A Project Report

On

Secret Image Shares In Visual Cryptography

Submitted in partial fulfillment of the

requirements for the degree of

BACHELOR OF TECHNOLOGY

In

Information and Communication Technology

Submitted by

K. Preethi Shree 113014097

R.Sofiya 113014122

Under the guidance of

Mr.R.Raja

Assistant Professor

SCHOOL OF COMPUTING

SHANMUGHA ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY (SASTRA UNIVERSITY)

(A university established under section 3 of the UGC act, 1956)

TIRUMALAISAMUDRAM

THANJAVUR-613401

APRIL 2013

SHANMUGHA ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY

SASTRA UNIVERSITY

THANJAVUR-613401

SCHOOL OF COMPUTING

BONAFIDE CERTIFICATE

THIS IS TO CERTIFY THAT THE PROJECT ENTITLED

SECRET IMAGE SHARES IN VISUAL CRYPTOGRAPHY

is a work done by

Preethi Shree.K-113014097

Sofiya.R-113014122

BACHELOR OF TECHNOLOGY

IN

INFORMATION AND COMMUNICATION TECHNOLOGY OF

SASTRA UNIVERSITY, Thanjavur during the year 2012-2013

Internal guide **AssociateDean/ICT**

Submitted for the university examination held on:

Internal Examiner **External Examiner**

SHANMUGHA ARTS, SCIENCE, TECHNOLOGY & RESEARCH ACADEMY

(SASTRA UNIVERSITY)

(A university established under section 3 of the UGC act,1956)

TIRUMALAISAMUDRAM

THANJAVUR-613401

Tamil Nadu, India

DECLARATION

We submit this project entitled "SECRET IMAGE SHARES IN VISUAL CYPTOGRAPHY", Thanjavur-613 401, in partial fulfilment for the award of B.Tech, Degree in Information and communication Technology and declare that this is our original work under the guidance of Prof.R.RAJA, AP II, SOC.

Date: Place:

Signature: Name: PREETHI SHREE.K

Signature: Name: SOFIYA.R

ACKNOWLEDGEMENT

Acknowledgements have always made us realize whom we have to thank when we complete our project. As we sit to write this, we realize how many people we would like to mention without whom, this project this would not have been possible.

We are very thankful to **Prof. R.Sethuraman, the Vice Chancellor of SASTRA UNIVERSITY** for providing a wonderful platform for us to work and complete this project.

We would also wish to express our thanks to **Dr.G.Bhalachandran, Registrar,** for his perpetual motivation a academic pursuits.

We would like to express our gratitude to **Dr.P.Swaminathan, The Dean-School of Computing**, for providing us with the excellent environment and the resources which helped us to finish this project.

We would also like to offer our thanks to **Dr.K.S.Ravichandran, Associate Dean, ICT** for his support and encouragement for completion of the project.

I am highly indebted to **Prof.Mr.R.RAJA, AP-II/ICT/SOC, SASTRA UNIVERSITY** for his constant supervision as well as for providing necessary information regarding the project.

Our special thanks to **Prof.G.Manikandan, AP-III/ICT/SOC,** for helping us in the initial stages of our project.

I also thank all the **Teaching and Non-teaching staff,** and those who have directly or indirectly helped me by extending their moral support and encouragement for completion of this project.

Our special thanks to Almighty and our parents for their blessings.

SYNOPSIS

Steganography is nothing but hiding information inside an image such that only sender and receiver knows about it. For high security message inside an image is encrypted in the sender side and it is decrypted in the receiver side using a symmetric key. For double protection to information within an image, we go for a combination of steganography and visual cryptography. Visual Cryptography is a special technique for encrypting image and which can be decrypted using correct key by human vision.

In the existing system, k out of n shares visual cryptography is used. That is the image is divided into n shares and at least k shares out of n shares are used to reveal the secret. Generally only image or text are used in visual cryptography and the security is less as can get the secret by combining k shares by trial and error. Moreover the contrast of the image is not maintained after the retrieval.

In the proposed system, initially a biometric image (fingerprint) is taken instead of an normal image. Using minutiae extraction, minutiae points of the fingerprint are located and the message is hidden inside these points namely the ridges using least significant bit algorithm. This stego image is then divided into n shares and the value of k which is used to retrieve the image is sent as key. Thus the stego image is retrieved without any loss in its contrast as the histogram error value is 0 and the secret message inside the stego image is decrypted correctly with security.

TABLE OF CONTENTS

S.NO	TITLE	PAGE NO
1	Introduction 1.1.Introduction to the company 1.2.Background of the project 1.3.Project description	1 1 2 4
2	Software project plan	16
3	Software requirement specification 3.1.Functional requirements 3.2.Non-functional requirements	17 17 18
4	System analysis 4.1.Use case diagram 4.2.Class diagram	19 19 20
5	Design 5.1.Front end	21 21

6	Code 6.1.Sample code 6.2.Snapshot	25 25 31
7	System Testing 7.1.Unit testing 7.2.Integration testing 7.3.Validation testing 7.4.System testing	37 37 38 38 38
8	Implementation 8.1.Problems faced 8.2.Lessons learnt	39 39 39
9	Future plans	40
10	Conclusion	41
11	References	42
12	Bibliography	43

1. INTRODUCTION

1.1 . Introduction to the company

SHANMUGA ARTS, SCIENCE, TECHNOLOGY & RESARCH ACADEMY [SASTRA] has carved a niche for itself as a centre for fostering and developing the body, mind and spirit of its students. SASTRA is totally committed to this three-fold flowering of the students entrusted to its care. Our blend of academic excellence and real world experience with moral values has earned SASTRA, national recognition. A sprawling campus housing a built up area of over 1.5 million square feet, a vibrant population of over 8000 students and over 600 teaching faculty have made SASTRA a landmark in the educational map of India. SASTRA offers various under graduate, post graduate courses in engineering, science, management and arts besides various doctoral programmes, and has state-of-the-art laboratories, a well-stocked library and one of the best computing facilities. With an ideal teacher-taught ratio, we strive for academic excellence through personalised attention. The mechanism established to support and monitors the students' progress assures success and satisfaction. Since its inception, SASTRA has achieved national standing in terms of academic performance, co-curricular and extra-curricular activities and in its commitment to social service. The standard of excellence of the courses is reflected in the grades awarded by the NAAC. SASTRA shapes its students' future by fostering a team work approach to instruction, encouraging interaction with faculty, providing access to hi-tech information, motivating them to develop new ideas and concepts, taking personal interest in students' career development and preparing them for success.

1.2. Background of the project

As long as people have been able to communicate with one another, there has been a desire to do so secretly. Two general approaches to covert exchanges of information have been: communicate in a way understandable by the intended parties, but unintelligible to eavesdroppers; or communicate innocuously, so no extra party bothers to eavesdrop. Naturally both of these methods can be used concurrently to enhance privacy. Naturally both of these methods can be used concurrently to enhance privacy. The formal studies of these methods, cryptography and steganography, have evolved and become increasingly more sophisticated over the centuries to the modern digital age. Methods for hiding data into cover or host media, such as audio, images, and video, were developed about a decade Steganography generally is subjected to less vicious attacks, however much data as possible has is to be inserted. Typical uses for steganography are for espionage, industrial or military.

