# Security System using Cryptography, Steganography and Watermarking

**Submitted in partial fulfillment of the requirement for the award of Degree of Bachelor of Technology in Computer Engineering Discipline**

**Submitted To**


**SVKM's NMIMS,**
**Mukesh Patel School of Technology Management & Engineering,**
**Shirpur Campus, Shirpur, Dist: Dhulia (M.H.)**

**Submitted By :**

**Sayed Shazeb, SAPID – 71202110007**
**Shubhra Chaturvedi, SAPID – 71202110006**
**Rahul Gangwal, SAPID – 71202110013**
**Anant Chaudhary, SAPID – 71202110019**

**Under The Supervision Of:**

**Prof. Mayank Sohani**
**(Asst. Prof., Computer Engineering Department)**

**DEPARTMENT OF COMPUTER ENGINEERING**
**Mukesh Patel School of Technology Management & Engineering**
**SESSION: 2014-15**

# CERTIFICATE

This is to certify that the work embodies in this Project entitled **"Security System using Cryptography, Steganography and Watermarking"** being submitted by

**"Sayed Shazeb" (SAP ID.: 71202110007)**

**"Shubhra Chaturvedi" (SAP ID.: 71202110006)**

**"Rahul Gangwal" (SAP ID.: 71202110013)**

**"Anant Chaudhary" (SAP ID.: 71202110019)**

for partial fulfillment of the requirement for the award of "**Bachelor of Technology** in **Computer Engineering"** discipline to "NMIMS, Mumbai (M.H.)" during the academic year 2014-15 is a record of bonafide piece of work, carried out by him under my supervision and guidance in the **"Department of Computer Engineering", MPSTME, Shirpur (M.H.).**

**APPROVED & SUPERVISED BY:**

**Prof. Mayank Sohani**
(Asst. Professor, Computer Engg. Department)

**FORWARDED BY:**

**(Dr. N.S. Choubey)**
H.O.D., Computer Dept.
MPSTME, Shirpur

**(Dr. M.V. Deshpande)**
Associate Dean
MPSTME, Shirpur

**DEPARTMENT OF COMPUTER ENGINEERING**
**Mukesh Patel School of Technology Management & Engineering**

# CERTIFICATE OF APPROVAL

The Project entitled **"Security System using Cryptography, Steganography and Watermarking"** being submitted by

**"Rahul Gangwal" (SAP ID.:71202110013)"**

**"Anant Chaudhary" (SAP ID.:71202110019)"**

**"Sayed Shazeb" (SAP ID.:71202110007)"**

**"Shubhra Chaturvedi" (SAP ID.:71202110006)"**

has been examined by us and is hereby approved for the award of degree **"Bachelor of Technology in Computer Engineering Discipline"**, for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the project only for the purpose for which it has been submitted.

**(Internal Examiner)** **(External Examiner)**

**Date:** **Date:**

**DEPARTMENT OF COMPUTER ENGINEERING**
**Mukesh Patel School of Technology Management & Engineering**

# DECLARATION

We,

**Rahul Gangwal**

**Anant Chaudhary**

**Sayed Shazeb**

**Shubhra Chaturvedi**

the students of **Bachelor of Technology** in **Computer Engineering** discipline, **session: 2014-15, MPSTME, Shirpur Campus,** hereby declare that the work presented in this Project entitled **"**Security System using Cryptography, Steganography and Watermarking**"** is the outcome of our work, is bonafide and correct to the best of our knowledge and this work has been carried out taking care of Engineering Ethics. The work presented does not infringe any patented work and has not been submitted to any other university or anywhere else for the award of any degree or any professional diploma.

**(Sayed Shazeb)**
**SAP ID.: 71202110007**
**(Shubhra Chaturvedi)**
**SAP ID.: 71202110006**
**(Rahul Gangwal)**
**SAP ID.: 71202110013**
**(Anant Chaudhary)**
**SAP ID.: 71202110019**

**Date:**

**DEPARTMENT OF COMPUTER ENGINEERING**
**Mukesh Patel School of Technology Management & Engineering**

# ACKNOWLEDGEMENT

*After the completion of this Major Project work, words are not enough to express my feelings about all those who helped me to reach my goal; feeling above this is my indebtedness to The Almighty for providing me this moment in life.*

