CHAPTER 1: INTRODUCTION

Introduction

1.1Steganography

Steganography is a talent and science of defeat information by embedding messages contained by other, apparently risk-free communication. Steganography moving parts by replacing bits of ineffective or else unexploited data in standard computer files (such as sound, graphics, HTML, text, or even floppy disks) through bits of dissimilar imperceptible information. This concealed information in sequence can be plain text, images, cipher, or even audio or video file.

Steganography (exactly sense covered or hidden writing) years back to prehistoric Greece, where general practices consisted of drawing letters or communication in wooden tablets and wrapping them through polish, and tattooing a removed hair from messenger's head, let his hair growing back, after that removing it again when he reach a destination and get in touch with end point.

1.2 Use of Steganography

Steganography from time to time is used while encryption is not acceptable. Otherwise extra frequently, in second - hand Steganography is used to additional encryption. An encrypted file may possibly at a standstill conceal information in sequence using Steganography; accordingly unvarying condition the encrypted folder or file is decrypted or deciphered. The concealed message or communication is not able to be visible.

Steganography is data hidden inside another data. Steganography is a technique used with encryption as another way to protect data. These are applicable on images, videos or on audio files. In most of the cases it is used with text files but now a day’s commonly used in images also. It gives an option to overcome the problem of piracy, unauthorized information leak. It also gives a way to hide information from other parties which may call third parties and this hidden information must be revealed to the considering person whom so ever it is renounced well thought-out a redoubtable assignment within itself. It has to be encrypted, which knows how to be almost it is impossible.

- One use of Steganography includes watermarking which hides copyright in sequence inside a watermark by collapsing files. It is not easily identified by the human naked eye.
- In the horrible incident happened in USA known as 9/11, terrorists used Steganography. In that case they just used a font conversion to pass away their message to their partners. The message was **"Q33N"** flight no; when **font Wingdings** used it becomes □✈▤▤☠□. This was the simplest way of using Steganography whose use makes this happen without unrevealing. It took almost 1 year to decode and get the meaning of the message.
- Military or other defence organizations widely use Steganography for the sake of confidentially for the period of 10 years (known as decades) yet if it is not computer based. For pattern, having a covert communication was tattooed on a soldier's removed hairs on his top head. His hair grow back during the course and just the once he completed his work, he would have to again removed his hair on top head only to disclose the concealed tattooed communication or letter to the selected for the recipient.

1.3 Steganalysis

The ability of identifying Steganography is identified to as Steganalysis. In the direction of placing it basically Steganalysis occupies identifying the make use of Steganography within a folder or files. It does not arrangement by way of annoying to decrypt the concealed communication in sequence contained by a file, immediately determining it. Steganalysis is the practice of attacking Steganographic methods for the revealing, withdrawal, damage and handling of the hidden data in a stego object. A good steganalyst must be careful of the methods and techniques of the Steganographic tools to efficiently attack.

- **Active Attack –** Active attacks are useful when Steganography is suspected but discovering the hidden message is insignificant. To remain the stego image unchanged and hide information behind it digital information is used. Text or message in embedded inside the image by changing the bit level information of the image, which is unnoticeable with necked eyes.
- **Passive Attack –** Message remains hidden in the image; passive attacks provide functionality to unpack hidden message.
- **Stego attack only:** In this type of attacks, only stego object is available for analysis.

- **Known Carrier/Cover attack:** Both the original cover and stego media are available for the steganographic analysis.
- **Known Message Attack:** In this case hidden message is known, analyzing the stego media for message embedded may help to attack similar systems.
- **Known Stego Attack:** In this attack cover, stego and the steganographic tool are used to be known.
- **Selected Stego Attack:** steganographic algorithm and stego media are known.
- **Selected Message Attack:** In this attack steganalyst implements many steganographic tools for a chosen message and analyses these stego media with the one which is to be analyzed and try to find the algorithm used in these process.

1.3.1 Steganalysis Approach

Visual Attack: It is analyzing the images visually like to consider the bit images and tries to find the visual difference in the images.

Structural Attack: Configure of the cover file frequently modifies the same as the information to be embedded or concealed. We are recognizing these feature arrangement alters can become aware of the continuation of secret file be hidden, e.g. In a palette based Steganography the palette of image is changed before embedding data to reduce difference between the number of colors and the adjacent pixel color should be very less.

Statistical Attack: Mathematical formulas are used in statistical attacks to analysis images statistically; this analysis shows the significance of the secret information in the image. Normally the secret message is more random than the unique information of the representation thus finding the formula to know the randomness revel the existence of data.

1.4 Applications of Steganography

- Steganography is approximately an indestructible system and is an advanced means of secret communication.
- Steganography can slip important communication without knowledge of anyone.

- Steganography can be used to follow violation of copyrights in a digital medium and can work wonders on internet.
- Soon, we can have authors, artists and musicians using Steganography to fight piracy.

1.5 Advantages and Disadvantages of Steganography

Advantages

- Steganography can be used to defend copyrights, put off piracy and work in the transfer of top secret data from one place to another place.
- In LSB Encoding method, it is hard to detect. In this original image is very similar to altered image. In this method embedded data resembles through the Gaussian noise.
- In Low Frequency Encoding, it is hard to detecting the message and the fundamental image data. It is share in same range.
- Mid Frequency Encoding technique altered the image/picture closely resembles to the original image. It is not susceptible to attacks such as translation and the rotation.
- It does not attract the attention of the attackers.
- It is difficult to prove that the Steganography exists.

Disadvantages

- The terrorist organizations are hiding photographs, maps of their targets and directions in favor of terrorist behavior on bulletin boards, communication passing through chat rooms and other websites using Steganography.
- If the Steganography fallen into wrong hands it can be create tremendous damage.
- In LSB Encoding message is hard to recover and if the image is subject to attack such as rotation and translation.
- In Low Frequency Encoding, it is significant damage to the appearance of the image and it is difficult to recover the message.
- Mid Frequency Encoding relatively easy to detect the hidden message.
- Image is distorted in High Frequency Domain Encoding, in this message is easily lost if the image subject to compression such as JPEG format.

1.6 Problem statement

Image Steganography is a concept of hiding image behind image. In the recent work FCAT, LSB3, Jae Gilyu; although the purpose of image Steganography is fulfilled but the image quality of generated stego image was not as good as it should be. It gives the viewer of the image hint that something in bounded behind image or hidden behind it. Image resolution of the resultant image was always the problem. Considering this problem we have designed KVL algorithm with a wide range of features. In the past techniques the lossless composition was missing. After reverse Steganography the image retrieved becomes dull and quality degrades.

1.7 Solution Statement

KVL considers the image superiority of the stego image representation as a prime factor. Visibility of the image must be equal to the original image. In KVL using the combination of Transform Domain and Image Domain Steganography we tried to get the better quality of the resultant image representation as well as of the secret image after reverse Steganography. In KVL we use LSB substitution method for hiding data behind an image; additionally we converted the whole secret image in the form of binary values using the RGB pixel values. To maintain the quality of the image processing we kept a ratio of 1:9; so that image don't get dumped and dull. The whole methodology is very simple and is of high programming standards. Extra Features of KVL Steganography are Image Compression, Cryptography, etc. KVL is totally a lossless technique.

1.8 Dissertation outline

This dissertation encounters in different part as on starting it deals with slight introduction of what I am going to do. The rest comes in the following sections:

- **Section II: -** In this part II the technology is detailed and compared with its latest update. Many referred paper have been discussed in this chapter to analyse the need of proposed work.
- **Section III: -** Proposed method will come over here with a detail introduction of KVL Algorithm.
- **Section IV: -** Result and Analysis.

- **Section V: -** The Conclusion
- **Section VI**: - Future work.
- **Section VII**:- References

Chapter 2 LITERATURE REVIEW

2.1 What is Steganography

Steganography is the science and art to representation of undetectable communication. This is skillful from beginning to end thrashing information in sequences within additional information, therefore thrashing the survival of the communicated data in sequence of the information. The origin of Steganography is originated from the Greek terminology “Stegos” meaning “cover” and “grafia” meaning “writing” [1] important it as “covered writing”. During an image Steganography representation the message is embedded completely in images.

Steganography refers to the science of “invisible" communication. It makes the information hidden behind other format of information may be images, text or videos; and hidden information is hide as that no one can sense it. Many people get confused in Steganography and cryptology because these both do the protection of secret or confidential information in a sequence. The differentiation among them is that Steganography occupies thrashing in sequence thus it become visible so that no information or message is concealed at all. If a human being analyses the thing or article in which useful information is concealed inside, then he/she will not determine that there is any concealed message or information, hence someone will not try in the direction of decrypt the concealed message.

2.2 History of Steganography

The history has presented limitless conditions anywhere by significant information have to pass through unfriendly or opponent territory to arrive at its target unobserved. People throughout the ages contain second-hand several clever methods to cover up in a sequence of information and when time passed it is approved the newer methods were improvement on the older ones and procedures were consistently revealed. A quantity of this example is:

- During World War II, invisible inks were used to conceal message in apparently pattern, innocent notes or words. General resources for invisible ink, vinegar, milk, urine and fruit juices. The merit of this method was that every one of these matters cast a shadows when

intense and was more than ever efficient throughout this time due to the detail that the resources were for all time with pleasure offered.

- A famous Greek, Aeneas the Tactician devised a method whereby holes demonstrating words or letters of the Greek alphabet were uninterested into a made of wood disk. Wool was after that threaded all the way through the gaps in direct that they would predict out the communication.
- In Ancient Greece, a method was used whereby a person was chosen as a messenger and had removed their head hairs. The covert text was tattooed against their hairless head and the hairs were approved to grow once another time to ordinary or usual duration. The messenger would followed by continue to the destination passing some security inspections and accessible themselves to the recipient of the message in sequence of information who would then remove the hairs on head of the messenger to understand the secret text. One main weakness to this process was the time lag.
- The Germans invented microdot technology for secret communication in 1941. In microdots, the information or communication were neither concealed nor encrypted except their size was too small to be observed by the bare eye [2]. Move forwards in microdot technology still carry on to now a day, the most recent growth being the embedding of a communication into strand of DNA by the employ of the procedure of genomic Steganography [3].
- Another method used in Ancient Greece was polishing enclosed tablets. The polish would be worn out off the tablet, the communication written on the wood below and the polish re-applied to conceal the message. The recipient of the tablet would follow by basically scrape off the polish just the once over to expose the communication for the message.

2.3 General Concepts of Steganography

Cover object: It passes on to the thing used as the transporter to inserted letters or message into the cover object. Various dissimilar bits and pieces have been engaged to inserted letters into cover object, e.g. images, HTML pages, audio file, video file as well as structures file.

Stego object: It passes on to the thing which is transport a secret communication. Therefore specified a cover up object and communication the purpose of the Steganographer is to create a Stego object which would bear the communication (hiding the information).

Steganalysis: Steganalysis is the procedure of distinguishing & analyzing unknown information in sequence contained by a file.

Redundant Bit: The pieces of secret message or in a row contained by a file which be able to altered or overwritten without damage the file.

Payload: In payload the message or information in a sequence which is to be covered.

2.4 Different categories of Steganography

In present basically three categories of Steganography. These are Technical, linguistic and digital. They can be further classified into further different types as shown in the diagram below.

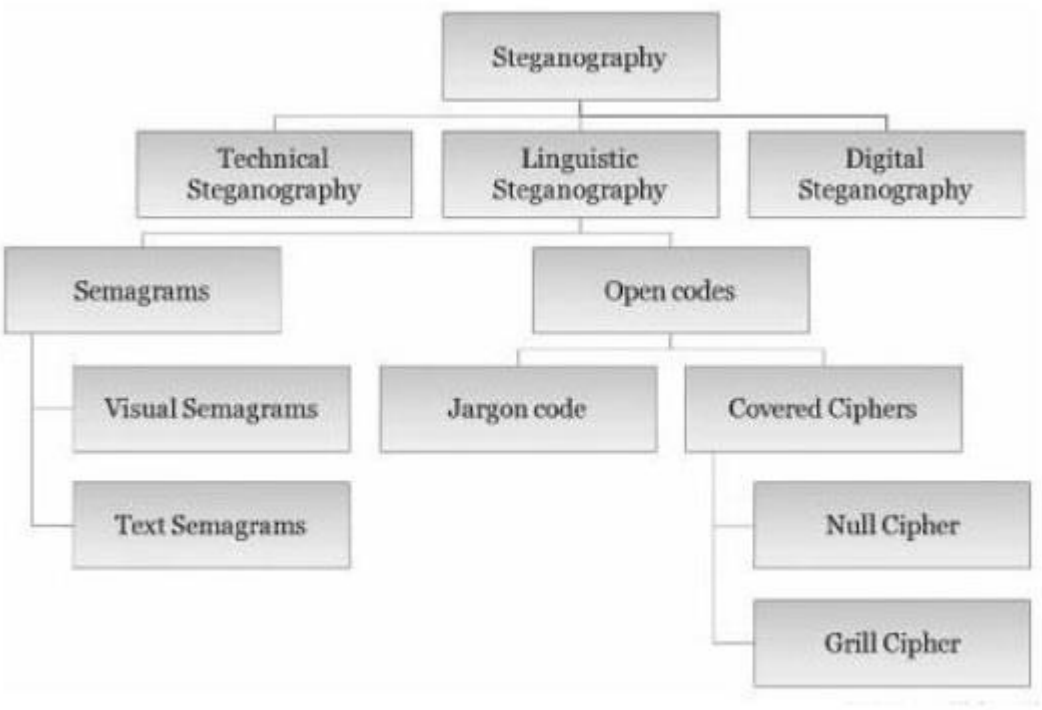


Figure 2.1

2.4.1 Technical Steganography

Technical Steganography is a modest broader in range for the reason that it does not automatically deal through the written statement still although it communicates through

information in a sequence. Technical Steganography is a technique of Steganography somewhere a mechanism, method, or tool is used to cover the communication .Some types of technical Steganography methods are:

Invisible ink: As discussed already invisible ink, in this case is one that uses an individual ink to facilitate is colorless and imperceptible until treated by an element temperature or in a particular light. Since indistinguishable ink does not include to be used to inscribe words it can carefully be consider an appearance of technical Steganography. There are various other patterns of undetectable ink:

- Typing a letter or message in a typewriter correction ribbon. A significant letter could be written in a blank space connecting the usual black band lines of manuscript and turn out to be noticeable barely in an extremely strong light.
- Using of hand stamps, it is visible only in black light similar to that used in night clubs and amusement parks.

Hiding Places: Effectiveness of Steganography depends on the place used for information hiding. We are well aware of fact that we can use any type of data to hide or as a cover message. Text can be hidden behind text, behind image, in videos, but the confidentiality remains high when we give preference to video images as cover. Some examples are a barrel of cocktail as in the case of Mary Queen of Scots, a tattoo on top of a man's head or the heel of a woman's shoe.

Microdots: Microdots are special dots which are not bigger in size than ½ millimeter and used in micro photography. The microdot has in use a new appearance in the up to date world and is individual used to exclusively identify motor crafts and other automobiles.

Computer based method: in a computer based method, the advancements in computer knowledge for the duration of the 1990s, this is the latest of the Steganography processes and can be very efficient in its inhabitant situation. There are various computer based techniques as well as addition of the bits, substitution of bits and additional bits.

2.4.2 Linguistic Steganography

Linguistic Steganography can be explained quite basically as several appearance of Steganography with the purpose of uses verbal communication in the cover. The basic two types of linguistic Steganography are unlocked Codes and manuscript Semagrams.