Visual cryptography secret sharing scheme offers a method for the management of secret key in the fields of economy, military affairs and so on. Suppose in a bank, for the reason of security, a strong room can only be opened when three managers get together. Or the problem of the missiles launch, it need at least two generals who turn their keys together to launch missiles. Thus secret sharing scheme is very useful in practices.

1.2.1. Existing system

Visual cryptography is a technique which allows visual information (Image, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers.

In k out of n visual cryptography scheme, image is divided into n number of shares that is a secret image is encrypted into n shares of cipher text, each printed on a transparency sheet, which are distributed among n participants. In the decryption process only k or more than k number of shares can reveal the original information. Less than k number of shares can not reveal the original information.

Here in visual cryptography it just protect the content of the message and it does not bother about the communicating parties that is whether the intended user is receiving the secret or not. Moreover the contrast of the image is lost on retrieval.

1.2.2. Proposed System

As visual cryptography just protect the content of the message , we go for a combination of steganography and visual cryptography where steganography is the process of hiding secret inside an image.

In this project instead of a normal image we use a biometric image namely fingerprint. Later for more security we go for identifying the unique feature of a fingerprint - minutiae points. We extract the minutiae points of the fingerprint using minutiae point extraction algorithm and the secret is hidden inside these minutiae points that is in ridges with a key using least significant bit algorithm.

Later this stego image is divided into n shares and the value of k which is used to recover the image depends on the number of users, that is each k users have their own shares.

In decryption, the stego image is reconstructed back by combining each shares of those k users. Here the reconstructed image is as such as original image. The contrast of the original image is not lost in reconstructed image as the value of histogram error is zero. The secret hidden inside the image is decrypted using the key.

1.3. Project description

The growing possibilities of Modern communication need the special mean of security on computer network. In the computer world, it is very important to keep secret information secret, private information private and protect the copyrights of data. To accomplish this task, new methods based on the principle of Image processing are being developed and used.

1.3.1. Minutiae Extraction

The minutiae considered in automatic identification systems are normally ridge bifurcations and terminations. In this project, fingerprint minutiae from skeletonized binary images are extracted. Besides classical methodologies for minutiae filtering, a new method is used for bridge cleaning based on ridge positions and curves instead of classical methods based on directional maps. The criteria and related algorithms are introduced for validating the endpoints and bifurcations.

The uniqueness of fingerprints is determined by the characteristics and the relationships of local ridges, which are also called minutiae. Minutiae are local discontinuities in terms of ridge endings and bifurcations of ridge flow patterns that constitute a fingerprint. The ridge ending is defined as the ridge point at which a ridge terminates, while the ridge bifurcation is defined as a point at which a single ridge splits into two. These two types of minutiae have been considered by the Federal Bureau of Investigation for the purpose of identification. The main task of the fingerprint minutiae extraction algorithm is to identify the quantity, type, position and direction of the minutiae. In a traditional automatic fingerprint identification system, fingerprint minutiae are mainly extracted based on thinning images or gray-level

images. However, the thinning images and gray-level images are a set of pixels. While looking at the image of a fingerprint, it is often regarded as a collection of curves instead of a set of pixels. Furthermore, traditional methods based on thinning images or gray-level images are sensitive to noise pixels. Therefore, we try to figure out a method to depict fingerprint images with a collection of curves rather than a set of pixels. Principal curves is to describe the structural information of fingerprint, since they can reflect the genuine structure of a data set.

Here minutiae point of the finger print is extracted inorder to hide secret text inside those unique features namely ridges of fingerprint. The secret is hidden inside by using the concept of least significant bit – steganography.

1.3.2. Steganography

Steganography is an art and science of hiding information within other information. The word itself comes from Greek and means hidden writing. In recent years cryptography become very popular science. As steganography has very close to cryptography and its applications, we can with advantage highlight the main differences. Cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the cipher text invisible to unauthorized users. Thus steganography when compared with cryptography has additional property that its output looks unobtrusively.

1.3.2.1. Image Steganography

Image steganography, covert embedding of data into digital pictures, represents a threat to the safeguarding of sensitive information and the gathering of intelligence.

An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper embedding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image.

The purpose of steganography is to convey a message inside of a conduit of misinterpretation such that the existence of the message is both hidden and difficult to recover when discovered. Basically the information hiding process in a Steganoraphic system starts by identifying a cover medium's redundant bits. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. The basic purpose is to make communication unintelligible to those who do not possess the right keys.

1.3.2.2. Image Encrypting and Decrypting

In this project, first step is steganography, that is to embed and hiding information is to pass both the secret message and the fingerprint in to the encoder, inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message.

A key is needed in the embedding process. By using the key, the chance of third party attackers getting hold of the stego image and decoding it to find out the secret information is reduced. A stego image is the original cover image with the secret information embedded inside. This image looks almost identical to the original fingerprint image as otherwise a third party attacker can see embedded information. Having produced the stego image, it is sent for visual cryptography shares. At the receiving end the stego image is fed into the system the public or private key that can decode the original key that is used inside the encoding process is also needed to detect the secret information.

1.3.2.3. LSB Based Steganography

Generally digital images are used in steganography which often have a large amount of redundant data and for this reason it is possible to hide message inside image file. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. These pixels make up the image's raster data. Image steganography is about exploiting the limited power of the human visual system (HVS). If any specific colour is viewed closely it has been observed that single digit modifications to the contribution level are imperceptible to the human eye (i.e. a pixel with a value of (255, 255, 0) is indistinguishable from (254, 255, 0)) in RGB colour representation.

The digital data related to images seem to be too large to be transmitted through the Internet. So techniques are used to reduce the data to a suitable size in order to display it in a reasonable amount of time across the Internet. This technique called compression is used to reduce the image data, resulting in smaller file sizes and plays a vital role in image based steganography methods. Image formats can mainly be divided into two categories based on compression, lossy and lossless. Both methods save storage space but have different results. Lossy compression (e.g. JPEG format) attains a high level of compression and thus saves more space but in doing so, the bits may be altered largely and the originality of the image may be affected. The JPEG compression algorithm uses floating point calculations for converting image and it results in rounding errors which may eliminate portions of the image which are not visible to the naked eye. Although this rarely causes a noticeable change to the image it can significantly alter or destroy any information that was hidden in the image.

Lossless compression maintains the original image data exactly and the lossless compression images are preferred for steganography as image media. Spatial domain

steganographic techniques, also known as substitution techniques, consists of simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be imperceptible to the human visual system (HVS).One of the methods to do so is to hide information in the least significant bit (LSB) of the image data. This embedding method is based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any change on the image. Least significant bit (LSB) is the most commonly used type of insertion scheme used currently in digital steganography. This method is probably the easiest way of hiding information in an image. The secret message is hidden by altering least significant bit in a certain layer of the image file.