*It's a great pleasure and moment of immense satisfaction for me to express my profound gratitude to Prof. Mayank Sohani, Assistant Professor, Computer Engg. Department, MPSTME, Shirpur, whose constant encouragement enabled me to work enthusiastically. Their perpetual motivation, patience and excellent expertise in discussion during progress of the project work have benefited me to an extent, which is beyond expression. Their depth and breadth of knowledge of Computer Engineering field made me realize that theoretical knowledge always helps to develop efficient operational software, which is a blend of all core subjects of the field. I am highly indebted to them for their invaluable guidance and ever-ready support in the successful completion of this project in time. Working under their guidance has been a fruitful and unforgettable experience.*

*We express my sincere thanks and gratitude to Dr. N.S. Choubey, Head, Computer Engineering Department, MPSTME, Shirpur, for providing necessary infrastructure and help to complete the project work successfully.*

*We also extend my deepest gratitude to Dr. Pradeep Waychal , Director, MPSTME, Shirpur Campus and Dr. M.V. Deshpande., Associate Dean, MPSTME, Shirpur Campus for providing all the necessary facilities and true encouraging environment to bring out the best of my endeavors.*

*We sincerely wish to express my grateful thanks to all members of the staff of computer engineering department and all those who have embedded me with technical knowledge of computer technology during various stages of B.Tech. Computer Engineering.*

*We would like to acknowledge all my friends, who have contributed directly or indirectly in this Major Project work.*

*The successful completion of a Major Project is generally not an individual effort. It is an outcome of the cumulative effort of a number of persons, each having their own importance to the objective. This section is a vote of thanks and gratitude towards all those persons who have directly or indirectly contributed in their own special way towards the completion of this project.*

*Rahul Gangwal*
*Anant Chaudhary*
*Sayed Shazeb*
*Shubhra Chaturvedi*

# ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. The word Steganography in the modern day usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits.

Cryptography, steganography and watermarking are widely used techniques for information-hiding in secured communication across internet and mobile transmission. Our project shows implementation of cryptography which uses AES algorithm that scrambles information so that it cannot be understood. Steganography uses LSB algorithm that attempts to prevent suspecting the existing of data by unintended recipient. Digital image watermarking provides copyright protections by hiding rightful information for declaring ownership. The embedding process creates a stego image by embedding the text encrypted behind an image using AES algorithm. The scheme is perfectly secure and very easy to implement. Further watermarking is also applied on the data so as to provide much security. Digital watermarking using LSB inserts a stego image behind another digital image. The signal, known as a watermark, can be used later to identify the owner of the work, to authenticate the content, and to trace illegal copies of the work.

# TABLE OF CONTENTS

# LIST OF FIGURES

CHAPTER 1

# INTRODUCTION

## 1.1 PURPOSE

We have chosen to use Cryptography, steganography and watermarking as our project . They are widely used techniques for information hiding in secured communication across internet and mobile transmission. Cryptography scrambles information so that it cannot be understood. Stenography attempts to prevent suspecting the existing of data by unintended recipient.

Digital image watermarking provides copyright protections by hiding rightful information for declaring ownership. The aim of this article is to present basis and comparative study of cryptography, steganography and watermarking used in information hiding. The purpose of this project is to present make a security system by comparative study of cryptography, steganography and watermarking used in information hiding.

## 1.2 SCOPE

The scope of the application is to provide : Confidentiality of the message: only the authorized recipient should be able to extract the content of the cipher. In addition, obtaining information about the content of the message (such as a statistical distribution of certain characters) should not be possible, once the cryptographic analysis becomes easier.

i. Message integrity: the recipient must be able to determine if the message was altered during transmission.
ii. Authentication of the sender: the recipient should be able to identify the sender and verify if it was him who sent the message.
iii. Irrevocability of the sender: it should not be possible to deny the authorship of the message.

## 1.3 OVERVIEW

Cryptography, steganography and watermarking are widely used techniques for information hiding in secured communication across internet and mobile transmission. Cryptography scrambles information so that it cannot be understood. Stenography attempts to prevent suspecting the existing of data by unintended recipient. Digital image watermarking provides copyright protections by hiding rightful information for declaring ownership. The aim of this document is to present basis and comparative working of cryptography, stegnography and watermarking used in information hiding.