An example of linguistic Steganography is NICETEXT. NICETEXT transform the cipher text in a form which is similar to the original text. The software mechanism by variety certain aspects of inscription by approach or by means of context-free grammar. NICETEXT relies on bulky code dictionaries consisting of terminology categorized by nature. NICETEXT transforms cipher text addicted to sentences by means of picking words through the corresponding codes used for the appropriate type categories in the word list table. The turnaround procedure basically parses human being words from the produced manuscript and uses codes starting from the word list table to reconstruct the cipher text [4].

Open Code: In this case, open code the frankly decipherable manuscript is generally well assembled. It preserves hold confident sentences or words in a definite correspondence can be exist in convinced spaces in the manuscript, or expressions can be exist concealed in reversed or vertical.

Masking: In masking techniques the wording near might be sentences or expressions opening by definite writing which contain significance or connotation. At hand be able to as well descriptions, etc., in so far as every variety of terminology is in actual fact masking.

Null Cipher: In null cipher, the covert manuscript might be rebuilder by captivating the primary, secondary or some correspondence letter of each expression. Concealed communication can in addition to exist establish crossways, perpendicularly, or in reverse to decipher, it possibly will besides compulsory to modify the release manuscript in a different form.

Cues: The necessary description of cues is a definite statement to become visible in the manuscript and transports the letter. During the wartime situations cures are used commonly send information to resistance troops. Radio show is conducted in which a particular word have a certain meaning and this is already know to the listener of the radio show; on occurrence of that word a fixed predetermined task is performed and actions are pursued if the text or statement is not used, the unusual information is toward exist tracked. This technique of statement is

incredibly useful because of its flexibility. The drawbacks are to facilitate cues have need of an excellent deal of research and frequently are not accomplished of assigning huge amounts of information.

Music: Music is not a verbal communication or not any language, it a sound which gives pleaser to the listener, but it is quite true that it can be used as a language if implied with Steganography. It conveys some meaning every time when written and used in a specific manner. It can be used to hide information via playing the notes in a pre-rendered manner which is coded and have some specific functionality. Listener may understand or can convert the notations in some words and can get the information hidden in the notes played. It is robust technique of data hiding as an inexperienced listener assumes it as just a normal tune.

Jargon Code: In a linguistic Steganography terminology or slang cipher generates an unwritten or written communication because the wrap used for the covert information. A slang oblique communication is a batch similar to a replacement code in several compliments, but as an alternative of substituting individual writing, the expressions themselves are altered [4].

Newspaper Code: It was originated and used all the way through the Victorian period, support in the day after journalists might be sent approximately somewhere not including charge. This scheme was used with the poor who can send information free of cost. A minute hole was pushed in excess of definite writing in the broadsheet, which after associated spelled out the documents weeks to accomplish certain positions.

Grilles: The framework or the cardano frame the same as it is mainly regularly called is merely a soft section of document or cardboard through holes placed approximately it. The covert communication is printed within the holes and after that the rest of the communication or information is packed in the region of the holes. The barely method is used, if the communication is understandable with the receiver, who has the exact frame or grill [4].

Text Semagrams: The manuscript semagrams work among graphical adaptations of the wording. They apprehension information to facilitate are small except nevertheless noticeable. In the present methods that work lacking manuscript additionally called actual semagrams. A number of varieties of manuscript semagrams and authentic semagrams are illustrated next.

Type Spacing and Offsetting: In this appearance of manuscript semagrams uses the blank space in a paper to represent the binary values. The blank space can be used for the connecting the human being expressions, the sentences are even connecting the subsections. Approximately several combinations are probable except to an end, if the manuscript is become visible to having in excess of blank space it can be focus to inspection [4].

Tiny Spaces: These are the extra spaces used in between words and when these are read in a fix pattern forms a binary value which could have some meaning and thus the Steganography is implemented using tiny spaces; totally depends on the frequency of these.

Old Typewriter Effect: In the typewriters we had to set manually roller to print the super and subscripts and carriage forwarded in the written text. This carriage can be considered in as a way to hide information in the form of sub and super scripts.

Real Semagrams: A real or actual semagrams realistic utilize is generally because a pointer of a better, earlier established ahead communication. For example, Bob needs to inform Alice that the whole thing is set for Tuesday night. A real semagrams might be a postcard through a picture of a Baga beach. This might be the approved upon code to point out positive. An additional semagram with a representation of an Alaskan mountain variety might mean unconstructive.

2.4.3 Digital Steganography

Digital file arrangements can be used for Steganography, other than the designs that are more appropriate are individuals among a high degree of idleness. Idleness can be described because of the bits of a purpose to facilitate give accurateness future greater than essential for the things utilize and show [5]. The unnecessary bits of a thing are individual's bits with the purpose of can be changed with no information and the modification being distinguished effortlessly [6]. Digital image and digital audio files particularly fulfill with this condition, whereas study has also revealed additional file formats with the purpose of used for information thrashing.

2.5 Types of Digital Steganography

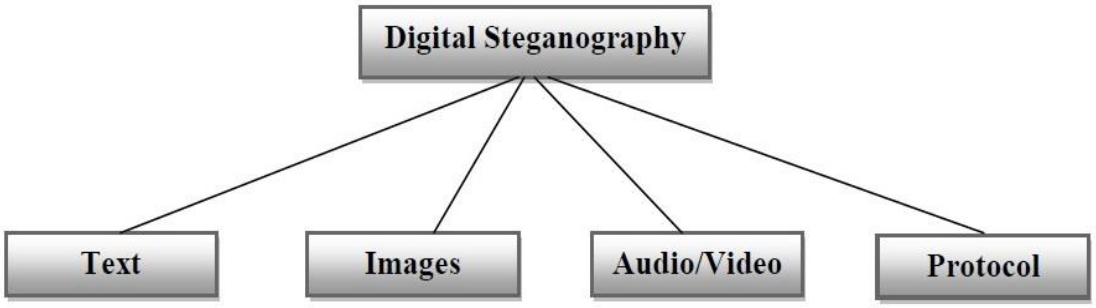


Figure 2: Types of Digital Steganography

Figure 2.2

2.5.1 Text Steganography

Texts Steganography can be categorizing in three fundamental groups are:

1. Format Based Random,
2. Statistical Generation
3. Linguistic Method.

Format based random Steganography works on the formatting of text. Text written in a particular format may be considered as information hidden. Formatting may involve insertion of spaces, misspellings, font resizing, etc.

Statistical generation technique generated the cover message with the help of some mathematical functions. It may be character or word sequencing. Randomly sequence gives place to hide secret information [5]. Another way of character randomization is word length.

Linguistic method considers linguistic properties of text. Message is hidden inside the linguistic structure and syntactic structure.

Some of the existing approaches of text Steganography are:

- Line Shift
- Word Shift
- Syntactic Method
- White Steg
- Spam Text

- SMS Texting
- Feature Coding
- SSCE (Secret Steganographic Code for Embedding)
- Word Mapping
- MS Word Document
- Cricket Match Scorecard
- CSS (Cascading Style Sheet)

2.5.2 Audio Steganography

In all-purpose Steganography relies on the limitation of the human being hearing and visual system. Audio Steganography obtains improvement of the psycho acoustical covering occurrence of the HAS (Human Auditory System). Auditory masking or psycho acoustical belongings cause to be a fragile attitude undetectable during the present of a physically powerful nature in its spectral/temporal region. HAS have low differential range although dynamically ranges 80 dB. Human actually can't perceive the low frequencies when they are mounted inside any tone or noise. These can be perceived using the special instruments and information may be gathered.

In the audio Steganography covert communication is surrounded into digitized audio signal which consequence insignificant changing of binary order of the consequent audio file and folders. There is commonly used process for audio Steganography as following:

- Parity Coding
- LSB Coding
- Spread Spectrum
- Phase Coding
- Echo Hiding

2.5.3 Video Steganography

Video documents are commonly collection of sounds and images. The techniques which are applicable on images and music files can be used for the video files also in combination. Commonly used method for the video files is DCT, it workings with altering the position of

video images within a videos, barely so that a great deal that it is not visible through the human naked eye. This is further defined concerning how DCT workings, DCT modifies principles of definite part of the video images, and it regularly surrounding them.

2.6 Image Steganography

In a digital computer, the images are a combination of facts and figures that represent special light intensities within unusual region of the images [7]. Images are combination of pixel and arranged in the form of matrix usually called as grid of pixels, remains in a rectangular map of pixels. Pixels are the points which form the image and color code over the pixel presents it. In an image pixels are read beginning of left to right and top to bottom formation in line by line in row manner.

In an image Steganography bit depth is known as the collection of bits in a color layout. It is used the number of bits in each pixel [9]. The negligible bit intensity in existing color system is 8 so that it means give explanation the color of each and every pixel in 8-bits representation [9]. Colorless and grayscale images are used 8-bits for each and every individual pixel and it is able to present 256 different color shades or color of gray. In a digital color image are usually accumulated in collection of 24-bit files. 24 bit pixel represents color pixel and color format can be in any of the format like RGB, CMYK, HSB, etc. In the RGB format the principle colors are RED, GREEN and BLUE. Every color is of 8 bits in a 24 bit color pixel and it gives shade range from 0-255 (256 shades) of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors [9]. Not to my surprise the larger amount of colors that can be displayed, the larger the file size [8].

2.6.1 Image Domain Steganography

Least Significant Bit

Least significant bit (LSB) toting up is a widespread, straightforward come close to to implant memorandum or in sequence in a coat representation [7]. The least significant bit of quite a lot of or every one of of the bytes contained by an illustration is untouched to a bit of the concealed meaning. At what time we are using a 24-bit illustration, a bit of every one of the RGB (red, green and blue) flush apparatus know how to be used.

At what time the numeral 202, which double depiction is 11001010. It is entrenched into the LSB of the representation the resultant is as track:

(11101101 11011101 11110100)

(10011110 11111101 11111100)

(10111111 11100010 10001011)

To hide one 8 bit number or message in LSB we require three 24 bit color pixel and thus the modification ratio becomes very low. Only three bits are change in one 24 bit color pixel and in rotate LSB of a pixel outcome in diminutive revolutionize in the concentration of the insignia. Revolutionize are so small so that not visible by necked eye. Even when appropriate cover images are used the difference between original and stego image remains null [7]. This process of hiding message can be made more secure using the shared key between sender and the receiver. He has no thought regarding the secreted in turn which pixels to objective lacking the undisclosed solution [12].

It is simplest outward appearance; LSB build use of BMP metaphors, because they boast used lossless solidity. Unluckily it is talented to hide from view a covert note in the interior a BMP dossier. In LSB only the negative thing is this that the cover size increases in a ration of 1:9 as per the size of secret image.

LSB and Palette Based Images

GIF image format is an image format regularly used to save images and known as Palette based images. GIF image format supports only a bit depth of less than or equal to 8 bits. It may store 256 colors maximum. These images store the color in palette and known as indexed images. Each pixel can be indexed to palette [13].

GIF metaphors are used in LSB pedestal steganography usually and have need of second endeavor and be concerned while accomplishment. If nearby palette admission are equivalent, there strength be unimportant or not able to be seen modify, but it ought to be the bordering palette doorway are exceptionally far removed from, the transform would be manifest [13]. Solitary promising resolution is to species the palette so that the shade divergence amid following colors is curtails [14]. An additional way not at home is to insert new insignia which are visually like to the offered insignia in the palette. This is compulsory to the inventive illustration encompass less only one of its brand ensign than the greatest numeral of insignia (this charge depends on the tad distance downward are used) [1]. By means of this come within reach

of, it ought to be carefully choosing the right swathe illustration. Fatefully it is tinker with the palette of alphabetical listing image vegetation an especially lucid autograph and construction it easier to discern.

A closing resolution of this dilemma is to utilize grayscale metaphors. In this predicament the 8-bit grayscale GIF image. Present are 256 diverse tinted lenses of grey [7]. The changes amid the colors are awfully deliberate and manufacture it harder to become aware of.

2.6.2 Transform Domain Steganography

JPEG compression

JPEG compression is used to compress the images of format jpeg or jpg. In jpeg or jpg format images there are three component of color RGB respectively known as Red, Green and Blue. These 3 components are converted to YUV format components; here Y is for luminance, and U & V are for the chrominance [1]. Human is responsive to luminance rather than chrominance [5]. In jpeg compression color data is down illustration to trim down the amount of illustration heading. Mechanism (U and V) are not speaking in straight and upright commands so by reducing these image sizes reduced by 2 [1].

Discrete Cosine Transform (DCT) is used for jpeg representation to make over them, other than comparable make over like DFT. These statistical make over convert the pixels in such a performance as to present the consequence of "scattering" the position of the pixel standards in excess of ingredient of the representation [5]. DCT on the whole exchange the image signal to frequency using the group of pixels in the formation of 8 × 8 pixel blocks and 64 DCT coefficients are generated [10]. It means all the 64 image pixels will be affected if the block of single DCT is modified.

Quantization is the main step of compression technique in this human eye property of finding difference in brightness change is challenged. Although human eye is very sensitive in finding out the difference in brightness of images over a big region, but this is reduced as JPEG compression uses quantization coefficients by dividing the images in blocks [1]. Huffman encoding is used to round the size of image and coefficients [5].

JPEG Steganography

In past decades it was considered that JPEG images are not good for the sake of steganography. Since they are used lossy solidity which consequential ingredient of the likeness statistics has being misused? Single of the main individuality of steganography is the element. In sequence unknown is reserved in the continual development and generates the probability of in sequence break. It is difficult for someone to hide a message in image which is not noticeable but due to JPEG compression it is possible because the ratio and region of human eye become small after its implementation.

Single of these possessions of JPEG is oppressed to construct revolutionize to the illustration imperceptible to the human being unclothed eye. For the period of the DCT adjustment segment of the firmness algorithm rounding blunder occurs which are not visible in coefficient data [7]. It gives a hint that the algorithm is of category lossy but this technique must not be used as the data may be lost during the stego process and retrieval of data from the stego image due the property and nature of algorithm which is lossy, since the density would devastate each and every one in sequence in the course of action. Therefore it is significant to make a distinction so as to the JPEG density algorithm is in point of fact not speaking into lossy and lossless modus operandi. The DCT with the quantization juncture outline constituent of the lossy tread, whereas the Huffman indoctrination used to auxiliary apply pressure the statistics notorious as lossless. Steganography preserve take position surrounded by these two stages. By means of the matching philosophy of LSB adding together or inclusion the memorandum is able to be entrenched into the slightest noteworthy bits of the coefficients earlier than be apposite the Huffman indoctrination. As a consequence of implant the in sequence at this juncture in the makeover sphere of influence, it is extremely easier said than completed to become aware of, since it is not in the illustration sphere of influence.

Image or Transform domain

In Figure 2, we are distinguishing various steganographic algorithms container what's more be classify as person in the likeness sphere of influence or in the makeover sphere of influence depending on the accomplishment.

Patchwork

Mélange is a statistical routine and it uses recurring blueprint indoctrination to hide from view a memorandum in an image [7]. It reiterates to secrete memorandum distribute it all the way

through the sum total illustration [13]. A pseudorandom integer originator is functional to top quality two piece of the illustration patch A, patch B [16]. Pixels in Solitary Square are pitch-black and in other are lightened. Let in patch A lightened and in patch B darkened [16]. This darkens and lightens process basically effects the intensities of the images block areas through a constant value [15]. Thus contrast is changed in image portions and hardly noticeable with human eye because the chrominance is only changed while the luminance remains unchanged [13].