In an image if MSBs is changed, it will have a noticeable impact on the color, however, changing the LSBs will not be noticeable to the human eye. The image formats typically used in the LSB substitution are lossless and the data can be directly manipulated and recovered. Lossless data compression makes use of data compression algorithms that allows the exact original data to be reconstructed from the compressed data. One of the most important features of lossless compression is to maximize the embedding capacity. The use of digital images for steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in pattern changes and luminance. Employing the LSB technique for data hiding achieves both invisibility and reasonably high storage payload.

The advantages of LSB based data hiding method is that it is simple to embed the bits of the message directly into the LSB plane of image and many techniques use these methods. The LSB modification does not result in image distortion and thus the resulting stego-image will look identical to the cover-image. Several variations of the basic LSB based steganographic techniques were described by Johnson, and Katzenbeisser. They also describe

a substitution technique for embedding message into the LSB bits of the palette of GIF or BMP image format.

Bailey and Curran provide an evaluation of various techniques concerning spatial steganographic that principally applies to GIF images. They discussed different strengths in terms of resistance to different types of steganalysis or their ability to maximize the size of the message that could be stored.

The LSB based data embedding differ in the way of information hiding process. Some of them embed the data inside an image file sequentially other randomly. In sequential LSB, the message is laid out across the image data sequentially. In the random embedding, the message bits are randomly scattered throughout the whole image using a random sequence to control the embedding sequence. Some modify pixels not in the whole image but in selected areas of it, and still others increase or decrease the pixel value of the LSB, rather than change the value.

In a image Steganography providing a strong focus on the LSB techniques in image Steganography. In this project by applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity.

Gutte and Chincholkar proposed a text Steganography method along with cryptography for secret communication. They used the LSB based method of steganography and also compared the data hiding at one LSB and two LSB positions and evaluated the performance parameters like Standard Deviation, MSE and Entropy etc. The data is encrypted using Extended Square Substitution Algorithm.

1.3.2.4. Encryption using LSB Technique

In LSB insertion method, a key is generated to distribute and hide the bits of a secret message into the least significant bit of the pixels within a fingerprint image. The transmitting and receiving end share the stego key, the output is a random sequence K1……..Kn where n is the length of message bits. The sequence is then used by the sender to generate the sequence of pixel indices yi where, y1 = K1 yi = yi-1 + Ki, i >2. Message bit, i would then be embedded into the LSB of the pixel, yi thus the order in which the secret message bits are embedded would be determined pseudo randomly. Since the receiver knows the seed k, he can reconstruct ki and therefore the entire sequence of pixel indices yi. In the random insertion method the random location of the pixels depends on a stego key, whose size k should be in the range n < k < I. Where n is the size of message and I is the size of cover image. The method commences by searching for the first prime number p that exceeds the key k, A primitive root a, is then obtained, which is a number whose powers generate all the distinct integers from 1 to (p-1) in some permuted order. Each power of this primitive root to generate these integers is called the discrete algorithm. This primitive root a, is then used to generate a set of random and distinct numbers, yi = ai mod p, where i is the bit index of the secret message. Bit i of the secret message then goes into LSB of pixel yi. In this way it is ensured that the bits of the secret message are inserted into distinct LSBs.

1.3.2.5. Decryption using LSB Technique

In a natural uncompressed image 24-bit BMP each pixel is represented by three colors (Red, Green & Blue), each of the color is 8-bit wide. The LSB of any color pixel of the typical scanned real image taken by any source contains least information about the image and is most random in nature. That is why the most appropriate and acceptable technique for hiding information in an uncompressed natural image is based on the replacing the LSB of

the color pixels by message bit. So that on an average only half of the LSBs are changed and it is assumed that, embedding message in this way is not going to destroy the statistics of the original image. This assumption is true if and only if the number of unique colors in the cover image is comparable to the total number of pixels in that image. In an uncompressed image the ratio of the number of unique colors to the total number of pixels is approximately 1:6 so that after LSB embedding which is equivalent of introducing noise, the randomness of the LSB pattern will increase. This increase in randomness is reflected in increased in number of closed color pairs which is utilized as the detection tool. The close color pair (X) and unique color (Y) is defined as follows. Two colors having individual components Red, Green & Blue are closed if the correlation factor of all individual components of both colors are 1 and both colors are unique if any one of the individual components of both colors are 1. For any uncompressed real image the ratio r gives us an idea about the relative number of close color pair with that of unique colors where, r = X/Y .It has been seen for an original image which does not have any encoded message the value of r is greater incomparision with an image which has a message already encoded in it. This happens has embedded message behaves as a random noise which increases the number of unique colors Y abruptly.

1.3.3. Visual Cryptography

Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System. This is the benefit of the visual secret sharing scheme. The encryption

technique requires a cryptographic computation to divide the image into a number of parts or we can call it shares. We divide the image into n number of shares.

Cryptography is study of mathematical technique to provide the methods for information security. It provides such services like authentication, data security, and confidentiality. Visual cryptography is one of the technique used in modern world to maintain the secret massage transmission. In this technique no need of any cryptographic algorithms likes symmetric (DES, AES, TRIPLE DES etc) and asymmetric (RSA, Diffie-Hellman, Elliptic Curve Cryptographic) algorithms. Noar and Shamir introduce visual cryptography in 1994.

This technique is used to reduce complexity of encrypted and decrypted method and also two way communication can be achieved very securely. Traditional techniques use private and public key concepts. But it could be achieved only by the distribution of keys. It uses the Diffie-Hellman approach and other mathematical computations are used for encryption and decryption. Visual cryptography is based on the images and is obtained by sending pixel information. Visual cryptography schemes depend on sub-pixels and its complexity, computation, reliability, etc. The image consists of black and white, gray scale color images. Visual cryptography uses participates to send secret information. It consists of multiple party or multi-party methods. It follows many different techniques like sub pixel, error diffusion, Boolean operation are used to specify particular method. Different technique methods are halftone visual cryptography, watermarking visual cryptography, extended visual cryptography.

1.3.3.1. Visual Cryptography (k out of n) Scheme

Visual cryptography and (k, n)-visual secret sharing schemes were introduced by Naor and Shamir. A sender wishing to transmit a secret message distributes n transparencies

among n recipients, where the transparencies contain seemingly random pictures. A (k, n)-scheme achieves the following situation: If any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only k - 1 recipients stack their transparencies, or analyze them by any other means; they are not able to obtain any information about the secret message.

A VCS splits an image into a collection of secret shares which are then printed on transparencies. These shares when separated will reveal no information about the original image (other than the size of it). The image can only be recovered by superimposing a threshold number of shares. This recovery process does not involve any computation. It makes use of the human vision system to perform the pixel-wise OR logical operation on the superimposed pixels of the shares. When the pixels are small enough and packed in high density, the human vision system will average out the colors of surrounding pixels and produce a smoothed mental image in a human's mind.