## 1.4 DEFINITIONS AND ACRONYMS

| **TERMS** | **DEFINATION** |
|---|---|
| Cryptography | Study of encryption principles/methods |
| Steganography | Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. |
| Watermarking | Watermarking is the process of hiding digital information in a carrier signal |
| Watermark | A watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light |
| Encrypt | Converting plaintext to cipher text. |
| Decrypt | Converting plaintext to cipher text. |
| JVM | Java Virtual Machine |
| Cipher text | coded message |
| Key | info used in cipher known only to sender/receiver |
| User | Reviewer or Author. |
| Software Requirement Specification | A document that completely describes all of the functions of a proposed system and the constraints under which it must operate. For example, this document. |
| Authentication | Process of identifying an individual. |

| | |
|---|---|
| Confidentiality | Hiding information from unauthorized access. |
| Integrity | Preventing information from unauthorized modification. |
| IDE | Integrated Development Environment |
| Steganalysis | The attempt of finding presence of secret content by visual analysis or statistical by algorithmic analysis |
| Stegosystem | Steganography System. |

CHAPTER 2

# LITERATURE SURVEY

## 2.1 CRYPTOGRAPHY

There are many aspects to security and many application. One essential aspect for secure communication is that of cryptography. There are some specific security requirements for cryptography, including Authentication, Privacy/confidentiality and Integrity non-repudiation[11].

Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

### i. AES algorithm for Cryptography

This standard specifies the a symmetric block cipher that can process blocks of 128 bits, using cipher keys with length 128,192 and 256 bits[12]. The input, the output and cipher key are each bit sequences containing 128,192,256 bits with the constraint that the input and output sequences have same length[13].

