internet are major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However the safety and security of long distance communications remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security particularly when it is combined with encryption.

1.2 Problem outline

Steganography is the technique of hiding confidential information within any media. This work deals with steganography based secret image sharing in which secret image is embedded into cover image using Eigen vectors and Eigen values relying upon the secret key. Therefore it is hard to concentrate the concealed data knowing the recovery systems. We have used peak signal to noise ratio (PSNR) to measure the quality of stego images. The quality of stego image can be measured in terms of other standard parameters like average difference, mean square error, normalized absolute error, normalized cross correlation coefficient and structural content. These standard parameters gave better results when compared with existing methods.

1.3 Objective

The main objectives of this work are safety and security of the data. This is particularly important when it is confidential data. Steganography is one of the techniques that provide high range of security by simply hiding the existence of communicated message in terms of digital mediums like text, image, audio and feature. Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the way of hiding the existence of the communicated message. In this way, if successfully it is achieved the message does not attract attention from eaves droppers and attackers.

1.4 Thesis outline

Chapter 2 presents the basic knowledge about the different data hiding techniques. Chapter 3 gives Literature survey, which is useful to know about the existing methods and their advantages and disadvantages. Chapter 4 introduces the baseline method. Chapter 5 explains the complete workflow of proposed method and finally, in Chapter 6 the experimental results and in Chapter 7 result analysis is presented. Conclusions and Future work are also presented.

1.5 Comparison among steganography, cryptography and watermarking

Cryptography

Cryptography is an approach of addressing secured message transmission, deals with the study of sending messages in hidden form. It enables only the intended readers to decrypt the hidden message with the help of key.

1. Method for transform Plain Text to Cipher Text:

All encryption calculations are focused around two huge belief systems: substitution, in which every element in the plaintext is mapped into an alternate element, and transposition, in which elements in the plaintext [1] are revised. The major necessity is that no data be lost.

2. Method for number of keys used:

There are some standard methods which are used with cryptography such as secret key, public key, digital signature and hash function.

Secret Key: With secret key cryptography, a solitary key is utilized for both encryption [2] and decrypting. The sender utilizes the way to scramble the plaintext and sends the figure content to the collector. The recipient applies the same key to decode the message and recoup the plaintext. Since a private key is utilized for both capacities, secret key cryptography is likewise called as symmetric encryption.

Public Key: Open key cryptography has been said to be the most noteworthy new improvement in cryptography in the last 300-400 years. Cutting edge Public Key Cryptography was initially illustrated. Openly by Stanford University instructor Martin Hellman and graduate understudy Whitfield Diffie in 1976. Their study portrayed a two-key crypto structure in which two gatherings could take part in a protected correspondence over a delicate interchanges channel without needing to impart a secret key.

Advanced Signature: The utilization of computerized mark originated from the need of guaranteeing the confirmation. The computerized mark is more like stamp or signature of the sender which is inserted together with the information and encodes it with the private enter to

send it to the next gathering. What's more, the mark guarantees that any change made to the information that has been marked is not difficult to identify by the collector.

Hash Function: The hash capacity [3] is a restricted encryption, the hash capacity is a generally characterized methodology or numerical recipe that speaks to a little size of bits which is produced from a considerable estimated document, the consequence of this capacity can be called hash code or hashes. The creating of hash code is quicker than different routines which make it more wanted for validation and trustworthiness.

Cryptographic hash capacities are highly utilized for advanced signature and shabby developments are very attractive. The utilization of cryptographic hash capacities for message validation has turned into a standard approach in numerous applications, especially web security protocols.

The verification and the honesty considered as primary issues in data security, the hash code can be connected to the first document then whenever the clients have the capacity check the validation and uprightness in the wake of sending the protected information by applying the hash capacity to the message again and contrast the result with the sender hash code, in the event that its comparable that is mean the message originated from the first sender without modifying in light of the fact that if there is any changed has been made to the information will changed the hash code at the beneficiary side.

3. Methodology for processing plain text:

A piece figure forms the info one square of components at once, delivering a yield obstruct for each one data piece. A stream figure forms the info components consistently, creating yield one component at once, as it comes. The proposed calculation utilizes a substitution figure strategy. It is a symmetric key calculation utilizing the procedure of stream figure.

1.6 Recent Approaches of Steganography

The common recent approaches of steganography explain the property of the media itself to convey a message.

The following media are the candidate for digitally embedding message: -

- Ordinary data
- Digital images
- Feature and Sound
- Datagram (IP)

1.6.1 Plaintext steganography

In this system the information is covered up inside an ordinary content document utilizing distinctive plans like utilization of chose characters, additional white spaces of the cover content and so forth [4].

How to use selected characters of cover Text:

Sender sends an arrangement of number (Key) to the receiver with a former declaration that the secret message is covered up inside the particular position of ensuing expressions of the spread content. Case in point the arrangement is '1, 2, 2, 3, 4, 2, 4,' and the spread content is "A group of five men joined today". So the masked message is "Behind ova". A "0" in the number arrangement will show a clear space in the recovered information. The message in the got spread content will be skipped if the quantity of characters in that expression is short of what the individual number in the arrangement (Key) which should likewise be skipped amid the methodology of information unhide.

How to use extra blank space characters of cover text:

Various additional white spaces are embedded between sequential expressions of cover content. This numbers are mapped to a cover message through a record of a lookup table. In case in point addition two spaces between nearby words show the number "2" which along these lines demonstrates a particular content of a look-up table which is accessible to the both imparting gatherings as an earlier assertion.

1.6.2 Digital image steganography

The most broadly utilized strategy today is packing away secret messages into a computerized picture. This steganography strategy misuses the shortcoming of the human visual framework (HVS). HVS can't identify the variety in luminance of colour [5] vectors at higher recurrence side of the visual range. A picture can be spoken to by an accumulation of colour pixels. Each of these qualities can be digitally communicated regarding parallel digits.

Case in point: a 24-bit bitmap will have 8 bits, speaking to each of the three-color qualities (red, green, and blue) at every pixel. On the off chance that we consider simply the red there will be 28 separate estimations of blue. The distinction somewhere around 11111111 and 11111110 in the worth for blue power is prone to be imperceptible by the human eye. Consequently, if the terminal beneficiary of the information is only human visual framework (HVS) then the Least Significant Bit (LSB) can be utilized for something else other than shade

data. This procedure can be specifically connected on advanced picture in bitmap organize and additionally for the packed picture arrangement like JPEG. In JPEG group, every pixel of the picture is digitally coded utilizing discrete cosine change (DCT). The LSB of encoded DCT parts can be utilized as the bearers of the shrouded message. Images are used as a popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

1.6.3 Sound and Feature Steganography

In sound steganography, mysterious information is installed into digitized sound signal which come about slight changing of double succession of the comparing sound document. There are a few procedures are accessible for sound Steganography. Some of them are as per the following:

- LSB Coding
- Phase Coding
- Echo coding

1.6.4 IP datagram Steganography

This is an alternate methodology of Steganography, which utilizes concealing information in the system datagram level in a TCP/IP based system like Internet. TCP/IP is a definitive model for information correspondence. System Covert Channel is the equivalent word of system steganography. General objective of this methodology is to make the stego datagram imperceptible by Network watchers like sniffer, Intrusion Detection System (IDS) and so on. In this methodology data to be stow away is set in the IP header of a TCP/IP datagram. A portion of the fields of IP header and TCP header in an Ipv4 system are picked for information stowing.

1.7 Steganalysis Techniques

The specifications of media are constantly altered in the wake of concealing any item into that. This can bring about the manifestation of corruption regarding quality or irregular qualities of the media Steganalysis strategies focused around surprising example in the media or Visual Detection of the same. For instance on account of Network Steganography uncommon example is presented in the TCP/IP parcel header. In a event that the parcel examination system for Intrusion Detection System of a system is focused around white rundown design (common example), then this strategy for system steganography can be crushed. On account of Visual discovery Steganalysis procedure a set of stego pictures are contrasted and unique cover pictures and note the obvious distinction. Signature of the concealed message can be inferred by contrasting various pictures. Editing or cushioning of picture additionally is a visual hint of concealed message on the grounds that some stego tool is trimming or cushioning clear spaces to fit the stego picture into settled size. Distinction in record estimate between cover picture and stego pictures, expand or lessening of novel colours in stego pictures can likewise be utilized as a part of the Visual Detection Steganalysis system.

1.8 Steganography Vs Cryptography

In cryptography, the framework is broken when the aggressor can examine the secret information. Decoding a Steganographic framework needs the aggressor to identify that steganography has been utilized and he finds himself able to peruse the inserted message [6].

What's more, the security of established steganography framework depends on mystery of the information encoding framework. When the encoding framework is known, the steganography framework is crushed.

The refinement in the middle of cryptography and steganography is a critical one, and is condensed by the accompanying table 1.

Table 1: Comparison of Steganography and Cryptography

Steganography	Cryptography
Unknown message transitory	Known message transitory
Steganography prevents unearthing of the incredibly subsistence of communication	Encryption prevents an unconstitutional from discovering the stuffing of a communication.
petite notorious technology	widespread knowledge
Technology still being developed for certain formats	Most of algorithm known by all
Once detected memorandum is well-known	Strong currently algorithms are presently opposed to attack, outsized high-priced computing authority is required for cracking.
Steganography does not amend the composition of the surreptitious message	Cryptography amend the composition of the surreptitious message

1.9 Steganography vs. Watermarking

Watermarking is utilized to confirm the character and legitimacy of the holder of a computerized picture. It is a methodology in which the data which checks the holder is implanted into the advanced picture or signal. These signals could be either features or pictures or sounds. For instance, celebrated specialists watermark their portraits and pictures. In the event that someone tries to duplicate the picture, the watermark is duplicated alongside the picture. Watermarking is of two sorts

1. Discernible watermarking
2. Indiscernible watermarking

1. Discernible Watermarking

As the name recommends, unmistakable watermarking alludes to the data noticeable on the picture or feature or picture. Obvious watermarks are regularly logos or content. Case in point, in a TV show, the logo of the telecaster is noticeable at the right half of the screen.

2. Indiscernible Watermarking

Undetectable watermarking alludes to including data in a feature or picture or sound as advanced information. It is not noticeable or detectable, yet it can be identified by diverse means. It might likewise be a structure or sort of steganography and is utilized for boundless utilization. It can be recovered effortlessly.

Applications

- It is used for copyright protection.
- It is used for source tracing.
- Annotation of photographs

CHAPTER 2

3. GENERAL LITERATURE SURVEY

The primary objective of steganography is to convey safely in a totally imperceptible way and to abstain from attracting suspicion to the transmission of concealed information. Amid the procedure, qualities of these strategies are to change in the structure and peculiarities so as not to be identifiable by human eye.

Advanced pictures, features, sound documents, and other machine records that contain perceptually unimportant or repetitive data can be utilized as covers or bearers to shroud secret messages. In the wake of implanting a secret message into the cover-picture, an alleged stego image is gotten. The fundamental model of steganography comprises of Carrier, Message, Embedding calculation and Stego key. The model for steganography is indicated in Figure 1. Transporter is otherwise called a cover-object, which inserts the message and serves to conceal its vicinity.

