**SECURED DATA TRANSMISSION USING WAVELET BASED STEGANOGRAPHY AND CRYPTOGRAPHY BY USING AES ALGORITHM**

ABSTRACT

The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. The digital watermarking plays an important role in embedding information into a digital image signal, for verification and identity of its owners. In discrete wavelet transform, “analysis filter bank “can be used for analyzing image signal by passing through it.. This filter bank consists of a low pass and a high pass filter at each decomposition stage. In this paper, a method to combine steganography (Least Significant Method) and cryptography (AES) is considered, so as to provide a more secure way for data transmission through any unsecured or public networks. Before embedding the text in image, text is encrypted using Advanced Encryption Standard (AES) algorithm. The text can be a sentence or a key with alphabetic words having the length of 8 characters. Using Least Significant Bit (LSB) method, the encrypted text is embedded into the “LL sub-band wavelet decomposed image”. The inverse wavelet transform is applied and the resultant image is transmitted to the receiver. Now at the receiver’s end, the image transformed using wavelet and encrypted text is extracted by using LSB method.

CHAPTER 1

# INTRODUCTION

* 1. **Overview**

The rapid and continuous development in information technology has forced computer networks to grow tremendously in a very short time. This results in facilitating electronic data transfer and in large amounts. The overwhelming advancement in the electronic ways of data exchange and the

Wide spread of image use has put a huge potential on both security and protection of confidential data from unauthorized admission. Accordingly, development of security systems is very critical to guarantee the security of data during transition through the internet.

Cryptography is considered as one of the most commonly utilized techniques to guarantee data security. In recent years, great development has been achieved in data encryption technology. Many data encryption approaches are currently used especially for digital image security. Random encryption keys are produced in these techniques, whereas the genuine content becomes invisible.

Steganography is the science and art of hiding information within a carrier, where no one, except the intended recipient, has the knowledge of the existence of hidden information. Steganography as a term is derived from the ancient Greek words “***steganos***”, which means covered and “***graphic***” which means writing. In this operation, a secret message is concealed in another piece

of normally looking information, which is known as the cover. This process aims to keep the secret information hidden without revealing any kind of suspicion to the viewer's.

Data security is paramount concern for all the net users irrespective of the network. The present day hackers are a threat to the data and the threat hangs like a Damocles sword. The transmission of data through any channel of communication needs strong encryption techniques for the purpose of data security. The recent trends and development in information technology highlights the need for safe, secure and protected transmission of data. The conventional encryption methods failed to give the desired result of protecting the data. Simple way is to come up with unique id and passwords, and a combination of alphabets & numerical .AES has emerged as a frontrunner and

efficient algorithm because of inherent inbuilt in advantage of better security with less implementation complexity. After extensive research in image coding, for image compression application, DWT works as a standard tool, for their data reduction capability. The complete image is compressed and transformed into a single data object by wavelet compression system, rather than block by block as in a DCT-based compression system. When the entire image is achieved there will be a uniform distribution of compression error across that image. An image resolution

enhancement in the wavelet domain is a subject of interest for further research and recently many new algorithms have been proposed. Of these the Discrete Wavelet Transforms (DWT) is the most-suited application. DWT decomposes an image into different sub-band images. Which can be named as low-low (LL), low-high (LH),high-low (HL), and high-high (HH).Here the sub-bands have the same size as the input image.

**DOMAIN INTRODUCTION**

**DIGITAL IMAGE PROCESSING**

**1.1GENERAL**

Digital image processing is the use of computer algorithms to perform image processing on digital images. The 2D continuous image is divided into N rows and M columns. The intersection of a row and a column is called a pixel. The image can also be a function other variables including depth, color, and time. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

* + 1. **THE IMAGE PROCESSING SYSTEM**

FIG 1.1 BLOCK DIAGRAM OF IMAGE PROCESSING SYSTEM

Digitizer

Mass Storage

Hard Copy Device

Display

Image Processor

Digital Computer

Operator Console

* **Digitizer**

Digitizing or digitizationis the representation of an object, image, sound, document or a signal (usually an analog signal) by a discrete set of its points or samples. Digital information exists as one of two digits, either 0 or 1. These are known as bits.

An image is digitized to convert it to a form which can be stored in a computer's memory or on some form of storage media such as a hard disk or CD-ROM. This digitization procedure can be done by a scanner, or by a video camera connected to a frame grabber board in a computer. Once the image has been digitized, it can be operated upon by various image processing operations.

* Microdensitometer
* Flying spot scanner
* Image dissector
* Videocon camera
* Photosensitive solid- state arrays.
* **Digital computer**

A computer is an electronic device that accepts raw data, processes it according to a set of instructions and required to produce the desired result. Mathematical processing of the digitized image such as convolution, averaging, addition, subtraction, etc. are done by the computer.

* **MASS STORAGE**

Mass storage devices used in desktop and most server computers typically have their data organized in a file system.The secondary storage devices normally used are floppy disks, CD ROMs etc.

* **OPERATOR CONSOLE**

The operator console consists of equipment and arrangements for verification of intermediate results and for alterations in the software as and when require. The operator is also capable of checking for any resulting errors and for the entry of requisite data.

* **Display**

Popular display devices produce spots (display elements) for each pixel:

* Cathode ray tubes (CRTs).
* Liquid crystal displays (LCDs).
* Printers.

Spots may be binary (e.g., monochrome LCD), achromatic (e.g., so-called black-and-white, actually grayscale for intensity), pseudo color or false colors (e.g., for intensity or hyper spectral data), or true color (color data displayed as such).

* + 1. **IMAGE PROCESSING FUNDAMENTAL**

Digital image processing refers processing of the image in digital form. Modern cameras may directly take the image in digital form but generally images are originated in optical form. They are captured by video cameras and digitalized. The digitalization process includes sampling, quantization. Then these images are processed by the five fundamental processes, at least any one of them, not necessarily all of them.

**1.1.2.1 Fundamental steps in image processing**

* 1. Image acquisition
  2. Image preprocessing
  3. Image segmentation
  4. Image representation
  5. Image description
  6. Image recognition
  7. Image interpretation
* **Image acquisition**

First we need to produce a digital image from a paper envelope. This can be done using either a CCD camera, or a scanner

* **Image preprocessing**

This is the step taken before the major image processing task. The problem here is to perform some basic tasks in order to render the resulting image more suitable for the job to follow. In this case it may involve enhancing the contrast, removing noise, or identifying regions likely to contain the postcode.

* **Image segmentation**

Segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as super pixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share certain visual characteristics.

* **Image representation**

Image process is the process of convert the input data to a form suitable for computer processing

* **Image description**

Image description is the process of extract features that result in some quantitative information of interest or features that are basic for differentiating one class of objects from another.

* **Image recognition**

Image recognition is the process of assign a label to an object based on the information provided by its descriptors.

* **Image interpretation**

Image interpretation is the process of assign meaning to an ensemble of recognized objects.

**1.1.2.2 Image types**

There are several ways of encoding the information in an image.

1. Binary image
2. Grayscale image
3. Indexed image
4. True color or RGB image

* **Binary image**

Each pixel is just blackor white. Since there are only two possible values for each pixel (0, 1), we only need one bitper pixel.

* **Grayscale image**

Each pixel is a shade of gray, normally from 0 (black) to 255(white). This range means that each pixel can be represented by eight bits, or exactly one byte. Other grayscale ranges are used, but generally they are a power of 2.

* **Indexed image**

An indexed image consists of an array and a color map matrix. The pixel values in the array are direct indices into a color map. By convention, this documentation uses the variable name X to refer to the array and map to refer to the color map.

* **True Color or RGB image**

Each pixel has a particular color; that color is described by the amount of red, greenand bluein it. If each of these components has a range 0–255, this gives a total of 2563different possible colors. Such an image is a “stack” of three matrices; representing the red, greenand bluevalues for each pixel. This means that for every pixel there correspond 3 values.

**1.1.2.3 image processing goals**

In virtually all image processing applications, however, the goal is to extract information from the image data. Obtaining the information desired may require filtering, transforming, coloring, interactive analysis, or any number of other methods.

To be somewhat more specific, one can generalize most image processing tasks to be characterized by one of the following categories:

Problem Domain

Knowledge

Base

Segmentation

Preprocessing

Image Acquisition

Recognition & interpretation

Representation & Description

Result

**FIG 1.2 BLOCK DIAGRAM OF FUNDAMENTAL SEQUENCE INVOLVED IN AN IMAGE PROCESSING SYSTEM**

1. Image enhancement
2. Image restoration
3. Image analysis
4. Feature extraction
5. Image registration
6. Image compression
7. Image synthesis

* **image enhancement**

This simply means improvement of the image being viewed to the (machine or human) interpreter's visual system. Image enhancement types of operations include contrast adjustment, noise suppression filtering, application of pseudo color, edge enhancement, and many others.

* **image restoration**

The purpose of image restoration is to "compensate for" or "undo" defects which degrade an image. Degradation comes in many forms such as motion blur, noise, and camera misfocus. In cases like motion blur, it is possible to come up with a very good estimate of the actual blurring function and "undo" the blur to restore the original image. In cases where the image is corrupted by noise, the best we may hope to do is to compensate for the degradation it caused.

* **image analysis**

Image analysis is the extraction of meaningful information from images. Image analysis operations produce numerical or graphical information based on characteristics of the original image. They break into objects and then classify them. They depend on the image statistics. Common operations are extraction and description of scene and image features, automated measurements, and object classification. Image analyze are mainly used in machine vision applications.

* **feature extraction**

Feature extraction involves simplifying the amount of resources required to describe a large set of data accurately. When performing analysis of complex data one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and computation power or a [classification](http://en.wikipedia.org/wiki/Statistical_classification) algorithm which [over fits](http://en.wikipedia.org/wiki/Overfitting) the training sample and generalizes poorly to new samples. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy.

* **image registration**

Image registration is the process of overlaying two or more images of the same scene taken at different times, from different viewpoints, and/or by different sensors. It geometrically aligns two images the reference and sensed images. The present differences between images are introduced due to different imaging conditions. Image registration is a crucial step in all image analysis tasks in which the final information is gained from the combination of various data sources like in image fusion, change detection, and multichannel image restoration.

Typically, registration is required in remote sensing (multispectral classification, environmental monitoring, change detection, image mosaicing, weather forecasting, creating super-resolution images, integrating information into geographic information systems (GIS)), in medicine (combining computer tomography (CT) and NMR data to obtain more complete information about the patient, monitoring tumor growth, treatment verification, comparison of the patient’s data with anatomical atlases), in cartography (map updating), and in computer vision (target localization, automatic quality control), to name a few.

* **image compression**

The objective of image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form.Image compression may be lossy or lossless. Lossless compression is preferred for archival purposes and often for medical imaging, technical drawings, clip art, or comics. This is because lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossy methods are especially suitable for natural images such as photographs in applications where minor (sometimes imperceptible) loss of fidelity is acceptable to achieve a substantial reduction in bit rate. The lossy compression that produces imperceptible differences may be called visually lossless.

* **image synthesis**

Image synthesis operations create images from other images or non-image data. Image synthesis operations generally create images that are either physically impossible or impractical to acquire.

**1.1.2**.**4 Applications of image processing**

Image processing has an enormous range of applications; almost every area of science and technology can make use of image processing methods. Here is a short list just to give some indication of the range of image processing applications.

* **Medicine**

Inspection and interpretation of images obtained from X-rays, MRI or CAT scans, analysis of cell images, of chromosome karyotypes. In medical applications, one is concerned with processing of chest X-rays, cineangiograms, projection images of transaxial tomography and other medical images that occur in radiology, nuclear magnetic resonance (NMR) and ultrasonic scanning. These images may be used for patient screening and monitoring or for detection of tumors’ or other disease in patients.

* **Agriculture**

Satellite/aerial views of land, for example to determine how much land is being used for different purposes, or to investigate the suitability of different regions for different crops, inspection of fruit and vegetables distinguishing good and fresh produce from old.

* **DOCUMENT PROCESSING**

It is used in scanning, and transmission for converting paper documents to a digital image form, compressing the image, and storing it on magnetic tape. It is also used in document reading for automatically detecting and recognizing printed characteristics.

* **RADAR IMAGING SYSTEM**

Radar and sonar images are used for detection and recognition of various types of targets or in guidance and maneuvering of aircraft or missile systems.

* **DEFENSE/INTELLIGENCE**

It is used in reconnaissance photo-interpretation for automatic interpretation of earth satellite imagery to look for sensitive targets or military threats and target acquisition and guidance for recognizing and tracking targets in real-time smart-bomb and missile-guidance systems.

CHAPTER 2

**LITERATURE SURVEY AND OUTCOME OF EXISTING LITERATURE**

This chapter briefly reviews, explains and discusses on existing literature review related with the current project which is “Traffic sign recognition using convolutional neural networks” that will be developed later. This chapter comprises three sections. The first section describes the overviews of Traffic sign. The subsections are the definition, type of Traffic sign. The second section is the review of some existing system that used same techniques and methods.