### ii. Advantages of using AES algorithm

- Very Secure
- Reasonable
- Main Characteristics : Flexibility and Simplicity

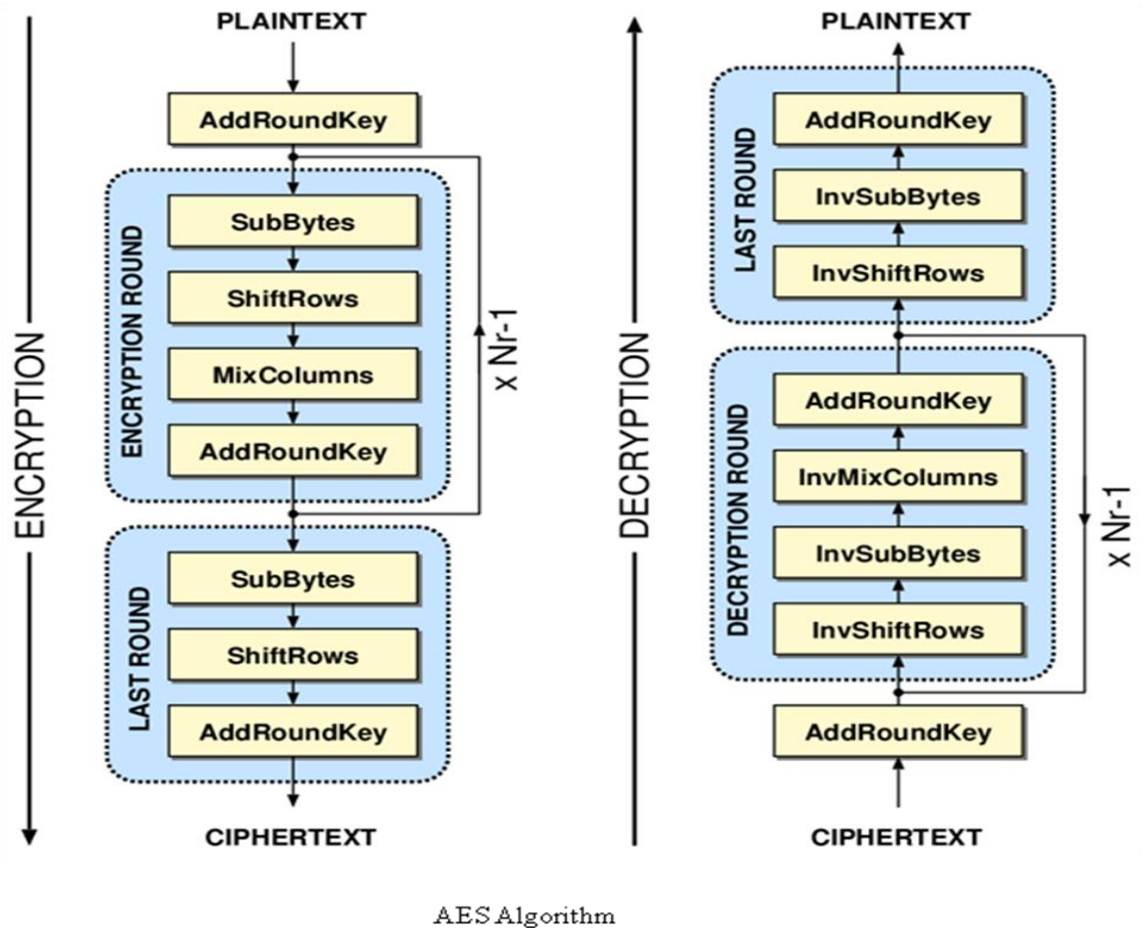


Figure 2.1 AES Description

## 2.2 STEGANOGRAPHY

In this section, we first give description of the typical LSB-based approaches including LSB in GIF [1], LSB replacement [6], EA-LSBMR [3], and some adaptive schemes including PVD with modulus function[10],difference expansion technique [2], hiding in edges [7],adaptive edges with LSB (AE-LSB) [11], hiding behind corners (HBC) [1] etc.

### i. LSB in GIF [1]

Palette based images, such as GIF images, are popular image file format commonly used on the Internet. GIF images are indexed images where the colors used in the image are stored in a palette or a color lookup table. GIF images can also be used for

LSB steganography , although extra care should be taken. The main issue with the palette based approach is that if one changes the least significant bit of a pixel, it could result in an entirely different color since the index to the color palette gets modified. One possible solution to this problem is to sort the palette so that the color differences between consecutive colors are minimized. The strong and weak points regarding embedding information in GIF images using LSB is that since GIF images only had a bit depth of 8, the total amount of information that could be embedded will be less. GIF images are vulnerable to statistical as well as visual attacks, since the palette processing which has to be done on the GIF image leaves a clear signature on the image. This approach was dependent on the file format as well as the image itself, since a wrong choice of image could results in the message being visible.

### ii. Steganographic Method based on Difference Expansion Technique [2]

Difference Expansion (DE) is a simple and efficient reversible data-embedding method used for digital images. Here the redundancy in the digital content is explored to achieve reversibility. In this method, one bit can be embedded into two consecutive pixels. So the maximum embedding capacity will be 0.5 bpp. The main advantage of this technique was that it discovers extra storage space by exploring the redundancy in the image content. Both the payload capacity limit as well as the visual quality of embedded images of the DE method are the best along with a low computational complexity. The difference expansion technique was later generalized so that n -1 bits can be embedded into n pixels, resulting the maximum embedding capacity (n-1)/n bpp. However, the difference expansion based reversible data hiding methods could not gain much popularity as the method double the differences between pixels in successive iteration. The distortions were larger and hence DE was vulnerable to statistical attacks. DE based technique had low payload capacity. The technique could not be used for applications demanding high visual quality.

### iii. Hiding Behind Corners [3]

Certain digital techniques do not take into account the cover's original information thereby they leave certain marks on the stego image. In Hiding Behind Corners (HBC), this was avoided by taking the cover's original information. Two algorithms

were used in HBC based on using image filters to determine the effective hiding places in an image. They were FilterFirst and BattleSteg. The strength of Filter First was that it eliminates the need to provide any additional information such as original image. It was also very effective in hiding information. Whereas the weakness of FilterFirst was that it was not secure, as an attacker can repeat the filtering process. It could be also much easier to retrieve the hidden information once the stego image is identified. The strength of BattleSteg was that it requires a password to retrieve the message. Its weakness includes the absence of a random seed so it was impossible to know where to place the shots and also it was possible for BattleSteg to never have a hit. Hiding Behind Corners approach effectively utilize edge areas but embedding capacity is less.

### iv. Hiding Secret Message in Edges of the Image (RELSB) [4]

Hiding Secret Message in Edges of the image introduced a new least significant bit embedding algorithm for hiding secret messages in non-adjacent pixel locations at the edges of images. Here the messages were hidden in regions which were least like their neighboring pixels i.e. regions that contain edges, corners, thin lines etc so that an attacker will have less suspicion of the presence of message bits in edges, because pixels in edges of an image appears to be much brighter or dimmer than their neighbors. Edges can be detected by edge detection filters such as a 3x3 window Laplacian edge detector .One common disadvantage of LSB embedding was that it created an imbalance between the neighboring pixels. Here this imbalance was avoided by flipping the gray-scale values among 2i-1, 2i and 2i+1. The various strengths of this scheme were that an attacker will have less suspicion to the presence of message bits in edges because pixels in edges appear to be either much brighter or dimmer than their neighbors and it was also secure against blind steganalysis. It also limits the length of the secret message to be embedded. The main disadvantage with this scheme was that the embedding capacity was relatively low. It could not make full use of edges during embedding.