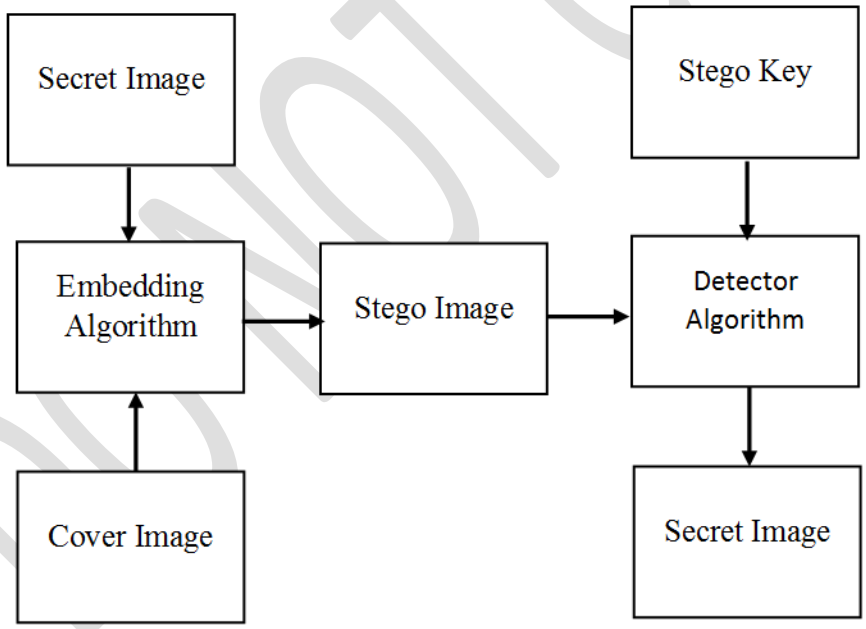

Figure 2.1 Model for Steganography

2.1 Basic Steganographic Techniques

This segment introduces some normal strategies utilized as a part of sound steganography. Figures and pseudo code are utilized as a part of spot of definite numerical recipes in endeavours to make the hypothesis more open to per users having simply an essential learning of steganography.

- **Substitution techniques:** surrogate redundant part of the cover-object with a secret information. These techniques are also called as spatial domain techniques [7].
- **Transform domain techniques:** entrench secret information in a transform space of the signal (e.g. in the frequency domain).
- **Spread spectrum techniques:** entrench secret information adopting ideas from spread spectrum communications.
- **Statistical techniques:** entrench information by changing some statistical properties of the cover-objects and use hypothesis-testing methods in the extraction process.
- **Distortion techniques**: store secret information by signal distortion and measure the deviation from the original cover in the extraction step.
- **Cover generation techniques:** do not entrench messages in randomly chosen cover-objects, but create covers that fit information that needs to be hidden.

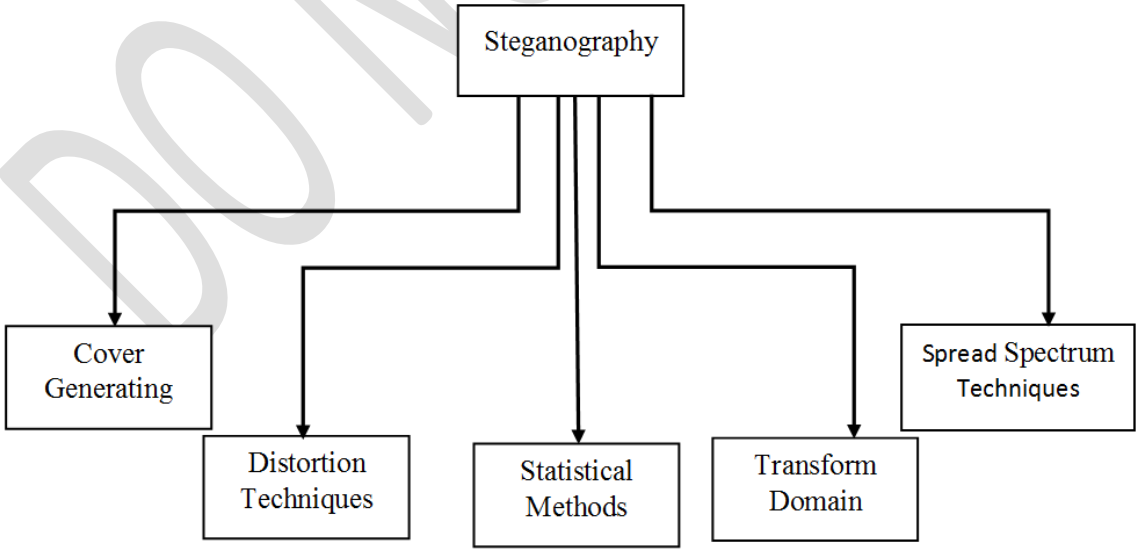

Figure 2.2 Basic Steganographic techniques

Distinguishing Steganography

As more procedures of concealing data are produced and enhanced, the techniques for discovering the utilization of steganography likewise progress. Most steganography methods include changing properties of the cover source and there are a few methods for discovering these progressions.

Text

While data can be covered up inside writings in such a path, to the point that the vicinity of the message must be recognized with information of the secret key, for instance when utilizing the prior specified system utilizing a freely accessible book and a mix of character positions to conceal the message, the vast majority of the systems include alterations to the cover source. These alterations can be caught by searching for examples in writings or disturbing thereof.

Images

In spite of the fact that pictures can be checked for suspicious properties in an extremely fundamental manner, discovering concealed messages normally obliges a more specialized methodology. Changes in size, record arrangement, last adjusted timestamp and in the colour palette may bring up the presence of a concealed message, yet this won't generally be the situation.

A broadly utilized method for picture filtering includes factual examination. Most Steganographic calculations that work on pictures, expect that the minimum noteworthy bit is pretty much irregular. This is nonetheless, a wrong supposition. While the LSB may not appear to be of much significance, applying a channel which just demonstrates the slightest huge bits will at present create a conspicuous picture. Since this is the situation, it can be presumed that the LSB are not irregular whatsoever, regardless contain data about the entire picture. At the point when embedding a shrouded message into a picture, this property changes. Particularly with scrambled information, which has high entropy, the LSB of the cover picture will no more contain data about the first, but since of the alterations they will now be pretty much irregular.

With a measurable investigation on the LSB, the contrast between arbitrary qualities and true picture qualities can undoubtedly be located. Utilizing this method, it is likewise conceivable to identify messages stowed away inside JPEG records with the DCT strategy, since this additionally includes LSB changes, despite the fact that these happen in the recurrence space.

Audio and feature

The method can be applied on sound records too, since the LSB adjustment method can be utilized on sounds too. With the exception of this, there are a few different things that can be recognized. High, imperceptible frequencies can be filtered for data and odd distortions or examples in the sounds may bring up the presence of a secret message. Additionally, contrasts in pitch, resound or foundation noise may raise suspicion.

Like executing steganography utilizing feature records as cover sources, the techniques for catching concealed data are additionally a consolidation of procedures utilized for pictures and sound documents. On the other hand, an alternate steganographic method can be utilized that is particularly powerful when utilized as a part of feature movies. The use of extraordinary code signs or motions is extremely hard to identify with a machine framework. This system was utilized as a part of the Vietnam War so detainees of war could impart messages secretly through the feature movies the adversary fighters made to send to the home front.

2.2 Defeating Steganograms

The most ideal method for expelling concealed messages from a plain content may be revamping and reformulating the substance. Revamping it utilizing diverse words and sentence developments will definitely uproot all methods for imitating a concealed message, since it will deal with practically every conceivable way information can be stored inside a plain content. The character position will no longer work on the grounds that the words have been changed, and the same is legitimate for the differentiations in white dispersing, since the content will have another design.

The main system that won't be covered by this method is the utilization of a freely accessible cover source.

2.2.1 Text

The most ideal method for expelling concealed messages from a plain content may be revamping and reformulating the substance. Modifying it utilizing diverse words and sentence developments will definitely evacuate all methods for repeating a shrouded message, since it will deal with just about every conceivable way information can be put away inside a plain content. The character position plans will no more work on the grounds that the words have

been changed, and the same is legitimate for the separations in white separating, since the content will have another design [8].

The only scheme that will not be covered by this system is the usage of an openly available cover source.

2.2.2 Images

Layering a picture utilizing lossy clamping will evacuate messages that are concealed utilizing the LSB alteration system. This will likewise happen when the picture is resized, the shade palette is adjusted or the colours themselves are altered. Change to an alternate picture position, which frequently utilizes an alternate sort of packing, will likewise help in uprooting concealed messages. Also modifying the luminescence for instance, will uproot watermarks in the obvious piece of a picture.

2.2.3 Audio and feature

The greater part of the strategies that can be utilized on pictures can likewise be connected on sound documents. Packing a sound record with lossy layering will bring about loss of the shrouded message as it will change the entire structure of a document. Additionally, a few lossy packing plans utilize the cut off points of the human ear further bolstering their good fortune by evacuating all frequencies that can't be listened. This will likewise uproot any frequencies that are utilized by a Steganographic framework which conceals data in that piece of the range.

An alternate conceivable method for uprooting steganograms is bringing down the bit rate of the sound document. All things considered, there will be less accessible space to store shrouded information and in this way; at any rate parts of it will get lost [9].

For feature, yet again once more, the same strategies with respect to pictures and sound documents can be connected to uproot concealed data. To thrashing the utilization of signals or motions nonetheless, human knowledge is still necessary, as machine frameworks are not yet fit for recognizing this with a sensible rate of achievement.

2.3 STEGANOGRAPHIC PROTOCOLS

There are essentially three sorts of Steganographic protocols utilized.

- Pure Steganography - no key is utilized.
- Secret-key Steganography - secret key is utilized.
- Public-key Steganography - open key is utilized.

Pure Steganography

It is characterized as a steganographic framework that does not oblige the trade of a figure, for example, a stego-key [10]. This technique for Steganography is the slightest secure means by which to convey secretly in light of the fact that the sender and recipient can depend just upon the assumption that no different gatherings are mindful of this secret message. Utilizing open frameworks, for example, the Internet, we know this is not the situation whatsoever.

Secret Key Steganography

It is characterized as a steganographic framework that obliges the trade of a secret key (stego-key) preceding correspondence. Secret Key Steganography takes a cover message and inserts the secret message within it by utilizing a secret key (stego-key). Just the gatherings who know the secret key can invert the procedure and read the secret message. Not at all like Pure Steganography where an apparent imperceptible correspondence channel is available, has Secret Key Steganography traded a stego-key, which makes it more vulnerable to block attempt. The profit to Secret Key Steganography is regardless of the possibility that it is caught; just gatherings who know the secret key can remove the secret message.