**An Overview of Encryption**

Information security has become more important in data storage and transmission. This chapter provides some security backgrounds that apply many encryption algorithms. The rapid development of data exchange in electronic ways and the widespread of image use have put a great potential on data security and safeguard of confidential data from accessible from unauthorized. Encryption is considered as one of the most commonly used approaches for ensuring high data security. In recent years, a great development has occurred in encryption technology, where many encryption methods are used for image security. These methods produce random encryption keys, whereas the actual content is not visible. Both of the encryption and decryption algorithms are

Designed and implemented to provide secure transfer of image data.

**Background and Previous Work in Steganography**

Information hiding techniques (steganography and watermarking) have recently received quite a bit of attention. At least one reason for this is the desire to protect copyrights of digital (audio, image and video). Other applications include intelligence communication, covert criminal communication, and the protection of various types of communication against illegal spy. Along with new and improved techniques for hiding information, techniques for detecting and (possibly removing) such information will appear in the scene. Hiding data refers to the process of secretly inserting information within a data source without changing its quality. It is the science and art of writing hidden messages in a way that either the sender or expected recipient doesn’t realize that the message is hidden. In data hiding process the actual information is not kept in its original format but it is transformed into another equivalent multimedia file such as images, videos or audios.

**TITLE:** “High capacity image steganographic model”

**AUTHOR:** Y. Lee, L. Chen,

**DESCRIPTION:** Steganography is an ancient art of conveying messages in a secret way that only the receiver knows the existence of a message. So a fundamental requirement for a steganographic method is imperceptibility; this means that the embedded messages should not be discernible to the human eye. There are two other requirements, one is to maximise the embedding capacity, and the other is security. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. However, how to decide on the maximal embedding capacity for each pixel is still an open issue. An image steganographic model is proposed that is based on variable-size LSB insertion to maximise the embedding capacity while maintaining image fidelity. For each pixel of a grey-scale image, at least four bits can be used for message embedding. Three components are provided to achieve the goal. First, according to contrast and luminance characteristics, the capacity evaluation is provided to estimate the maximum embedding capacity of each pixel. Then the minimum-error replacement method is adapted to find a grey scale as close to the original one as possible. Finally, the improved grey-scale compensation, which takes advantage of the peculiarities of the human visual system, is used to eliminate the false contouring effect. Two methods, pixelwise and bitwise, are provided to deal with the security issue when using the proposed model. Experimental results show effectiveness and efficiency of the proposed model.

**TITLE:** “A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography”

**AUTHOR:** M. IndraSena Reddy,

**YEAR: 2013**

**DESCRIPTION:** Steganography and cryptography methods are used together with wavelets to increase the security of the data while transmitting through networks. In the discrete wavelet transform, an image signal can be analyzed by passing it through an analysis filter bank. This analysis filter bank consists of a low pass and a high pass filter at each decomposition stage. Another technology, the digital watermarking is the process of embedding information into a digital (image) signal which may be used to verify its authenticity or the identity of its owners. The watermark to be embedded is ‘text’. Before embedding the plain text into the image, the plain text is encrypted by using Data Encryption Standard (DES) algorithm. The plain text can be any sentence in English, and the key can be anything in English with a length of 8-characters. The encrypted text is embedded into the LL subband of the wavelet decomposed image using Least Significant Bit (LSB) method. Then the inverse wavelet transform is applied and the resultant image is transmitted to the receiver. At the receiver’s end, the image is transformed using wavelet, from the LL subband the encrypted text is extracted by using the LSB method and the result is decrypted using DES.

**TITLE:** “Secured Data Transmission using Wavelet based Steganography and Cryptography”,

**AUTHOR:** M. IndraSena Reddy, K Subba Reddy and V Uday Kumar,

**YEAR: 2013**

**DESCRIPTION:** Steganography and cryptography methods are used together with wavelets to increase the security of data while transmitting through networks. In discrete wavelet transform, “analysis filter bank “can be used for analyzing image signal by passing through it. This filter bank consists of a low pass and a high pass filter at each decomposition stage. The digital watermarking plays an important role in embedding information into a digital image signal, for verification and identity of its owners. In this paper the embedded information is applied as text. Before embedding the text in image, text is encrypted using Advanced Encryption Standard (AES) algorithm. The text can be a sentence or a key with alphabetic words having the length of 8 characters. Using Least Significant Bit (LSB) method, the encrypted text is embedded into the “LL sub-band wavelet decomposed image”. The inverse wavelet transform is applied and the resultant image is transmitted to the receiver. Now at the receiver”s end, the image transformed using wavelet and encrypted text is extracted by using LSB method. The paper also shows how the AES algorithm is used in decryption of result.

# TITLE: Reversible data hiding scheme using reference pixel and multi-layer embedding.

**AUTHOR:** Zeng XT, Li Z, Ping LD

**YEAR: 2012**

**DESCRIPTION:**

This paper presents a [lossless](https://www.sciencedirect.com/topics/mathematics/lossless) [data hiding](https://www.sciencedirect.com/topics/computer-science/data-hiding) scheme. The proposed scheme is based on the pixel difference [histogram](https://www.sciencedirect.com/topics/mathematics/histograms) shifting to spare space for data hiding. Pixel differences are generated between a reference pixel and its neighbors in a pre-assigned block. After the difference histogram shifting, a [large number](https://www.sciencedirect.com/topics/mathematics/largest-number) of data can be embedded into the cover image, and multi-layer embedding is used to improve the [hiding capacity](https://www.sciencedirect.com/topics/computer-science/hiding-capacity). Different from previous works based on histogram shifting the proposed scheme can extract the hidden data and recover the exact original cover image with no extra information except the length of hidden data and the stego-image itself. [Experimental results](https://www.sciencedirect.com/topics/engineering/experimental-result) show that the average pure [payload](https://www.sciencedirect.com/topics/engineering/payload) among eight commonly used [grayscale images](https://www.sciencedirect.com/topics/engineering/grayscale-image" \o "Learn more about Grayscale Image from ScienceDirect's AI-generated Topic Pages) is up to 1.08 bits per pixel (bpp) while keeping low distortion.

**TITLE:** Distortion less data hiding based on integer wavelet transform

**AUTHOR:** Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su

**YEAR: 2003**

**DESCRIPTION:** A novel distortionless image data hiding algorithm based on integer wavelet transform that can invert the stego-image into the original image without any distortion after the hidden data are extracted is proposed. This algorithm hides data into one (or more) middle bit-plane(s) of the integer wavelet transform coefficients in the middle and high frequency subbands. It can embed much more data compared with the existing distortionless data hiding techniques and satisfy the imperceptibility requirement. The image histogram modification is used to prevent greyscales from possible overflowing. Experimental results have demonstrated the validity of the algorithm.

**TITLE:** Data hiding using edge detector for scalable images

**AUTHOR:** Jung KH & Yoo KY.

**YEAR: 2014**

**DESCRIPTION:** In this paper we propose a data hiding method that utilizes image interpolation and an edge detection algorithm. Image interpolation algorithm enlarges a cover image before hiding secret data in order to embed a large amount of secret data. Edge detection algorithm is applied to improve a quality of stego-image. Experimental results show that the proposed method can embed a large amount of secret data while keeping visual quality better than previous works. We demonstrate that the average capacity is 391,115bits, and the PSNR and quality index are 44.71dB, 0.9568 for gray images when threshold value is 4 and the embedding bits are given to 2 respectively.

**TITLE:** A fast and secure image hiding scheme based on LSB substitution.

**AUTHOR:** Chang CC, Lin MH, Hu YC

**YEAR: 2002**

**DESCRIPTION:** The improving technology and the ubiquity of the Internet have allowed more and more people to transmit data via the Internet. The contents of the transmission can be in the form of words, voices, images, or even computer animation. To protect the contents from interceptors' attention, the image hiding technology thus emerged. Some contents transmitted via the Internet can be confidential data such as highly valued product design blueprints or war plans, so it is important to pay more attention to the security of the transmitted data, or what we called secret image in this paper. The point of this paper is to enhance the security of the secret image without causing too much distortion to the host image and in the meantime to shorten the image hiding process time. For better protection, we adopted encryption process DES. In addition, we used greedy algorithm to shorten hiding process and to protect the host image from being severely distorted.

To test our proposed method to see whether it indeed achieved its objective, we used two sets of images in our experiment. The results of the experiments showed, when k = 2, our PSNR is close to that of Wang *et al.*'s optimal LSB substitution, but is not significantly different from that of simple LSB substitution. However, our method took approximately only 1/7 of the time consumed by Wang *et al.* When k = 3, our PSNR is significantly higher than that of simple LSB substitution. The experimental results confirmed that our method could effectively protect host image quality and shorten the overall hiding time when it enhanced the security of the secret image.

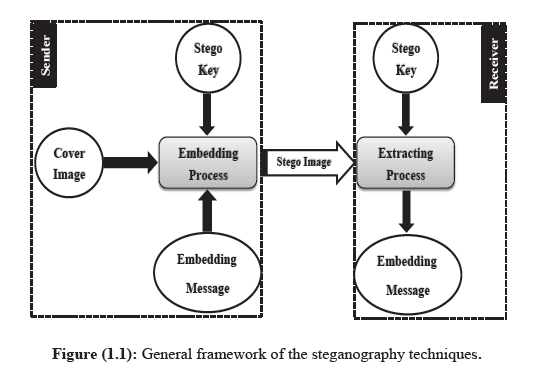
CHAPTER 3

**PROBLEM STATEMENT OF PROJECT**

The Steganography is used as an approach for hiding digital information in a digital image, therefore it is considered as a means of communication that is used to transfer secret messages. However, transferring large amount of confidential data safely is dependent on the size of the cover image transmitted and used between related parties. In this work, the goal was to secure the transmitted data and prevent it from looking suspicious. This is carried out using steganography techniques and system encryption algorithms together for the purpose of improving these fundamental aspects of hiding digital information in an image. Some digital properties which can be used to determine the ability of Steganography and enhance the image used in the concealment quality were applied to guarantee reliable transition approach of secret data.

Generally, the fundamental framework for an image steganography model that could be utilized in copyright protection or concealing communication is demonstrated in Figure (1.1). Two main processes are involved in image steganography model consists, which are the embedding process and the extracting process. The first process is used to hide or embedding the secret message in a certain image, which is known the cover image.

In hidden communication techniques, the cover image is no more than an innocent piece of information that is used to hide the secret information. whereas in copyright protection techniques, the cover image is the important information that needs protection and the hidden message could be a copyright mark. In the embedding process, a stego key is used to make the embedded message difficult to extract without passing this key.



The stego image represents the output of the message embedding process. This image includes the original image holding the hidden secret message. At the recipient side the embedded message is retrieved from the stego image either to verify the image copyright or to complete the hidden communication process. The stego key is used in the embedding process and it has to be used in the extracting process. Researchers are still working to find sophisticated techniques for hiding information to keep in track with the rapid evolution and advancement in technologies used in hiding information and networking.

**MOTIVATION**

The purpose of the steganography is not only preventing others from knowing the hidden information, but also removing the suspicion in having hidden information. The distinctive thing in techniques used in hiding information is to stay in track with modern technologies and their ability to be used in all computer media (texts, image, audio, video and network packets).The

message is a confidential document to be transmitted and camouflaged in the carrier so that it becomes difficult to detect. There are two main aspects in any steganography system, which are steganography capacity and imperceptibility. However, these two properties are confusing with each other. This is because it is very hard to increase capacity while maintaining the steganography imperceptibility of a steganography system. Furthermore, there are still limited methods of concealing information for use with data transfer communication protocols, which can be unconventional but their future is promising.

**OBJECTIVES AND SCOPE OF PROJECT**

The aim of this thesis is to improve and propose a new hybrid technique for data security through integration between cryptography and steganography algorithms. This system is used to embed an encrypted secret message into a cover image to get high imperceptibility and durability with minimal deterioration in the received stego image. The main objectives of this work were

to:

* Develop a security system for hiding text data in an image using steganography techniques (**LSB** and **DWT**) individually.
* Develop a hybrid security system which integrates both data encryption (**AES**) and steganography techniques (**LSB** and **DWT**) to increase data imperceptibility, robustness and performance of stego image.
* Evaluate the efficiency of the developed system in securing and retrieving the original data.
* To enhance the security of the data transmission.
* To Design a method that is robust against hacking.
* To improve image quality and embedding capacity.

**CHAPTER 4**

**EXISTING SYSTEM AND PROPOSED SYSTEM METHODOLOGY**

**EXISTING SYSTEM**

To hide the secret information, the message is embedded in cover text by using some embedding algorithm.The image Steganography allows the two parties to communicate secretly by allowing copyright protection and using digital watermark. The revised LSB matching was proposed to improve by applying lowering the number as a modification.To improve the image quality, the optimal LSB substitution, the approximately optimal LSB substitutions based on genetic algorithm and the modulus LSB substitution proposed.

In cryptographic solutions DES and AES will provide the security but from cryptography point of view they differ one is symmetric and another one is asymmetric.

**EXISTING SYSTEM DRAWBACKS**

* The conventional encryption methods failed to give the desired result of protecting the data.
* DES is breakable, as the key is 56-bit length .
* The existing Encryption Standard comparatively slower.