Patchwork approach only embeds one bit at a time and this is the biggest disadvantage of it. To overcome this problem bits could be embedded in proportion by subdividing the image [17]. Though it contain difficulty but it in addition encompass an improvement, so as to the underground memorandum is disseminated greater than the inclusive illustration, consequently it be supposed to one plot of land be smashed as well as the others possibly will unmoving live to tell the romance [13]. This on the other hand, depends on the volume of the significance, prearranged that the significance knows how to no more than be continual right through the illustration if it is undersized an adequate amount. If the significance is moreover full-size in volume, it knows how to no more than be surrounded previously [7]. This come within contact of is for all time used as an individual and separate, independent approach. It hardly depends on the host image and looks like robust approach for hiding the message in images [17].

Spread Spectrum

Spread spectrum technique spread the message throughout the cover-image which is about to be hidden and this property makes it hard to be detected [11]. Marvel et al. have proposed a system which was combination of spread spectrum communication, in this arrangement fault be in charge of regulations and illustration dealing out to secrete in sequence in supplementary descriptions [15].

Spread spectrum broadens the band girth of tapered band indicator all the way through a crowd of frequencies over an announcement set of connections [15].

Spreading process is done by fitting tapered band waveform among a spacious crew waveform such as colorless clamor. In dispersion band performance bandwidth is distributed so the narrowband frequency becomes low and its energy goes downgrade and remains undetected. In this message is combined with cover image after hiding it in noise format [15]. Because the

control of the entrenched indication is a great deal inferior than the authority of the wrap picture. The entrenched picture is not obvious to the person look at or by processor investigation devoid of right of entry to the unique representation [15].

LSB in BMP – When implant a meaning in a "raw" illustration, that have not be distorted with density, such so as to BMP illustration, present survive a replacement amid the invisibility of the meaning and the quantity of in sequence that be able to be entrenched. BMP illustration is bright to trouncing realistically a great significance, excluding the detail that additional bits are tainted consequences in a better likelihood that the tainted bits be able to be see with the person bare look at. The main shortcoming concerning LSB in BMP metaphors is of course the misgiving that strength arise as of a very great BMP illustration life form put on the air amid diverse gathering, so that BMP icon is not broadly used any longer.

Recommended applications: LSB in BMP illustration is for the most part appropriate for submission somewhere the spotlight is on the quantity of in sequence to be convey and not on the concealment of that in sequence.

LSB in GIF – The physically powerful and feeble position concerning implant in sequence in GIF metaphors by means of LSB be supplementary or less the similar as folks of by means of LSB with BMP representation. The chief dissimilarity is that the GIF metaphors merely have a bit deepness of 8 and the quantity of in sequence that can be obscured is fewer than with BMP illustration. GIF metaphors are for the most part disposed to algebraic – or diagram assault – while the palette handing out that have to be completed vegetation a very unambiguous autograph on the reflection. In this approach it needy on the file layout as glowing as the illustration itself, so that the wide of the mark preference of illustration can result in the significance being discernible.

Recommended applications: LSB in GIF representation is a exceptionally capable algorithm to use what time implant a levelheaded quantity of information in a grayscale reflection.

JPEG compression – JPEG solidity leads to a stego illustration with a small echelon of visibility of out of sight or underground in order. This composes the push in makeover sphere of influence and it's regularly used and incredibly in style files design to accumulate metaphors. Accordingly it is assembly the slightest apprehensive algorithm to be used. On the

supplementary furnish, the development of the firmness is a very geometric modus operandi, making it second easier said than done to put into operation.

Recommended applications: The JPEG representation file arrangement knows how to be used for the majority appliance of steganography, but is more than ever proper for metaphors that have to be exchange a few words over an unfasten structure atmosphere like the Internet.

Patchwork – The prime shortcoming of the hodgepodge loom is the petite quantity of in sequence that can be out of sight in one illustration. These material goods can be misrepresented to be full of more in sequence but one possibly will encompass to furnish up the confidentiality of the in sequence. The most important improvement of Patchwork's is its forcefulness aligned with malevolent or unintended illustration management. It be supposed to be a stego illustration using hodgepodge may be harvest or turn around, so that the significance statistics might be misplaced but as the significance is repetitively entrenched in the representation, the preponderance of the in sequence will continue to exist.

Recommended applications: crazy-quilt is chiefly proper for put out a little quantity of exceptionally perceptive in sequence.

Spread spectrum – This is the full-bodied modus operandi of in sequence hitting in illustration adjacent to the arithmetic come within reach of as it distribute the in sequence and go over it all the way through and this modus operandi apposite to steganography payable to its distinctiveness.

2.7 Techniques of Steganography

2.7.1 Substitution Technique

Alternate outmoded fraction of a cover up with an underground meaning instance: Least Significant Bit (LSB) replacement. In this technique the cover file bits are replaced with the bits of secret message. Replacement bits are chosen like in a ways so that it remains unnoticeable. Bits replaced are kept as low or in high ratio between cover file gets replaced, so it will also influence the victory of this scheme As a wide-ranging regulation, with all supplementary bit that is reinstate the probability of uncovering boost, but in numerous suitcases added than solitary bit per coat up file byte can be reinstate fruitfully [18].

LSB bits are substituted most commonly is substitution techniques of information hiding as changing the LSB bits hardly modifies the image and image remains as same as original when viewed with necked eyes. The main improvement of this scheme is that it is trouble-free to be aware of and put into operation.

Example:

11000100 10000110 10101001 10101101

01110001 01100101 01101010 01100110

In LSB substitution we use color codes which are formed with 8 bits each and may be for red, green or blue.

Example:

We are having color code or say bit value as 11111111 which is equivalent to 255 if a single bit will be change will definitely change the color code. Last bit of 8 bits is considered as least significant bit as change in its value will affect the color code nominally.

Like 11111111 is change to 11111110 will change code to 254 but MSB is changed than it becomes 01111111 which is 127 and this code difference is easily noticeable.

10000111 10000010 10101001 11001101

01111010 01100001 01101010 10100110

This is out of sight memorandum; which is the numeral of a closet in a bus workspace, so with the intention of closet quantity 213 characterize as double numeral is 11010101

In LSB method we will use 220 as message and will hide it within cover.

10000100: 0 is substituted with 1 because change arrives.

10000110: 0 is substituted with 1 because change arrives.

10001001: 1 is left as it is as same in both cover and message.

10001101: 1 is left as it is as same in both cover and message.

01111001: 1 is left as it is as same in both cover and message.

01100101: 1 is left as it is as same in both cover and message.

01001010: 0 is left as it is as same in both cover and message.

00100110: 0 is left as it is as same in both cover and message.

Only two bytes among of the 8 bytes of cover message are changed and our message gets hidden in it with the help of minimum changes and thus is not predictable. It was just a demo of image steganography when this is done over kilobytes or megabytes of data it becomes impossible to detect the secret information in the image and difference is unnoticeable. Color code remains same and image looks as the original.

The LSB system does include its disadvantage. from time to occasion it is depending on the pixel, alter the LSB can appreciably modify the pixel's property, manufacture a give the impression of living being out of leave in the figure or photograph and as a result subject matter to revealing. This predicament can be restricted the quantity of substitute bits and consequently the volume of the covert meaning. Another impenetrability with this replace method of note thrashing is the similes fighting to be alter. If the representation is crop or rotate the algorithm will not be talented to come across which smallest amount important bits are part of the memorandum and which ones are now theoretical to exist nearby.

2.7.2 Transform Domain Technique

Implant undisclosed meaning in a makeover liberty of plaster model: Steganography in the Discrete Cosine Transform (DCT) sphere of influence. This modus operandi is also awfully efficient and an insignificant trickier. Principally, make over sphere of influence practice hide memorandum statistics in the "change leave" of an indication. More than the complex now a day citizens are drive metaphors backside and into view, and a large amount habitually they exercise JPEG layout. JPEGs density uses the perception of removal of further statistics or pointless amount of information without which image can be created without any loss. It works on the

principle of approximation of the original image to a small scaled image; that modify, that estimate, is make over liberty, and that revolutionize can be used to bury in sequence [19].

Discrete Cosine Transform (DCT) is the grounding for JPEG density and it can be subjugated for in sequence hitting. Single of the procedures, precise DCT coefficients is in style and budding manner of image hitting. It creates a quantization table in which the coefficients are maintained and relative difference between location points is determined. Comparative results generated play an effective role. Bits are matched as result comparison. Matching occurs then everything is correct else the coefficients are replaced by each other and swapping is done; again the whole process is applied.

2.7.3 Spread Spectrum Technique

Direct Sequence- Information is portioned into to small chunks of data in direct sequence spectrum technique and all the divided portions are allocated a fixed bandwidth within a frequency channel. Data signal is modulated or combined with high data rate for the sake of high distance journey bit series that separate the statistics according to a prearranged increase share. Pointless statistics tempo bit succession policy helps the indication refuse to accept intrusion and allow the novel information to be healthier if any of the in sequence bits are spoiled during the spread [20].

Frequency Hopping- This procedure divides an extensive portion of the bandwidth field into several achievable convey frequencies. Habitually occurrence get campaign use a lesser amount of rule and are not expensive, but the show of direct string broaden variety system is regularly superior and supplementary consistent.

2.7.4 Statistical Technique

Statistical manner use what is identifies a”1-bit” Steganographic process. This manner push in one bit of in order only in a digital hauler, and thus fashion a numerical revolutionize in the cover specify by a “1” a swathe left unmoved specify by a “0”. This system’s triumph is support on the recipient’s talent to make a distinction between personalized and original coat [21].

2.7.5 Distortion Technique

Amass in order by indication twist instance: be different the detachment stuck between successive outline and vocabulary to send out secret in order. This system of Steganography creates revolutionize in a swathe purpose to hide in sequence. The surreptitious note is improved after the algorithm put side by side the misused, imprecise plaster with the creative [19].

2.7.6 Cover Generation Technique

Encode in sequence in the system a coat is generate illustration: computerized production of English manuscript. Swathe production means are maybe the largest part exclusive of the six types. Usually a plaster entity as preferred to hide a memo in but with the target of is not the holder here probable. A coat age band method in point of fact creates a swathe for the one and only idea of hitting in sequence. Spam impersonate is a brilliant instance of a envelop age bracket scheme.

2.8 Literature review

Atallah M. Al – Shatnawi [23]: - In this paper, a new Steganography procedure is accessible, implemented and analyzed. The proposed method hides the secret message based on searching about the matching bits. This can be compared with LSB benchmark process and implementation of this is done to hide the information. Like we want to hide message "I will dance like this only" in 2 image of format type BMP images. Results can be compared based on the ratio of equality in bits and non equal bits between the pixel color values and the covert message values. The proposed method is well-organized, uncomplicated and fast. It is tough to attack and improve the image quality; hence it is obtained 83% of an accuracy ratio.

Mamta.Juneja and Parvinder S. Sandhu [24]: - The proposed system is an approach used to embed text into gray image (BMP).It enables the user to present the method with both cover and text, and get a resulting image that contains the concealed text inside. The method uses LSB technique to put in secret image or message in cover image after apply cryptographic algorithms. Key is generated via standard key generation algorithm RC4, proposed system aim to provide improved robustness, security due to multi-level security architecture along with faster embedding and extraction process irrespective of size of embedded text.

Mamatha.T [25]: - these documents believe an in series theoretic symbol for steganography by a motionless contestant life form planned. The opponent's task of individual stuck between an in the obvious coat memo C and adapted communication S have covered in order is interpret as a difficult mess. The memorandum is the job of sculpture of a few quality or book. Each book or qualities of the memo can be signifying as an ASCII cost which is also even or odd integer. Depending on this uniformity, the disposition is encrypted in a dissimilar way. This thesis describe how an still or odd encryption base on ASCII worth is functional and how encrypted communication is untouched by Gray code and implant with image or image can sheltered the memo and thus create cryptanalyst's job complex.

Ravinder Reddy Ch, Roja Ramani A[26]: - In this planet, the in sequence move using complex or internet is fast rising since it is consequently easier as healthy as earlier to send out the statistics to phone side or purpose. So, a lot of folks and industry citizens use to transport business papers, significant memo or in turn by way of internet. Sanctuary is a most insignificant matter while transport the statistics via internet for the reason that any unlawful human being can scythe or cut the statistics and put together it of no price or get clutch of in succession unintentional to him. The chief tip of this copy is to look into the extremity steganography algorithms and stenographic request such so as to it provide good solitude or safety. The future comes up to provide superior safety and be able to defend the message from stego assault. The representation motion doesn't modify a large quantity and it is irrelevant when we set in the memo into the picture and the illustration is cramped with the private code word. So, it is not promising to shatter the statistics by hacker or unlawful people.

Ankita Gangwar, Vishal Shrivastava[27]: - This paper bring in a best move toward for Least Significant Bit (LSB) based on representation steganography that improve the obtainable LSB replacement method to perk up the refuge level of covert in order. First the covert in sequence is encrypted using a key produce by a few average key age band algorithm; it avert unofficial admittance. In chain is hidden in definite section of envelop figure. For this grounds, momentous the improvement scheme, everyone can dig up the veiled in turn. When it is secreted in definite site and segment of cover up representation afterward it becomes hard to take out the in turn until good algorithm is not old and right key is not practical.

Mrs. Richa Raja Gautam, Prof. Rakesh Kumar Khare [28]: - The charming rise in Mobile message in the last a small number of decades, guide the condition of the secure e-mail of information sandwiched between mobile handset. Particularly refuge matter a lot during program of metaphors and cartridge. Model illustration or envelop reproduction is used in this system and it advise a more inconvenient and held tactic. Key randomized is and used the key and the chief representation both concurrently entrenched on the model illustration. The equal input will be afterward used by the handset to extract the secreted illustration surrounded by the model representation.

S. Mohanapriya [30]: - Mobiles are the well-liked message medium nowadays; it is often used to transport in order over net. Data flow as of one position to additional and need to be confined. To put into practice it encryption can play a very important role flanked by two communicate human being over portable networks. There are quite a few method are used for speak covert mail for fighting rationale or in organize to guarantee the seclusion of message relating amid two parties. Steganography is taking lay of cryptography or creation an enormous edifice with it. By means of MMS and SMS figure are remove and in order can be store up in the rear them without problems. It is the good amount reliable practice for top secret announcement. Hiding in rank, mainly in descriptions has been a further resolution for secret statement. There are so loads of procedure for steganography and cryptography. Representation steganography is frequently used. Minute encryption algorithm is chunk symbols algorithm. It is simple and nippy but unsurpassed for mobile purpose.

B. Sharmila and R. Shanthakumari [31]: - In LSB statistics beating is done at tiny tempo which skeleton the illustration hitting impression, to triumph over this crisis edging uncovering is used. Present are quite a few algorithms which uses boundary recognition methods for illustration hitting. 'Edge adaptive image steganography based on LSBMR algorithm' works on the hoary-balance metaphors and at hand consequences after investigate routine of periphery recognition for painted metaphors (JPEG). When by means of it for the blush figure it gets bespoke tiny bit and PSNR and MSE are premeditated.

B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, M.Gomathymeenakshi [32]: -Today the civilization is of opposition and age is of internet and in order. It makes it significant to remain the in order secure. In order is put away behind metaphors; plaintext is pop

in into metaphors which barely modify the metaphors. Illustration pixels are look into and accustomed with the in sequence to be protected and this is branded as OPAP (Optimal Pixel Adjustment Process).