### v. Adaptive Data Hiding Edge Areas of Images with Spatial LSB Domain Systems (AE-LSB) [7]

Here a new adaptive least-significant bit (LSB) steganographic method based on pixel-value differencing (PVD) was proposed. The difference value of two consecutive pixels estimates how many secret bits to be embedded into the two pixels. Pixels located in the edge areas were embedded with more secret bits than that located in smooth areas. The range of difference values were adaptively divided into lower level, middle level, and higher level. The readjusting phase ensures that the two consecutive pixels belong to the same level both before and after embedding. The range [0, 255] of difference values was divided into different levels. For extracting data exactly, the difference values before and after embedding must belong to the same level. This scheme provides more capacity and better quality than the PVD and was an improved version of PVD. The main disadvantage with this scheme was that it was less tolerant to steganalysis.

### vi. Steganographic Method based on Pixel Value Differencing and Modulus Function [10]

High Quality Steganographic method with PVD and Modulus function was an extension of PVD [8] based approach. This technique first calculates the difference value between two consecutive pixels and then modulus operation was used to calculate their remainder. The secret data were embedded into the two pixels by modifying their remainder. The hiding capacity of the two consecutive pixels depends upon the difference value taken. Lesser the difference value smoother the area, so only less secret data could be embedded and vice versa. The strength of the scheme was that it could greatly reduce the visibility of the hidden data than the PVD method. Since the scheme used the remainder of the two consecutive pixels it was more flexible. However, a loophole exists in the PVD [8] method. Unusual steps in the histogram of pixel differences reveal the presence of a secret message. The modified pixels will be spread around the whole stego image and many smooth regions gets contaminated.

### vii. Data hiding method based on interpolation technique [11]

Reversible data hiding method based on Interpolation Technique (IT) concealed data into interpolation errors. Instead of using the nearest neighbour interpolation technique, an image interpolation algorithm was used to obtain the interpolation errors. The reference pixels are adaptively selected in the cover image and pixels other than the reference pixels are interpolated. Interpolation errors are obtained by subtracting the interpolated pixels from the original image. Data bits were concealed by modifying the interpolation errors. Because reference pixel values were not changed in the embedding process, the same set of interpolated pixels could be obtained in the decoding process and thus, the embedded data bits could be extracted and the original image was restored. In this technique, they reduced the number of reference pixels in smooth regions and increased the number of reference pixels in complex regions. But the distortions in the output image were much higher in histogram shifting method [12].However, in most cases, the number of reference pixels affects the payload and the stego image quality.

Interpolation Technique is less secure against image manipulations and steganalysis due to the presence of LSB replacement style asymmetry.

## 2.3 DIGITAL WATERMARKING

In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many articles and papers.
These properties include:

1) A digital watermark should be perceptually invisible to prevent obstruction of the original image.
2) A digital watermark should be statistically invisible so it cannot be detected or erased.
3) Watermark extraction should be fairly simple. Otherwise, the detection process requires too much time or computation.

4) Watermark detection should be accurate. False positives, the detection of a nonmarked image, and false negatives, the non-detection of a marked image, should be few.

5) Numerous watermarks can be produced. Otherwise, only a limited number of images may be marked.

6) Watermark should be robust to filtering, additive noise, compression, and other forms of image manipulation.

7) The watermark should be able to determine the true owner of the image.

Figure 1 shows a general watermarking scheme. For transmission, the watermark W is generated as a pseudo-random sequence to ensure statistical invisibility. Signal information, such as DCT coefficients, are extracted from the original image I and embedded into the information. The watermarked image I' is formed with no visible differences between I and I'. For watermark detection, a suspected image J is taken and its signal information is obtained. A suspected watermark V is extracted based on knowledge of the original image I and the watermark W. A similarity measure S is performed on V and W. Popular measures include the cross-correlation and correlation coefficient. Finally, S is compared to a threshold t. If S is larger than the threshold, then the watermark W is detected. Otherwise, no watermark is detected.