**PROPOSED SYSTEM**

In this paper, a new method is used to send the data in a more secured manner. In this paper, a new method is used to send the data in a more secured manner. The given text which is to be transmitted is encrypted with one of the symmetric key techniques: AES with the given key. In this process by using the key, the given text is encrypted. Then this resultant text is decrypted with the same key. (Here, the key is of length 56-bit.) Then, that cipher text is embedded into the LL sub-band of the wavelet transformed image. The method to embed the data is the Least Significant Method. This method is described in Algorithm-1. Note that, as we are modifying the LSB (±1 or no change to the given pixel value) since our human eye cannot find the difference between the original image and the watermarked image. Once the cipher text is embedded into the LL sub-band, inverse wavelet transform is applied. Then this resultant image is sent to the receiver.

2.1. **Algorithm-1: Least Significant Method**

Begin

Step-1: Read the value of the pixel.

Step-2: Convert it to its equivalent binary form.

Step-3: Modify the least significant bit accordingly.

End.

**Algorithm-2: AES is a block cipher.**

It contains the byte substation, shift rows, mix columns and then add round key.

At the receiver’s end, the receiver does the forward wavelet transform of the received image. Now, from the LL sub-band, the text is extracted. The extracted text which has encrypted form is decrypted using the one key. The wavelet-based steganography has a new concept irrespective of application of wavelets. Here the information is stored in terms of wavelet coefficients of an image. But in the LSB technique there is a change in the bits of actual pixels.

**PROPOSED SYSTEM BLOCK DIAGRAM**

**TRANSMITTER**

**INPUT IMAGE**

**DISCRETE WAVELET TRANSFORM (DWT)**

**DECOMPOSED IMAGE**

**HIGH FREQUENCY COEFFICIENTS**

**LOW FREQUENCY COEFFICIENTS**

**HH**

**LL**

**TEXT**

**ENCRYPTION (AES)**

**INVERSE DISCRETE WAVELET TRANSFORM**

**SEND IMAGE**

**KEY**

**HL**

**FIGURE 1: PROPOSED SYSTEM ARCHITECTURE AT SENDER SIDE.**

**RECEIVER**

**FORWARD WAVELET TRANSFORM**

**DECRYPTION (AES)**

**ORIGINAL TEXT**

**RECEVIED IMAGE**

**KEY**

**FIGURE 2: PROPOSED SYSTEMAT ARCHITECTURE RECEVIER SIDE.**

**PROPOSED SYSTEM ADVANTAGES**

* Our proposed method shows better performance compared to existing.
* It is safe, secure and protected transmission of data.
* AES is faster.
* In AES we can use 128,192 or 259 bits long key ,so AES key is harder to break than DES,
* The encrypted text is embedded in the LL-sub-band of the wavelet transformed image.

**CHAPTER 4**

**SYSTEM REQUIREMENT SPECIFICATION**

System requirement specifications gathered by extracting the appropriate information to implement the system. It is the elaborative conditions which the system need to attain. Moreover, the SRS delivers a complete knowledge of the system to understand what this project is going to achieve without any constraints on how to achieve this goal. This SRS not providing the information to outside characters but it hides the plan.

**4.1 Hardware Requirements**

The necessary hardware regarding private PC that comprises configuration as specified as follows:-

1. Processor: Intel core i5.

2. Disk capability: 1GB for MATLAB only.

3. RAM: 2GB.

**4.2 Software Tool used**

The necessary program regarding private PC that comprises configuration as specified as follows:-

1. Windows 7(64-bit) operating system.

2. MATLAB 7.14 Version R2014a

.

**4.2.1 Overview of MATLAB**

MATLAB is built up by means of math works intended for fourth-generation programming language. A variety of process approved within MATLAB contains control concerning the matrix, purpose as well as plotting of data, execution regarding algorithms, design of user interface, as well as integrating by means of programs formed within other languages like C, C++, and java. Despite mathematical calculation, MATLAB can be meant for representational calculation as well. MATLAB can be meant for embedded methods and by the guide regarding extra package known as simulink. Specifically MATLAB permit intended for matrix estimation as well as thus can be intended for image processing. MATLAB is simple towards gaining knowledge of a variety of device boxes used for it; an illustration is image processing toolbox.

MATLAB interfaces programming surroundings, calculation as well as mental picture. This contains integrated correcting, data compositions as well as object-oriented correcting devices. These integrated tasks create MATLAB appropriate used for education as well as do research. To resolve scientific trouble MATLAB includes other benefits than usual programming language like c plus java. MATLAB arrived into promotion in 1984 in addition to now it is employed globally. Additional graphical instructions are offered within MATLAB that builds the visual effects obtainable right away. A variety of device box contains signal processing, simulation, control theory as well as some former that are employed extensively in science and technology. The lone disadvantage regarding MATLAB is expenditure worry.

**4.2.2 Image Processing Toolbox**

Image processing device box permits carrying out image improvement, deblurring of image, characteristic identification, decreasing of noise, image segmentation, arithmetical alteration, as well as registration of image. Image processing device intended for the execution regarding methods proposed are specified below:-

1. Fundamental import as well as export

2. Display

3. Thresholding

**Fundamental import as well as export functions**

Fundamental import as well as export functions permits images obtained by means of image accomplishment plans for example, digital cameras, medical imaging devices such as CT and MRI, microscopes, satellite and airborne sensors, telescopes, and other scientific instruments. Hence those images can be observed; analyzed, as well as process these images into numerous data types, together with single-accuracy as well as double-accuracy floating-point in addition to signed as well as unsigned 8-bit, 16-bit, plus 32-bit integers. Import as well as export functions are accustomed to carry out read as well as write process on images.

**Display function**

Display purpose is accustomed to illustrate the images that are interpreted by means of the import purpose. This purpose permits towards making displays by means of graphics as well as wording, images within a particular window as well as specific displays for example outline plot, histogram and so on.

**Thresholding**

Thresholding is a simple system concerning image segmentation. As of a gray scale image, thresholding can be able to be accustomed to generate binary images. Within thresholding section, the intensity not more than an appropriate value within input image will be displayed as black (intensity is zero) as well as the left out intensities will be made white (intensity is one) then displayed. This procedure is done in the direction of obtaining the segmented image.

**4.2.3 Features of Matlab**

* Interactive background meant for aim investigation as well as resolving the difficulty.
* MATLAB is a sophisticated language intended for creating, calculating as well as building up a purpose.
* It contains numerical tasks such as figures, calculus, sorting out, developments, mathematical integration, as well as working out equations.
* Graphics integrated intended for visualization.
* Intended for generating traditional plot integrated equipments is accessible.
* Troubles as well as way outs are given in well-known numerical symbol.

**4.2.4 SOFTWARE REQUIREMENTS**

* MATLAB 8.3 Version R2014a

**MATLAB**

The MATLAB high-performance language for technical computing integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

* Data Exploration ,Acquisition, Analyzing &Visualization
* Engineering drawing and Scientific graphics
* Analyzing of algorithmic designing and development
* Mathematical functions and Computational functions
* Simulating problems prototyping and modeling
* Application development programming using GUI building environment.

Using MATLAB, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran.

**CHAPTER 5**

**SYSTEM DESIGN**

**PROPOSED SYSTEM BLOCK DIAGRAM**

**TRANSMITTER**

**INPUT IMAGE**

**DISCRETE WAVELET TRANSFORM (DWT)**

**DECOMPOSED IMAGE**

**HIGH FREQUENCY COEFFICIENTS**

**LOW FREQUENCY COEFFICIENTS**

**HH**

**LL**

**TEXT**

**ENCRYPTION (AES)**

**INVERSE DISCRETE WAVELET TRANSFORM**

**SEND IMAGE**

**KEY**

**HL**

**FIGURE 1: PROPOSED SYSTEM ARCHITECTURE AT SENDER SIDE.**

Advanced Encryption Standard (AES) is a symmetric encryption algorithm in which we can use only one key for both encryption and decryption that can be used by sender and receiver. In AES we can use 128,192 or 259 bits long with each of them contains 2128,2192 and 2256 combinations. The secrecy maintained by the key is secured **and** authentication is maintained the key itself. In this both the keys must be kept secret. But without knowing private key or at least other information impossible to decode the cipher text. With the help of public key and algorithm it must be insufficient to find the private key. We need secrecy and authentication, only one key is enough that is private key for encryption. In cryptographic solutions DES and AES will provide the security but from cryptography point ofview they differ one is symmetric and another one is asymmetric. AES key is harder to break than DES, and both need more dealing out to distribute keys between sender and receiver. The AES algorithm formulated in the figure

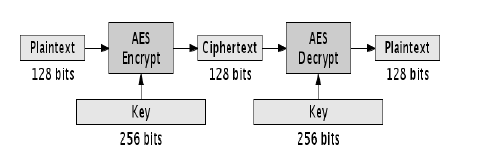
below.



The Advanced Encryption Standard (AES) is a crypto standard defined by the National Institute for Standards and Technology (NIST) in the United States. It is a result of a contest organized in 1997. NIST has encouraged existing parties all over the world to submit proposals for new standards. He was required of the proposals submitted to support block size of (128) bits, at least,

as well as the three main volumes consist of (128 192 and 256) bits. Three years later, the Rijndael Algorithm, designed by Joan Daemen and Vincent Rijmen, was announced as winner. The final standard AES was presented in 2001. Demonstrates the Block Cipher Operation. The important reason behind the success of the Rijndael algorithm was its simpilisity and easy

to implement at both software and hardware levels.



**Figure (2.8):** Block Cipher Operation.

Encryption with AES (Rijndael) algorithm consists of adding the initial round key. This is followed then by this application function round of the function (*Nr* - 1) times and (*a* = Nal) round with *a* a little (mod *i*) and the round function. The round suction consists of the (subbytes, shiftrows and mixcolumns) steps and an addition of the round key. The Mix Columns step is careless in the (Nal) round. The following give rise to describe a high level of

AES (Rijndael) algorithm:

By testring Rijndael (byteString plaintextBlock; key)

1 InitState (plaintextBlock; state)

2 AddKey (state; key0)

3 for i 1 to Nr - 1 do

4 - SubBytes (state)

5 - ShiftRows (sate)

6 - MixColumns (state)

7 - AddKey (state; keyi)

8 SubBytes (state)

9 ShiftRows (state)

10 AddKey (state; keyNr )

11 return state;

Both that hat each one of the inputs and outputs of the blocks AES (Rijndael) algorithm is to be in chains in the form of bytes. First, the state will be creating a matrix with a plain text block, and then work on the matrix filled (column by column). Then it is taken cipher text of the matrix state after the last round.

At this time, the note will be read matrix (column by column). All the steps function round of (subbytes, shiftrows, mixcolumns and Add key). It is invertible in the opposite direction [18]. The following are the steps of of the AES (Rijndael) algorithm and the type of output layers:

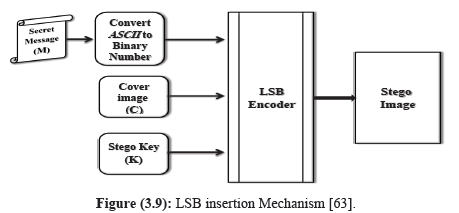
*  **Subbytes** (nonlinear layer( .
*  **Shif trow** (linear mixing layer( .
*  **Mixcolumn** (nonlinear layer).
*  **Addroundkey** (key addition layer).

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. This technique modifies the last significant bit (right most bit) of the RGB values of the pixel data image based on it its binary coding. Replacing Least Significant Bit is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by normal human vision [63]. This method makes it difficult for the human eye to discern hidden data, therefore it is quite effective. Moreover, the modifications that are made could be attributed to the noise that may already exist in the image. Digital images are mainly of two types:

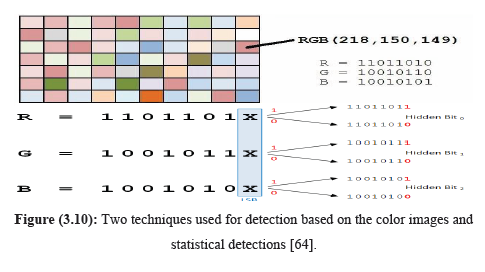
**1. 8 bit images**: In 8 bit images, one bit of information can be hidden.

**2. 24 bit images**: In 24 bit images, three bits of information can embedded in each pixel, one in each LSB position of the three eight bit values. Changing the LSB does not change the appearance of the image. Therefore the resultant stego image appears almost the same as the cover image.

Figure (3.9) shows the diagram of applying LSB algorithm on both the cover and hidden images.



In this work, we have use two techniques for detection, the first one is the detection with the color images, and the second is the statistical detections when the original images are available in the web secure database. The LSB Encoding Detection in Color Images is illustrated in Figure (3.10):



It could be noticed from the above image that the LSB of the pixel value in the cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remains unchanged; if not, set the LSB of C(i, j) to m. the S(i,j) is the stego image. The procedures used in message embedding are described as follow [44]:

Where, LSB (C(i, j)) refers to the LSB of cover image C(i,j) and m is the next message bit to be embedded. The following example, illustrates how the LSB modification was used in the proposed embedding technique. Suppose we would like to embed the message letter “**C**” in the LSBs of an image. The process is performed as follows [65]:

**Inputs:** Text file, cover image and secret key.

**Output:** Stego image.

**1.** Convert the message data from decimal to binary (C = 10000011(

**2.** Read the cover image pixels values.

**3.** Convert the cover image pixels values from decimal to binary.

**4.** Break the message to be hidden into single bits and take a number of bytes equal to it from the cover image.

**5.** Replace the LSB of cover data by one bit of the data to be hidden. So the Bit (1) is inserted into LSB of (11010010) to become (00010101). This step is repeated for all the bits of the Message to be embedded.