M.I.Khalil [33]: - It is from time to time not sufficient to keep the inside of a letter covert, it may also be necessary to remain the extinction of the communication or in sequence covert. The manner or performance used to concern this is vocation Steganography, and it is the modus operandi of beating one average of communiqué within a further. Many unlike delivery service file format (text, sound or image) are able to be used, but digital metaphors are the most in style because of their occurrence on the association or Internet. Essentially, the letter hiding is ended after recognize the superfluous bits of wrap illustration and implant the pin turn into the outmoded bits and manufacture a stego representation. In this manuscript we will thrash out the occasion of hitting short auditory note inside a digital illustration. The planned draw near or system encrypts the acoustic meaning before hitting it in figure or photograph heading. The system of extract the acoustic letter from stego figure will be discussed as fighting fit.

Mr. Pushparaj P. Nerkar, Vishwajit K. Barbudhe, Prof. Aumdevi K. Barbudhe [34]: - In this document, we here a story practice to implant covert meaning in the wrap reflection. The basic impression of the projected practice is by trouble-free Least Significant Bit (LSB) switch. In this planned practice a steganography system that pertain a modus operandi to set in a wavelet compacted covert meaning limited by the Least Significant Bit (LSB) of the envelop illustration pixels in a unambiguous model or model. The planned procedure results in growing the hidden meaning capability and safety measures or isolation level. The underground or covert memorandum won't be evident after implant and know how to be pulled out in a while.

V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P. Chenna Reddy [35]: - The utterance Steganography is copied of Greek statement steganos and it means “Covered” and graphy earnings “Writing”. It refers the discipline of “invisible” communiqué. To hide unnamed in order in various file format, there survive a large series of steganographic process a few are supplementary easier said than done and a few are straightforward. The Least Significant Bit (LSB) insert modus operandi suggests that the statistics veiled in the least momentous bits of the illustration and the individual eyes would not be gifted to perceive the veiled illustration in the

swathe file. By using this technique we can conceal our metaphors in 8-Bit, 24-Bit, Grayscale arrangement.

Vijay Kumar Sharma, Vishal Shrivastava [36]: - Steganography is a bough of communication or in order hiding. It tolerates the populace to talk in covert. As more and more stuff turn out to be nearby by electronic means, the in charge of of steganography on our life will go on to breed. Much off the record in order was leak to a opponent solid using steganographic gear that hide the in rank in melody and illustration or photograph archive. The reason of steganography is an significant motivation for characteristic assortment. In contemporary years, many winning steganography method contain been predictable or future. They feature up to by Steganalysis. Steganalysis is a kind of assault on Steganography Algorithms. To make it safe and echo against the Steganalysis attack, a newest steganographic algorithm or coordination for 8-bit (grayscale figure) or 24-bit (color illustration) is to be had. MSB of top covert account or significance are replacing with LSB of envelop likeness. It augments eminence of ending icon radically with small second computational involvedness or impenetrability. The most evil glasses case MSE connecting the stego-figure and the plaster/ wrap -illustration is follow-on. The trial outcome give you an idea about that the stego-picture is illustration impractical to tell apart from the novel cover-illustration when n<=4, since of improved PSNR computation which is premeditated by this procedure. It moves toward the statement that if the trait or a typical is perceptible, the point of harass is clearly identifiable, therefore the aim here is for eternity to coat up the very extinction of the rooted statistics.

Chapter 3 PROPOSED WORKS

3.1 Image Processing

Image dispensation is a process to switch a figure into digital outward appearance and achieve some maneuver on figure meting out, in this regulate to get an improved icon or to haul out a little priceless in turn from it. It is an outward manifestation of warning sign payment in which contribution is illustration approximating tape casing or snap and amount fashioned may be likeness or individuality connected with that metaphors. Generally illustrations dealing out organization comprise luxury descriptions as 2-D signal while be appropriate beforehand set indication dispensation method to them.

There are three basic image processing steps are include

1. Importing the image with digital photography or by optical scanner.
2. Manipulating and analyzing the reflection which takes account of data density and illustration upgrading and spot prototype that is not to able to be seen person eyes like settlement photograph.
3. Production is the previous phase in which consequence can be distorted representation or account that is bottom on representation examination.

3.1.1 Fundamental Purpose of Image processing

Image Acquisition- The first procedure is to obtain a digital image. To do this we want to image sensor equipment having the capacity to digitize the gesture shaped by the antenna. The antenna possibly will be a line up- check camera, a TV camera, and to.

Image Enhancement- It is a character district of picture dealing out which is worn to commence aspect that is concealed or to emphasize sure skin tone of attention in an illustration.

Image Restoration- It is as glowing deal with taming the outward appearance of a symbol. But it is concluded by way of the probabilistic or arithmetic design of diagram frightful setting.

Image Recognition - It is developments that dispense a sticker to an illustration stand on it that means the information provided by its descriptors and the accepted image is interpreted by assigning a meaning to it.

Visualization- Image processing to observe the objects are invisible.

Image Retrieval- Try to find the significant image for the image processing.

Image Sharpening and Restoration- In this we provide the improved the visible quality of the original image and return without restoration good image quality.

Measurement of Pattern- In this we are dealing with different objects in an image to find out the pattern of the image.

Colour Image Processing- As we know, to restore the natural characteristics of an image it is necessary to preserve the colour information associated with an image. For this purpose we go for the colour image processing.

Wavelets and Multi Resolution - This is the base for representative metaphors in similar amount of representation declaration. Mainly it is in a job for photograph data density and for pyramidal illustration where descriptions are subdivided into sequentially into slighter region.

Compression- This way is used for the cargo space necessary to salt away an illustration or the bandwidth requisite to transmit it which is on the whole noteworthy in internet purpose.

Segmentation - It may be defined as portioning an input image into its constituent parts of objects. It is very important to differentiate between different objects in an image as in the case of systems working for crowd control, or traffic control. In character recognition, the key role of segmentation is to extracting individual characters and words from the background.

Morphological Processing- In this we are dealing by means of equipment for takeout image mechanism. It is helpful in account and the symbol of the silhouette of illustration.

3.1.2 Types of Image Processing

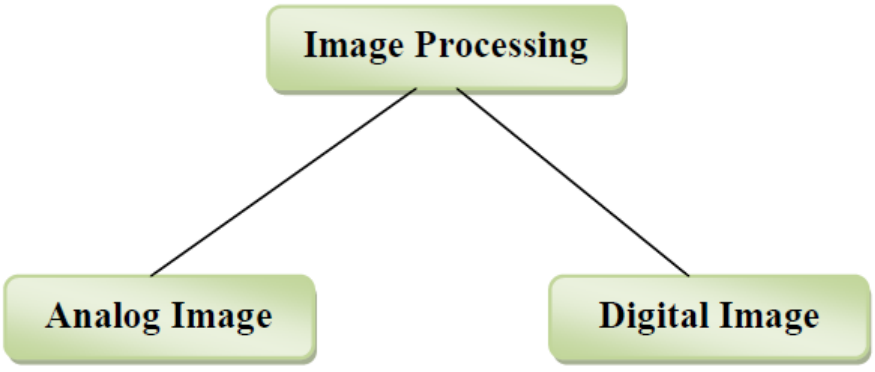


Figure 3.1

Analog Image Processing

Analog or chart system of representation dispensation can be used for the solid reproduction like photographs and printouts. A being who examine the representation use dissimilar ground rules of clarification while with these chart procedure. The figure dispensation is not now incomplete to district to have to be careful but on facts of the self who is investigate the representation. Association is an extra significant tool in figure dispensation during illustration system. So analyzer relates a grouping of statistics defense and individual understanding to illustration dispensation.

Digital Image Processing

Digital Image dispensation methods assist in treatment of the digital metaphors by using processor. At the similar occasion as uncooked statistics as of imaging sensors as of settlement stage enclose deficit. To get in excess of such fault and to get individuality of in sequence, it has to commence dissimilar stage of dispensation. Generally three phase that every one types of statistics have to undergo while with Digital manner are giving out of the illustration, augmentation and exhibit the illustration and the in sequence mining from the illustration.

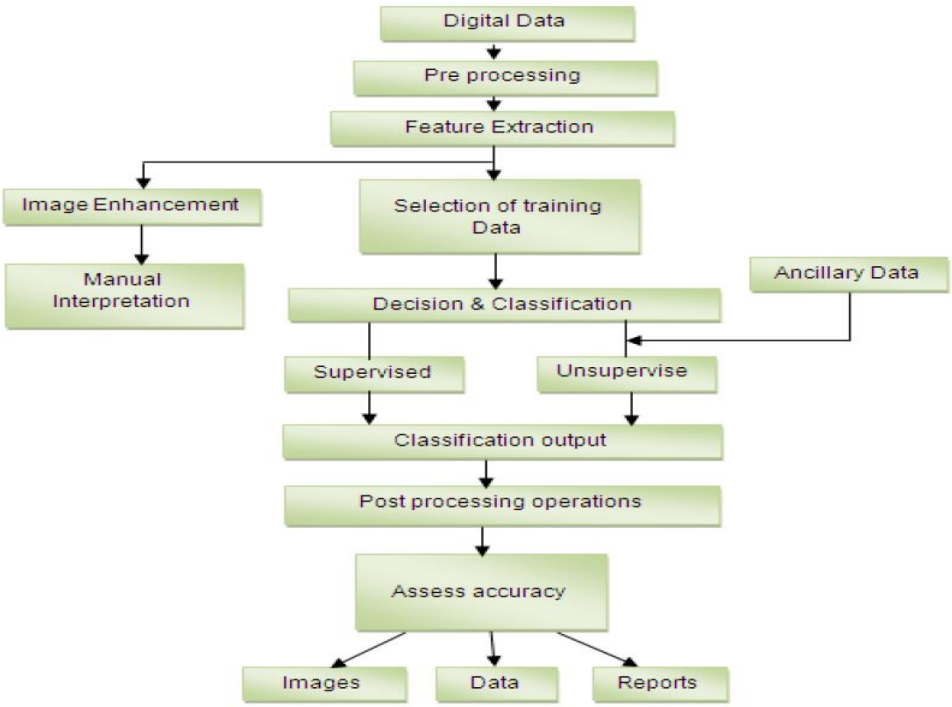


Figure 3.2

3.1.3 Applications of Image Processing

Intelligent convey arrangement – This procedure be able to be used in transfer sign gratitude and mechanical digit plate acknowledgment.

Remote Sensing – In this reason, sensors imprison the movies or metaphors of the earth's exterior using multi phantom scanners or by isolated intelligence satellites. Then these metaphors are transmitting to the soil posting anywhere they dig up progression. These practices rally round us to take to mean the regions old in urban arrangement, torrent cover, undeveloped construct scrutinize, supply recruitment etc.

Moving object tracking – This reason facilitates to assess motion limit and gain illustration confirmation of the touching article. The types of dissimilar move toward to path objects are:

- Activity based tracking
- Acknowledgment based tracking

Defense surveillance – To stay a look at on ground and mountain, we use protection observation systems such as mid-air or in the air observation scheme. This classification is too used to place and notice the types of marine boat. The major function is to sort the variety of substance there in the water corpse part of the representation The dissimilar parameter for illustration distance end to end, width, locale, boundary, density are used to classify the substance. It is necessary to recognize the distribution of this substance in dissimilar instructions to offer particulars all probable pattern of the yacht. We can know the complete marine setting from the spatial distribution of this substance.

Biomedical Imaging techniques – In errand of checkup judgment unlike types of imaging tools such as Ultrasound, X- ray, CPU support tomography (CT) and all that are used. The illustration of MRI, X- ray, and CPU give support to tomography (CT) are given below.

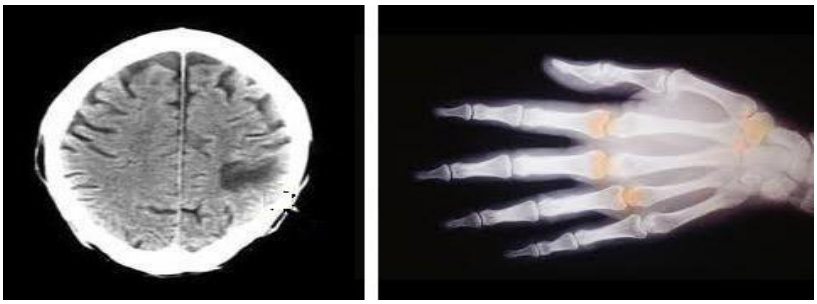


Figure 3.3

Heart sickness classification: –To order heart ailment, we are necessary to recognize the mass of the empathy and its silhouette and this is potential after judgment. We investigate the metaphors at radiographic point for improved judgment.

Lung disease identification: – In container of X- rays, the area that comes into view dim comprise air as area that appear lighter are hard tissues. Frame is additional broadcasting not obvious than tissues. The sympathy, the ribs, the diaphragm and thoracic backbone that divide the upper body hollow space from the abdominal hollow space are obviously see on the X-ray silver screen.

Digital mammograms– This is used to become conscious of the breast tumour. The mammograms are able to be analyzing using picture dispensation technique such as form psychoanalysis, segmentation, trait taking out, difference augmentation etc.

Automatic illustration examination structure– In this reason it is recover the excellence and efficiency of the creation in the manufacturing.

Automatic examination of glowing lantern thread– This procedure engages assessment of the corm developed practice. When the threads of bulb are owing to no evenness for a small occasion a double illustration piece is produce. Silhouettes recognize the non consistency in the playing field of the emotional cabling in the lantern. This practice is organism used by the GEC.

Automatic surface inspection systems– In the metal business it is significant to recognize the mistake on the facade. In errand of amount, it is required to notice any variety of abnormality on the turn metal facade in the blistering or frosty gently sloping refine in a strengthen deposit The reflection handing out modus operandi such as periphery discovery, consistency detection and the fractional scrutiny and all that are used for the gratitude.

3.2 Least Significant Bit (LSB) Substitution

Cover file have bits which are replaced or swapped with the secret image bits. Few bits are replaced so it hardly makes the presence in the human eye; this is called replacement. The figure of bits in the wrap folder that obtain replacement will too alter the achievement of this manner. As a broad law, with the every extra bit with the purpose of is put back the chances of discovery amplify, but in lots of luggage additional than one bit for each wrap folder byte be able to be put back productively [12].

LSB Substitution Technique for Embedding

STEP 1: The Host/Cover image and the watermark or message image are read. The message image is converted into a matrix.
STEP 2: Elements are normalized and intensity measures are rounded off.
STEP 3: Determine the size of both images.
STEP 4: Expansion Matrix is determined and watermark table or gird is created and values saved in binary format.
STEP 5: Elements are represented as pixel format in binary. LSB are set accordingly as both the cover and secret image matrix are of same size.
STEP 6: Matrix values are hidden in watermark cover image and Measure of type PSNR are calculated.

LSB Substitution Technique for Extraction

STEP 1: The watermarked image is converted to the Matrix of pixel values and the pixel values are in a binary format.
STEP 2: Watermarked image size Mw (height) and Nw (Width) is determined.
STEP 3: Expansion matrix is generated via converting LSB values to binary format.
STEP 4: Bits are grouped on the basis of number of bits per pixel.

3.3 Run Length Encoding (RLE) Technique

Run-length indoctrination is a statistics density algorithm that is support by the majority bitmap file arrangement, such as TIFF, BMP, and PCX. RLE is appropriate for squeeze any kind of

statistics with the exemption of its in rank happy, but the contented of the statistics will transform the density ratio accomplish by RLE. Still although virtually every RLE algorithms cannot finish the high density ratios of the added tricky density system, RLE is equally nippy to accomplish and uncomplicated to employ, making it a good deputy to also using a intricate density algorithm or send-off your depiction statistics uncompressed.