Public Key Steganography

It takes the ideas from Public Key Cryptography as clarified underneath. Open Key Steganography is characterized as a steganographic framework that uses an open key and a private key to secure the correspondence between the gatherings needing to impart secretly. The sender will utilize general society key amid the encoding methodology and just the private key, which has an immediate scientific association with the general population key, can interpret the secret message. Open Key Steganography gives a more solid strategy for actualizing a steganographic framework on the grounds that it can use a considerably more powerful and looked into engineering in Public Key Cryptography. It furthermore has diverse levels of security in that undesirable get-togethers ought to first partner the use with

steganography and thereafter they would need to evaluate how to part the computation used by the all-inclusive community key structure before they could obstruct the mystery message

Applications

- Secure secret correspondences where cryptographic encryption systems are not accessible.
- Secure secret correspondence where solid cryptography is unimaginable..
- In a few cases, for instance in military applications, even the information that two gatherings impart can be of substantial vitality.
- The medicinal services, and particularly therapeutic imaging frameworks, might a whole lot advantage from data concealing strategies.
- Steganography is utilized as a part of present day printers.
- It is purportedly utilized by knowledge administrations.

CHAPTER 3

4. LITERATURE SURVEY IN PROBLEM DOMAIN

Ran-Zan Wang et al., proposed a method in 2005[11] tended for ensuring pictures that includes the scattering of the secret picture into numerous shadow pictures. This supplies a strategy with a higher tolerance against information debasement. This strategy has high security however the PSNR worth is low.

Keeping in mind the end goal to attain a high implanting limit with satisfactory stego quality, Mabolghasemi et al., in 2008 [12] proposed a technique. This strategy gives great PSNR esteem yet in this system recreated picture is discovered to be distorted.

Xian-ting Zeng et al., proposed a method in 2011 [13] tended to the reasonable usage of lossless information concealing plan. This plan is focused around pixel distinction histogram moving to extra space for the information covering up. Pixel contrasts are produced between a reference pixel and its neighbours in a preassigned piece. After the distinction histogram moving an expansive number of information can be inserted into the cover picture. PSNR quality is more contrasted with Ran-Zan Wang technique which is relevant to just concealing the data.

S.M. Masud Karim et al., proposed a method in 2011 [14]. This work presents a best approach for slightest noteworthy bit (LSB) on picture steganography that improves the current LSB substitution systems to enhance the security level of concealed data. This strategy gives great security issue and PSNR esteem than general LSB based picture steganography systems, yet here the disadvantage we need to send the secret key to recover the concealed data at recipient side.

Manoj Sharma et al., proposed a method in 2011 [15]. This work is effective of picture concealing which is focused around unitary comparability change including count of Eigen qualities and Eigen vectors and afterward changing it into an askew grid. It can incredibly enhance the security of the arrangement of the framework, power of picture covering up. Anyway here we need to send Eigen vector lattice as an unscrambling key to recover the secret at receiver.

Alaa A. Jabbar Altaay et al., proposed a method in 2012 [16]. It depicts steganography is a manifestation of security system through indistinct quality, the signs and craft of concealing the presence of a message in the middle of sender and planned beneficiary. This methodology great impeccability, payload and vigorous yet here the nature of stego is low when contrasted with Manoj Sharma et al., method.

Nadeem Akthar et al., proposed a method in 2013 [18] .This work is concerned with actualizing Steganography for pictures, with a change in both security and picture quality. The particular case that is executed here is the variety of plain LSB Algorithm. The stego picture quality if enhanced by utilizing bit reversal method. Here less number of Least Significant Bits is adjusted in examination to plain LSB technique enhancing the PSNR of stego image.

R Praveen Kumar et al., proposed a method in 2013[19].The change strategies create more noise in the picture when the data has been inserted. To maintain a strategic distance from the noise distortion in the picture the LSB insertion strategy is utilized to embed the bits in a picture by utilizing irregular number of generators. In this technique before installing the secret data into a picture the secret data has been layered utilizing the wavelet transform measures. Got bits after packing are encoded by utilizing quantum gates

Manoj Kumar Ramaiya et al., proposed a method in 2013[20]. This work is focused around the Data Encryption Standard (DES) utilizing 64 bit piece size of plain content and 56 bits of secret key. The pre-processing gives abnormal state of security as extraction of picture is impractical without the learning mapping tenets of S-Box and secret key of the capacity however here the downside of this technique is we need to utilize decoding key to recover the message at recipient. Subsequently there is an extension to lessen the 56 bit key to some lesser worth to get the best possible result.

Ekta Dagar et al., proposed a method in 2014 [17] .This work is a technique for disguising data into a cover picture to conceal it. It introduces a novel system for picture steganography focused around LSB utilizing X-Box mapping where they utilize a few X-Boxes having remarkable information. This mapping gives sufficient security to the payload yet PSNR quality is to a degree less when contrasted with Manoj Sharma et al., method.

.

CHAPTER 4

5. BASELINE METHOD

4.1 Problem statement and how it is related to society

In this contemporary epoch computers and web are significant correspondence media that join diverse parts of the world as one worldwide virtual world. Therefore, individuals can undoubtedly trade data and separation is no more a hindrance to correspondence. However the security and safety of long separation interchanges remains an issue. This is especially vital on account of private information. The need to take care of this issue has prompted the improvement of Steganography plans. Steganography is a capable security tool that gives an abnormal state of security especially when it is consolidated with encryption.

4.2 Reference work:

Embedding the secret data into the least significant bits (LSB) of the cover medium is the most frequently used technique known as the LSB embedding in the literature. Exploiting Modification Direction method is used to hide the shared values into covers. The method also utilizes modulus operator to recover original cover pixels. Stego image PSNR is approximately 47 dB for gray level covers. The method provides 4–7 dB increase respectively on the stego image quality compared to others. Stego images have also higher PSNR (43 dB) for dithered covers.

The method uses modulus operator to embed the shared values into cover images to improve the stego image quality according to traditional LSB embedding scheme. However, the modulus operator causes underflow and overflow for dithered images. On the other hand, embedding strategy based on modulus operator prevents the use of dithered images as cover images. Here use of Exploiting Modification Direction (EMD) method with a specially crafted equation to hide the shared values into cover images with less distortion according to LSB embedding. Using EMD during the embedding procedure ensures the visual quality of stego images independent from the intensity range of the cover images (dithered or grayscale) as shown in the experimental results.

In result PSNR of stego images are approximately 47 dB for gray level cover images and 43 dB for binary cover images. Improving secret capacity of the method without a loss in PSNR is considered as future work.

CHAPTER 5

6. PROPOSED METHOD

In this method we are embedding the diagonalized form of the blocks of secret image (which is to be achieved by Unitary Similarity Transformation) into the blocks of cover image. The eigenvector matrix used for transformation is transmitted and is used as decryption key. From the stego image received, the secret image could be obtained by using the eigen vector matrix of secret image. The idea of dividing the image into blocks has been taken from, "Triangular Algorithm of Image Hiding" [21].

5.1 Scheme Description

Here, for simplicity we are taking both (cover image and secret image) as 8-bit grayscale images. Here we are applying transformation only on secret image rather than on cover image. Let the cover and secret images are denoted by C and S respectively and are of same size $M_C \times N_C$ and $M_S \times N_S$ respectively. First, the secret image is to be partitioned into blocks of particular size (I×J). Unitary similarity transformation is then applied on secret image to convert it into a diagonal matrix i.e. having elements only at diagonal positions. The cover-image and the secret image can be represented by

$$C = \{C_i ; 0 \leq i \leq \frac{M_c * N_c}{I * J}\} \quad (1)$$

$$S = \{S_i ; 0 \leq i \leq \frac{M_S * N_S}{I * J}\} \quad (2)$$

The secret image can be recovered by applying inverse transformation using the eigen value matrix denoted as K.

5.2 Algorithm

Figure shows the basic procedure involved in our scheme. For the cover image C and secret image S, steps involved in image hiding have been summarized below:

Image Partitioning: The secret-image and cover-images are partitioned so as to obtain the secret-image blocks Si and cover-image blocks Ci (i=1,...,N).

Calculation of Eigen values and Eigen vectors:

Find out the eigen values and the respective eigen vectors for each block in secret image. The eigen vector matrix Qi generated will act as the encryption key for secret image extraction. For number of blocks to be N, eigen values can be calculated using following equation.

$$|S_i - \lambda I| = 0 \quad (3)$$

Where Si is a n×n matrix represented by each block.

The eigen values can be written as

$$\lambda_1\ \lambda_2\ \lambda_3\ \ldots\ldots\ldots\lambda_4$$

And the corresponding eigen vectors can be calculated

$$S_i\, q_i = \lambda\, q_i \qquad (4)$$

Where i=1,2,3…..N and j=1,2,3….n.

Let us define a matrix Q as,

$$Q_i .= [q_1, q_2, q_3 \ldots\ldots q_n]$$

Unitary Similarity Transformation:

Transform each matrix represented by each block into a diagonal matrix by using unitary similarity transformation as mentioned above. This eigen values represent the diagonal elements of this matrix.

$$A_i = Q_i^{-1} S_i Q_i \qquad (5)$$

Where A_i is a diagonal matrix and is given as,

$$A_i = \begin{bmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_2 \end{bmatrix}$$

Normalization:

Divide the elements of diagonal matrix by the highest value among them so as to get the normalized form between zero and one represented as $A_{i,norm}$.

Embedding secret image:

Add the results to the cover image blocks thereby embedding the secret image into it.

$$E_i = C_i + A_{i,norm}$$

Where Ei is the block embedded image.

Stego image generation:

The stego image can be obtained by combining the resultant blocks. This image obtained can be transmitted along with the encryption key.

Extraction:

Subtract the cover image from the received image and multiply the resultant by the maximum value and get the diagonal matrix. Now take the inverse of the eigen vector matrix and obtain the secret image by using the following equation

$$S_i = Q_i\, A_i\, Q_i^{-1} \qquad (6)$$

5.3 Proposed Technique

The process of image hiding and the recovery of the secret image can be understood with the help of following example. Here we are using a 512x512 pixels image of the Cameraman as a cover image, and a 512x512 pixels image of Lena as a secret-image, and then divide them into blocks.

Image Hiding Process:

Step 1: Finding the eigen values and eigen vectors

After partitioning the images into blocks, next step is to find the eigen values and eigen vectors for each block in the secret image. The eigen vector matrix Q acts as encryption key for the restoration of secret image.

Step 2: Applying Unitary Similarity Transformation

Q is used to transform the S matrix into a diagonal matrix Λ having the eigen values at diagonal positions only, using unitary similarity transformation given in equation (5).

Step 3: Embedding secret image and getting stego image

Each element of matrix A is divided by maximum value among them so as to normalize them. The normalized matrices are then added to the corresponding blocks of cover image to get the stego-image.

It can be seen that only the elements in diagonal positions are manipulated and this is the beauty of our scheme.

Similar operations are to be applied on all blocks of secret and cover image. The blocks are then combined again to get the final stego image.