**FORWARD WAVELET TRANSFORM**

**DECRYPTION (AES)**

**ORIGINAL TEXT**

**RECEVIED IMAGE**

**KEY**

**FIGURE 2: PROPOSED SYSTEMAT ARCHITECTURE RECEVIER SIDE.**

**5.1 Data Flow Diagram**

A data flow diagram (DFD) is an illustration in a graphical form. It is an illustration concerning the "run" of information all the way through in a sequence, representing its procedure part. Frequently they are a beginning move employed towards building a general idea regarding the method that will be detailed later on. A DFD demonstrates the variety of input data in sequence to with output as of the method, in which the information will approach as of plus exit towards, in addition to in what the information will be accumulated. It doesn’t demonstrate in sequence regarding the instance of procedures, or else in sequence regarding whether the procedures will work sequentially or else separately.

**FLOW CHART:**

KEY

ENCRYPTION

LL sub-band

LL sub-band

TEXT

IMAGE

WAVELET TRANSFORM

INVERSE WAVELET TRANSFORM

SEND IMAGE

WAVELET TRANSFORM

ENCRYPT Text

DECRYPTED DATA

EXTRACTED DATA

**FIGURE 2: FLOW OF PROPOSED SYSTEM**

**Conversion from Plain Text to Cipher Text**

AES is a block cipher. It operates on plain text with a block of bits and returns cipher text with the same size. In this algorithm we have performed 10/12/14 rounds. It contains the byte substation, shift rows, mix columns and then add round key. The sub-stution of each byte uses one table with a 16x16 bytes and it contained a permutation of all specified values. Each byte of state is replaced by the byte indexed with row and column. In shift rows is used circular byte. Shift in each, the 1st row is unchanged and the 2nd row is 1 byte circular shift to the left and the 3rd row is 2 bytes circular shift to the left likewise it may process and decrypt inverts using circular shift to right. In the mix columns, each column is processed and separated and each byte is replaced by a value dependent on all bytes in the column. And add round key is a XOR state with 128-bits of key processed by column and inverse for decryption. AES decryption is not identical to encryption since the steps done in reverse order but is defined as equivalent inverse cipher with steps as for encryption by using inverse of each step with a different key.

**Selecting an Image file**

First, select any image file, behind which the user wants to hide data. The image which is selected should have fixed height and width. Now save the image file as in jpeg extension and the image appears as an original image file.

**Image Steganography**

**For Sender Side**

In this, The sender will select the original image in jpeg extension format. Now the sender read the file using „imread􁪃 function. And convert the image file from rgb to gray using a function „rgb2gray􁪃. After this read the text and convert that text into a binary format. Then the key is read and the text is converts into encrypted format .When the wavelet transformation function.The image can divide into the sub bands as LL, LH, HL , HH. The binary cipher has to be put into LL Sub band. We can apply the inverse wavelet transformation function and convert the image into its original size. And the image is sent to the receiver.

**Creating Stego Image file**

For creating stegno Image file, combine stego text file and stego image file using digital watermarking. This forms the stego image text file at transmitter side in which hidden text is present.

**For Receiver Side**

When the receiver reads the text file using „fread􁪃 it gets converted into an image. For this receiver apply the wavelet transformation function and divide the image into four sub bands as LL, LH, HL, HH. Now choose the required LL sub band from the image. Using extractionfun2 ( ) to extract the code from image and convert it into hexadecimal format and then store it into a variable „extra1􁪃.Now decrypt the encrypted code.

**Image Recovery**

The image file is read by the function „imgread􁪃 and the text file is opened using fopen function and is stored into a variable „fid􁪃. Using the function fread it is stored into a variable „a􁪃. Now convert the text file into the image file using matrix representation. Here to perform some addition and subtractions on the matrix it is placed into the proper sub band i.e., LL, LH, HL, HH. The image can be recovered by the text.

CHAPTER 6

**FUNCTIONAL MODULES**

**MODULE 1**

**An Overview of Encryption**

Information security has become more important in data storage and transmission. This chapter provides some security backgrounds that apply many encryption algorithms. The rapid development of data exchange in electronic ways and the widespread of image use have put a great potential on data security and safeguard of confidential data from accessible from unauthorized. Encryption is considered as one of the most commonly used approaches for ensuring high data security. In recent years, a great development has occurred in encryption technology, where many encryption methods are used for image security. These methods produce random encryption keys, whereas the actual content is not visible. Both of the encryption and decryption algorithms are designed and implemented to provide secure transfer of image data.

**This chapter includes the follows topics:**

**1 –** Introduction to Information Security,

**2 –** History of Cryptography,

**3 –** Types of Cryptography (Encryption),

**4 –** Image Encryption,

**5 –** Digitai image concept,

**6 –** Major image Encryption Techniques,

**7 –** Summary.

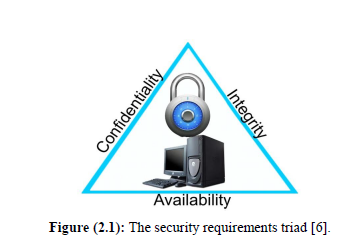
**2.1. Introduction to Information Security:**

Information security is a means to an end and not the end in itself. In business, the existence of an effective information security program is usually secondary to the need to make a profit. In the public sector, information security is secondary to the stability of its services. The must not lose sight of these goals and targets.

The Digital communication is an integral part of life. With the advent of digital technology, This has become more sophisticated than ever. Moreover, information has become the most expensive commodity in the sense of the most sought-after in the world today. In addition, the rapid growth of the age of the computer for all documents and audio and video recordings being digitized. This has increased the need to ensure the security and integrity of any document, audio and video to maintain privacy, piracy and mass reproduction. This condition varies from one individual to another. The different techniques used to ensure that privacy is encryption [4]. The confidential information may be considered such as military secrets, banking transactions, and so on must be guarded against unauthorized access. As a result, developing a new field of study is called "information security". Information security is a science that deals with the secure transfer of critical information from one person to another. This should happen by maintaining the integrity and authentication, confidentiality and non-repudiation, in such a way that the transmitted information can not be accessed by unauthorized person only the sender and receiver [5]. This is considered the core of information security that provides a structure for all other aspects of information security.

The information security has three primary goals for information security, which are confidentiality, integrity, and availability as illustrated in Figure (2.1)

* **Confidentiality (secrecy)**: Refers to maintain the restrictions authorized access to information and disclosure, including ways to protect the privacy of personal and confidential information. Loss of confidentiality is the unauthorized disclosure of information.
* **Integrity:** Deals guard against the alteration of the information inappropriately or destruction, including ensuring non repudiation of the information and authenticity. Loss of integrity is the unauthorized modification or destruction of information. Availability of secure access in timely and reliable information on time.
* **Availability:** Disable access to or use of information or information system. When they put these three principles together and the information we have and will be well protected. In addition to multiple sources of information security attacks, there are also many types of information security attacks.



**Figure (2.1):** The security requirements triad [6].

Every data communication transaction must met some of the goals related to information security. Most of these goals include the common security of information in addition to the three mentioned before [7]:

**1. Identification (Entity authentication):** It the identity of the entity (person, credit card, etc.).

**2. Authorization:** Is the transportation to another entity, with official approval to do to be a certain thing.

**3. Message authentication:** Is backing a source of information, which is also known known as the origin of the data authentication.

**4. Validation of information:** It is a way to provide a timely authorization of the use or manipulation of information.

**5. Time-stamping:** Is the record time of creation or existence of information.

**6. Signature:** Is a way to link the information to the entity.

**2.1.1. Security Implementation:**

Four complementary courses of action are involved in security implementation [8]:

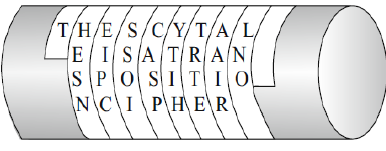
* **Prevention:** An ideal security system aims to prevent unauthorithed attacks. However, this is not practical in most cases, because there are many threats that prevention is a reasonable goal.
* **Detection:** The absolute protection in some cases, are not possible, while it is possible to detect security attacks. For example, there is intrusion detection systems are designed for the purpose of detecting the presence of an individual or unauthorized individuals register to enter the system.
* **Response:** It refers to the system in response to stop the attack and prevent further damage. This is in case if security mechanisms detect an ongoing attack.
* **Recovery:** It referes to the backup of the security system in case if it is compromising the integrity of the data. As in the former case, you can restore the correct copy of the data that can be recharged.

**2.2. Cryptography**

**2.2.1. History of Cryptography:**

Cryptography is a rather old business; however it seems closely connected with modern electronic communication. Possible to give an early example and return to about (2000 BC), when it was used non standard hieroglyphs "secret" in the civilization of ancient Egypt. The Egyptian days ago, it has been the use of encryption in one form or the other in a lot sometimes, if not more, and that the cultures that developed a written language. For example, there are no

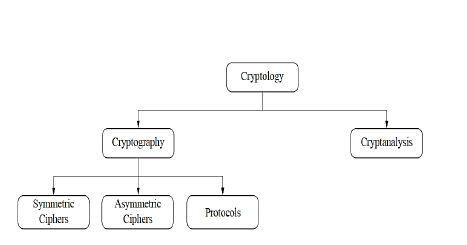
documented cases of secret writing in the civilization of ancient Greece, a Skital of Sparta, Figure (2.2), or that you know the famous blades Caesar. This work focuses on modern cryptographic approaches in issues related to data security and their relationship with cryptography.



**Figure (2.2):** Scytale of Sparta [9].

Figure (2.3) provides an overview to the field of cryptography. The first thing

that we notice is that the most general term is cryptology and not cryptography.



**Figure (2.3):** Overview of the field of cryptology [9].

Cryptology is divided into two main sections, namely:

* **Cryptography**: It the science of secret writing the main goal is to hide the true meaning of the message used.
* **Cryptanalysis**: It is a science or art of coding systems break down. Sometimes you might think that the break be available and should not be included in the classification of a serious scientific discipline. Although these days most of cryptanalysis by researchers in academia and of central importance to modern coding systems. We will never know whether they are safe or not [9].

The Cryptanalysis is considered as an integral part of cryptology, because it is the only way to assure that a cryptosystem is secure. Cryptography is a general word, which has sub-categories.

Cryptography can be defined as working to transform the data into a secret code to carry more than the public network. Therefore, the sender was able to secure sensitive information and mission or to transmit it through non secure networks or non-protected storage, so the data will not be available to only one recipient.

**2.2.2. Cryptography Main Concepts:**

A large number of technical and legal skills are requires to achieve information security in an electronic society. The provision of technical means is through encryption. Since the Cryptography or (Cryptology) is considered the practice and study techniques for secure communication, in the presence of third parties, it called the (adversaries). More generally, it is about building and analysis protocols that overcome the influence of adversaries. The encryption modem intersects the disciplines of mathematics, computer science, and electricalengineering. Cryptography is not the only means by which the provision of information security, but it is one set of technologies [10].

**2.2.2.1. Cryptography Goals:**

One of the things it offers Cryptography, which is the number of security objectives and to ensure data privacy, and do not change the data and so on. Because of the advantages of a major security coding and it is used widely today. Among all targets the security of the information listed above, the following four objectives are considered the foundation. These objectives are (confidentiality, authentication, integrity and non repudiation) [11]. The primary goal of Cryptography is sufficiently address each of these four areas that have been mentioned in both theory and practice. Encryption is working on the prevention and detection of fraud and other malicious activities.

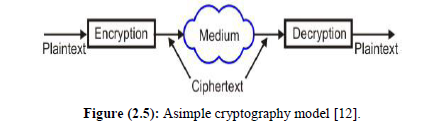
**2.2.2.2. Major Concepts:**

Encryption cryptography is the process of encoding messages in way hackers can not read it, but that can be authorized pesonnal. In the encryption system (**E** = the message), it is encrypted (**P** = plain text) using the encryption algorithm that transforms them into unreadable (**C** = cipher text). This is done using the encryption key, which explains how the message to be encrypted. Only

authorized party, is able to decode text using symbols and codes (**D** = decryption algorithm), which usually requires (**K** = secret decryption key). Usually it needs to generate key encryption algorithm system for technical reasons, to produce random keys [12].

The role of cryptography can be illustrated as a simple model of cryptography as demonstrated in Figure (2.5). The basic idea of encryption is to modify the content of the message in a certain way only allow the legal recipient can rebuild its content. The discrete valued cryptosystem can be described by:

*  **P**: It is a symbol a set of possible plain texts.
*  **C**: It is a symbol a set of possible cipher texts.
*  **K**: It is a symbol a set of possible cipher keys.
*  **E,D**: It is a symbol a set of possible encryption and decryption transformations.