RLE workings by sinking the bodily mass of a repeating cord of font. This replicate cord, recognized as sprint, is typically prearranged into two bytes. The primary byte of the cord symbolizes the figure of font in the run and is recognized the run reckon. In real fact, a programmed run can comprise 1 to 128 or 256 font; the run reckon more often than not hold as the integer of typescript minus single (a value in the range of 0 to 127 or 0 to 255). The next byte is the rate of the cord or spirit in the run which is in the variety of 0 to 255, and is recognized as the run price.

This algorithm consists of put back large series of replicate in sequence with merely single thing of this statistics followed by argue against presentation how a lot of times this article is frequent. Near the clearer let's see a cord sequence instance is:

AAAAABBBBBBBBXXXXXXXXXXXXXCCCCCCCYYYYYYYAAAXXXX

This cord's extent is **47** and as we know how to see there is lots of repetition. By the run-length technique we put back some run with shorter cord chain followed by contradict.

A5B8X13C7Y7A3X4

The duration of this cord is **15**, which is about **33%** of the preliminary extent.

Variation of RLE Technique

Present are a figure of alternatives of run-length indoctrination. Picture statistics is typically run-length encoded in a sequential procedure that lavishness the picture statistics as a 1-D watercourse, quite than as a 2-D chart of statistics. In sequential dispensation, a bitmap is prearranged initializing at the higher absent bend and leaving on absent to correct crossways each scrutinize row (that means the X axis) to the base right bend of the bitmap (shown in Figure 9-2, a). But alternate RLE system can also be on paper to program statistics downward the extent of a bitmap (it means the Y axis) down the editorial (shown in Figure 9-2, b), to program a

bitmap into 2-D ground wrap (shown in Figure 9-2, c), or the still RLE to program pixels on a slanting in a zig-zag loom (shown in Figure 9-2, d). The strange RLE alternative such as this previous single strength is used in extremely listening carefully application but is typically fairly uncommon.

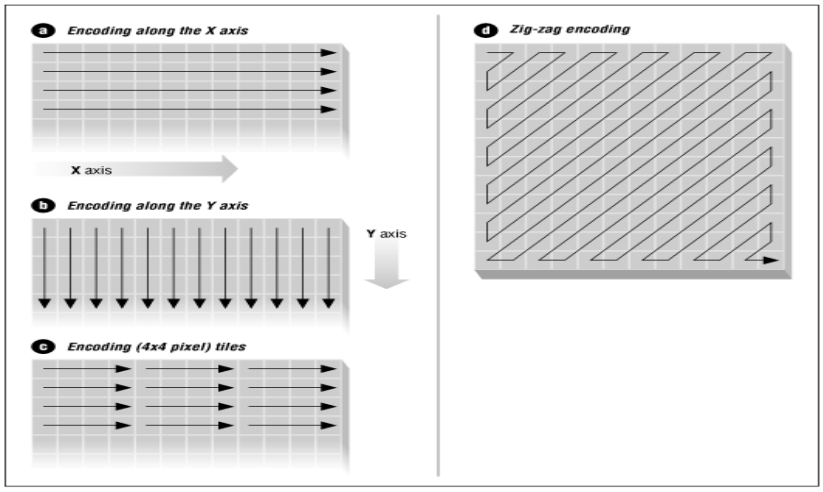


Figure 3.4 RLE Variation

One more infrequently-meet RLE alternative is a lossy run-length encoding algorithm. RLE algorithms are typically lossless in their practice. Though, removal data through the indoctrination scheme, usually by zeroing away one or two slightest important bits in every pixel, it can amplify density ratios devoid of damagingly worrying the look of very multifaceted images. This RLE technique alternative works well only by real planet images that hold many small variations in pixel principles.

Flow Chart

The basic flow chart of RLE Algorithm is given below

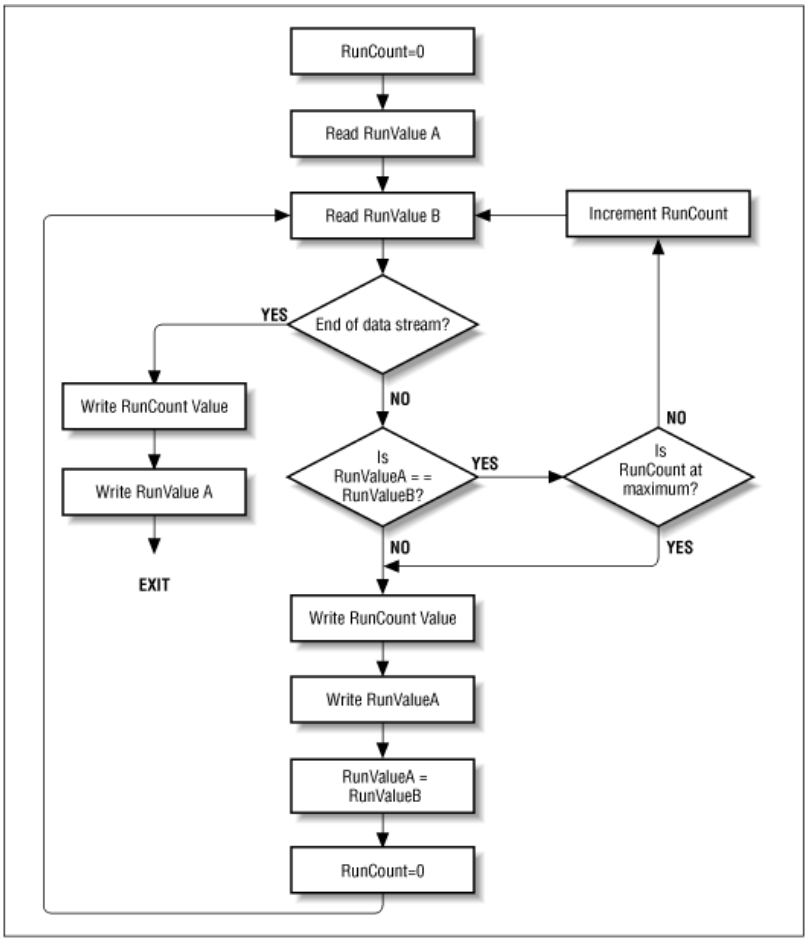


Figure 3.5 Basic RLE Flow Chart

3.4 Triple DES

The Data Encryption Standard (DES) is urbanized via an IBM group within 1974. It was then accepted as a general set in 1977. Triple DES is three moments slower than usual DES except it can be a lot of times extra protected if it is used in correct way. Triple DES benefit from a huge contract with wider utilize than DES since DES is so simple to smash with today's fast advancing knowledge. In 1998 the EFF using a specially urbanized CPU called the DES Cracker and it is directed to crack DES in fewer than 3 existences. 88 billion keys for each second can be procedure by the DES Cracker encryption whittles. Also, present can be a hardware machine which can look for all probable DES keys in about 3.5 hours and at a price of one million dollars. It is directly dish up to express that any association with restrained possessions can crack during DES with extremely little attempt these days. No rational safety specialist would think using DES to defend data.

Triple DES is just another form of DES process. It takes three times 64-bit keys, for an in general key extent is 192 bits. During the confidential Encryption, you on the whole kind in the whole 192-bit (24 character) key quite than incoming every of the three keys independently. The Triple DES DLL then break the key gives by the consumer into three associate keys and padding the keys if essential so they are every 64 bits extended. The encryption procedure is similar as normal DES, the only dissimilarity is that it is frequent three times and that's why it is named Triple DES. The easy text or statistics is encrypted with the primary key then decrypted with next key, and finally encrypted with the third key.

Therefore, Triple DES scurry three times slower than normal DES, but it is more secure if used correctly the process for decrypting amazing is the similar as the procedure for encryption, bar it is executed in turn around procedure. Similar to DES, statistics is encrypted and decrypted in 64-bit big pieces. Unluckily, there are some flimsy keys to one ought to be conscious of every three keys. The primary and next keys and the next and third keys are the equivalent.

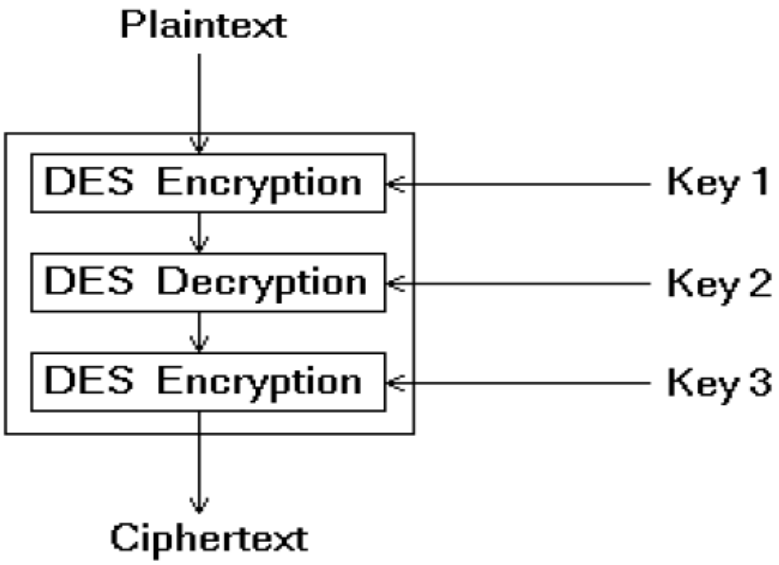
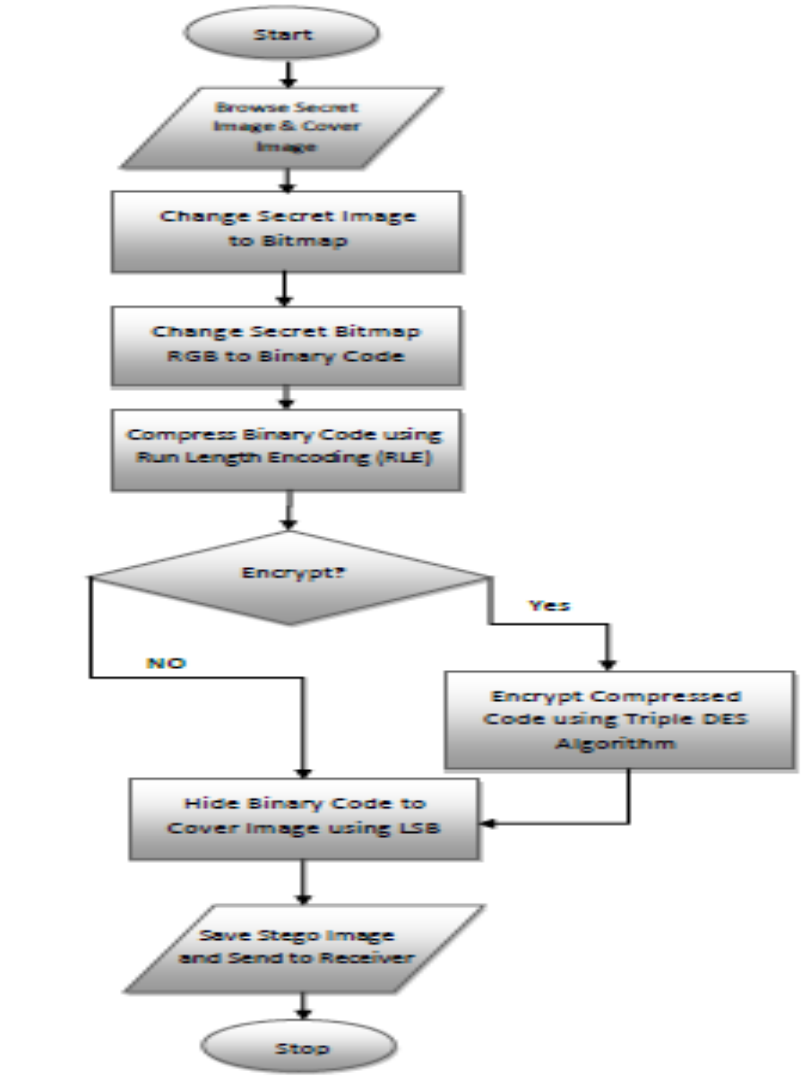


Figure 3.6

3.5 KVL Algorithm

LSB algorithm is used many time for the sake of steganography and implemented by people successfully in the area of text and images. In KVL algorithm we have tried to ambient the effort of people and make an extra effort to make the standards of steganography high than previously created. We have not only proposed the algorithm for steganography but also implement it with other algorithms of compression and cryptography. We have used LSB, RLE and Triple DES as the principle algorithms in our proposed work. We require two images; that is one as cover image and other is the secret image which we actually want to hide behind the cover image and want to transfer over the medium as a protected file. We get the secret image and change it to binary formation and then compress it using the Run Length Encoding Scheme. This conversion is done only by using the small concepts of how the digital number is converted to the binary number which is called as binary conversion of numbers. This is the basics of the computer technology and we have read it in our golden days of study when computer arrived in our life. Colors used in the RGB format have integer values and these can be regulated to binary information as a computer machine works only on zero and ones. This is done for the whole image. It becomes a large amount of binary information which required to be compressed and then the encryption which is optional is performed and next the reminder is secreted in the wrap representation by the LSB substitution and transferred over the network. Receiver end the whole process is reversed and the person willing to get the message receives the message by applying the reverse steganography KVL algorithm. Here we used Triple DES algorithm with MD5 hash generation methods to generate the hash code for the key passed by the user to encrypt the compressed binary information.