Early VCS' are mainly focused on black-and-white secret images. If the original image is not black and white, for example, a gray-scale image, dithering is employed to pre process the original image that could degrade the image quality.

.

1.3.3.2. k out of n Secret Image Sharing Scheme

In this system a file of size will divided into pieces, each of size , then these pieces are encoded into coded pieces and stored at nodes. In cryptography, secret sharing offers a similar scheme, which means a technique for sharing a secret to a group of members, each of which holds a portion of the secret. The secret can only be retrieved when a certain number of

members combine their shares together, while any combination with fewer than shares has no extra information about the secret than 0 shares. By using the method based on Shamir threshold scheme, a file can be split into small sub-files. With any combination of these t sub files, the original file can be recovered without errors.

It is a very important embranchment of the modern cryptography. Secret sharing is a technique for sharing a secret to a group of participants, each of which holds a portion of the secret. The secret can only be retrieved when a certain number *t* of members combine their shares together, while any combination with fewer than *t* shares has no extra information about the secret than 0 shares.

Since Shamir and Blakley firstly proposed their own secret sharing schemes in 1979 respectively, the issues of secret sharing are studied widely in the last several decades. The secret sharing scheme offers a method for the management of secret key in the fields of economy, military affairs and so on. Suppose in a bank, for the reason of security, a strong room can only be opened when three managers get together. Or the problem of the missiles launch, it need at least two generals who turn their keys together to launch missiles. Thus secret sharing scheme is very useful in practices.

1.3.3.3. Threshold Scheme

Let *t*, *n* be positive integers with *t* <= *n*. A (t, n) threshold scheme is a method of sharing a message *M* among a group of *n* members. The message can only be retrieved when a certain number *t* of members combine their shares together, while any combination with fewer than *t* shares has no extra information about the secret than 0 shares.

1.3.3.4. Shamir Threshold Scheme

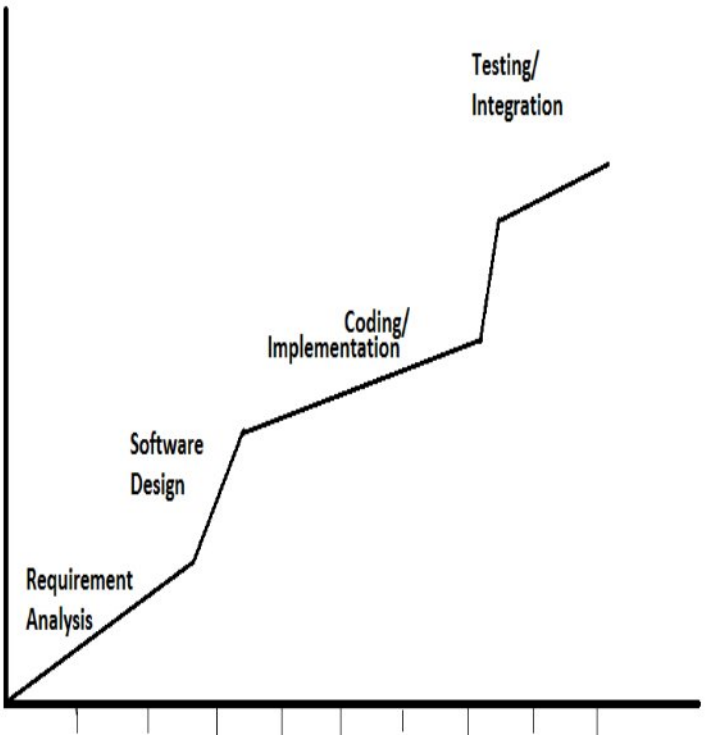
In this, we have a prime p, which is larger than all the possible message and also larger than the number of participants. All the calculations are carried out mod p. Here, we can also use a composite number n, however, it will not guarantee the matrices we obtain

might have inverses. Suppose we want to share a secret message, which is represented as a number mod p . There are n persons and when any t persons get together, they can retrieve the secret by their sharing parts.

1.3.3.4. Distribution Storage based on Secret Sharing Schemes

This project represent how to use the Shamir threshold scheme to accomplish Distributed Storage. A gray image is used to illustrate this algorithm, since values of byte and pixel are both between 0 and 255. By this scheme, the original image will be split into n different parts and any combination of t different parts can recover the image without errors. This scheme (t,n) is called threshold schemes in this project. For any other file, we can simply transform each byte from binary number into decimal number, and then we can use the blow scheme to finish distributed storage.

2. SOFTWARE PROJECT PLAN



3. SOFTWARE REQUIREMENT SPECIFICATION

3.1. Functional requirements

3.1.1. Use case-Textual Description

Sender:

Read Fingerprint.

Extract minutiae points.

Hiding text in minutiae points.

Dividing stego image into n shares.

Receiver:

Retrieving the image from k shares.

Retrieving the hidden text from retrieved image.