**Figure (2.5):** Asimple cryptography model [12].

**2.2.3. The Basic Terminology in Cryptography:**

* **Plain Text:** It refers to the original message sender that the wants to communicate with another person.
* **Cipher Text:** It to the message that cannot be understood by anyone. In other words it is a meaningless message, where the original message (plain text) you will turn to the message unreadable and incomprehensible through an encoder before the actual message transfer.
* **Encryption:** It explans is the process used to convert (plain text) into (cipher text), which is called as Encryption. Encryption technique are used to send secret messages and encoded through a private and secure channel. The encryption process will need two main things, which are the basics of each algorithm encryption algorithm and key.
* **Decryption:** It reverses the encryption process. In other words, any process to convert (cipher text) to (plain text).We use the decryption technique side in the second technique (receiver) so as to obtain the support of the original (cipher text message). Here, the process also needs to decryption algorithm and key to make sure the message is sent.
* **Key:** It refers to a numerical or alpha numeric text or a special character. And this key is used on the first two phases as encryption (plain text) and the second time decryption of (cipher text) the selection is very important in the cryptography key to the security of the encryption algorithm mainly depends directly on it. When the same key is used for encryption and decryption it is called as symmetric key cryptography. On the other hand, when it is the use of different keys in the cryptographic mechanism, Where it is to use a special encryption key one, and another, and the second is used is different from the decryption key. Where this mechanism is called as Asymmetric Cryptography Key as illustrated in Figure (2.6) [13].

**Advanced Encryption Standard (AES) Algorithm:**

The Advanced Encryption Standard (AES) is a crypto standard defined by the National Institute for Standards and Technology (NIST) in the United States. It is a result of a contest organized in 1997. NIST has encouraged existing parties all over the world to submit proposals for new standards. He was required of the proposals submitted to support block size of (128) bits, at least,

as well as the three main volumes consist of (128 192 and 256) bits. Three years later, the Rijndael Algorithm, designed by Joan Daemen and Vincent Rijmen, was announced as winner. The final standard AES was presented in 2001.

.The important reason behind the success of the Rijndael algorithm was its simpilisity and easy

to implement at both software and hardware levels. Encryption with AES (Rijndael) algorithm consists of adding the initial round key. This is followed then by this application function round of the function (*Nr* - 1) times and (*a* = Nal) round with *a* a little (mod *i*) and the round function.

The round suction consists of the (subbytes, shiftrows and mixcolumns) steps and an addition of the round key. The Mix Columns step is careless in the (Nal) round. The following give rise to describe a high level ofAES (Rijndael) algorithm:’

Both that hat each one of the inputs and outputs of the blocks AES (Rijndael) algorithm is to be in chains in the form of bytes. First, the state will be creating a matrix with a plain text block, and then work on the matrix filled (column by column). Then it is taken cipher text of the matrix state after the last round.

At this time, the note will be read matrix (column by column). All the steps function round of (subbytes, shiftrows, mixcolumns and Add key). It is invertible in the opposite direction [18]. The following are the steps of of the AES (Rijndael) algorithm and the type of output layers:

*  Subbytes (nonlinear layer( .
*  Shif trow (linear mixing layer( .
*  Mixcolumn (nonlinear layer).
*  Addroundkey (key addition layer).

By testring Rijndael (byteString plaintextBlock; key)

1 InitState (plaintextBlock; state)

2 AddKey (state; key0)

3 for i 1 to Nr - 1 do

4 - SubBytes (state)

5 - ShiftRows (sate)

6 - MixColumns (state)

7 - AddKey (state; keyi)

**8** SubBytes (*state*)

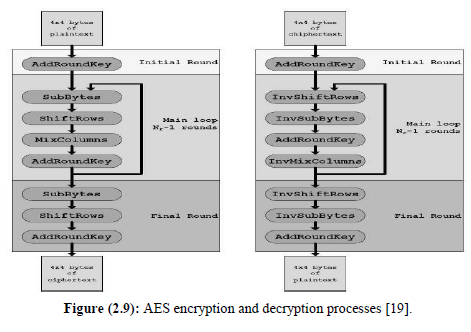
**9** ShiftRows (*state*)

**10** AddKey (*state; keyN****r*** )

**11** return *state*;

**AES as Hardwired Electronics:**

AES is a symmetric cipher where the same key is used on both sides. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192, or 256 bits. When longer messages are sent, they are divided into 128 bit blocks. Obviously, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process. A 128 bit message block can be thought of as organized in a two dimensional 4×4 byte array. AES encryption has four main operations that are repeated multiple times, and work on bytes, rows, and columns of this array. Figure (2.9) illustrates the AES encryption and decryption processes.



**Figure (2.9):** AES encryption and decryption processes [19].

**Evaluation Criteria for AES:**

The main demand of the AES algorithm submission is requir you must be a block cipher, which supports the length of the block consists of a 128 bit key lengths are: (128, 192, and 256) bits. The following evaluation criteria were used in evaluating the call for proposals [20]:

**1. Security:** Is one of the most important factors in the evaluation in terms of**:**

* Are compared to the actual security algorithm for other algorithms provided.
* It is important to ensure the integrity of the foundation of mathematics used to maintain the security of the algorithm.
* The other security factors that are by the public and that are discovered during the evaluation process.

**2. Cost:** This section includes the following**:**

* The licensing requirements, as the AES algorithm should be available and not exclusive.
* Must be Are available as well (Excellent computational efficiency, memory capacity) requirements.

**3. The algorithm and implementation of characteristics:** This includes the following**:**

* Flexibility, which are intended to provide the key tools such as:

(PRNG, MAC generator, retail, stream cipher).

* Must provide a suitable environment between (Hardware and software) used and also provides (The ease and simplicity).

The following Table (2.1) summarizes the performance analysis and

comparison AES algorithms.

**Table (2.1):** Performance analysis and comparison such as AES.

**No. Features Advantages**

**1** Encryption Fast

**2** Decryption Fast

**3** Key size (length) 128 bits. 192 bits. 256 bits

**4** The block size 128 bits

**5** Rounds 10. 12 or 14

**6** Speed depends on Key Fast

**7** Security Excellent security (Insecure )

**8** Cost Cheaper

**9** Implementation Simple

**10** Power consumption Low

**Advantages of Asymmetric Key:**

Asymmetric Key cryptography has the following advantages:

**1.** In PKC will note there is no need to be the exchange of keys, which will remove the key distribution problem.

**2.** In order to increase the key PKC security feature, which the private keys do not ever need to be transmitted or disclosed any person who handles them.

**3.** It can also be told to PKC that is working to provide digital signatures, which can be repudiated.

**Disadvantages of Asymmetric Key:**

The main disadvantage of using PKC is the time complexity for encryption. Nowadays, and note that there are some methods of the secret encryption key to be local or popular, and that the advantage of being much faster than PKC method.

**MODULE 2**

**Overview of Steganography:**

**Steganography Defined:**

Steganography is the science and art of hiding information within a carrier, where no one, except the intended recipient, has knowledge of the existence of hidden information. The word originates from the ancient Greek words "steganos" (covered) and "graphic" (writing), literally meaning "covered writing" .a process of secret communication where a piece of information (a secret message) is hidden into another piece of innocent looking information, popularly called a cover, in such a way that the existence of the secret information remains concealed without raising any suspicion in the minds of the viewer's.

**3.1.2. The Element S of Steganography:**

Two pieces of data are required in steganography, which are the cover and the data to be hidden [42]:

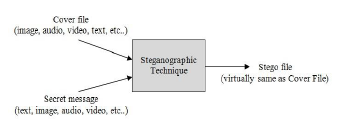
**1. The Cover**

The cover refers to the medium into which the data we will be embedded. The effectiveness of the steganography technique is dependent up on selecting the most appropriate cover. The cover also works as a container for the given message. Steganography is based on hiding the data behind the cover to protect it from being known as secure, dislike encryption. Therefore the embedded data can be retrieved once the embedding is suspected. Image, video, audio and

other file formats can be used to embed secret messages.

**2. The Data**

The data that are required to be hidden should be serializable in order to be embedded bit by bit in the cover. The size of data shouldn’t exceed the cover size in order to contain all the data. In case of images, both the cover and the data may have the same number of pixels; however the cover will have more color information for each pixel than the hidden data. Figure (3.1) shows the fundamental approach of steganography process [43].



**Figure (3.1)**: Fundamental approach of steganography process [43].

Generally, any steganography system consists of two phases encoding or embedding phase and decoding or extracting phase. A stego key is used to encode or embed the secret message into a covert innocent message as illustrated in Figure (3.2), which shows a general steganography Model [43]. The secret key steganography can be defined as the quintuple (**C, M, K, DK,**

**and EK**) where:

 **C**: the set of possible covers.

 **M**: the set of secret message.

 **K**: the set of secret keys.

 **Ek** : C ×M×K→C

With the property that **DK (EK(c, m, k), k) = m** for all **m Є M, c Є C** and k **Є K.**

The items above are described in the following [43]:

 **Emb (m):** refers to data or signal to be hidden in another media.

 **Stego (s):** refers to the object which is carrying a hidden message.

 **Cover (c):** The input to the information hiding process which represents the innocent carrier signal or file.

 **Stego key (k):** This is additional unimpeded secret data which may be required in the information hiding process. This key is required to retrieve the embedded message in its final target.

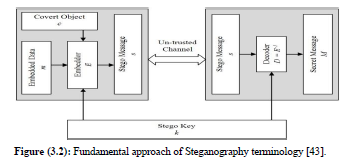


Figure (3.3) shows the main functions of steganography. The secret information is hidden in an image (known as cover image) with the stego key by the sender. This image is transmitted over a communication channel. The stego key is used to extract the hidden secret information at the other end. The medium used in this case is a digital JPEG image, however other formats such

as audio, and video can be used. A possible formula of the process may be represented as [44]:

***Cover (image, audio, video) + embedded message + stego key = stego- message***

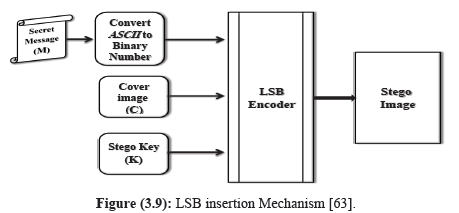
Some terminology has been used such as 'cover', 'embedded', and 'stego'. The term "cover" refers to description of an original, innocent massage, data, audio, video, and so on. The sender of a message has to embed hidden information in a cover, called stego. Steganography is an alternative tool for privacy and security.

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. This technique modifies the last significant bit (right most bit) of the RGB values of the pixel data image based on it its binary coding. Replacing Least Significant Bit is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by normal human vision [63]. This method makes it difficult for the human eye to discern hidden data, therefore it is quite effective. Moreover, the modifications that are made could be attributed to the noise that may already exist in the image. Digital images are mainly of two types:

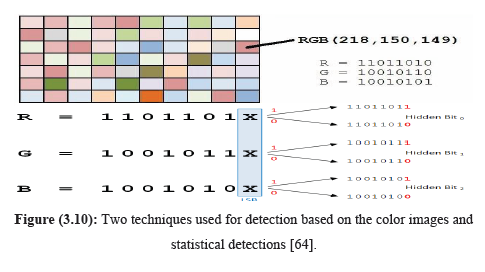
**1. 8 bit images**: In 8 bit images, one bit of information can be hidden.

**2. 24 bit images**: In 24 bit images, three bits of information can embedded in each pixel, one in each LSB position of the three eight bit values. Changing the LSB does not change the appearance of the image. Therefore the resultant stego image appears almost the same as the cover image.

Figure (3.9) shows the diagram of applying LSB algorithm on both the cover and hidden images.



In this work, we have use two techniques for detection, the first one is the detection with the color images, and the second is the statistical detections when the original images are available in the web secure database. The LSB Encoding Detection in Color Images is illustrated in Figure (3.10):



It could be noticed from the above image that the LSB of the pixel value in the cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remains unchanged; if not, set the LSB of C(i, j) to m. the S(i,j) is the stego image. The procedures used in message embedding are described as follow [44]:

Where, LSB (C(i, j)) refers to the LSB of cover image C(i,j) and m is the next message bit to be embedded. The following example, illustrates how the LSB modification was used in the proposed embedding technique. Suppose we would like to embed the message letter “**C**” in the LSBs of an image. The process is performed as follows [65]:

**Inputs:** Text file, cover image and secret key.

**Output:** Stego image.

**1.** Convert the message data from decimal to binary (C = 10000011(

**2.** Read the cover image pixels values.

**3.** Convert the cover image pixels values from decimal to binary.

**4.** Break the message to be hidden into single bits and take a number of bytes equal to it from the cover image.

**5.** Replace the LSB of cover data by one bit of the data to be hidden. So the Bit (1) is inserted into LSB of (11010010) to become (00010101). This step is repeated for all the bits of the Message to be embedded.

**The Advantages and Disadvantages.**

The LSB is characterized by its simplicity in embedding the bits of the message directly into the LSB plane of cover image [68]. Working with the LSB does not result in a human perceptible difference. This is because the amount of the change is small. Consequently, the obtained stego image will look typical to the cover image and it will not be visible to the human eye.

The **advantages** of LSB can be summarized in its popularity, easy to understand, high perceptual

transparency, and low degradation in image quality. On the other hand, the **disadvantages** are low robustness to malicious attacks, vulnerability to accidental noise, and low temper resistance.