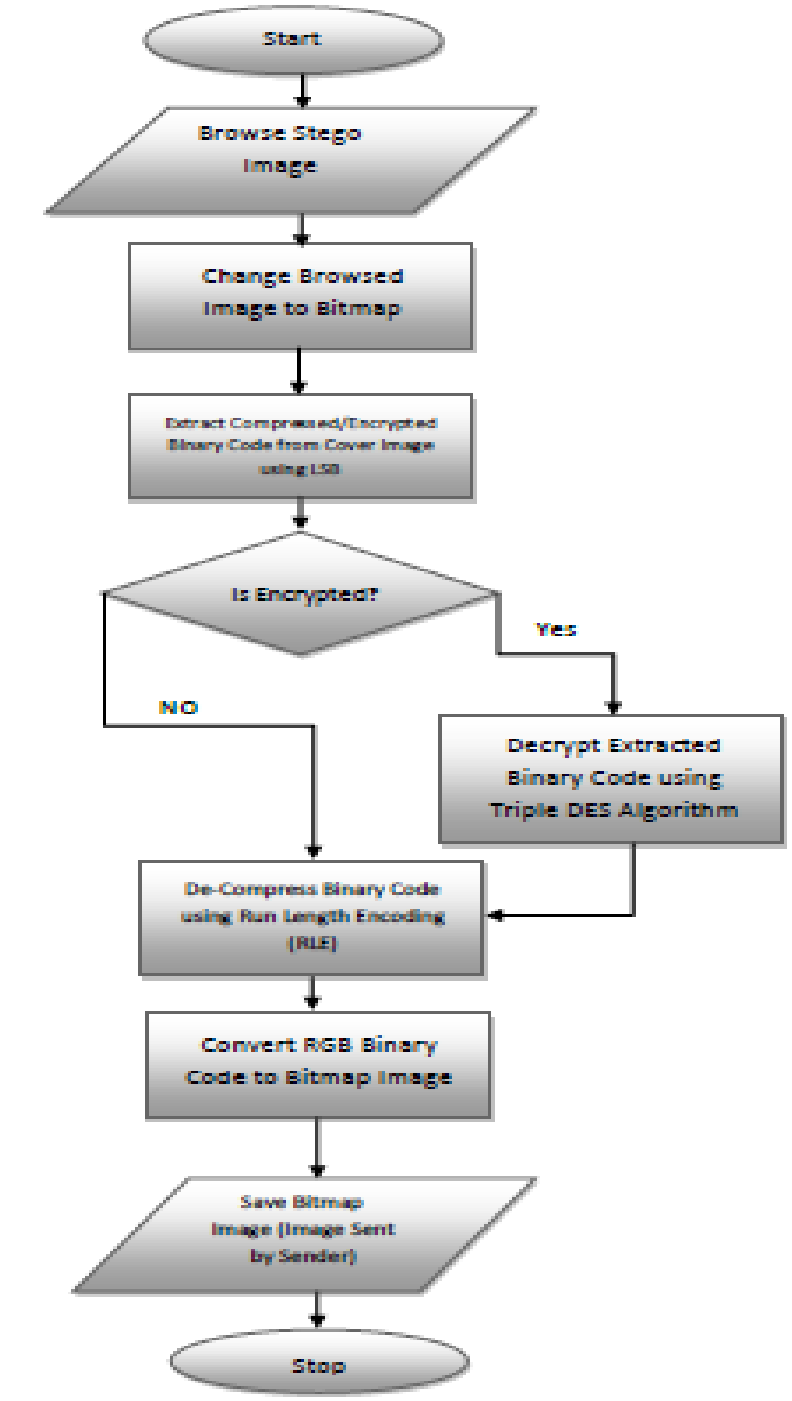
Flowchart of Image Hide with KVL Algorithm



Flow-Chart of Image Steganography: Image Hiding

Figure 3.7

Flowchart of Image Extraction with KVL Algorithm



Flow-Chart of Image Steganography: Image Extraction

Figure 3.8

KVL Algorithm for Image Hiding

Hide Image/Message (secret, cover, key)

1. Start
2. Resize Secret and Cover Image in 1:9
3. Read Secret Image as Bitmap
4. Read Cover Image as Bitmap
5. Change Secret Image Pixel RGB component values to Binary Code
6. Compress Binary Code using RLE Compression Algorithm
7. Check for Key
8. If Key is not blank
9. Apply Triple DES Encryption using the key
10. Embed Encrypted Binary Code in to the Cover Image Pixel Components using LSB Algorithm
11. Save Stego Image to Computer
12. Transfer it over the Network with the shared key
13. Stop

KVL Algorithm for Image Extraction

Extract (stego_image, key)

1. Start
2. Read Stego Image as Bitmap
3. Extract Secret Image Encrypted Binary Code from the Stego Image using LSB Algorithm
4. If Key is not blank
5. Apply Triple DES Decryption using the key
6. Decompress Binary Code using RLE Compression Algorithm
7. Convert RGB Binary Code to Secret Image RGB Component
8. Save Secret Image to Computer
9. Stop

Code Snippest

Function used for Steganography

```
public static Bitmap embedText(string text, Bitmap bmp)
public static string extractText(Bitmap bmp)
public static int reverseBits(int n)
public static string bmp_to_string(Bitmap bmp)
public static string find_binary(int num)
public static Bitmap string_to_bmp(String text)
public static double change_binary_to_int(string binary_value)
```

Binary Code Hiding using LSB Substitution Algorithm

```
switch (colorUnitIndex % 3)
{
    case 0:
        {
            if (s == State.hiding)
            {
                R += charValue % 2;

                charValue /= 2;
            }
        } break;
    case 1:
        {
            if (s == State.hiding)
            {
                G += charValue % 2;

                charValue /= 2;
            }
        } break;
    case 2:
        {
            if (s == State.hiding)
            {
                B += charValue % 2;

                charValue /= 2;
            }

            bmp.SetPixel(j, i, Color.FromArgb(R, G, B));
        } break;
}
```

Binary Code Extraction from image using LSB Substitution Algorithm

```
switch (colorUnitIndex % 3)
{
    case 0:
        {
            charValue = charValue * 2 + pixel.R % 2;
        } break;
    case 1:
        {
            charValue = charValue * 2 + pixel.G % 2;
        } break;
    case 2:
        {
            charValue = charValue * 2 + pixel.B % 2;
        } break;
}
```

Pixel Color Code Conversion to Binary Data

```
pixel = Color.FromArgb(pixel.R, pixel.G, pixel.B);

R = pixel.R; G = pixel.G; B = pixel.B;

r_value += find_binary(R) + find_binary(G) + find_binary(B);
```

Binary Code to Image Pixel Conversion

```
// Change Binary to Int
R = (int)change_binary_to_int(r_value);
G = (int)change_binary_to_int(g_value);
B = (int)change_binary_to_int(b_value);
```

RLE Compression (Encoding/Decoding)

```
public static string encode(string text)
public static string decode(string text)
```

RLE Encoding

```
if (current_char == last_char)
{
    count++;

    if (i == text.Length - 1)
    {
        if (count > 1)
        {
            while (count > 0)
            {
                if (count <= 9)
                {
                    if (count == 1)
                        result_text += last_char;
                    else
                        result_text += last_char + count.ToString();

                    count = 0;
                }
                else
                {
                    result_text += last_char + "9";
                    count -= 9;
                }
            }
        }
        else
            result_text += last_char;
    }
```

RLE Decoding

```
if (int.Parse(current_char.ToString()) > 1)
{
    count = int.Parse(current_char.ToString());
    while (count > 1)
    {
        result_text += last_char;
        count--;
    }
}
else
{
    last_char = current_char;
    result_text += last_char;
}
```

Cryptography Functions

```
public static string Encrypt(string toEncrypt, bool useHashing, string key)
public static string Decrypt(string cipherString, bool useHashing, string key)
```

MD5 Hash Code Generation

```
MD5CryptoServiceProvider hashmd5 = new MD5CryptoServiceProvider();
keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(key));
hashmd5.Clear();
```

Triple DES

```
TripleDESCryptoServiceProvider tdes = new TripleDESCryptoServiceProvider();
tdes.Key = keyArray;
tdes.Mode = CipherMode.ECB;
tdes.Padding = PaddingMode.PKCS7;
```

Encryption Code

```
ICryptoTransform cTransform = tdes.CreateDecryptor();
byte[] resultArray = cTransform.TransformFinalBlock(toEncryptArray, 0, toEncryptArray.Length);
tdes.Clear();
return UTF8Encoding.UTF8.GetString(resultArray);
```

Calculation of SNR, MSE and PSNR

```
public static double Calculate_SNR(Bitmap stego, Bitmap cover)
public static double Calculate_MSE(Bitmap stego, Bitmap cover)

double psnr_value = 10 * Math.Log10((255 * 255) / (mse_value / 3))
```