Restoration of secret Image:

The decryption of the secret image can be achieved by first subtracting the cover image from the stgeo image and then multiplying the resultant by the maximum value which is also to be provided along with the decryption matrix.

The result obtained is the matrix A and the secret image can be obtained by using inverse unitary similarity transformation given by equation (6). This is to be done for each block and then these blocks are to be combined to get the final result.

5.4 Embedding algorithm for proposed method

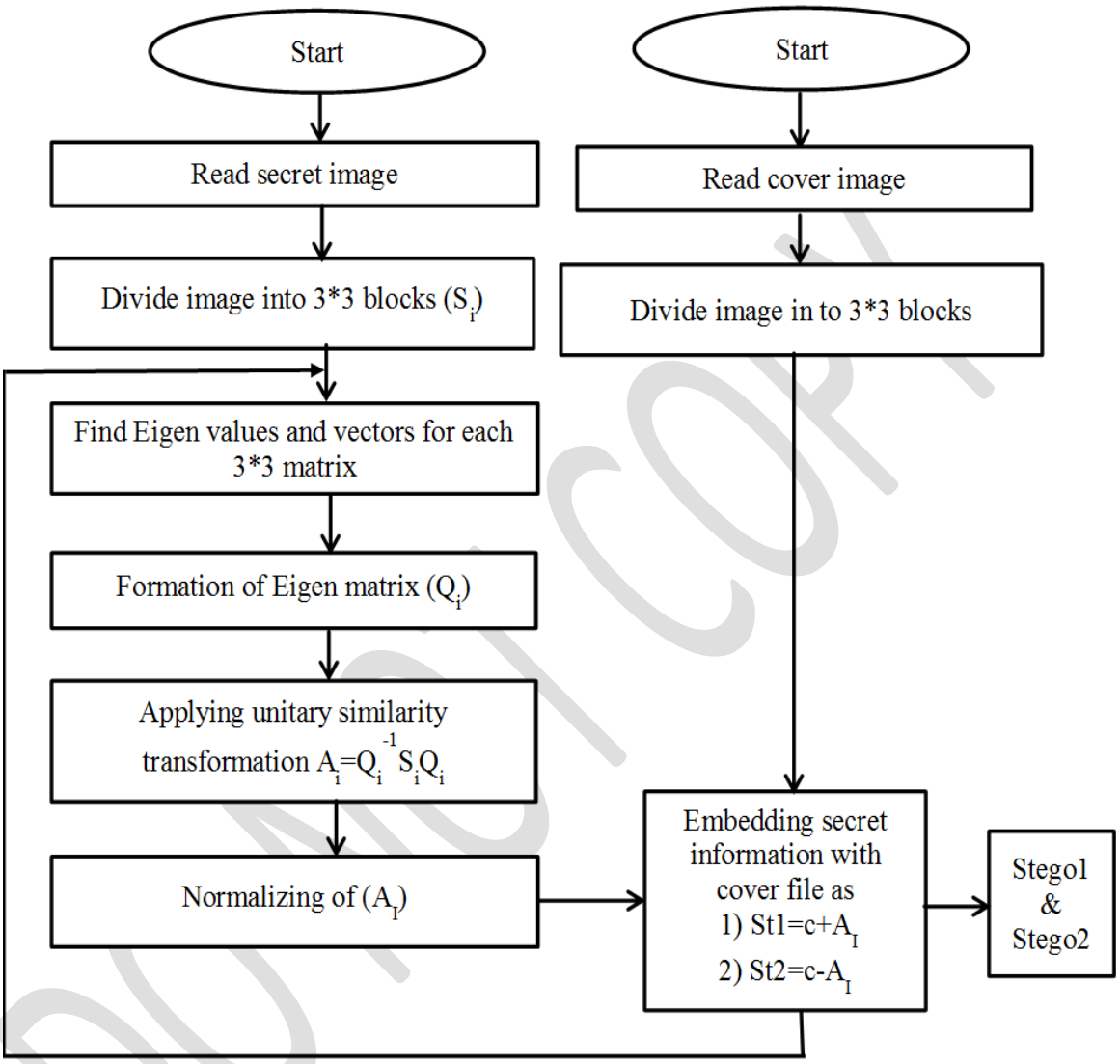

Figure 5.1 Embedding Algorithm for Proposed Method

5.4.1 Steps involved in embedding algorithm

Step 1: Read secret image and cover image independently.

Step 2: Divide secret image and cover image into square frameworks utilizing block division processing.

Step 3: Find Eigen values and Eigen vectors for every 3X3 frameworks of secret image.

Step 4: Formation of Eigen vector lattice for (Q_i) for each square block of secret image.

Step 5: Apply unitary similarity transformation by using equation ($Ai = Q_I^{-1} S_I Q_I$)

Step 6: Normalization of A_i to Acquire A_I.

Step 7: Embedding secret information with cover image keeping in mind the end goal to acquire stego image 1 and stego image 2.

$$\text{Stegoimage1} = C_I + A_I$$

$$\text{Stegoimage2} = C_I - A_I$$

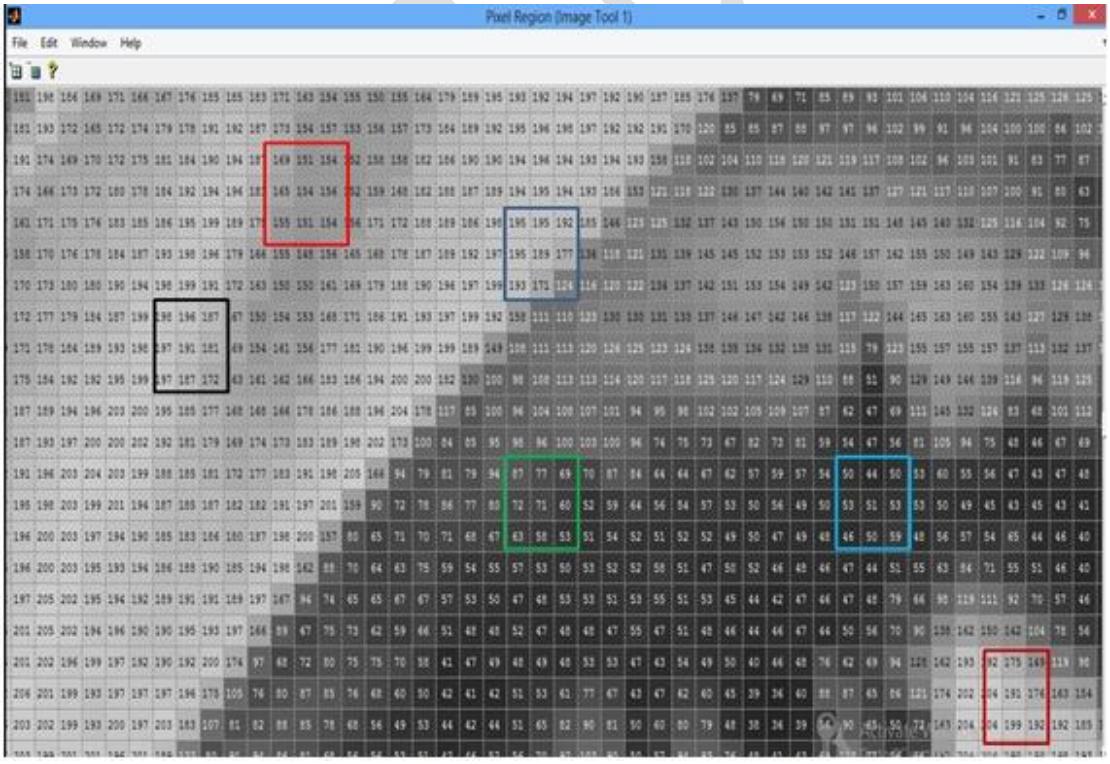

Figure 5.2 Blocks of Secret image

5.5 Reconstruction algorithm for proposed method

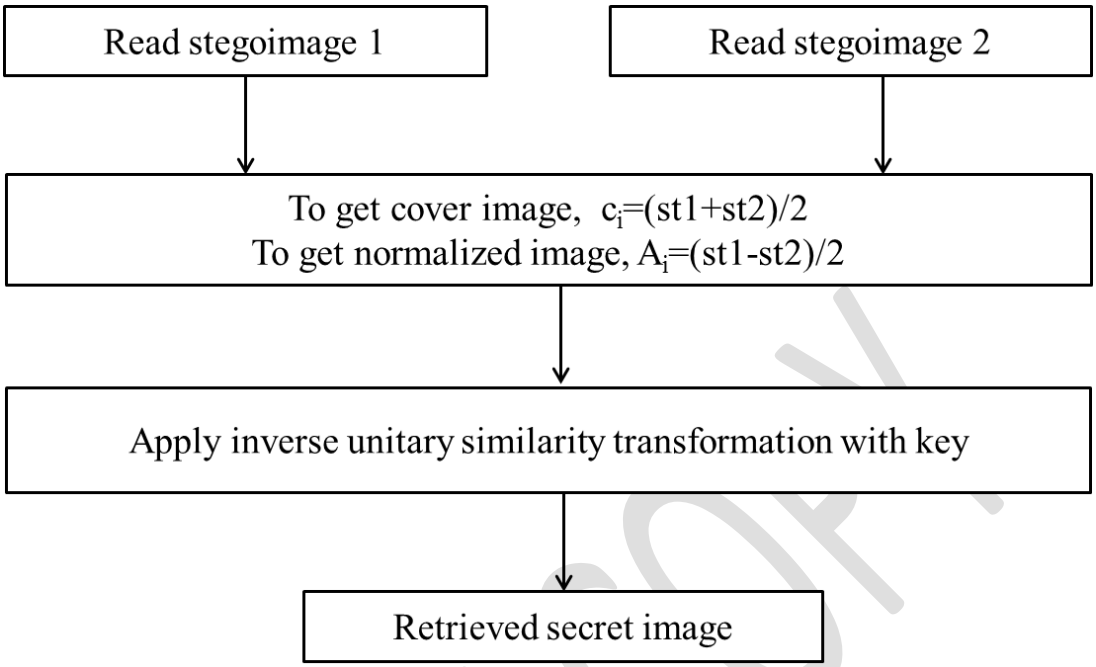

Figure 5.3 Reconstruction algorithm for Proposed Method

5.5.1 Steps involved in reconstruction algorithm for proposed method

Step 1: Read stego image 1 and stego image 2 independently.

Step 2: To get cover image average pixel values in stego images.

C_I= (st1+st2)/2.

Step 3: To get normalized image subtract stego image 1 from stego image 2 and divide the resultant with 2.

A_I= (st1-st2)/2.

Step 4: multiply matrix A_I with key in order to get A_i

Step 5: Apply inverse unitary similarity transformation with key in order to get secret image.

CHAPTER 6

7. EXPERIMENTAL RESULTS

In the proposed method of image hiding quality and embedding capacity, visual perception of Stego images are the main considerations. Result analysis of proposed scheme with various standard cover images and secret images are shown in next chapter.