**CHAPTER 7**

**IMPLEMENTATION**

The execution stage regarding the task is that the complete aim is essentially changed keen on running code. Intend regarding the stage is towards interpreting the aim keen on a finest likely result within an appropriate programmed language. In this section, it covers up the execution phase concerning the task, providing particulars regarding the programmed language as well as improvement background employed. It as well provides a general idea about the important sections regarding the task by means of its bit by bit course.

The execution phase involves the following tasks:-

* Cautious scheduling.
* Examination regarding structure as well as constraints.
* Aim concerning the techniques towards accomplishing the conversion.
* Assessment concerning the conversion technique.
* Accurate judgment about the choosing of the proposal.
* Suitable choosing regarding the language intended for function growth.

**7.3 INTRODUCTION**

**MATLAB** (**mat**rix **lab**oratory) is a [numerical computing](http://en.wikipedia.org/wiki/Numerical_analysis) environment and [fourth-generation programming language](http://en.wikipedia.org/wiki/Fourth-generation_programming_language). Developed by [Math Works](http://en.wikipedia.org/wiki/MathWorks), MATLAB allows [matrix](http://en.wikipedia.org/wiki/Matrix_(mathematics)) manipulations, plotting of [functions](http://en.wikipedia.org/wiki/Function_(mathematics)) and data, implementation of [algorithms](http://en.wikipedia.org/wiki/Algorithm), creation of [user interfaces](http://en.wikipedia.org/wiki/User_interface), and interfacing with programs written in other languages, including [C](http://en.wikipedia.org/wiki/C_(programming_language)), [C++](http://en.wikipedia.org/wiki/C%2B%2B), [Java](http://en.wikipedia.org/wiki/Java_(programming_language)), and [Fortran](http://en.wikipedia.org/wiki/Fortran).

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the [MuPAD](http://en.wikipedia.org/wiki/MuPAD" \o "MuPAD) [symbolic engine](http://en.wikipedia.org/wiki/Computer_algebra_system), allowing access to [symbolic computing](http://en.wikipedia.org/wiki/Symbolic_computing) capabilities. An additional package, [Simulink](http://en.wikipedia.org/wiki/Simulink), adds graphical multi-domain simulation and [Model-Based Design](http://en.wikipedia.org/wiki/Model_based_design) for [dynamic](http://en.wikipedia.org/wiki/Dynamical_system) and [embedded systems](http://en.wikipedia.org/wiki/Embedded_systems).

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of [engineering](http://en.wikipedia.org/wiki/Engineering), [science](http://en.wikipedia.org/wiki/Science), and [economics](http://en.wikipedia.org/wiki/Economics). MATLAB is widely used in academic and research institutions as well as industrial enterprises.

MATLAB was first adopted by researchers and practitioners in [control engineering](http://en.wikipedia.org/wiki/Control_engineering), Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of [linear algebra](http://en.wikipedia.org/wiki/Linear_algebra) and [numerical analysis](http://en.wikipedia.org/wiki/Numerical_analysis), and is popular amongst scientists involved in [image processing](http://en.wikipedia.org/wiki/Image_processing). The MATLAB application is built around the MATLAB language. The simplest way to execute MATLAB code is to type it in the Command Window, which is one of the elements of the MATLAB Desktop. When code is entered in the Command Window, MATLAB can be used as an interactive mathematical [shell](http://en.wikipedia.org/wiki/Shell_(computing)). Sequences of commands can be saved in a text file, typically using the MATLAB Editor, as a [script](http://en.wikipedia.org/wiki/Shell_script) or encapsulated into a [function](http://en.wikipedia.org/wiki/Functional_programming), extending the commands available.

MATLAB provides a number of features for documenting and sharing your work. You can integrate your MATLAB code with other languages and applications, and distribute your MATLAB algorithms and applications.

**7.4 FEATURES of matlab**

* High-level language for technical computing.
* Development environment for managing code, files, and data.
* Interactive tools for iterative exploration, design, and problem solving.
* Mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, and numerical integration.
* 2-D and 3-D graphics functions for visualizing data.
* Tools for building custom graphical user interfaces.
* Functions for integrating MATLAB based algorithms with external applications and languages, such as C, C++, Fortran, Java™, COM, and Microsoft Excel.

MATLAB is used in vast area, including signal and image processing, communications, control design, [test and measurement](http://www.mathworks.in/applications/t_m), financial modeling and analysis, and computational. Add-on toolboxes (collections of special-purpose MATLAB functions) extend the MATLAB environment to solve particular classes of problems in these application areas.

MATLAB can be used on personal computers and powerful server systems, including the [Cheaha](http://docs.uabgrid.uab.edu/wiki/Cheaha" \o "Cheaha) compute cluster. With the addition of the Parallel Computing Toolbox, the language can be extended with parallel implementations for common computational functions, including for-loop unrolling. Additionally this toolbox supports offloading computationally intensive workloads to [Cheaha](http://docs.uabgrid.uab.edu/wiki/Cheaha" \o "Cheaha) the campus compute cluster.MATLAB is one of a few languages in which each variable is a matrix (broadly construed) and "knows" how big it is. Moreover, the fundamental operators (e.g. addition, multiplication) are programmed to deal with matrices when required. And the MATLAB environment handles much of the bothersome housekeeping that makes all this possible. Since so many of the procedures required for Macro-Investment Analysis involves matrices, MATLAB proves to be an extremely efficient language for both communication and implementation.

**7.4.1 INTERFACING WITH OTHER LANGUAGES**

MATLAB can call functions and subroutines written in the [C programming language](http://en.wikipedia.org/wiki/C_(programming_language)) or [FORTRAN](http://en.wikipedia.org/wiki/Fortran). A wrapper function is created allowing MATLAB data types to be passed and returned. The dynamically loadable object files created by compiling such functions are termed "[MEX-files](http://en.wikipedia.org/wiki/MEX_file)" (for **M**ATLAB **ex**ecutable).

Libraries written in [Java](http://en.wikipedia.org/wiki/Java_(programming_language)), [ActiveX](http://en.wikipedia.org/wiki/ActiveX) or [.NET](http://en.wikipedia.org/wiki/.NET_Framework) can be directly called from MATLAB and many MATLAB libraries (for example [XML](http://en.wikipedia.org/wiki/XML) or [SQL](http://en.wikipedia.org/wiki/SQL) support) are implemented as wrappers around Java or ActiveX libraries. Calling MATLAB from Java is more complicated, but can be done with MATLAB extension, which is sold separately by Math Works, or using an undocumented mechanism called JMI (Java-to-Mat lab Interface), which should not be confused with the unrelated Java that is also called JMI.

As alternatives to the [MuPAD](http://en.wikipedia.org/wiki/MuPAD" \o "MuPAD) based Symbolic Math Toolbox available from Math Works, MATLAB can be connected to [Maple](http://en.wikipedia.org/wiki/Maple_(software)) or [Mathematica](http://en.wikipedia.org/wiki/Mathematica" \o "Mathematica).

Libraries also exist to import and export [MathML](http://en.wikipedia.org/wiki/MathML" \o "MathML).

* **Development Environment**
* Startup Accelerator for faster MATLAB startup on Windows, especially on Windows XP, and for network installations.
* [Spreadsheet Import Tool](http://www.mathworks.in/videos/matlab/new-spreadsheet-import-tool-in-r2011b.html?type=shadow) that provides more options for selecting and loading mixed textual and numeric data.
* Readability and navigation improvements to warning and error messages in the MATLAB command window.
* [Automatic variable and function renaming](http://www.mathworks.in/videos/matlab/new-automatic-variable-and-function-renaming-in-r2011b.html?type=shadow) in the MATLAB Editor.
* **Developing Algorithms and Applications**

MATLAB provides a high-level language and development tools that let you quickly develop and analyze your algorithms and applications.

* **The MATLAB Language**

The MATLAB language supports the vector and matrix operations that are fundamental to engineering and scientific problems. It enables fast development and execution. With the MATLAB language, you can program and develop algorithms faster than with traditional languages because you do not need to perform low-level administrative tasks, such as declaring variables, specifying data types, and allocating memory. In many cases, MATLAB eliminates the need for ‘for’ loops. As a result, one line of MATLAB code can often replace several lines of C or C++ code.

At the same time, MATLAB provides all the features of a traditional programming language, including arithmetic operators, flow control, data structures, data types, [object-oriented programming](http://www.mathworks.in/products/matlab/object_oriented_programming.html) (OOP), and debugging features.

MATLAB lets you execute commands or groups of commands one at a time, without compiling and linking, enabling you to quickly iterate to the optimal solution. For fast execution of heavy matrix and vector computations, MATLAB uses processor-optimized libraries. For general-purpose scalar computations, MATLAB generates machine-code instructions using its JIT (Just-In-Time) compilation technology.

This technology, which is available on most platforms, provides execution speeds that rival those of traditional programming languages.

* **Development Tools**

MATLAB includes development tools that help you implement your algorithm efficiently. These include the following:

**MATLAB Editor**

Provides standard editing and debugging features, such as setting breakpoints and single stepping

**Code Analyzer**

Checks your code for problems and recommends modifications to maximize performance and maintainability

**MATLAB Profiler**

Records the time spent executing each line of code

**Directory Reports**

Scan all the files in a directory and report on code efficiency, file differences, file dependencies, and code coverage

**Designing Graphical User Interfaces**

By using the interactive tool GUIDE (Graphical User Interface Development Environment) to layout, design, and edit user interfaces. GUIDE lets you include list boxes, pull-down menus, push buttons, radio buttons, and sliders, as well as MATLAB plots and Microsoft ActiveX® controls. Alternatively, you can create [GUIs](http://www.mathworks.in/discovery/matlab-gui.html) programmatically using MATLAB functions.

**5.5 The MATLAB System**

The MATLAB system consists of five main parts:

* **Development Environment**.

This is the set of tools and facilities that help you use MATLAB functions and files. Many of these tools are graphical user interfaces. It includes the MATLAB desktop and Command Window, a command history, and browsers for viewing help, the workspace, files, and the search path.

* **The MATLAB Mathematical Function Library**.

This is a vast collection of computational algorithms ranging from elementary functions like sum, sine, cosine, and complex arithmetic, to more sophisticated functions like matrix inverse, matrix eigenvalues, Bessel functions, and fast Fourier transforms.

* **The MATLAB Language**.

This is a high-level matrix/array language with control flow statements, functions, data structures, input/output, and object-oriented programming features. It allows both "programming in the small" to rapidly create quick and dirty throw-away programs, and "programming in the large" to create complete large and complex application programs.

* **Handle Graphics**.

This is the MATLAB graphics system. It includes high-level commands for two-dimensional and three-dimensional data visualization, image processing, animation, and presentation graphics. It also includes low-level commands that allow you to fully customize the appearance of graphics as well as to build complete graphical user interfaces on your MATLAB applications.

* **The MATLAB Application Program Interface (API).**

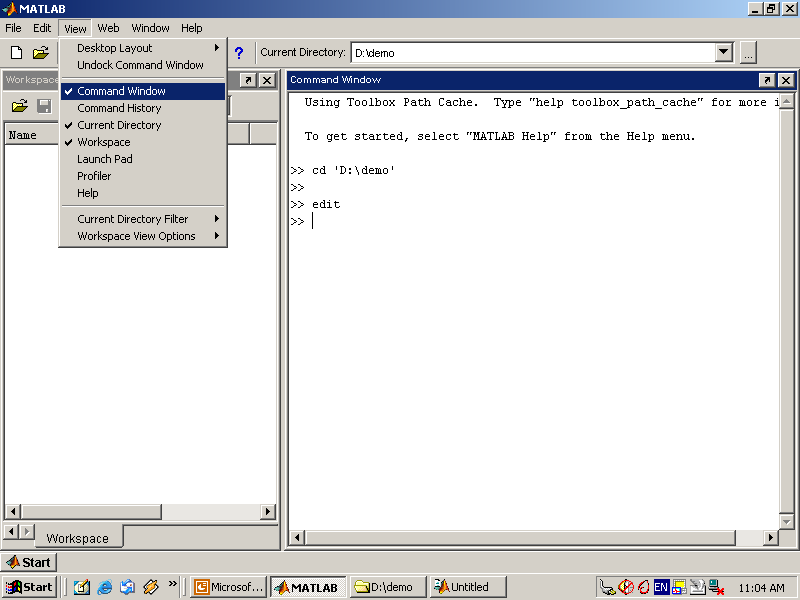
This is a library that allows you to write C and FORTRAN programs that interact with MATLAB. It include facilities for calling routines from MATLAB (dynamic linking), calling MATLAB as a computational engine, and for reading and writing MAT-files.

**7.5.1 DESKTOP TOOLS**

This section provides an introduction to MATLAB's desktop tools. You can also use MATLAB functions to perform most of the features found in the desktop tools. The tools are:

* Current Directory Browser
* Workspace Browser
* Array Editor
* Editor/Debugger
* Command Window
* Command History
* Launch Pad
* Help Browser

**Command Window**



Use the Command Window to enter variables and run functions and M-files.

* **Command History**

Lines you enter in the Command Window are logged in the Command History window. In the Command History, you can view previously used functions, and copy and execute selected lines. To save the input and output from a MATLAB session to a file, use the diary function.