Project Snaps

Image Hiding

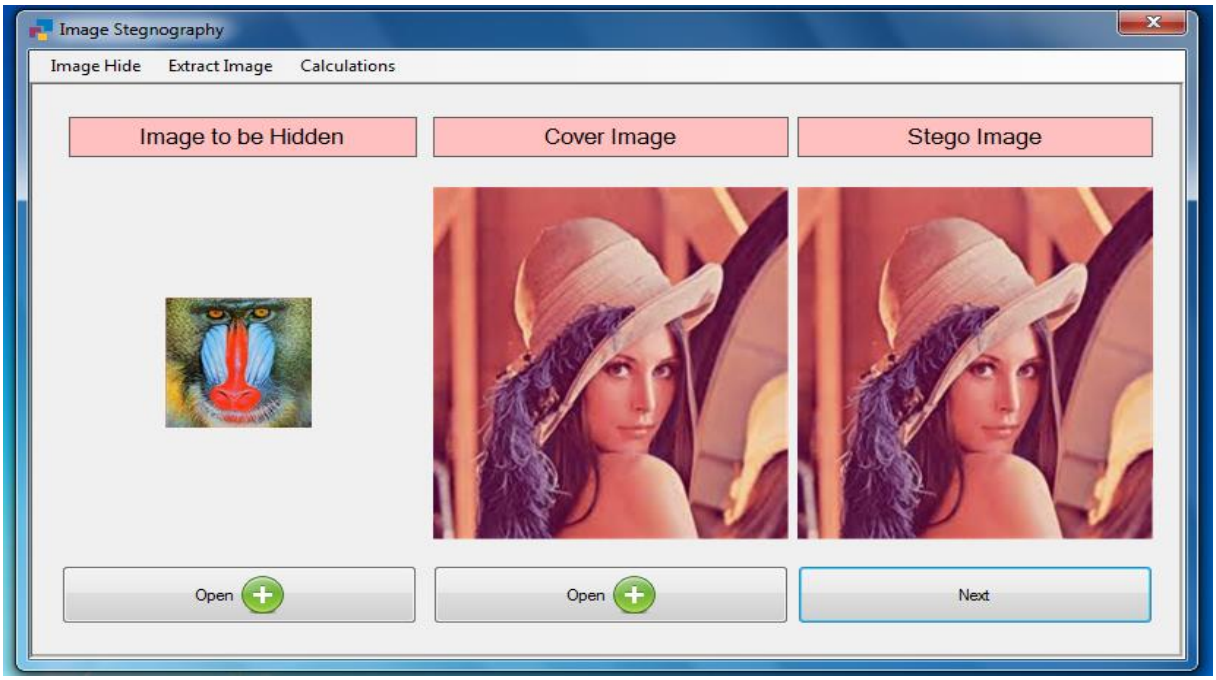


Figure 3.9

Image Extraction Encryption Key

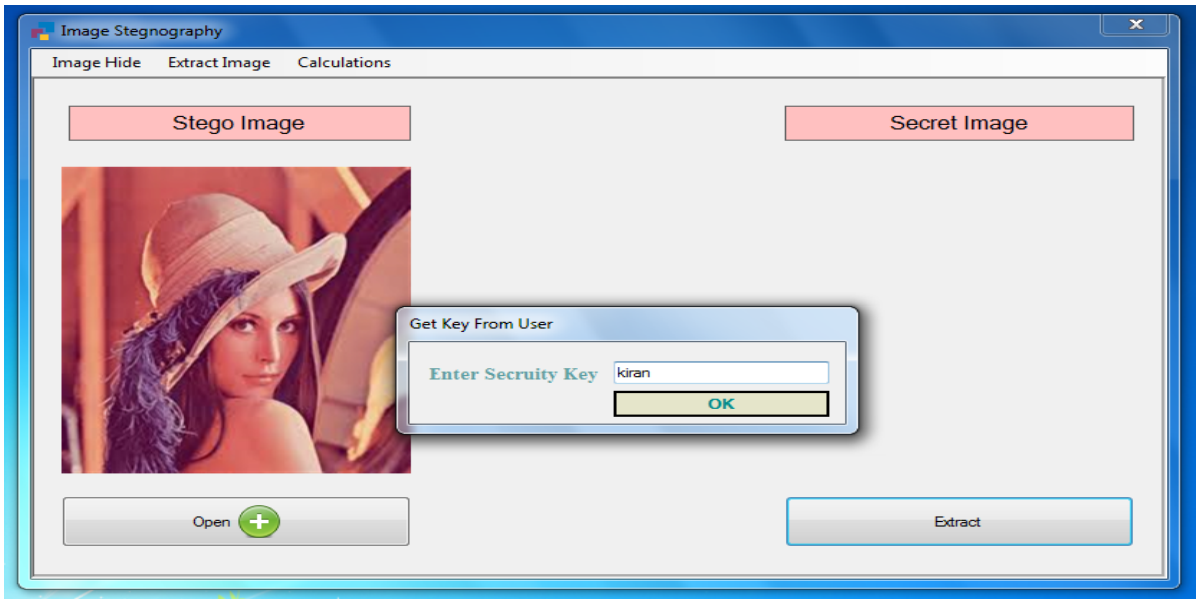


Figure 3.10

Extracted Image

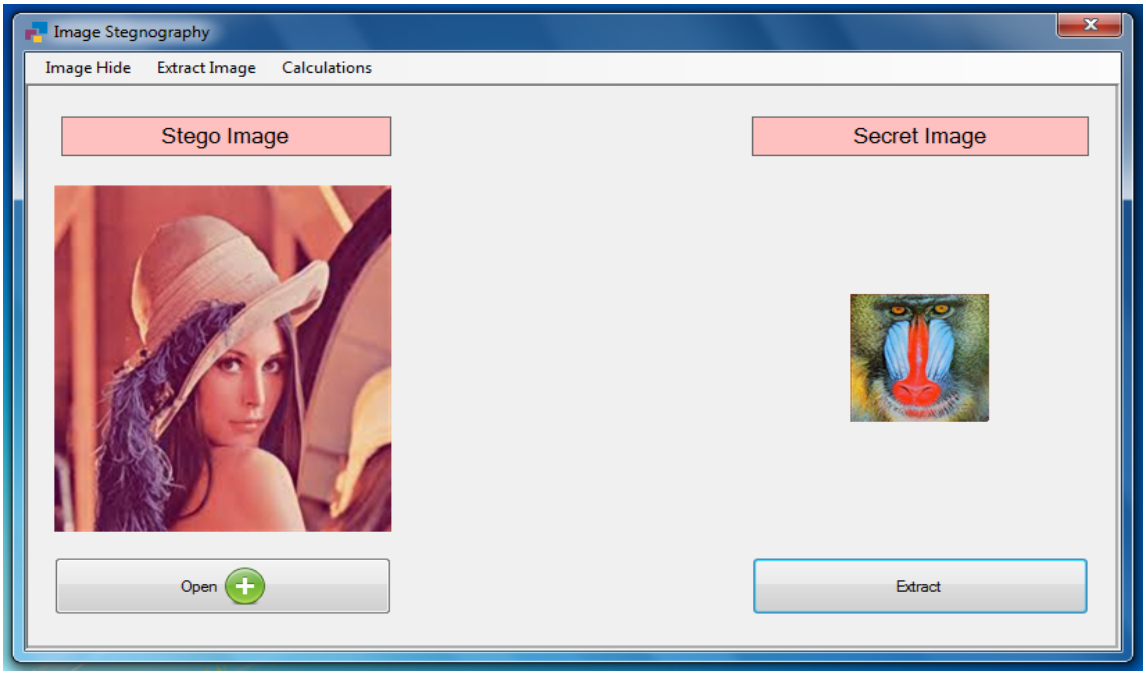


Figure 3.11

Calculation Form

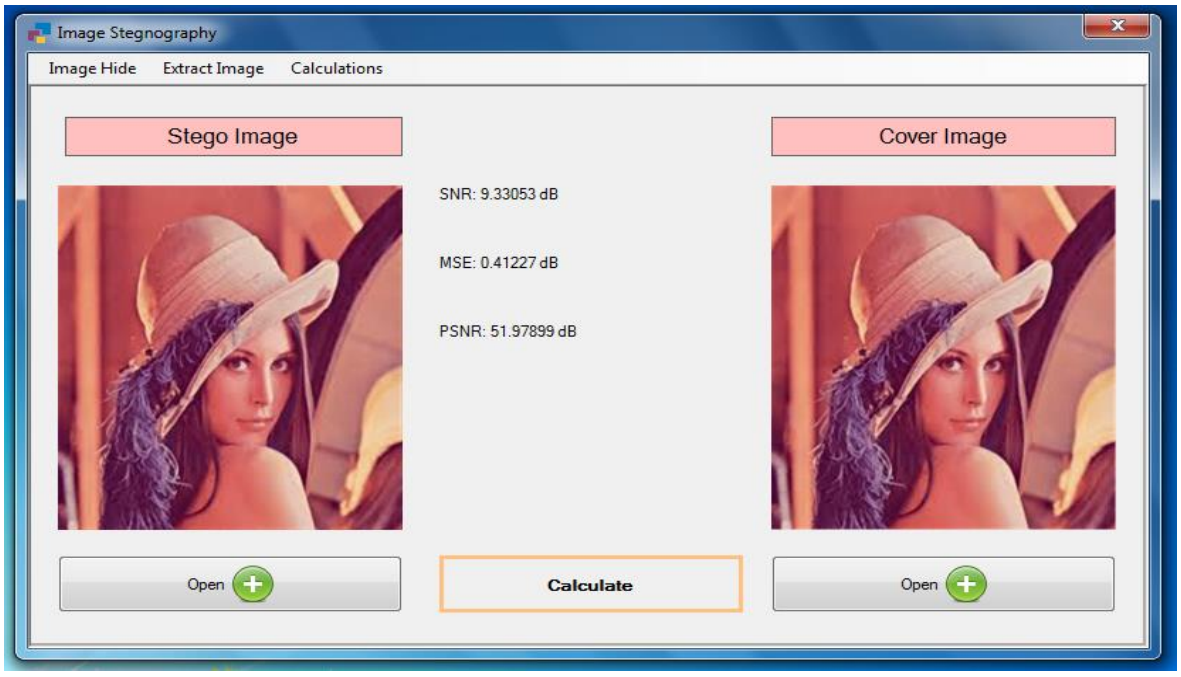


Figure 3.12

CHAPTER 4 RESULT ANALYSIS

Here in the KVL algorithm we have proposed a method which is showing far better results compared to the other techniques. We have analyzed result on the basis of time consumption and PSNR value comparison. First we have given tables and graphs which are showing the time consumption based on the passes used in the algorithm; i.e. Image Hiding, Image Extraction and then worked to find the full time consumed in the whole process. In the meanwhile we observed the values of SNR, MSE and PSNR for a collection of different-different 8 images with a single cover image. These all images are hidden behind the cover images in an orderly manner and their respective values are noted down. After doing the whole analysis process we found the average values and plotted them in the graph which makes stronger our proposed technique over the others. Results are below mentioned for the expert's reviews:

Figure 4.1 Lena Cover Image

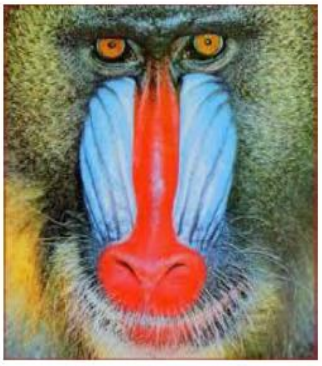


Figure 4.2 Baboon Secret Image

Figure 4.3 Lena Stego Image

Images Used for all Techniques

Result Analysis and Comparison Techniques

Lena Image	LSB3	Jae Gilyu	First component alteration technique	Improved LSB	KVL Method
PSNR	37.92	38.98	46.11	46.65	51.98

Table 4.1

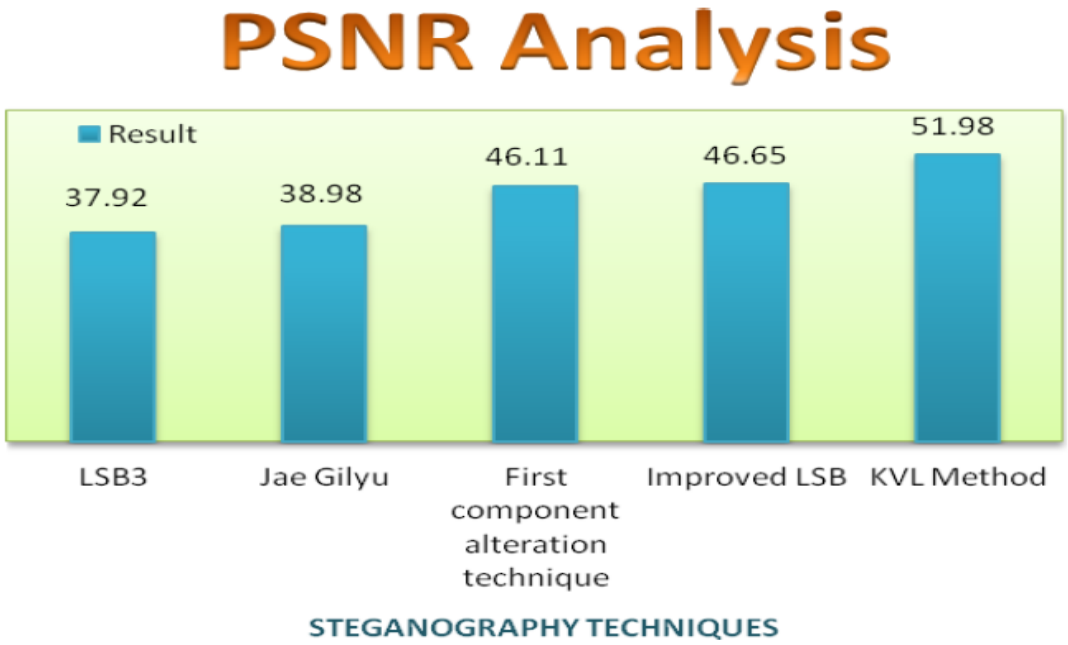


Figure 4.4 Graph of PSNR Analysis

Graph: Performance Analysis

Performance Measurements

Time Calculation for Image Hiding (sec)

Image ID	Time Consumed in Seconds
1	8.7024977
2	11.2886457
3	11.8956804
4	10.1255791
5	11.905681
6	13.2277566
7	12.9117385
8	10.350592
Total	90.408171

Table 4.2

Average Time Consumed=Total Time Consumed by all images/no of images

AT = TT/N; AT = 90.408171/8 = 11.301021375 sec

Different Image ID and Corresponding Time consumed for Image Hiding (sec)

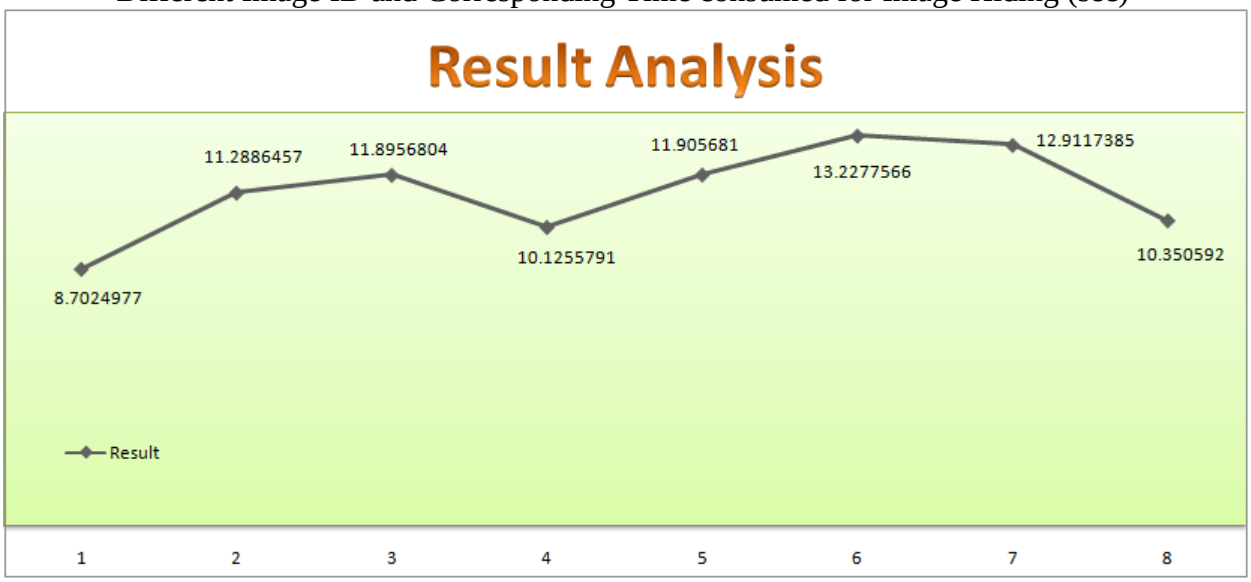


Figure 4.5

Time Calculation for Image Extraction (sec)

Image ID	Time Consumed in Seconds
1	37.0891214
2	41.5683775
3	42.7804469
4	39.2012421
5	41.264368
6	42.5644346
7	42.4574284
8	38.3831954
Total	325.3086143

Table 4.3 Image Extraction

AT = 325.3086143/8 = 40.6635767875 sec

Different Image ID and Corresponding Time consumed for Image Extraction (sec)

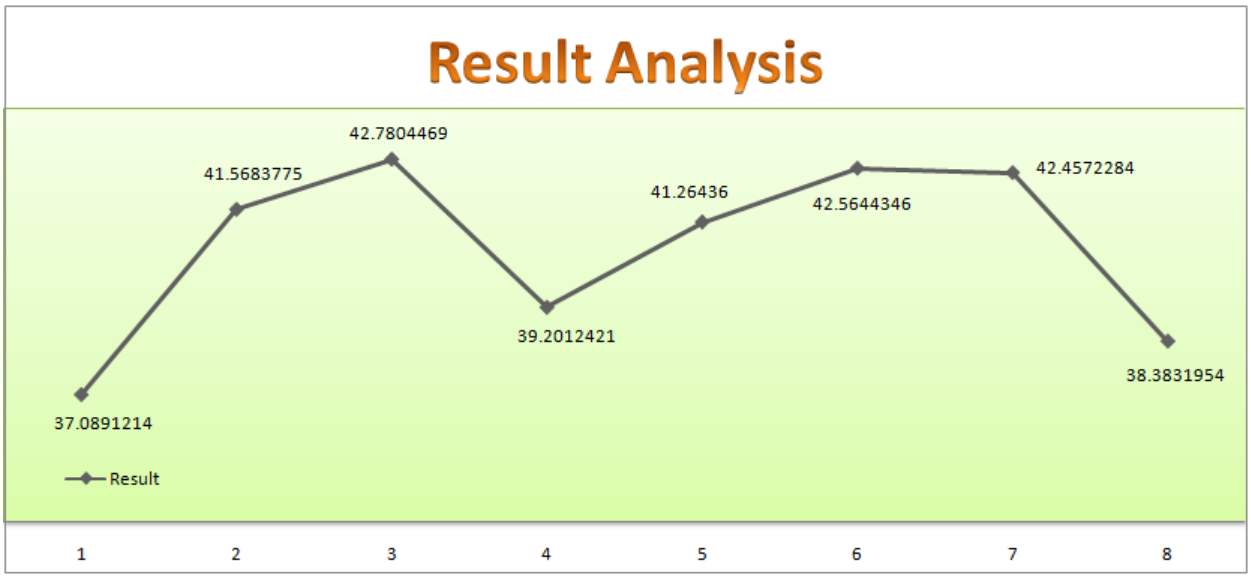


Figure 4.6

Time Calculation for Steganography Performance (Image Hiding + Image Extraction) (sec)

Image ID	Time Consumed in Seconds
1	45.7916117
2	52.8570232
3	54.6761273
4	49.3268212
5	53.1700241
6	55.7921921
7	55.3691669
8	48.7337874
Total	**415.7167539**

Table 4.4

AT = 415.7167539/8 = 51.9645942375 sec

Time consumed by Steganography (Image Hiding + Image Extraction) (sec)

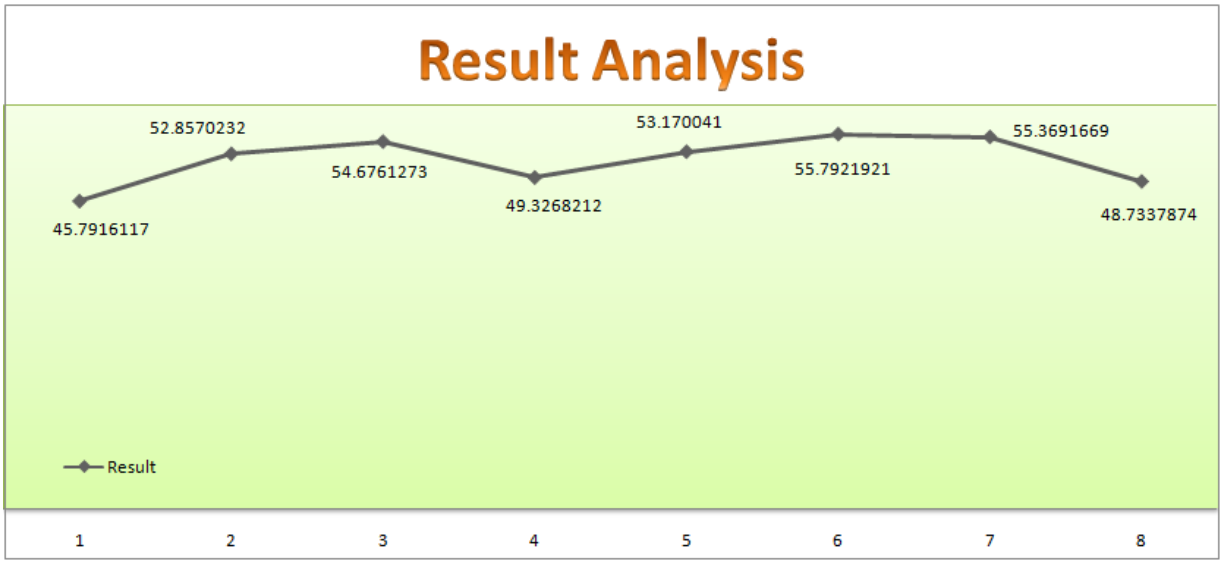


Figure 4.7

SNR Calculation

SNR Signal-to-noise ratio expressed in dB

$$\mathrm{SNR} = 10 \cdot \log_{10} \left[\frac{\sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y)]^2}{\sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y) - t(x,y)]^2} \right]$$

Calculation of SNR Value in different secret images (dB)

Image ID	SNR Value in dB
1	13.77836
2	14.61867
3	14.80942
4	14.30856
5	14.77239
6	15.00346
7	15.02958
8	14.84595
Total	**117.16639**

Table 4.5

Average SNR = Total/8 = 117.16639/8 = 14.64579875 dB

Graph for SNR Value for Different Secret Image (dB)

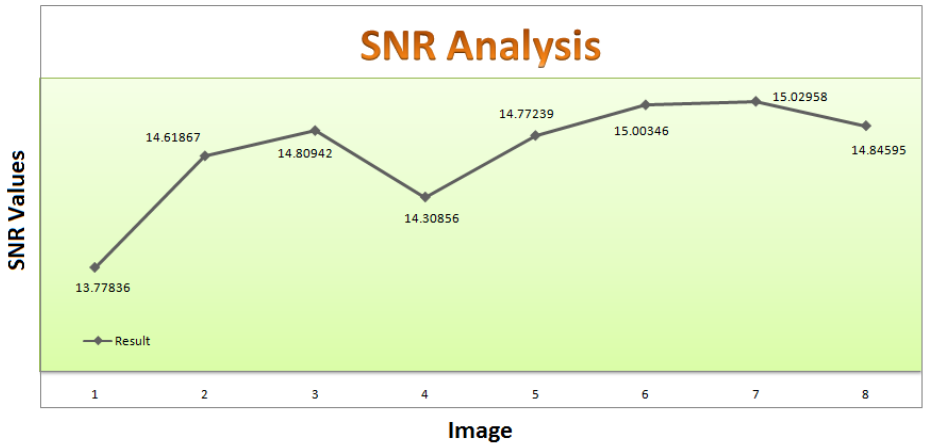


Figure 4.8

MSE Calculation

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Calculation of MSE value in different images (dB)