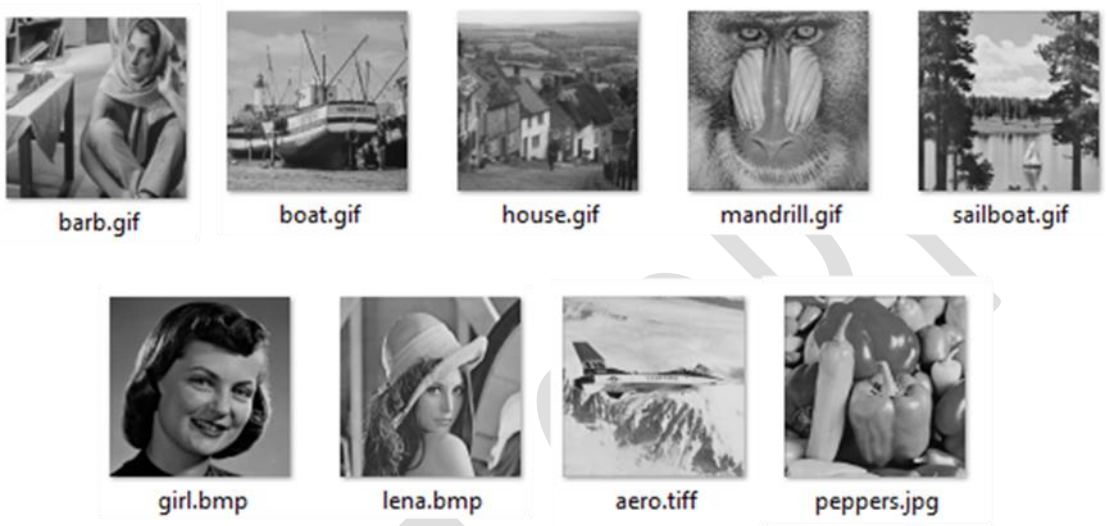

Figure 6.1 Secret and Cover Images

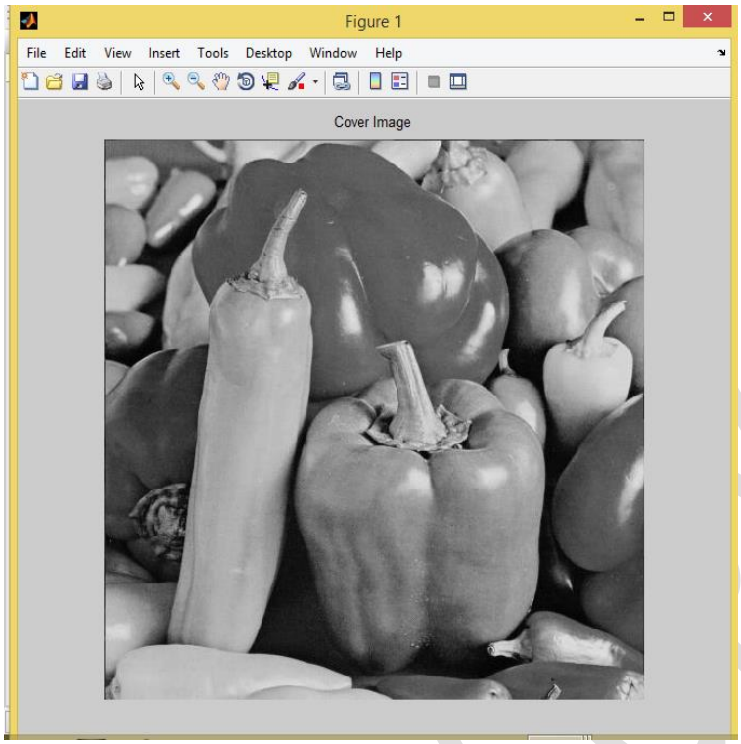

Figure 6.2 Cover Image

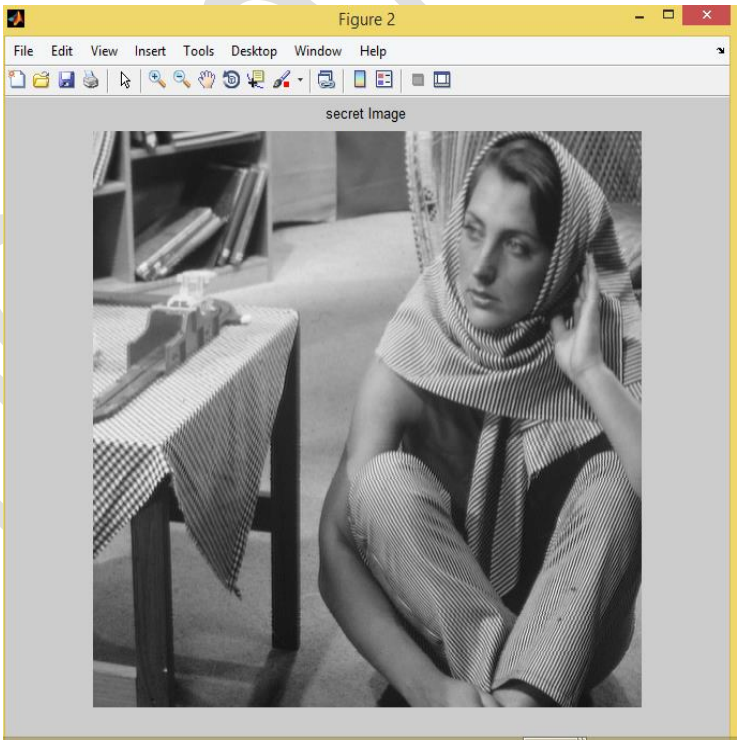

Figure 6.3 Secret Image

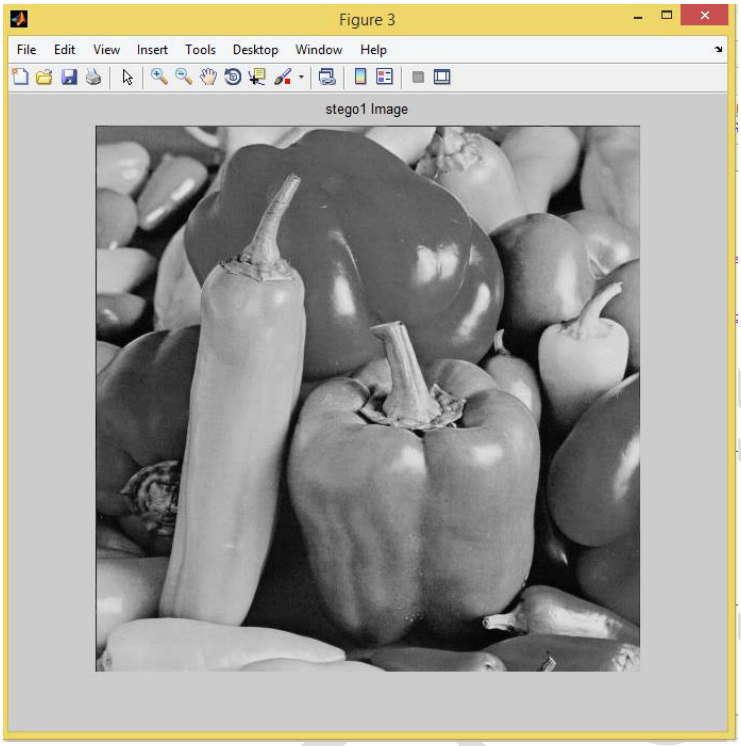

Figure 6.4 Stego1 Image

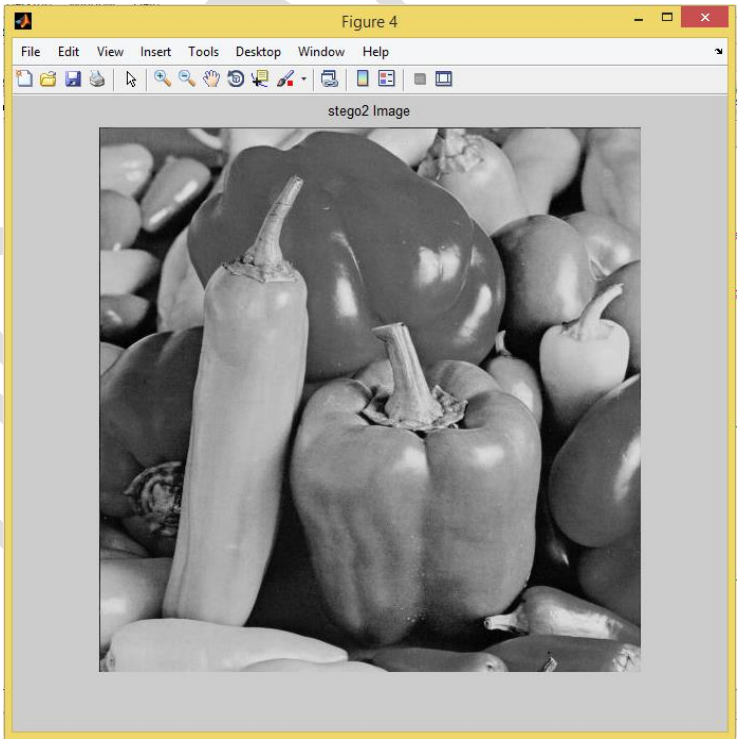

Figure 6.5 Stego2 Image

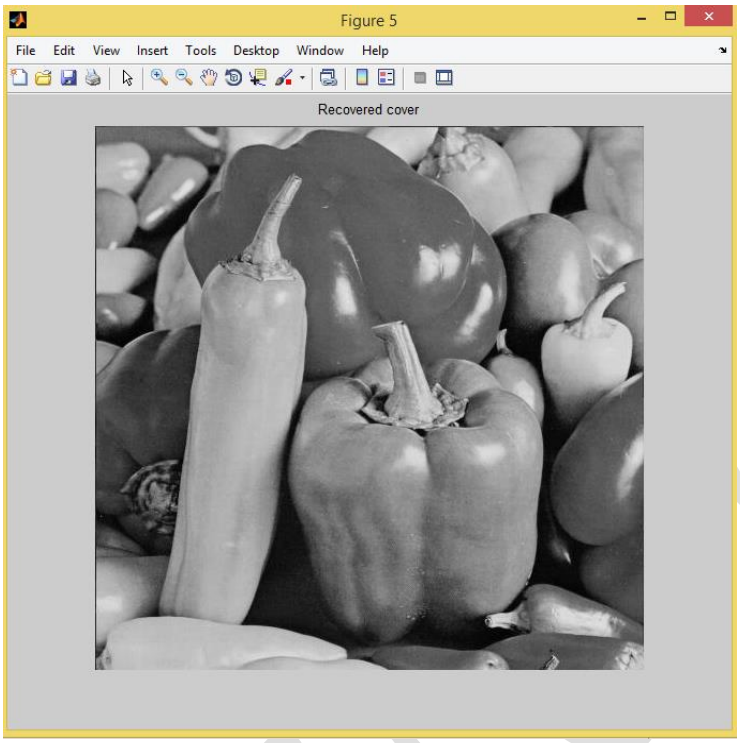

Figure 6.6 Recovered Cover Image

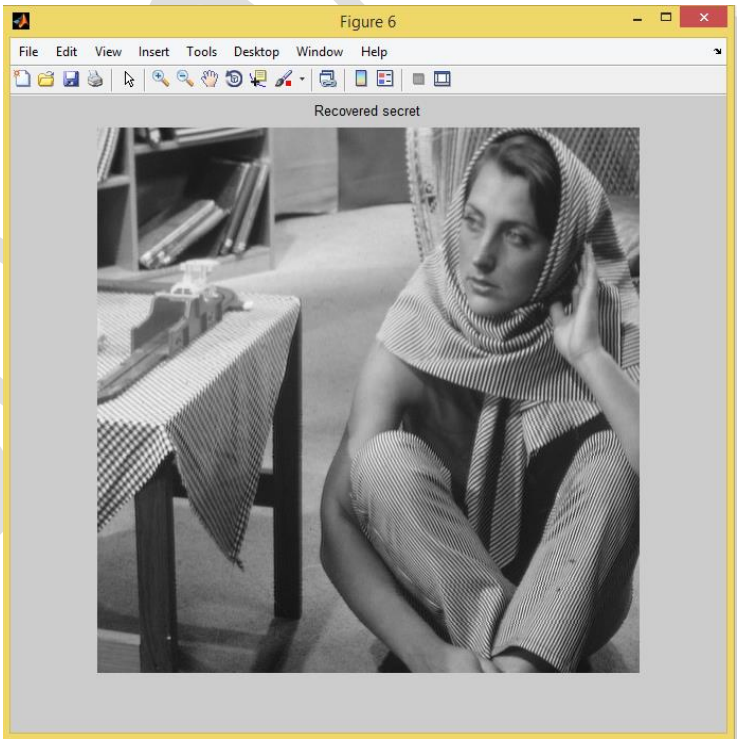

Figure 6.7 Recovered Secret Image

CHAPTER 7

8. QUALITY OF STEGO

The qualities of Stego images with the various cover images are presented in Table 2 and Table 3.The simplest and most widely used full-reference image quality measure is the MSE and PSNR. These are appealing because they are simple to calculate, have clear physical meanings, and are mathematically convenient in the context of optimization. They both have low computational complexities MSE and PSNR are acceptable image similarity measures when the images in question differ by simply increasing distortion of a certain type. MSE and PSNR do not model the human visual system. Advantage of MSE and PSNR are that they are very fast and easy to implement. However, they simply and objectively quantify the error signal. With PSNR, greater values indicate greater image similarity, while with MSE greater values indicate lower image similarity.

Mean Squared Error [MSE]:

One obvious way of measuring this similarity is to compute an error by subtracting the cover image from the reference, and then computing the average energy of the error. The mean-squared-error (MSE) is the simplest, and the most widely used, full-reference image quality measurement.

Where MSE is the Mean Square Error between cover image and Stego image. MSE is calculated as

$$\mathbf{MSE} = \frac{1}{PQ}\sum_{i=1}^{P}\sum_{j=1}^{Q}\left(O_{ij} - S_{ij}\right)^2$$

O_{ij} and S_{ij} are the pixel values of cover and Stego images respectively.

Peak Signal to Noise Ratio [PSNR]:

The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation

$$\mathbf{PSNR} = 10\log_{10}\left[(255)^2/\mathbf{MSE}\right] \quad \text{(in dB)}$$

Normalized Absolute Error [NAE]:

The large the value of NAE means that image is poor quality. NAE is defined as

$$\mathbf{NAE} = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}|O_{ij} - S_{ij}|}{\sum_{i=1}^{P}\sum_{j=1}^{Q}|O_{ij}|}$$

Structured content [SC]:

SC is also correlation based measure and measures the similarity between two images. The large the value of SC means that image is poor quality. SC is defined as

$$\mathbf{SC} = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}|O_{ij}|^2}{\sum_{i=1}^{P}\sum_{j=1}^{Q}|S_{ij}|^2}$$

Average Difference [AD]:

AD is simply the average of difference between the cover image and stego image. This measure shows the average difference between the pixel values and is defined as

$$\mathbf{AD} = \sum_{i=1}^{P}\sum_{j=1}^{Q}\frac{|O_{ij}-S_{ij}|}{PQ}$$

Normalized Cross Correlation [NK]:

The closeness between two digital images can also be quantified in terms of correlation function. These measures measure the similarity between two images, hence in this sense they are complementary to the difference-based measures. It measures is given by the equation

$$\mathbf{NK} = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}(O_{ij}*S_{ij})}{\sum_{i=1}^{P}\sum_{j=1}^{Q}O_{IJ}^2}$$

Least Mean Square Error [LMSE]:

Quality is determined mainly by the visibility of distortion in flat areas where it is more visible and consequently the effects minimum changes are also important.

$$\mathbf{LSME} = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q}[O_{ij}-S_{ij}]^2}{\sum_{i=1}^{P}\sum_{j=1}^{Q}|O_{ij}|^2}$$

Maximum Difference [MD]:

MD is the maximum of the error signal (difference between the cover image and stego image). It is given by

$$\mathbf{MD} = \mathrm{MAX}|O_{ij} - S_{ij}|$$

7.1 Result Analysis

Table 2: Quality assessment of Stego image 1

Secret image: barb

Cover Images	MSE	PSNR	AD	SC	NCC	MD	LMSE	NAE
Lena	0.250	54.140	-0.249	0.996	1.001	1.000	0.0159	0.0020
Mandrill	0.250	54.140	-0.249	0.996	1.001	1.000	0.0013	0.0019
Girl	0.250	54.140	-0.249	0.995	1.002	1.000	0.0189	0.0030
Aircraft	0.250	54.140	-0.249	0.997	1.001	1.000	0.0106	0.0014
boat	0.250	54.140	-0.249	0.996	1.001	1.000	0.0097	0.0018
House	0.250	54.140	-0.249	0.996	1.001	1.000	0.0092	0.0022
peppers	0.250	54.140	-0.249	0.996	1.001	1.000	0.0130	0.0021

Table 3: Quality assessment of Stego image 2

Secret image: barb

Cover Images	MSE	PSNR	AD	SC	NCC	MD	LMSE	NAE
Lena	0.250	54.140	0.249	1.0035	0.998	1.000	0.0159	0.0020
Mandrill	0.250	54.140	0.249	1.003	0.998	1.000	0.0013	0.0019
Girl	0.250	54.140	0.249	1.004	0.997	1.000	0.0189	0.0030
Aircraft	0.250	54.140	0.249	1.002	0.998	1.000	0.0106	0.0014
boat	0.250	54.140	0.249	1.003	0.998	1.000	0.0097	0.0018
House	0.250	54.140	0.249	1.003	0.998	1.000	0.0092	0.0022