3.2. Non functional requirements

3.2.1. Resource requirements

3.2.1.1. Hardware requirements:

System : Intel core I3

Hard disk : 320GB

RAM : 2GB

3.2.1.2. Software requirements:

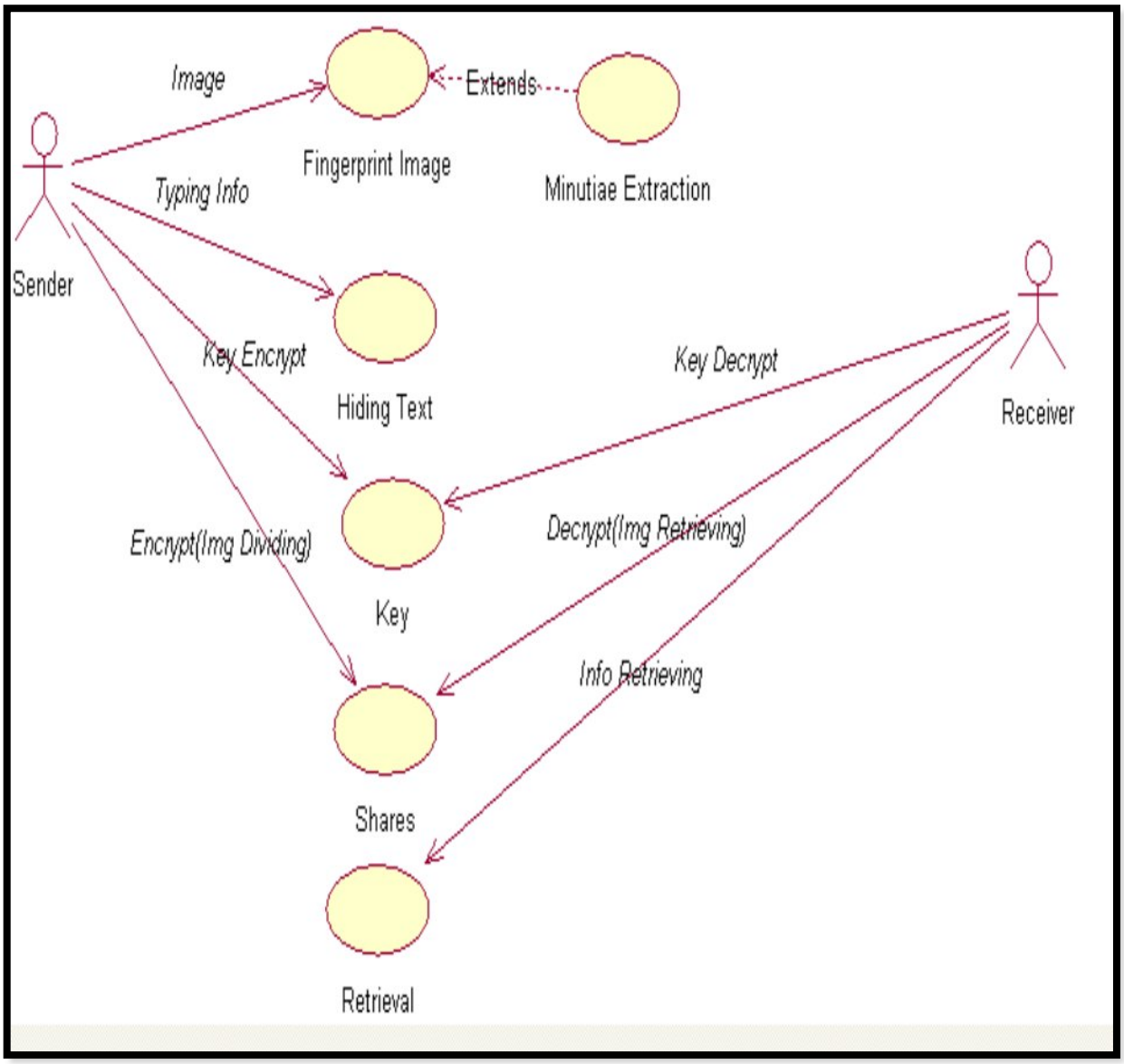
Operating systems : Windows 7

Front End : MATLAB

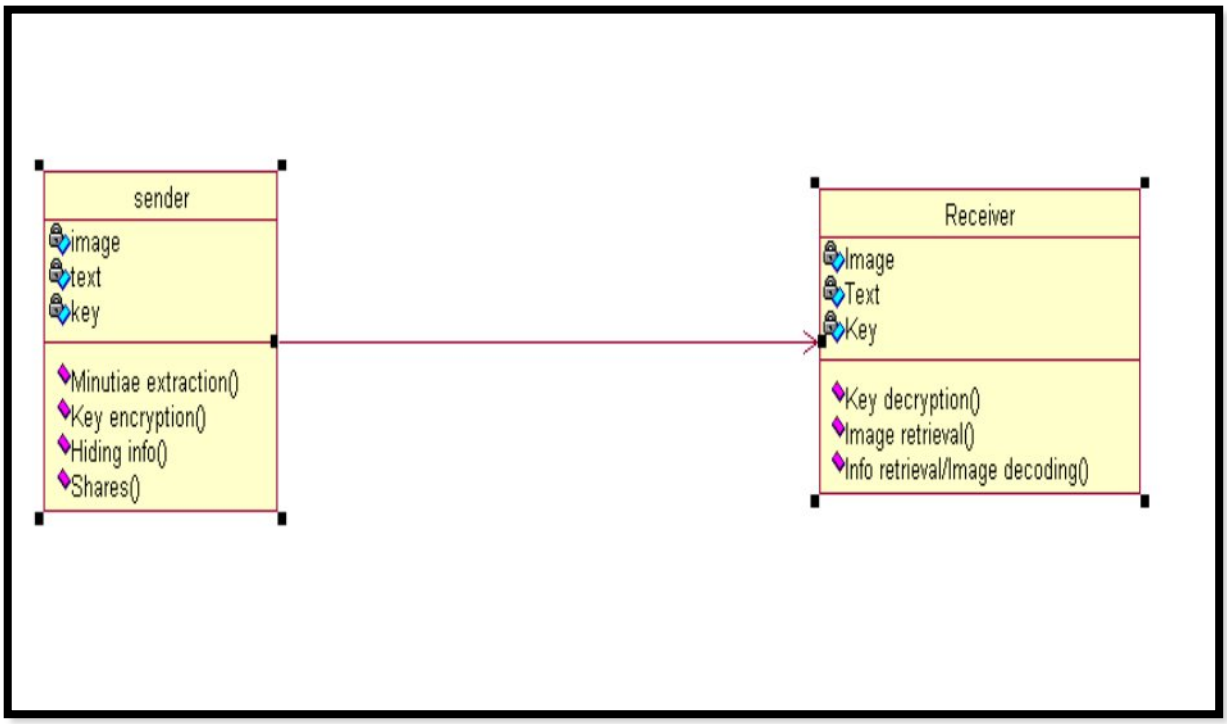
Version : 7.7

4. SYSTEM ANALYSIS

4.1. Use case Diagram



4.2. Class diagram



5. DESIGN

5.1. Front end design

5.1.1. MATLAB Language

MATLAB (matrix laboratory) is a numerical computing environment and fourth generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and Fortran. Using MATLAB, you can analyze data, develop algorithms, and create models and applications. The language, tools, and built-in math functions enable you to explore multiple approaches and reach a solution faster than other traditional programming language.

MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming. Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolicengine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems. You can use MATLAB for a range of applications, including signal processing and communications, image and video processing, control systems, test and measurement and computational finance.

The main advantage: it is an interpreted language for numerical computation. It allows one to perform numerical calculations, and visualize the results without the need for complicated and time consuming programming. Matlab allows its users to accurately solve problems, produce graphics easily and produce code efficiently.

5.1.2.Matlab Basics - Variables

A variable in Matlab is like a variable in algebra - it's a name given to some number. In Matlab, you can name any single number or multiple numbers at once, in which case the variable is a vector or an array of numbers. A single number is called a scalar variable in Matlab, but a single variable name can represent a huge array of numbers of arbitrary size and dimension. Creating a variable or manipulating it is done with = statements, where the left side of the = is your variable name, and the right side is the value you want it to take. If the name doesn't already exist, an = statement will create it. If it is already taken for a variable, an = statement can be used to re-assign that variable name values. You can change a whole variable at once or simply a few of the numbers (or characters, or whatever) within it.

There are several types of variables you can use in Matlab. These include various kinds of numbers - integer, floating point, complex - as well as alphanumeric characters (arrays of characters can be treated as strings). A given standard array can only hold one 'type' of thing - an integer array can only have integer values, a character array can only have characters as values. There are two specialized forms of variables – Cell Arrays and Structure Arrays

Cells array are like normal arrays, but each element of a cell array can contain anything - any number type, any other array, even more cells. Cell arrays are accessed like normal arrays, but using curly braces instead of standard parentheses. You can refer to the cell itself with standard parentheses or the contents with the curly braces. The command “cell” will also make empty cell arrays. There are also various utilities to convert arrays back and forth between cell arrays and standard arrays.