Image ID	MSE Value in dB
1	0.24274
2	0.28314
3	0.29462
4	0.26554
5	0.29341
6	0.31019
7	0.31029
8	0.31028
Total	**2.31021**

Table 4.6

Average MSE = Total/8 = 2.31021/8 = 0.28877625 dB

Graphs for MSE Value for Different Images (dB)

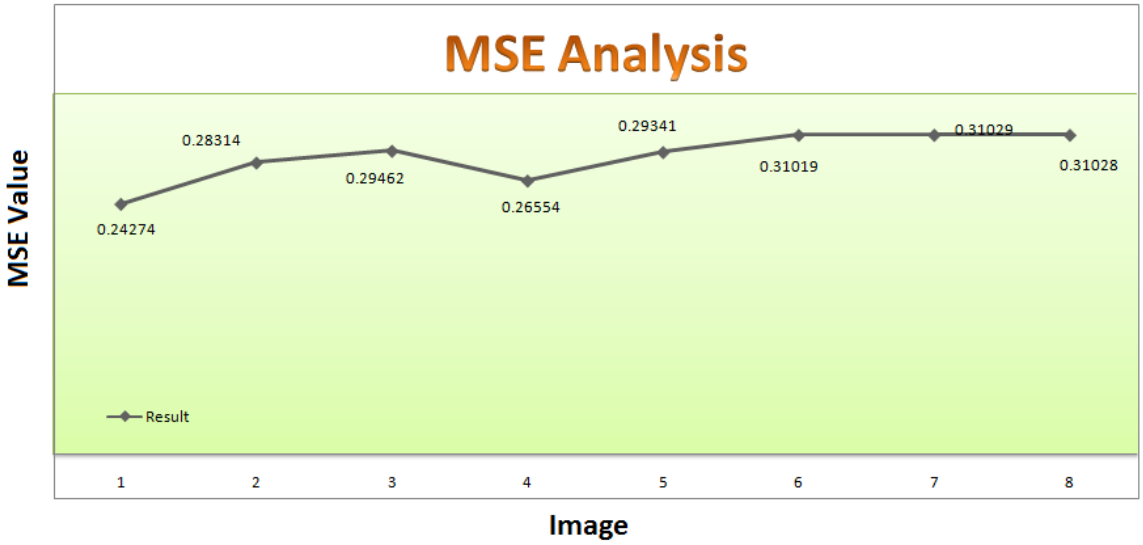


Figure 4.9

PSNR Calculation

PSNR Peak signal-to-noise ratio expressed in dB

$$\mathrm{PSNR} = 10 \cdot \log_{10} \left[\frac{\max(r(x,y))^2}{\frac{1}{n_x \cdot n_y} \cdot \sum_{0}^{n_x-1} \sum_{0}^{n_y-1} [r(x,y) - t(x,y)]^2} \right]$$

Calculation of PSNR Value for different images (dB)

Image ID	PSNR Value in dB
1	54.27945
2	53.61079
3	54.43818
4	53.88945
5	53.45601
6	53.21453
7	53.21308
8	53.21327
Total	**429.31476**

Table 4.7

Average PSNR = Total/8 = 429.31476/8 = 53.664345 dB

Graph for PSNR Value for Different Images (dB)

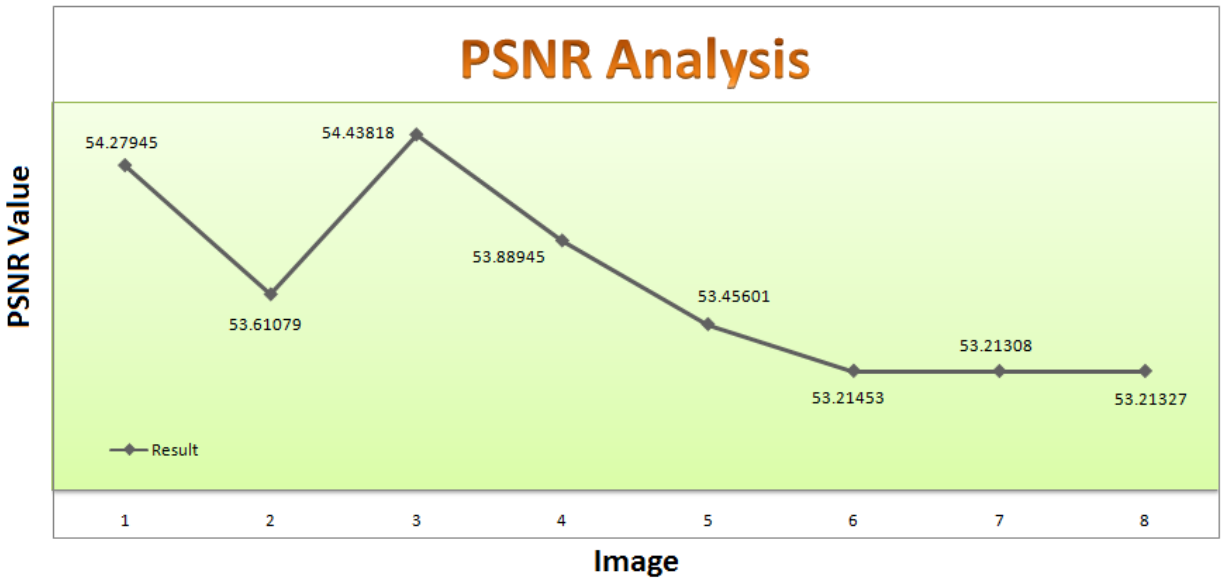


Figure 4.10

Images Used for the Result Consideration

Figure 4.11 Cover Image

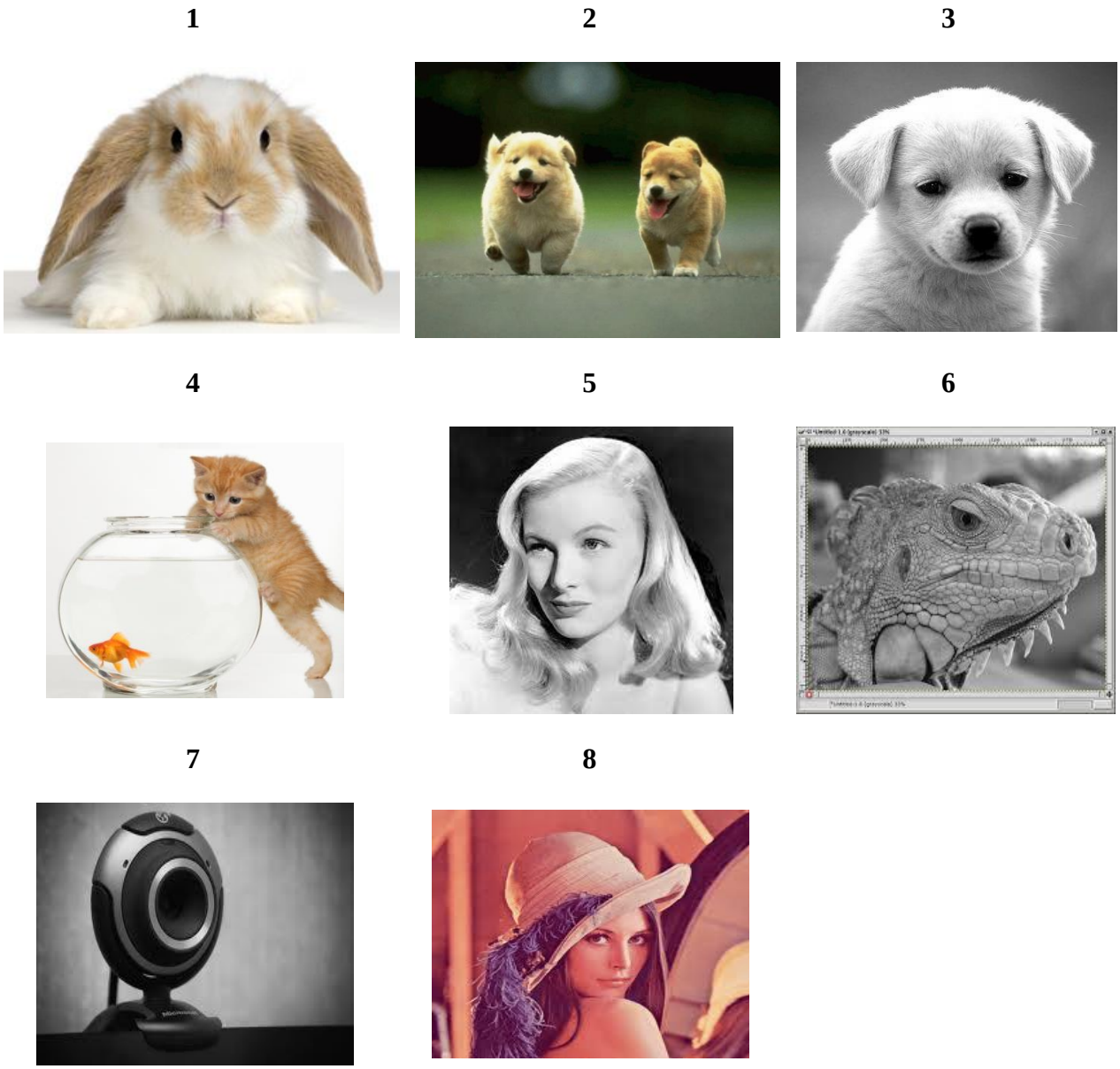


Figure 4.12 Different Secret Images with their respective ID

CHAPTER 5 CONCLUSION & FUTURE WORK

Conclusion

KVL is an algorithm proposed for the implementation of steganography on the concept of LSB (Least Significant Bit) Substitution. Secret image is converted into the binary format and then bytes are grouped. MSB (Most Significant bits) of Secret image are taken and hidden inside the cover image LSB bits. 8 bit secret information or message is hidden inside a group of 3 RGB pixels means 24 bit 3 pixels are used to hide information of 8 bit. KVL is proposed as a technique which guarantees the quality of image and stego image remain same as the original, minute differences occurs in it. This is also supported by the result PSNR values. High values of PSNR supports the statement mentioned.

Future Work

We have proposed this algorithm for static images, and the quality of steganography is kept high. Video are still a new topic of research and requires more commitment than the image steganography. Although we all are known that videos are nothing but the grouping of frames per second. If we can capture the frames and become able to modify them and retransmit as the order they appeared will give us a chance to implement the video steganography. So what we will try to use this research in video based steganography and keep the standards as high as we did for the still images.

REFERENCES

[1] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[2] McGill, “Steganography: The right way”. SANS Institute, 2005.

[3] Haykin, S., Communication Systems, 4th edition, John Wiley and Sons, Inc, 2001. Chang Chin Chen,Chen Tung Shou, Chung Lou Zo, “A steganographic method based upon JPEG and quantization table modification”, Information Sciences Journal, May 2001.

[4] http://www.hackersonlineclub.com/steganography.

[5] Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19th National Information Systems Security Conference, 1996.

[6] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998.

[7] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998.

[8] “Reference guide: Graphics Technical Options and Decisions”, http://www.devx.com/projectcool/Article/19997.

[9] Owens, M., “A discussion of covert channels and steganography”, SANS Institute, 2002.

[10] Krenn, R., “Steganography and Steganalysis”, http://www.krenn.nl/univ/cry/steg/article.pdf.

[11] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, 47:10, October 2004.

[12] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998.

[13] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, Proceedings of the 2nd Information Hiding Workshop, April 1998.

[14] Chandramouli, R., Kharrazi, M. & Memon, N., “Image steganography and steganalysis: Concepts and Practice”, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[15] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., “Spread Spectrum Steganography”, IEEE Transactions on image processing, 8:08, 1999.

[16] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, 1996.
[17] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., “Information Hiding – A survey”, Proceedings of the IEEE, 87:07, July 1999.
[18] Jackson et. al., “Blind Steganography using Computational immune System”, IJDE 1:4, 2003.
[19] Katzenbeisser S, Peticolas FAP, “Information Hiding techniques for Steganography and Digital Watermarking”, Artech House Publishers, 2000
[20] Yousaf MI et.al., “Direct Sequence spread spectrum Techniques with residue No-system”, IJEEE, 3:4, 2009.
[21] www.cs.washington.edu/education/courses/csep590/.../banerjee.doc
[22] T. Morkel, J.H.P.Eloff, M. S. Olivier, “An Overview of Image Steganography”.
[23] Atallah M. Al-Shatnawi, “A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Science, Vol.6, 2012, No. 79, 3907-3915.
[24] Mamta.Juneja and Parvinder S. Sandhu, “An Improved LSB Based Steganography with Enhanced Security and Embedding/Extracting”, 3rd International Conference on Intelligent Computational Systems (ICICS’2013) January 26-27, 2013 Hong Kong (China).
[25] Mamatha.T, “ A Data Hiding Model for Image Steganography Using Primes: Towards Data Security”, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 3, May 2012.
[26] Ravinder Reddy Ch, Roja Ramani A, “The Process of Encoding and Decoding of Image Steganography Using LSB Algorithm”, IJCSET, November 2012, Vol 2, Issue 11, 1488-1492.
[27] Ankita Gangwar, Vishal Shrivastava,“Improved RGB –LSB Steganography Using Secret Key”, International Journal of Computer Trends and Technology, Volume 4 Issue 2-2013.
[28] Mrs. Richa Raja Gautam, Prof. Rakesh Kumar Khare, “Real Time Image Security for Mobile Communication Using Image Steganography”, International Journal of Engineering Research & Technololgy(IJERT) ISSN: 2278-0181, Vol.1 Issue 8, October – 2012.
[29] Shikha Sharda, Sumit Budhiraja, “ Image Steganography: A Review”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013.

[30] S. Mohanapriya, “Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones”, International Journal of Emerging Technology and Advanced Engineering, ISSN 225-2459, Volume 2, Issue 5, May 2012.
[31] B. Sharmila and R. Shanthakumari, “Efficient Adaptive Steganography for Color Images Based on LSBMR Algorithm”, ICTACT Journal on Image and Video Processing, February 2012, Volume: 02, Issue: 03.
[32] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, M.Gomathymeenakshi, “An Improved Steganographic Technique Using LSB Replacement on a Scanned Path Image”, International Journal of Network Security, Vol.15 , No.1, PP. 314-318, Jan 2013.
[33] M.I. Khalil, “Image Steganography: Hiding Short Audio Messages within Digital Images”, JCS & T, Vol. 11 No. 2, October 2011.
[34] Mr. Pushparaj, P. Nerkar, Vishwajit K. Barbudhe, Prof. Aumdevi K. Barbudhe, “Steganography for Colored Images”, International Journal of Electronics Communication & Soft Computing Science and Engineering, ISSN: 2277-9477, Volume 2, Issue 2.
[35] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr. P.Chenna Reddy, “Implementation of LSB Steganography and Its Evaluation for Various File Formats”, Int. J. Advanced Networking and Applications, Volume: 02, Issue: 05,Pages:868-872 (2011) .
[36] Vijay Kumar Sharma, Vishal Shrivastava, “A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection”, Journal of Theoretical and Applied Information Technology, Vol. 36 No. 1,15th February 2012.