* **Running External Programs**

You can run external programs from the MATLAB Command Window. The exclamation point character! is a shell escape and indicates that the rest of the input line is a command to the operating system. This is useful for invoking utilities or running other programs without quitting MATLAB. On Linux, for example,!emacs magik.m invokes an editor called emacs for a file named magik.m. When you quit the external program, the operating system returns control to MATLAB.

* **Launch Pad**

MATLAB's Launch Pad provides easy access to tools, demos, and documentation.

* **Help Browser**

Use the Help browser to search and view documentation for all your Math Works products. The Help browser is a Web browser integrated into the MATLAB desktop that displays HTML documents.

To open the Help browser, click the help button in the toolbar, or type helpbrowser in the Command Window. The Help browser consists of two panes, the Help Navigator, which you use to find information, and the display pane, where you view the information.

* **Help Navigator**

Use to Help Navigator to find information. It includes:

* **Product filter**

Set the filter to show documentation only for the products you specify.

* **Contents tab**

View the titles and tables of contents of documentation for your products.

* **Index tab**

Find specific index entries (selected keywords) in the MathWorks documentation for your products.

* **Search tab**

Look for a specific phrase in the documentation. To get help for a specific function, set the Search type to Function Name.

* **Favorites tab**

View a list of documents you previously designated as favorites.

* **Display Pane**

After finding documentation using the Help Navigator, view it in the display pane. While viewing the documentation, you can:

* **Browse to other pages**

Use the arrows at the tops and bottoms of the pages, or use the back and forward buttons in the toolbar.

* **Bookmark pages**

Click the Add to Favorites button in the toolbar.

* **Print pages**

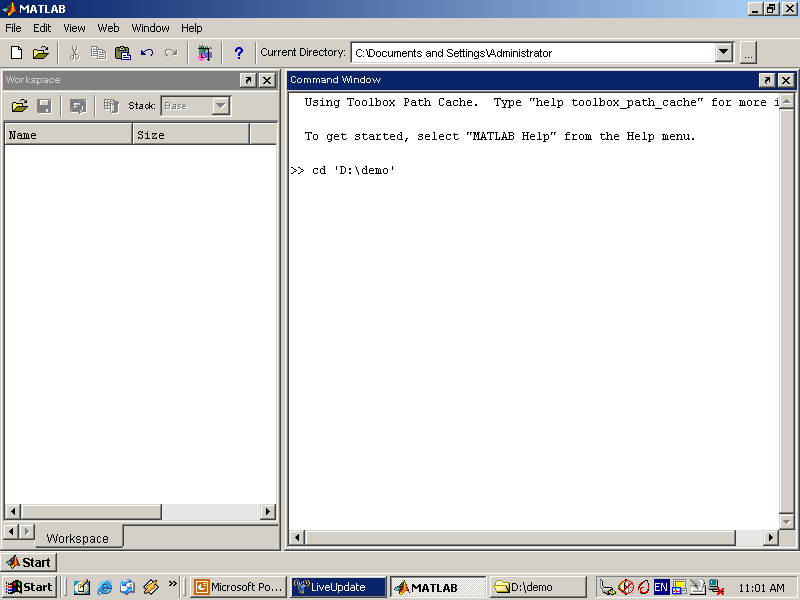
Click the print button in the toolbar.

* **Find a term in the page**

Type a term in the Find in page field in the toolbar and click Go.

Other features available in the display pane are: copying information, evaluating a selection, and viewing Web pages.

**Current Directory Browser**

****

MATLAB file operations use the current directory and the search path as reference points. Any file you want to run must either be in the current directory or on the search path.

**Search Path**

To determine how to execute functions you call, MATLAB uses a search path to find M-files and other MATLAB-related files, which are organized in directories on your file system. Any file you want to run in MATLAB must reside in the current directory or in a directory that is on the search path. By default, the files supplied with MATLAB and MathWorks toolboxes are included in the search path.

* **Workspace Browser**

The MATLAB workspace consists of the set of variables (named arrays) built up during a MATLAB session and stored in memory. You add variables to the workspace by using functions, running M-files, and loading saved workspaces.

To view the workspace and information about each variable, use the Workspace browser, or use the functions who and whos.

To delete variables from the workspace, select the variable and select Delete from the Edit menu. Alternatively, use the clear function.

The workspace is not maintained after you end the MATLAB session. To save the workspace to a file that can be read during a later MATLAB session, select Save Workspace As from the File menu, or use the save function. This saves the workspace to a binary file called a MAT-file, which has a .mat extension. There are options for saving to different formats. To read in a MAT-file, select Import Data from the File menu, or use the load function.

* **Array Editor**

Double-click on a variable in the Workspace browser to see it in the Array Editor. Use the Array Editor to view and edit a visual representation of one- or two-dimensional numeric arrays, strings, and cell arrays of strings that are in the workspace.

* **Editor/Debugger**

Use the Editor/Debugger to create and debug M-files, which are programs you write to run MATLAB functions. The Editor/Debugger provides a graphical user interface for basic textediting, as well as for M-file debugging.

You can use any text editor to create M-files, such as Emacs, and can use preferences (accessible from the desktop File menu) to specify that editor as the default. If you use another editor, you can still use the MATLAB Editor/Debugger for debugging, or you can use debugging functions, such as dbstop, which sets a breakpoint.

If you just need to view the contents of an M-file, you can display it in the Command Window by using the type function.

**7.5.2 ANALYZING AND ACCESSING DATA**

MATLAB supports the entire data analysis process, from acquiring data from external devices and databases, through preprocessing, visualization, and numerical analysis, to producing presentation-quality output.

* **Data Analysis**

MATLAB provides interactive tools and command-line functions for data analysis operations, including:

* Interpolating and decimating
* Extracting sections of data, scaling, and averaging
* Thresholding and smoothing
* Correlation, Fourier analysis, and filtering
* 1-D peak, valley, and zero finding
* Basic statistics and curve fitting
* Matrix analysis

**Data Access**

MATLAB is an efficient platform for accessing data from files, other applications, databases, and external devices. You can read data from popular file formats, such as Microsoft Excel; ASCII text or binary files; image, sound, and video files; and scientific files, such as HDF and HDF5. Low-level binary file I/O functions let you work with data files in any format. Additional functions let you read data from Web pages and XML.

**Visualizing Data**

All the graphics features that are required to visualize engineering and scientific data are available in MATLAB. These include 2-D and 3-D plotting functions, 3-D volume visualization functions, tools for interactively creating plots, and the ability to export results to all popular graphics formats. You can customize plots by adding multiple axes; changing line colors and markers; adding annotation, Latex equations, and legends; and drawing shapes.

**2-D Plotting**

Visualizing vectors of data with 2-D plotting functions that create:

* Line, area, bar, and pie charts.
* Direction and velocity plots.
* Histograms.
* Polygons and surfaces.
* Scatter/bubble plots.
* Animations.

**3-D Plotting and Volume Visualization**

MATLAB provides functions for visualizing 2-D matrices, 3-D scalar, and 3-D vector data. You can use these functions to visualize and understand large, often complex, multidimensional data. Specifying plot characteristics, such as camera viewing angle, perspective, lighting effect, light source locations, and transparency.

3-D plotting functions include:

* Surface, contour, and mesh.
* Image plots.
* Cone, slice, stream, and isosurface.

**7.5.3 PERFORMING NUMERIC COMPUTATION**

MATLAB contains mathematical, statistical, and engineering functions to support all common engineering and science operations. These functions, developed by experts in mathematics, are the foundation of the MATLAB language. The core math functions use the LAPACK and BLAS linear algebra subroutine libraries and the FFTW Discrete Fourier Transform library. Because these processor-dependent libraries are optimized to the different platforms that MATLAB supports, they execute faster than the equivalent C or C++ code.

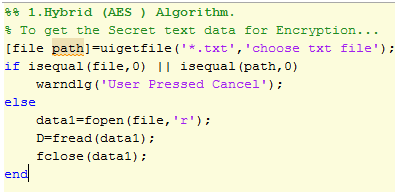
MATLAB provides the following types of functions for performing mathematical operations and analyzing data:

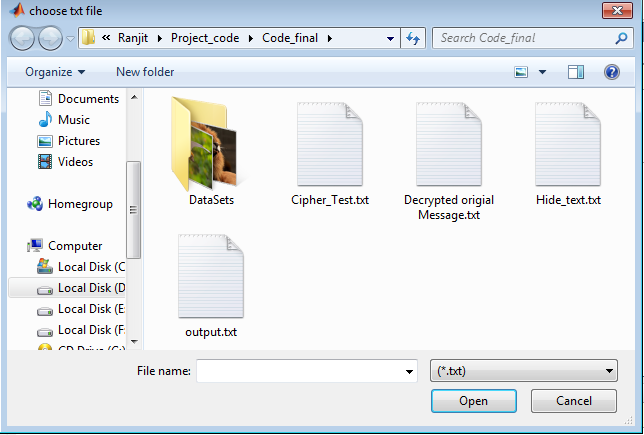
* Matrix manipulation and linear algebra.
* Polynomials and interpolation.
* Fourier analysis and filtering.
* Data analysis and statistics.
* Optimization and numerical integration.
* Ordinary differential equations (ODEs).
* Partial differential equations (PDEs).
* Sparse matrix operations.

MATLAB can perform arithmetic on a wide range of data types, including doubles, singles, and integers.

**Conversion from Plain Text to Cipher Text**

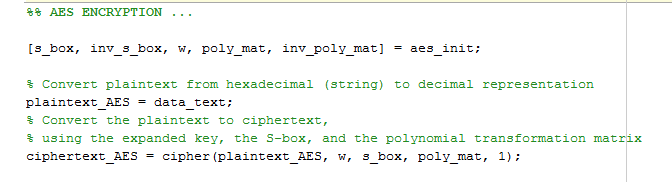
**Read text file to hide**





Chose text file for encryption

AES ENCRYPTION

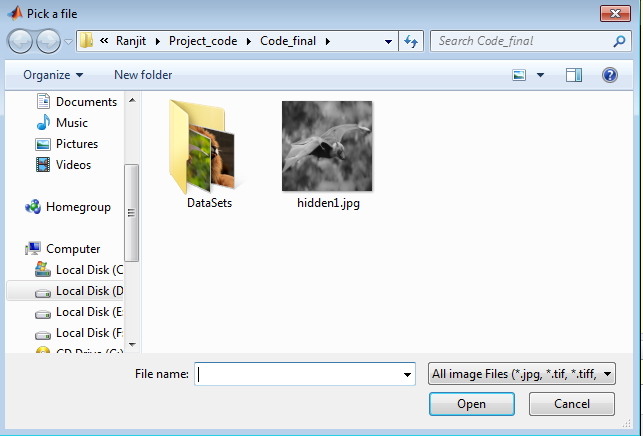


AES is a block cipher. It operates on plain text with a block of bits and returns cipher text with the same size. In this algorithm we have performed 10/12/14 rounds. It contains the byte substation, shift rows, mix columns and then add round key. The sub-stution of each byte uses one table with a 16x16 bytes and it contained a permutation of all specified values. Each byte of state is replaced by the byte indexed with row and column. In shift rows is used circular byte. Shift in each, the 1st row is unchanged and the 2nd row is 1 byte circular shift to the left and the 3rd row is 2 bytes circular shift to the left likewise it may process and decrypt inverts using circular shift to right. In the mix columns, each column is processed and separated and each byte is replaced by a value dependent on all bytes in the column. And add round key is a XOR state with 128-bits of key processed by column and inverse fordecryption.AES decryption is not identical to encryption since the steps done in reverse order but is defined as equivalent inverse cipher with steps as for encryption by using inverse of each step with a different key.

EMBEDDING ENCRYPTED TEXT IN THE COVER IMAGE 

**Selecting an Image file**

First, select any image file, behind which the user wants to hide data. The image which is selected should have fixed height and width. Now save the image file as in jpeg extension and the image appears as an original image file.

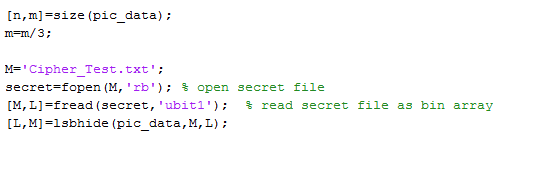


**Image Steganography**

In this, The sender will select the original image in jpeg extension format. Now the sender read the file using „imread􁪃 function. And convert the image file from rgb to gray using a function „rgb2gray􁪃. After this read the text and convert that text into a binary format. Then the key is read and the text is converts into encrypted format .When the wavelet transformation function.The image can divide into the sub bands as LL, LH, HL , HH. The binary cipher has to be put into LL Sub band. We can apply the inverse wavelet transformation function and convert the image into its original size. And the image is sent to the receiver.

**Creating Stego Image file**

For creating stegno Image file, combine stego text file and stego image file using digital watermarking. This forms the stego image text file at transmitter side in which hidden text is present.

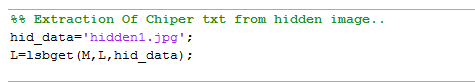


**For Receiver Side**

When the receiver reads the text file using „fread􁪃 it gets converted into an image. For this receiver apply the wavelet transformation function and divide the image into four sub bands as LL, LH, HL, HH. Now choose the required LL sub band from the image. Using extractionfun2 ( ) to extract the code from image and convert it into hexadecimal format and then store it into a variable „extra1􁪃.Now decrypt the encrypted code.