peppers	0.250	54.140	0.249	1.003	0.998	1.000	0.0130	0.0021

AD: Average Difference

SC: Structural Content

NCC: Normalized Cross Correlation

LMSE: Least Mean Square Error

NAE: Normalized Absolute Error

MSE: Mean Square Error

PSNR: Peak Signal to Noise Ratio

MD: Maximum Difference

7.2 Benefits of Proposed method

- Low computation cost in the encryption and decryption.
- It is possible to choose any large value to normalize eigen values, which can also act as encryption key, thereby making it difficult to crack the algorithm.
- This algorithm is simple and can be easily implemented. It can greatly improve the security of the system, robustness of image-hiding. The quality of stego-image and the recovered image is improved up to a certain extent and is evident from the high PSNR of stego image.

CONCLUSION AND FUTURE SCOPE

Conclusion

In this work proposed steganography process, the secret image can be embedded in the cover image by using simple unitary similarity transformation. The eigen value matrix can be transmitted along with the stego-image and will act as key to recover the secret image. Also this scheme gives best PSNR given in Tables which is evident from the quality of stego image. We only have to add the diagonal form of secret image and hence less storage memory is required. It is possible to choose any large value to normalize eigen values, which can also act as encryption key, thereby making it difficult to crack the algorithm. Therefore the scheme can be easily implemented and the security of information is assured to a considerable extent. By adopting this strategy, the visual quality of the stego images is enhanced and the probability of discovery is reduced simultaneously. We conclude that our scheme which involves unitary similarity transformation proposes an efficient and easier approach for image hiding.

Future Scope

A new approach for improvisation of security aspect in steganography has been proposed in this work. This method gives good image quality and having good payload compared to existing methods. The reversibility property of the proposed hiding scheme is a practical solution for preserving valuable cover images, such as military and medical images. The future work revolves around the transmission of multiple secret files securely at a still lesser size compared to that of the size required to transmit each file independently. The visual quality of the stego-image is to be made better by maintaining good embedding capacity. The same technique can be implementing in terms of other digital mediums like audio and feature.

BIBILOGRAPHY

[1]. Agniswar dutta et al., "New data hiding algorithm in matlab using encrypted secret message", IEEE, International conference on communication systems and network technologies, 262-267, 2011 IEEE.

[2]. Sure.srikanth et.,al " compression efficiency for combining different embedded image compression techniques with Huffman encoding "international conference on communication and signal processing, 816-820,2013 IEEE.

[3]. Hamzeh hajizaadeh et., al " A new high capacity and EMD- based image steganography scheme in spatial domain" IEEE transactions on information forensics and security,634-673, 2013 IEEE.

[4]. Hedieh sajedi, mansour jamzad "cover selection steganography method based on similarity of image blocks" IEEE, International conference on computer and information technology workshops,pages 379-384,march 2008.

[5]. Himakshi et., al "Bi-directional pixel-value differencing approach for RGB color image" IEEE transactions on data hiding techniques, 47-52,2013 IEEE.

[6]. Kede ma et al., "revesible data hiding in encrypted images by reserving room before encryption" IEEE transactions on information forensics and security, 553-562,2013 IEEE.

[7]. Ali daneshkhah et al., "A more secure steganography method in spatial domain",IEEE, Internatiuonal conference on intelligent systems, modelling and simulation, 189-194, 2011 IEEE.

[8]. Supriya rai et al., "A novel keyless algorithim for steganography"2012 IEEE.

[9]. Soumya Zaghbani et., al " data hiding in spatial domain using chaotic map" IEEE conference on image processing,37-43,2013 IEEE.

[10]. Loung viet nguyen et al., "The method of hiding steganography without key exchanging and original image" 408-412, 2012 IEEE.

[11]. Ran-zan wang et al., "Secret Image sharing with all shadow images", ELSEVIER, Pattern Recognition Letters 27(2006), pages 551-555, October, 2005.

[12]. Mabolghasemi, Haghainia K Faez "Steganalysis of LSB matching based on co-occurance matrix and removing most significant bit planes" IEEE, International Conference on Intelligent Information Hiding and Multimedia Signal Processing pages 1527-1530,March,2008

[13]. Xian –ting zeng et al., "Reversible data hiding scheme using reference pixel and multi-layer embedding", ElSEVIER, Electron. Commun. (AEU) 66(2012), pages 532-539, November, 2011.