Structures are like regular variables that are made up of other variables. So a single structure contains several 'fields,' each of which is a variable in its ownright, with a name and

a particular type. Fields can be of any type - numbers, letters, cells, or even other structures. You can make a structure with the “structcommand”, where you specify fields and valuesand remove them with the “rmfield” command. Structures can be put in arrays or vectors, so long as all the structures in the array or vector have the exact same field names and types. Typing the name of a structure will always tell you all its fields and what they are.

5.1.3.Workspace

When you start Matlab, it opens a chunk of memory on the computer called the "workspace." When you create a variable, it exists in the workspace, and it stays there until you clear it, or until you re-assign that variable. Only variables in the workspace can be used or manipulated. You can easily tell what variables are present in the workspace with the command “whos” . You can save a whole workspace to the disk with the command “save filename”; this will create a binary file with a .mat extension in your present working directory. That .mat file contains all the variables you've just saved, and you can clear the workspace and then load those variables again with the command “load filename”. You can clear the whole workspace at once with clear or clear any individual variable name with “clear variable”.

5.1.4.The colon operator

Last among the real basic things in Matlab is the colon operator, which operates as shorthand for a whole range of numbers at once. The expression 1:10 is shorthand for "every number between one and ten, inclusive, counting by ones". You can specify a different number to count by simply by putting a different number between two colons, so that every number between them are counted accordingly. You can use the colon operator to make values for arrays and also use it in indexing other arrays, where it's particularly powerful.

You can use the colon operator by itself as shorthand for "all rows" or "all columns;" with the 4x4 a array, the expression =a(:,1:2) would give me ***[1 2; 1 2; 1 2; 1 2].***

5.1.5.Function Defintion

The first line of a function m-file must be of the following form.

function [output_parameter_list] = function_name(input_parameter_list) .The first word must always be ``function". Following that, the (optional) output parameters are enclosed in square brackets [ ]. If the function has no output_parameter_list the square brackets and the equal sign are also omitted. The function_name is a character string that will be used to call the function. The function_name must also be the same as the file name (without the ``.m") in which the function is stored. In other words the MATLAB function, ``foo", must be stored in the file, ``foo.m". Following the file name is the (optional) input_parameter_list. There can exactly be one MATLAB function per m-file.

5.1.6.Input and Output parameters

The input_parameter_list and output_parameter_list are comma-separated lists of MATLAB variables.Unlike other languages, the variables in the input_parameter_list should never be altered by the statements inside the function. Expert MATLAB programmers have ways and reasons for violating that principle, but it is good practice to consider the input variables to be constants that cannot be changed. The separation of input and output variables helps to reinforce this principle.

The input and output variables can be scalars, vectors, matrices, and strings. In fact, MATLAB does not really distinguish between variables types until some calculation or

operation involving the variables is performed. It is perfectly acceptable that the input to a function is a scalar during one call and a vector during another call.

6.CODE

6.1. Sample Code

6.1.1. Steganography - Encrypt

```
function [success] = encrypt(msg,key)
num = 1000-length(msg); % Number of space to end of MSG.
if num < 0, error('This message is too long to encode.'); end
newmsg = [msg,repmat(' ',1,num)];
msgmat = dec2bin(newmsg)-48;
pic=hideimage(msgmat);
B = pic(:,:,1);
[piclt picht] = size(B);
len = piclt-2;
ht = picht-3;
keyb = key(end:-1:1);
r = cumsum(double(key));
col = cumsum(double(keyb));
A = zeros(len,ht);
A = matri(A,r,col,len,ht,key);
id = find(A==1);
for v = 1:1000
```

```
for u = 1:7
if msgmat(v,u)==1;
if rem(B(id(u+7*(v-1))),2)==0
B(id(u+7*(v-1))) = B(id(u+7*(v-1)))+1;
End
elseif rem(B(id(u+7*(v-1))),2)==1
B(id(u+7*(v-1))) = B(id(u+7*(v-1)))-1;
end
end
end
newpic = pic; newpic(:,:,1) = B;
[filen pth] = uiputfile({'*.bmp';'*.jpg'},'Save Encoded File As');
```

6.1.2. Minutiae Extraction

```
function [pic]= hideimage(txt)
[filen pth] = uigetfile({'*.bmp';'*.jpg'},'Choose image');
pic = imread([pth filen]);
pic=imresize(pic,[150 150]);
[filen pth] = uiputfile({'*.bmp';'*.jpg'},'Save Encoded File As');
imwrite(pic,[pth filen]);
X=imread([pth filen]);
Bimg = im2bw(X,0.5); % Image is converted into Binary
figure;imshow(Bimg);title('Input Image');
smoothimg = medfilt2(Bimg, [3 3]);
Timg= ~bwmorph(smoothimg,'thin',inf); %Skeleton of the finger print morphological
s=size(Timg);% Size of the image
```

```
ht=s(1);
wd=s(2);
N=3;
n=1; %(N-1)/2
r=ht+2*n;
col=wd+2*n;
double temp(r,col);
temp=zeros(r,col);
bifur=zeros(r,col);
rid=zeros(r,col);
temp((n+1):(end-n),(n+1):(end-n))=Timg(:,:);
S=zeros(r,col,3);
for i=1:3
S(:,:,i) = temp .* 255;
end
for a=(n+1+10):(ht+n-10)
for b=(n+1+10):(wd+n-10)
c=1;
for i=a-n:a+n
d=1;
for j=b-n:b+n
mat(c,d)=temp(i,j);
d=d+1;
end
c=c+1;
```

```
end
if(mat(2,2)==0)
rid(a,b)=sum(~mat(:));
bifur(a,b)=sum(~mat(:));
end
end
end
[rid1 rid2]=find(rid==2);
l1 =length(rid1);
for i=1:l1
S((rid1(i)-3):(rid1(i)+3),(rid2(i)-3),2:3)=0;
S((rid1(i)-3):(rid1(i)+3),(rid2(i)+3),2:3)=0;
S((rid1(i)-3),(rid2(i)-3):(rid2(i)+3),2:3)=0;
S((rid1(i)+3),(rid2(i)-3):(rid2(i)+3),2:3)=0;
if n <= size(txt,2)
text('units','pixels','position',[i 100],'fontsize',20,'string',txt(n),'visible','on');
n=n+1;
else
break
end
end
[bifur1 bifur2]=find(bifur==4);
l2 =length(bifur1);
for i=1:l2
S((bifur1(i)-2):(bifur1(i)+2),(bifur2(i)-2),1:2)=0;
```

```
S((bifur1(i)-2):(bifur1(i)+2),(bifur2(i)+2),1:2)=0;

S((bifur1(i)-2),(bifur2(i)-2):(bifur2(i)+2),1:2)=0;

S((bifur1(i)+2),(bifur2(i)-2):(bifur2(i)+2),1:2)=0;

end

figure;imshow(S);title('Minutiae');
```