**Image Recovery**

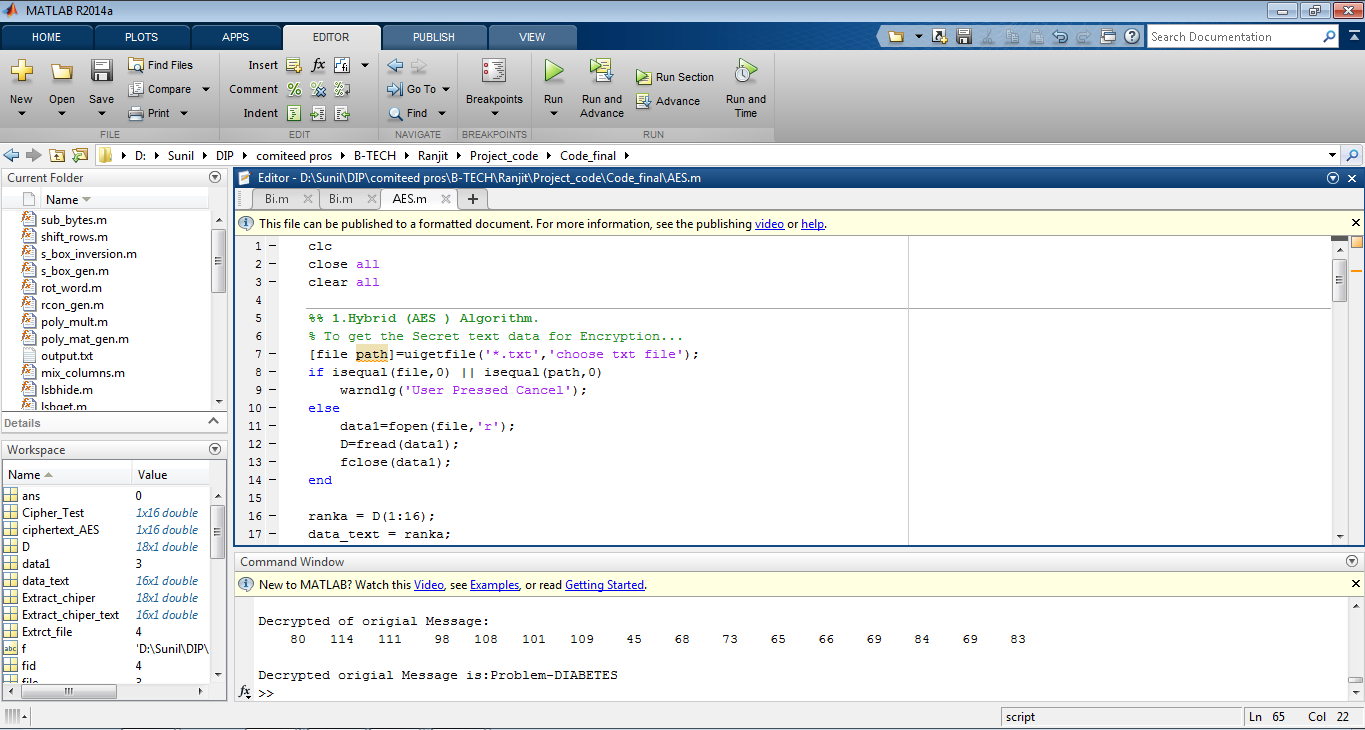
The image file is read by the function „imgread􁪃 and the text file is opened using fopen function and is stored into a variable „fid􁪃. Using the function fread it is stored into a variable „a􁪃. Now convert the text file into the image file using matrix representation. Here to perform some addition and subtractions on the matrix it is placed into the proper sub band i.e., LL, LH, HL, HH. The image can be recovered by the text.



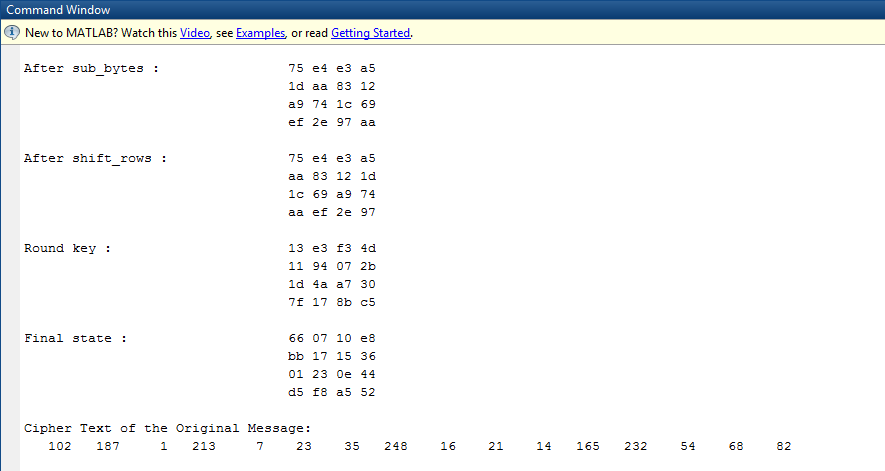
# DECRYPT THE HIDE TEXT

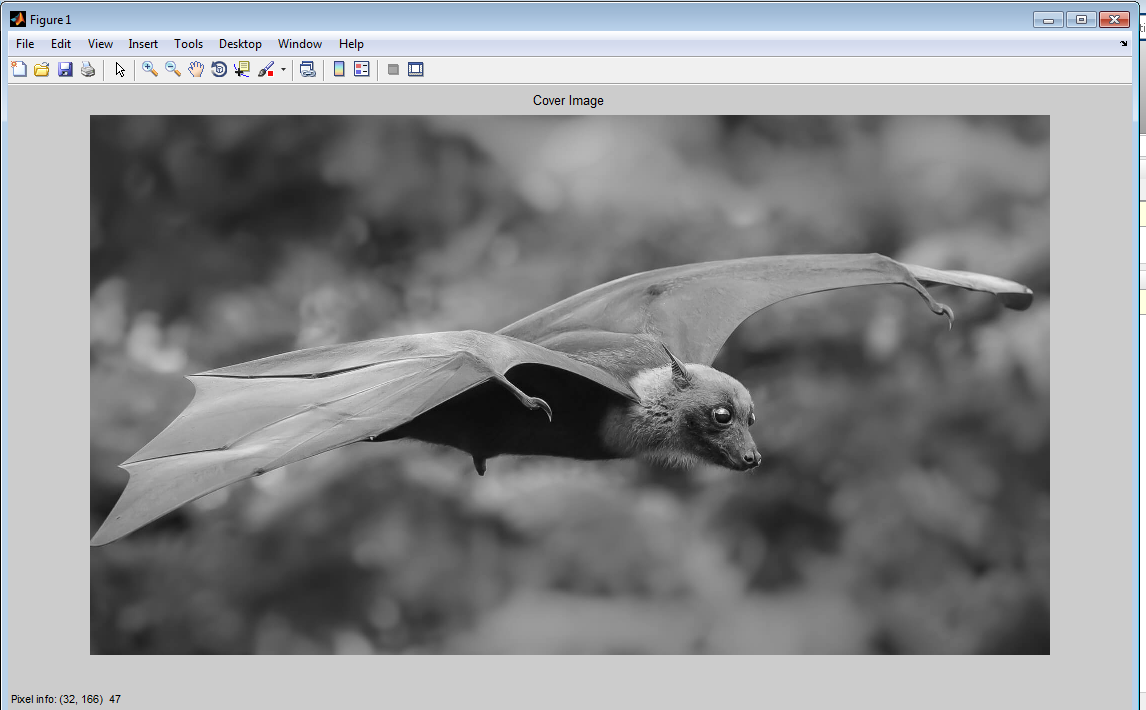
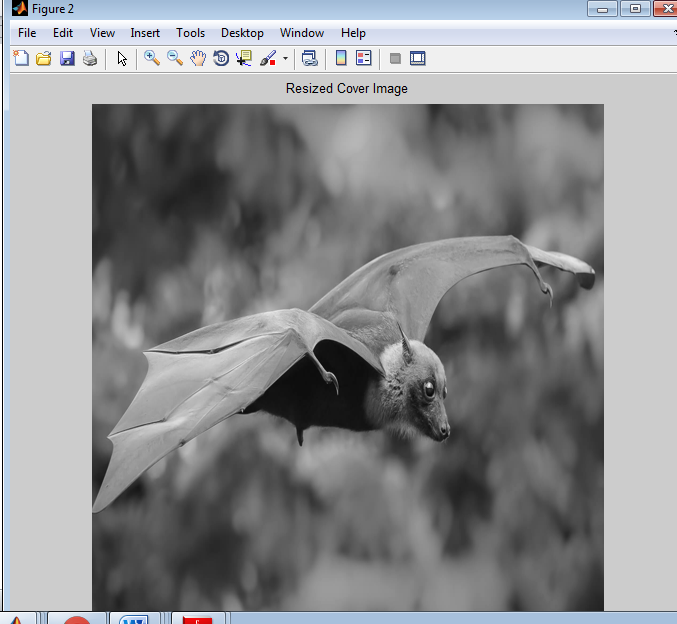
# Chapter 8

## RESULTS

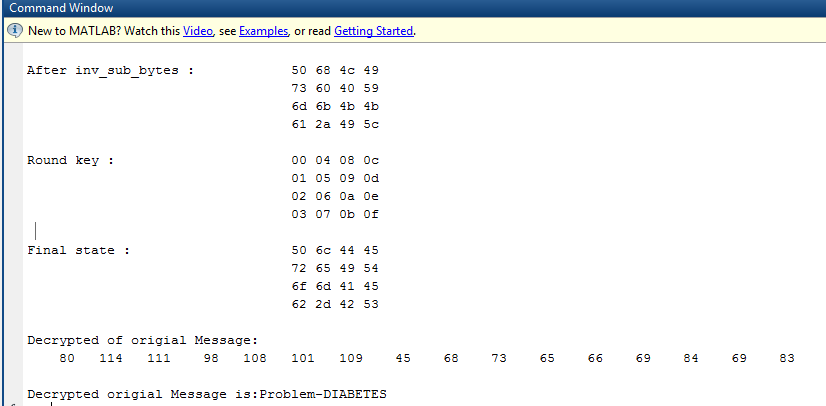


**FIG: MATLAB CODE**



**FIG: SAMPLE IMAGES OF DATASETS.**



**FIG: INPUT COLOUR IMAGE**

# Chapter 9

**CONCLUSION AND FUTURE SCOPE**

The cryptographic algorithm alone is not a very secure way to be used for the data transmission. So a new method which combines cryptography and steganography is provided to give much better option for data transmission. Inn this project a method to combine steganography (Least Significant Method) and cryptography (AES) is considered, so as to provide a more secure way for data transmission through any unsecured or public networks. To further increase the security of the data,the encrypted text is not embedded in the image itself. Instead,it is embedded in the

LL-subband of the wavelet transformed image.

REFERENCES

[1]. Zeng XT, Li Z, Ping LD Reversible data hiding scheme using reference pixel and multi-layer embedding. Int J Electron Commun (2012) 66:532–539.

[2]. Chan CK, Cheng LM Hiding data in images by simple LSB substitution. Pattern Recogn (2004)37:469–474.

[3]. Johnson NF & Jajodia S Exploring steganography: seeing the unseen. Comput Pract (1998)26–34.

[4]. Swanson M, Kobayashi M, Tewfik A Multimedia data embedding and watermarking technologies. (1998)Proc IEEE 86(6):1064–1087.

[5]. S. Kartalopoulos, “Security of Information and Communication Networks”, Wiley-IEEE Press, (2009).

[6]. N. F. Johnson and S. Katzenbeisser, Information Hiding, ch. A survey of steganographic techniques. Artech House, Norwood, MA, (2000).

[7]. Y. Lee, L. Chen, “High capacity image steganographic model”, IEEE Proceedings on Vision, Image and Signal Processing (2000)147, 288 -294.

[8]. Mielikainen J LSB matching revisited. IEEE Signal Processing Letters(2006) 13:285–287.

[9]. Chang CC, Lin MH, Hu YC A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recog(2002) 16(4):399–416

[10]. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn (2001)34(3):671–683

[11]. Thien CC, Lin JC A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn(2003) 36:2876–2881

[12]. Jung KH & Yoo KY Data hiding using edge detector for scalable images. Multimedia Tools and Appl doi:(2013)10.1007/s11042-012-1293- 84.

[13]. Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W Distortionless data hiding based on integer wavelet transform. IEE Electronics Letters (2002)38:1646–1648.

[14]. M. IndraSena Reddy, “A Practical Approach for Secured Data Transmission using Wavelet based Steganography and Cryptography”, International Journal of Computer Applications (2013)(0975 – 8887)Volume 67– No.10.

[15]. VVS Kumar M. IndraSenaReddy , “Image Compression Techniques by using wavelet transform”, Journal of information engineering and applications,(2012) Vol.2, No.5,35-39.

[16]. M. IndraSena Reddy, K Subba Reddy and V Uday Kumar, “Secured Data Transmission using