[14]. S. M Masud Karim, Md. Saifur Rahman, Md. Ismail Hossaiu, "A new approach for LSB based Image steganography using secret key" IEEE, International Conference on Computer and Information Technology [ICCIT 2011] 22-24 December, 2011.

[15]. Manoj Sharma et al., "Image Hiding using unitary similarity Transformation". IEEE, International conference on image information processing (ICIIP 2011).

[16]. Alaa A.jabbar et al., "An introduction to image steganography techniques" IEEE, International conference on advanced computer science applications and technologies (2012 IEEE).

[17]. Ekta Dagar, sunny dagar, "LSB Based Image Steganography using X-box Mapping" IEEE, International conference on advances in computing, communications and informatics (ICACCI) 2014 IEEE.

[18]. Nadeem Akthar et al.,"Enhancing the security and quality of LSB based Image Steganography".IEEE 5th International conference on computational intelligence and communication networks 2013 IEEE.

[19]. R Praveen Kumar, V Hemanth, M Shareef,"Securing Information Using Steganoraphy", IEEE International conference on circuits power and computing technologies[ICCPCT_2013].

[20]. Manoj Kumar Ramaya, Naveen Hemrajani, Anil Kishore Saxena "Improvisation of security aspect in steganography applying DES",IEEE International conference on communication systems and network technologies 2013 IEEE.

[21]. H Wang and Limin Qu, Fengru Wang "A Triangular Algorithm of Image-Hiding" Proceedings of the 8th World Congress on Intelligent Control and Automation, 2010.

.

APPENDIX A

DIGITAL IMAGE PROCESSING

Background

Digital image processing is an area characterized by the need for extensive experimental work to establish the viability of proposed solutions to a given problem. An important characteristic underlying the design of image processing systems is the significant level of testing & experimentation that normally is required before arriving at an acceptable solution. This characteristic implies that the ability to formulate approaches & quickly prototype candidate solutions generally plays a major role in reducing the cost & time required to arrive at a viable system implementation.

Definition

An image may be defined as a two dimensional function f(x,y), where x & y are spatial coordinates, & the amplitude of f at any pair of coordinates (x , y) is called the intensity or gray level of the image at that point. When x, y & the amplitude values of f are all finite discrete quantities, we call the image a digital image. The field of DIP refers to processing digital image by means of digital computer. Digital image is composed of a finite nmber of elements, each of which has a particular location & value. The elements are called pixels.

Image

An image is represented as a two dimensional function f(x, y) where x and y are spatial coordinates and the amplitude of f at any pair of coordinates (x, y) is called the intensity of the image at that point.

Gray scale image

A gray scale image is a function I of the two spatial coordinates of the image plane.

U(x, y) is the intensity of the image at the point (x, y) on the image plane.

I takes non-negative values assume the image is bounded by a rectangle [0, a]

x[0, b]; [0, a] x [0, b] $\longrightarrow$ [0, info)

Color image

It can be represented by three functions, R for red, G for green and B for blue.

An image may be continuous with respect to the x and y coordinates and also in amplitude. Converting such an image to digital from requires that the coordinates as well as the amplitude to be digitized. Digitizing the coordinate's values is called sampling. Digitizing the amplitude values is amplitude values is called quantization.

Image as Matrices

The preceding discussion leads to the following representation for a digitized image function:

$$f(x, y) = \begin{bmatrix} f(0,0) & f(0,1) \ldots\ldots\ldots & f(0,N-1) \\ f(1,0) & f(1,1) \ldots\ldots\ldots & f(1,N-1) \\ & \vdots & \\ f(M-1,0) & f(M-1,1) \ldots\ldots\ldots & f(M-1,N-1) \end{bmatrix}$$

The right side of this equation is a digital image by definition. Each element of this array is called image element, picture element, pixel or pel. The terms image and pixel are used throughout the rest of our discussion to denote a digital image and its elements.

A digital image can be represented naturally as a MATLAB matrix:

$$f = \begin{bmatrix} f(1,1) & f(1,2) \ldots\ldots\ldots & f(1,N) \\ f(2,1) & f(2,2) \ldots\ldots\ldots & f(2,N) \\ & \vdots & \\ f(M,1) & f(M,2) \ldots\ldots\ldots & f(M,N) \end{bmatrix}$$

Where f(1,1) = (0,0) (note the use of a monoscope font to denote MATLAB quantities). Clearly the two representations are identical, except for the shift in origin. The notation f(p ,q) denotes the element located in row p and the column q. For example f(6,2) is the element in the sixth row and second column of the matrix f. typically we use the letters M and N respectively to denote the number of rows and columns in a matrix.

A 1xN matrix is called a row vector whereas an Mx1 matrix is called a column vector. A 1x1 matrix is a scalar.

Matrices in MATLAB are stored in variable with names such as A, a, RGB, real array and so on. Variables must begin with a letter and contain only letters, numerals and underscores. As noted in the previous paragraph, all MATLAB quantities are written using mono-scope characters. We use conventional roman, italic notation such as f(x, y), for mathematical expressions.

Reading images

Images are read into the MATLAB environment using function imread whose syntax is

Imread('filename')

S.no	Format name	Description	Recognized Extension
1	TIFF	Tagged Image File Format	.tif, .ti
2	JPEG	Joint Photograph Expert Group	.jpg, .jpeg
3	GIF	Graphics Interchange Format	.gif
4	BMP	Windows Bitmap	.bmp
5	PNG	Portable Network Graphics	.png
6	XWD	X Window Dump	.xwd

Table A.1 Image File Formats

Here filename is a spring containing the complete of the image file (including any applicable extension). For example the command line reads (above table) image chest x-ray into image array f.

>> f = imread('8.jpg');

Note that use of single quotes (') to delimit the string filename. The semicolon at the end of command line is used by MATLAB for suppressing output. The prompt symbol (>>) designates the beginning of a command line, as it appears in the MATLAB command window.

APPENDIX B

B.1. SOFTWARE REQUIREMENT

B.1.1. MATLAB

Millions of engineers and scientists worldwide use MATLAB® to analyse and design the systems and products transforming our world. MATLAB is in automobile active safety systems, interplanetary spacecraft, health monitoring devices, smart power grids, and LTE cellular networks. It is used for machine learning, signal processing, image processing, computer vision, communications, computational finance, control design, robotics, and much more. The matrix-based MATLAB language is the world's most natural way to express computational mathematics. Built-in graphics make it easy to visualize and gain insights from data. The desktop environment invites experimentation, exploration, and discovery. These MATLAB tools and capabilities are all rigorously tested and designed to work together.

MATLAB helps you take your ideas beyond the desktop. You can run your analyses on larger data sets, and scale up to clusters and clouds. MATLAB code can be integrated with other languages, enabling you to deploy algorithms and applications within web, enterprise, and production systems.

Key Features

- High-level language for scientific and engineering computing
- Desktop environment tuned for iterative exploration, design, and problem-solving
- Graphics for visualizing data and tools for creating custom plots
- Apps for curve fitting, data classification, signal analysis, control system tuning, and many other tasks
- Add-on toolboxes for a wide range of engineering and scientific applications
- Tools for building applications with custom user interfaces
- Interfaces to C/C++, Java®, .NET, Python, SQL, Hadoop, and Microsoft® Excel®
- Royalty-free deployment options for sharing MATLAB programs with end users

B.1.2. Typical uses of MATLAB

- Math and computation
- Algorithm development
- Data acquisition
- Data analysis ,exploration and visualization
- Scientific and engineering graphics

MATLAB is an intelligent framework with fundamental information component is a cluster that does not oblige measurements. This permits you to tackle numerous specialized numerical processing issues, particularly whose with framework and vector network plans, client would take to compose a system in a scalar non-intuitive dialect, for example, C, C++, FORTRAN, Mat lab code.

MATLAB peculiarities of an extra application-particular arrangement called tool compartments. Vital to clients of MATLAB, tool compartments permit to learn and apply scientific reckoning innovation. Tool stash is accumulations of MATLAB capacities of M-documents and that broaden the MATLAB environment to take care of specific issues. In which tool kits are accessible incorporate all signs and frameworks,

- ✓ signal processing
- ✓ image processing,
- ✓ control systems,
- ✓ neural networks,
- ✓ Fuzzy logic,
- ✓ wavelets,
- ✓ simulation,

B.1.3. Peculiarities of MATLAB

- Advance algorithm for high performance in the field matrix, vector matrix and algebra numerical computation.
- A large collection mathematical functions they ability to predefine mathematical functions.
- Mat lab perform 2D-Dimensional -and 3D-Ddimensional graphics for plotting and displaying data