6.1.3. Steganography - Decrypt

```
function msg = decrypt(key)

pic2 = imread([pth filen]);

B = pic2(:,:,1);

[piclen picht] = size(B);

len = piclen-2; ht = picht-3; keyb = key(end:-1:1);

r = cumsum(double(key)); col = cumsum(double(keyb));

A = zeros(len,ht);

A = matri(A,r,col,d1,d2,key);

id = find(A==1); msgmat = zeros(1000,7);

for v = 1:1000

for u = 1:7

end

end

msg = char(bin2dec(num2str(msgmat)))';

end
```

6.1.4. Visual Cryptography - Shares

```
function RequiredShadowImage = GetRequiredShadowImage(Shadow_Image,Users)

TT = length(Users);

for i = 1:TT
```

```
    RequiredShadowImage(:,i) = Shadow_Image(:,Users(i));
    end;
function Shadow_Image = GetShadow_Image(P_Im,w,base)
TT = int32(size(P_Im));
P_Im = int32(P_Im);
w=int32(w);
base = int32(base);
Shadow_Image = int32(zeros(TT(1),w));
for i=1:w
for j = 1:TT(2)
Shadow_Image(:,i) = Shadow_Image(:,i) + mod(P_Im(:,j)*i^(j-1), base);
end;
end;
Shadow_Image = mod(Shadow_Image,base);
```

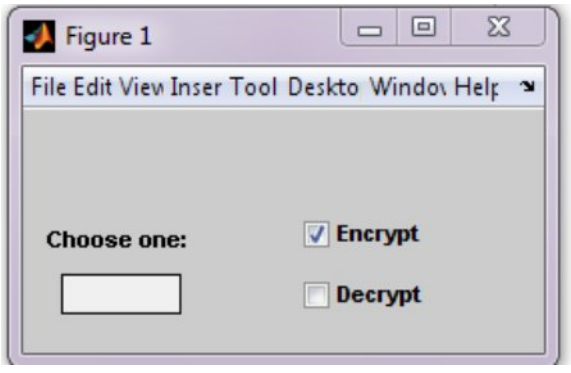
6.1.5. Visual Cryptography – Recovered Image

```
function RecoveredImage = RecoverImage(RequiredShadowImage,Users,Height,Width,base)
TT = size(RequiredShadowImage);
xx = ones(TT(2),TT(2));
for i = 1:TT(2)
```

```
xx(:,i) = xx(:,i).*(Users.^(i-1))';

end;

for i = 1:TT(1)

if(mod(i,100)==0)

disp(sprintf('%d of %d',i/100,floor(TT(1)/100)));

end;

RecoveredImage(i,:) = solveEq(xx,RequiredShadowImage(i,:),base);

end;

RecoveredImage = reshape(RecoveredImage(:),Height,Width)';
```

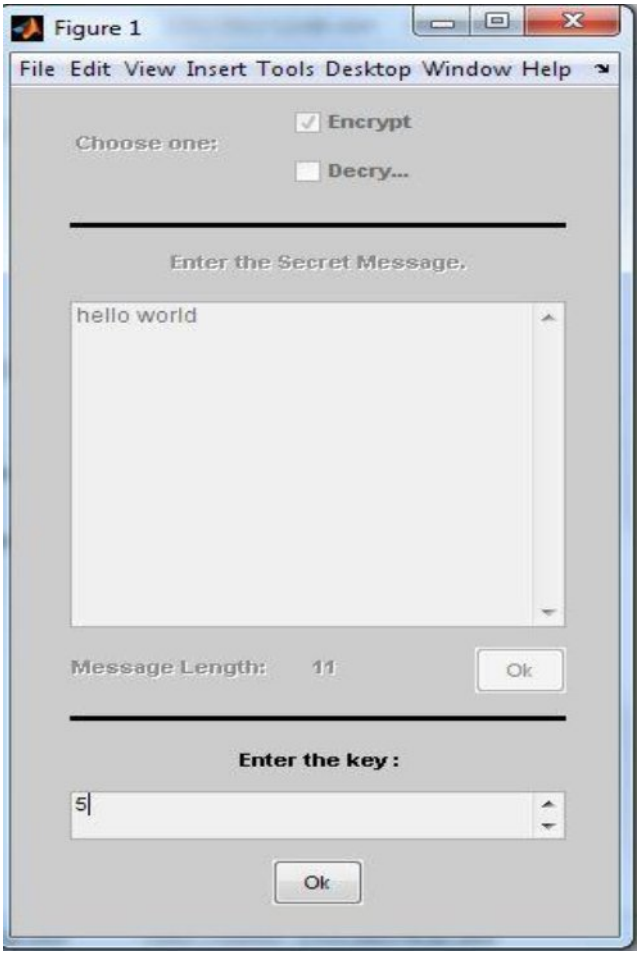
6.2. Snapshot

6.2.1 Encrypt



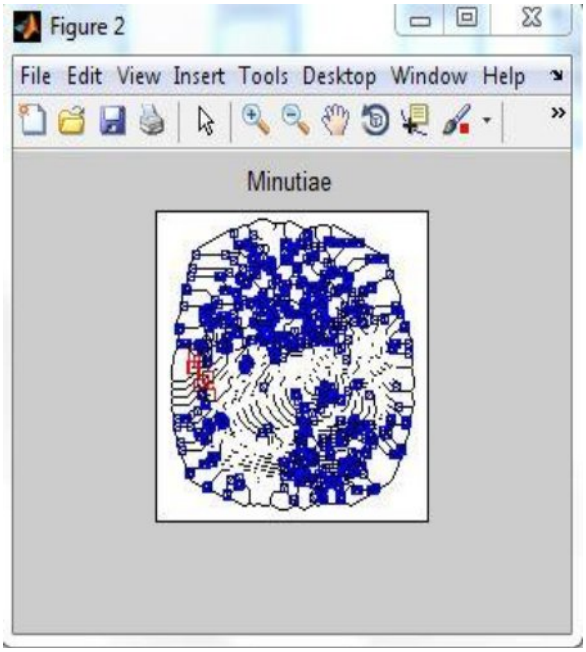
Encrypt is selected.

Message is entered for hiding.



Key value is entered

Input Image



Minutiae Extraction

\

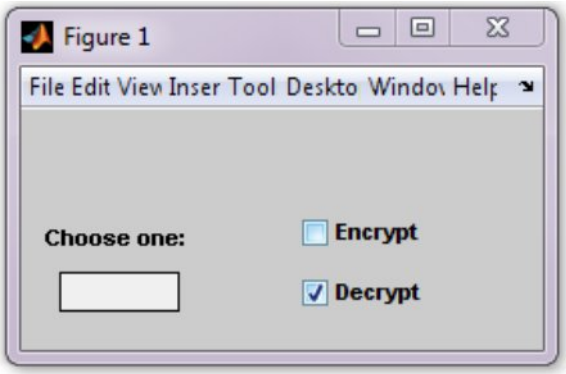
Encrypted Image

Stego image divided into shares.

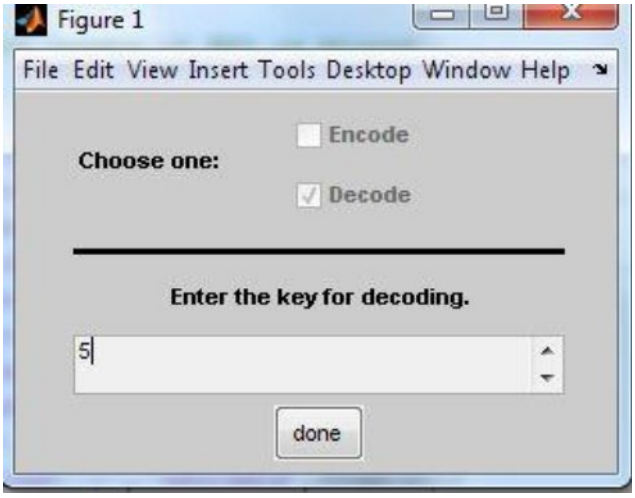
Shadow Image 1 + Shadow Image 2 +..... k Shadow Images

Recovered Image from Shadow Images.

6.2.2 Decrypt



Decrypt is selected.



Key is entered.

Retrieved Secret Message.

7. SOFTWARE TESTING

When a system is to be developed, it is hoped that it performs properly. In practice, some errors always occur. The main purpose of testing a system is to discover the errors and correct them. A successful test is one which finds an error. Software testing can be implemented at any time in the development process. Traditionally most of the test effort occurs after the requirements have been defined and the coding process has been completed. The objectives of system testing are: To ensure that during operation the system will perform as per specification, To make sure that the system meets user's requirements during oeration, To verify that the controls incorporated in the system function as intended, To make sure when correct inputs are fed to the system, the outputs are correct, To make sure that during operation, incorrect input, processing and outputs will be deleted. Thus the main objective of software testing is to maintain and deliver a quality product to the client. Every software is expected to meet its needs. So when a software is developed it is required to check whether it fulfills those requirements.

The main goal of software testing is to know the errors of the software before the user finds them. A good tester is one who makes the software fail. He should always be in a mentality to destruct the software. A software tester should not be the one who makes the software. One of the advantage is if we test early it will help to determine the overall product feasibility.

7.1.Unit Testing

Unit testing is checking the performance of each software modules. It is typically done by the programmer and not by testers, as it requires detailed knowledge of the internal

program design and code. The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. Thus unit testing is successfully verified in our implementation.

7.2 Integration Testing

Integration testing is the phase in software testing in which individual software modules are combined and tested as a group. In this testing groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.The purpose of integration testing is to verify functional, performance and reliability requirements placed on major design items. Thus integration testing is successfully verified.

7.3 Validation Testing

Validation testing is to determine to check whether an implemented system fulfills its requirements. The checking of data for correctness or for compliance with applicable standards, rules, and conventions. From testing perspective: fault,malfunction and failures are detected. Thus validation testing is checked successfully.

7.4 System Testing

System testing is actually a series of different tests whose main purpose is to fully exercise the computer-based system. Although each testing has different purpose, all work to verify that system elements have been properly integrated and perform allocated function. Thus system testing is achieved successfully.

8. IMPLEMENTATION

8.1 Problems faced:

Some particular problems faced are listed as follows

1. After encryption to maintain correlation between images was tricky.
2. Recovering the divided images was complex.

8.2 Lessons learnt:

1. Fingerprint image importance.
2. Usage of minutiae extraction in fingerprint image.
3. Calling of various functions in Matlab.
4. Importance of image sharing.
5. Different ways of text hiding, dividing images.

9. FUTURE PLANS

This project can be extended further for many applications namely in bank for providing pin number to their customers which is now a quite big process. This can be implemented by sending the pin to the customer using their finger print which can be taken from the bank's database server. In this project, time taken for reconstructing the original image using visual cryptography is quite high, which can be reduced.

10. CONCLUSION

In this project, a combination of steganography and visual cryptography was introduced . By which the protection of the content of message was achieved by using (k,n) visual cryptography scheme where the original image was divided into n shadow shares which was recovered with k shadow shares out of n . Further the authentication of the communicating parties was achieved by using the concept of steganography where the secret message was hidden inside the original image which was finally retrieved correctly without any loss from the recovered image. Thus the combination of visual cryptography and steganography enhance the security.

11. REFERENCES

- Rana, Puja Devi; Singhrova, Anita; Deswal, Suman: "Design and Implementation of K-Split Segmentation Approach for Visual Cryptography**",** International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 2, Issue 8, August 2012.
- Askari, Nazanin; Moloney, Cecilia; Heys, Howard M.: "Application of Visual Cryptography to Biometric Authentication", Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, Canada, 2011.
- Chandramathi S; Kumar, Ramesh R; Suresh R & Harish S: "An Overview of Visual Cryptography", International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474, Volume 1, Issue 1, 2010.
- Bansal, Roli; Sehgal, Priti; Bedi Punam: "Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Volume 8, Issue 5, No 3, September 2011.
- Reddy, Amamath M; Bala, Shanthi P; Aghila G; "COMPARISON OF VISUAL CRYPTOGRAPHIC SCHEMES", International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Volume 3, No. 5, May 2011.
- Alkharobi, Talal Mousa; Alvi, Aleem Khalid: "New algorithm for halftone image visual cryptography", King Fahd University of Pet. & Min, Dhahran, Saudi Arabia, 2004.
- Kandar, Shyamalendu; Dhara, Bibhas Chandra: "k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence", International Journal of Computer Applications (0975 – 8887), Volume 25, No.11, July 2011.

11.1. BIBLIOGRAPHY

- http://www.ijest.info/docs/IJEST11-03-05-257.pdf
- http://necec.engr.mun.ca/ocs2011/viewpaper.php?id=60&print=1
- http://onlinelibrary.wiley.com/doi/10.1002/047172386X.app1/pdf
- http://www.ijcaonline.org/volume25/number11/pxc3874377.pdf
- http://www.ccse.kfupm.edu.sa/~akalvi/myweb/9.pdf
- http://www.ijsrp.org/research-paper-0812/ijsrp-p0888.pdf
- http://arxiv.org/ftp/arxiv/papers/1201/1201.1422.pdf
- http://www.mathworks.in/support/solutions/en/data/1-1BALJ/?solution=1-1BALJ
- http://blogs.mathworks.com/steve/
- http://www.ijetae.com/
- http://www.mathworks.in
- http://www.developer.com
- http://www.wikipedia.com
- http://stackoverflow.com
- http://codeproject.com