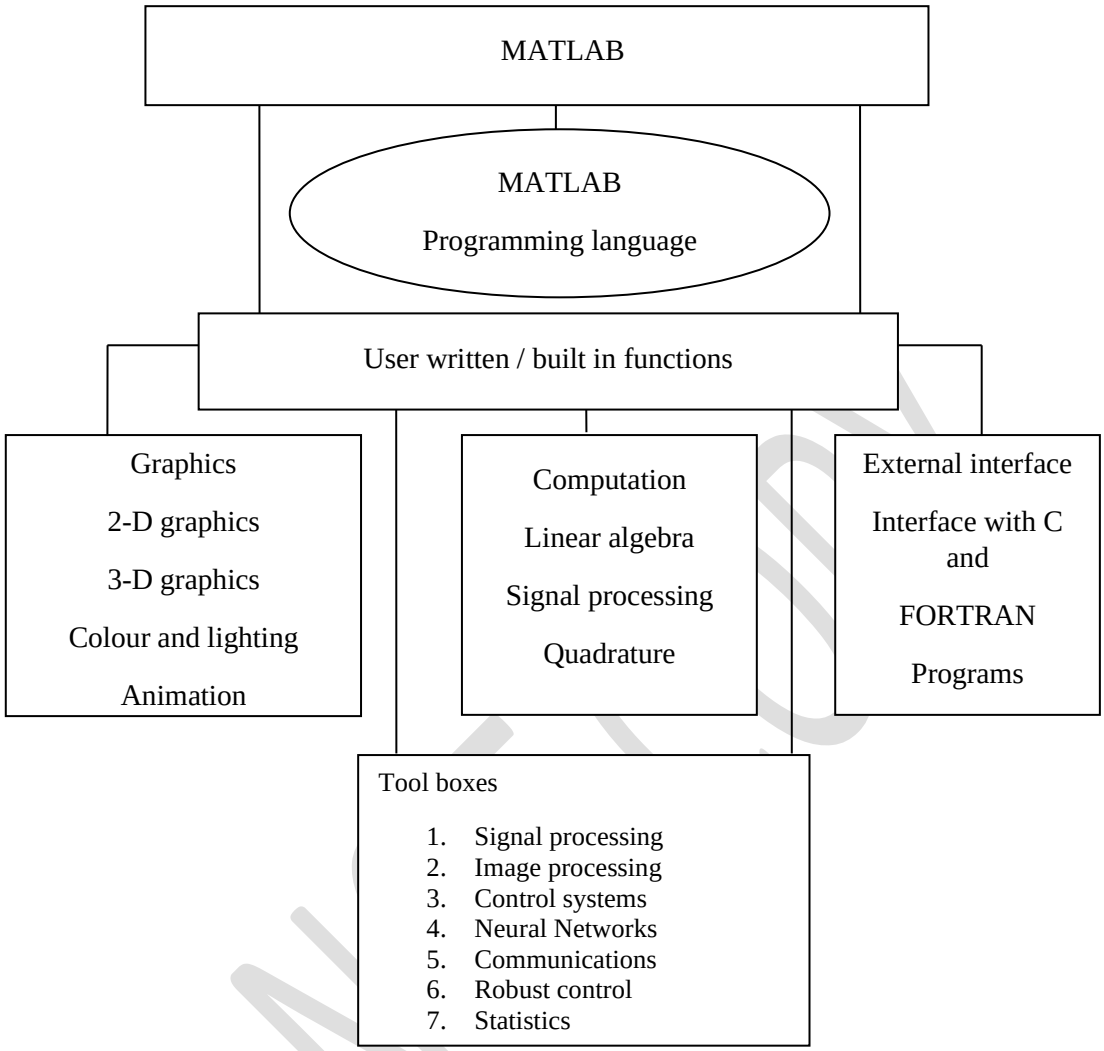

Figure B.1: Peculiarities of MATLAB

The MATLAB system consist of following parts

- User Development Environment
- The MATLAB Mathematical Function
- The MATLAB Language
- The Graphical User Interface(GUI) construction
- The MATLAB Application Program Interface (API)

User Development Environment

This is the situated of instruments and offices help client use MATLAB capacities. A number of these devices are graphical client interfaces (GUI). It incorporates MATLAB Desktop, Command Window, Command History, an Editor/ Debugger and Browsers for survey help, the giving workspace, M- records and the hunt way to clients.

The MATLAB Mathematical Function

This is an accumulation of numerical computational calculations capacities like whole, sine, cosine, and complex number-crunching, and refined capacities like framework reverse, lattice Eigen values, vector network , Bessel capacities, and quick Fourier changes and Wavelets.

The MATLAB Language

This is an abnormal state framework/cluster dialect with control stream explanations, capacities, information structures, data/yield, and article arranged programming. It permits both "programming in the little" to quickly make fast projects, and "programming in the extensive" to make finish huge process and complex application programs.

The GUI development

MATLAB has broad offices for showing grid vectors and frameworks like charts, and additionally clarifying and printing of these diagrams. It incorporates abnormal state capacities for 2d-dimensional and 3d-dimensional information, picture handling, and presentation illustrations. It additionally incorporates some low level capacities that permit you to completely appearance of illustrations and to construct a graphical client interfaces on MATLAB applications.

The Graphical User Interface (GUI) is an intelligent framework that serves to give great correspondence between the client and framework. The practical operation of the GUI is good with the Applets in JAVA. The MATLAB Toolbox gives more capacities to make GUI primary casings. The Guis can be made by the GUIDE (Graphical User Interface Development Environment) which is a bundle in MATLAB Toolbox.

The GUI makes the process so natural to work and diminishes the danger. GUIDE, the MATLAB Graphical User Interface Development Environment gives a set of instruments to make graphical client interfaces (Guis). These instruments enormously rearrange the methodology of outlining and building Guis. We can utilize the GUIDE devices to create client capacities.

Lay out the GUI: Layout Editor, we can lay out a GUI effortlessly by clicking and

Program the GUI: GUIDE naturally creates a M-document that controls how the GUI works. The M-record start the GUI and contains a system for all the GUI call backs – the orders that are executed when a client clicks a GUI part. Utilizing the M-document manager, we can add project code to the call backs to perform the capacities. Aide stores a GUI in two documents, which are created the first run through when we spare or run the GUI.

A FIG-document, with augmentation .fig, which contains a complete portrayal of the GUI format and the parts of the GUI: push catches, menus, tomahawks, et cetera.

An M-document, with expansion .m, which contains the code that controls the GUI including the call backs for its segments.

These two documents compare to the assignments of lying out and programming the GUI. When we lay out of the GUI in the Layout Editor, our work is put away in the FIG-document. When we program the GUI, our work is put away in the M-record.

The MATLAB Application Program Interface (API)

This is a predefined library that permits you to compose C, C++and FORTRAN programs that communicate with MATLAB. It includes facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, for reading and writing MAT-files.

B.1.4 MATLAB Working Environment

MATLAB Desktop

Matlab desktop is the main Matlab application window. The desktop contains five sub windows, the command window, the workspace browser, the current directory window, the command history window, and one or more figure windows, which are shown only when the user displays a graphic.

Window	Purpose
Command Window	Main window, enters variables, runs programs.
Figure Window	Contains output from graphic commands.
Editor Window	Creates and debugs script and function files.
Help Window	Provides help information.
Command History Window	Logs commands entered in the Command Window.
Workspace Window	Provides information about the variables that are stored.
Current Folder Window	Shows the files in the current folder.

Table B.1: MATLAB Windows

Command Window:

The Command Window is MATLAB's main window and opens when MATLAB is started. It is convenient to have the Command Window as the only visible window. This can be done either by closing all the other windows, or by selecting Command Window Only in the menu that opens when the Layout icon on the Tool strip is selected. To close a window, click on the pulldown menu at the top right-hand side of the window and then select Close. To type a command the cursor is placed next to the command prompt (>>).

The semicolon (;):

When a command is typed in the Command Window and the Enter key is pressed, the command is executed. Any output that the command generates is displayed in the Command Window. If a semicolon (;) is typed at the end of a command, the output of the command is not displayed. Typing a semicolon is useful when the result is obvious or known, or when the output is very large.

Typing %:

When the symbol% (percent) is typed at the beginning of a line, the line is designated as a comment. This means that when the Enter key is pressed the line is not executed. The% character followed by text (comment) can also be typed after a command (in the same line). This has no effect on the execution of the command.

The clc command:

The clc command (type clc and press Enter) clears the Command Window. After typing in the Command Window for a while, the display may become very long. Once the clc command is executed, a clear window is displayed. The command does not change anything that was done before.

Figure Window:

The Figure Window opens automatically when graphics commands are executed, and contains graphs created by these commands.

Editor Window:

The Editor Window is used for writing and editing programs. This window is opened by clicking on the New Script icon in the Tool strip, or by clicking on the new icon and then selecting Script from the menu that opens.

Help Window:

The Help Window contains help information. This window can be opened from the Help icon in the Tool strip of the Command Window or the toolbar of any MATLAB window. The Help Window is interactive and can be used to obtain information on any feature of MATLAB.

MATLAB Functions

Image file input and output have several important commands to access and manipulate the images. Some are listed in Table 5.

Image File I/O

Function Format	Description
Imread	Read Image File.
Imwrite	Write Image File.
Imfinfo	Return information about image file.

Table B.2: Image File I/O functions in MATLAB

Built-In Functions

MATLAB contains a number of functions for performing computations which require the use of logarithms, elementary math functions and trigonometric math functions. List of these commonly used elementary MATLAB mathematical built-in functions are given in Tables

Function	Description
abs(x)	Computes the absolute value of x.
log(x)	Computes ln x, the natural logarithm of x to the base e.
log10(x)	Computes log10 x, the common logarithm of x to the base 10.
sqrt(x)	Computes the square root of x.
clear	Clears the workspace, all variables are removed.
clear all	Clears all variables and functions from workspace.
clf	Clears figure window.
cd	Changes the current working directory.
quit	Quits MATLAB.
exit	Same as quit.

size(A)	Returns a row vector [m,n],where and m are the size n m × n of the array A
C = max(A)	If A is a vector, C is the largest element in A. If A is a matrix, C is a row vector containing the largest element of each column of A.
inv(A)	Returns the inverse of a square matrix
if, else, elseif	The several forms of MATLAB if blocks are as follows: **if** variable block of statements executed if variable variable 1 is "true" **end** block of statements **end** block of statements **if** variable1 block of statements executed if variable1 non-zero is "true" **else** block of statements **else** executed if neither **if** variable1 block of statements executed if non-zero is "true" **else if** variable 2 is "false" i.e., zero is "true" **end** variable is "true"
break	Terminates the execution of a **for** or **while** loop. Only the innermost loop in which **break** is encountered will be terminated.
return	Causes the function to return at that point to the calling routine. MATLAB M-file functions will return normally without this statement.
while	The form of the MATLAB loop is **while** variable block of statements executed as long as the value of variable is "true"; i.e., non-zero **end**
double	Convert symbolic matrix to double
fprintf	fprintf(fileID,formatSpec,A1,...,An) applies the formatSpec to all elements of arrays A1,...An in column order, and writes the data to a text file. where fileID : An integer file identifier formatSpec: String that describes the format of the output fields.

disp	Display text or array
mat2cell	Convert array to cell array with potentially different sized cells.
ischar	Determine whether item is character array
uint8	8-bit unsigned integer array
zeros	Create array of all zeros
Inf	Infinity
nargin	nargin returns the number of input arguments passed in the call to the currently executing function.
nargout	nargout returns the number of output arguments specified in the call to the currently executing function.

Table B.3: Built-in Functions in MATLAB

Arithmetic operators	
Matrix operators	Array operators
+ Addition	+ Addition
– Subtraction	– Subtraction
* Multiplication	.* Array multiplication
^ Exponentiation	.^ Array exponentiation
/ Right division	./ Array right division
\ Left division	.\ Array left division

Table B.4: Element-by-element operations

Eigenvalues and Eigenvectors

Consider the following equation:

$$AX = \lambda X \qquad ...(1.1)$$

where A is an n × n square matrix, X is a column vector with n rows and λ is a scalar. The values of λ for which X are non-zero are called the eigenvalues of the matrix A, and the corresponding values of X are called the eigenvectors of the matrix A.

Equation (1.1) can also be used to find the following equation:

$$(A - \lambda I)X = 0 \qquad ...(1.2)$$

where I is an n × n identity matrix. Equation (1.2) corresponding to a set of homogeneous equations and has non-trivial solutions only if the determinant is equal to zero, or

$$|A - \lambda I| = 0 \qquad ...(1.3)$$

Equation (1.3) is known as the characteristic equation of the matrix A. The solution to Eq.(1.3) gives the eigenvalues of the matrix A.

MATLAB determines both the eigenvalues and eigenvectors for a matrix A.

eig(A):

Computes a column vector containing the eigenvalues of A.

[Q, d] = eig(A):

Computes a square matrix Q containing the eigenvectors of A as columns and a square matrix d containing the eigen values (λ) of A on the diagonal. The values of Q and d are such that Q * Q is the identity matrix and A*X equals λ times X.