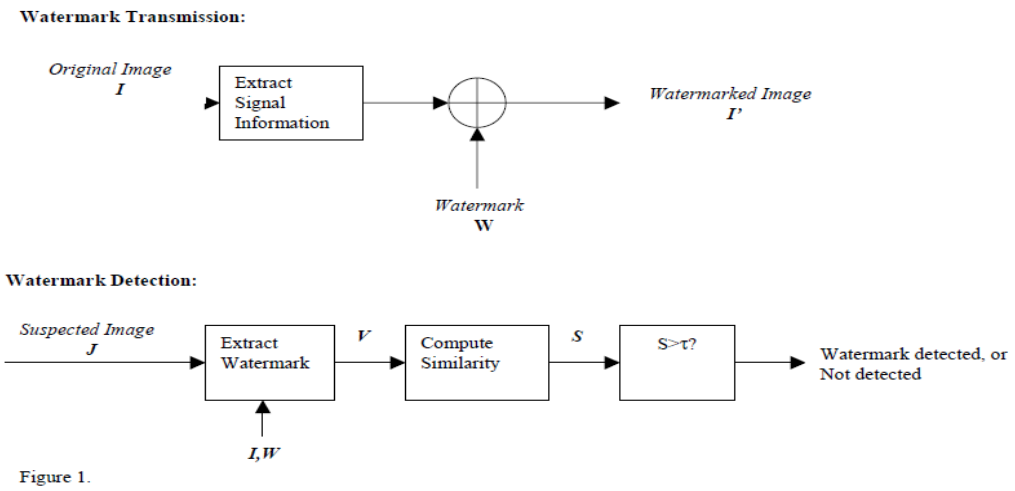


Figure 2.3 Digital watermarking

## i. Watermarking Techniques:

Many watermarking methods have been proposed in the literature. Schyndel, Tirkel, and Osborne [4] generated a watermark using a m-sequence generator. The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. Schyndel et al. showed that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, was not robust to additive noise. Cox et al. [1] noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image. The watermark was based on 1000 random samples of a N(0,1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image, and the inverse DCT was taken to retrieve the

**Watermark Transmission:**

Extract Signal Information Original Image **I** Watermark **W** Watermarked Image **I'**

**Watermark Detection:**

Suspected Image **J** Compute Similarity Extract Watermark S>t? Watermark detected, or Not detected **I,W V S** Figure 1. watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping, and rescanning. Xia, Boncelet, and Arce proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini et al. first generated a watermarked image from DCT

coefficients. Then spatial masking was performed on the new image to hide the watermarkDelaigle et al. proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were generated and then modulated on a random carrier. This image served as the watermark, and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image.

CHAPTER 3

# PROBLEM DEFINITION AND PROPOSED SOLUTION

## 3.1 PROBLEM DEFINITION

Problem statement describes the following problems:

i. There are various important information is exchanged via network. Various intruder or attacker tries to intrude into your system. If your information is not secret then attacker kept your private information and misuses them by modifying it i.e. loss of integrity .

ii. Information gets compromised when information is accessed by intruder i.e. loss of confidentiality.

iii. Suppose that A wants to send message to B ,when A sends the message to the network suppose an intruder takes a hold of a message and presents to B as if he is legitimate sender of the message, so intruder in unauthorized sender of message.

## 3.2 PROPOSED SOLUTION

i. The proposed solution is to make a single application that will provide three layer of security for the user data.

ii. Encrypt/Decrypt data using cryptography to address the loss of confidentiality.

iii. Hide the data behind image, audio etc to provide additional layer of security.

iv. Watermark an image using watermarking to address the problem of unauthorized sender of a message.

v. User interface will be having three checkboxes for cryptography, steganography and watermarking. Based on the user selection of checkboxes user will be provided the functionalities of cryptography, steganography and watermarking other functionalities will be disabled.

- **Cryptography**

- The internet is a lawless place, and people have access to all sorts of information. What is keeping people from stealing your credit card number when you purchase something online?
- Cryptography is the study of sending and receiving secret messages. We will see how websites protect buyers through mathematics.
- There are two ways to encrypt a message: via a private key encryption or via a public key encryption.

- **Steganography**

- Consider a scenario, wherein, we have to send the confidential documents to our clients or we have to send a secret message to the destination, so how can we send a message secretly to the destination?
- Using steganography, information can be hidden in carriers such as images, audio files, text files, videos, and data transmissions.

- **Digital Watermarking**

- What are the credentials for that document??
- Using Digital watermarking, a code is embedded inside an image.
- With this application, user will be able to encrypt and decrypt plain text.
- Hide the data behind image, audio etc.
- Watermark an image using watermarking.
- There will be only two type of user for our system administrator and user.
- Administrator can grant access to the user who has registered on the system; furthermore he can perform basic operations like encryption, decryption, steganography and watermarking and also administrator will be able to retrieve the historical records of all the user.
- Administrator will be having similar interface as that of user, only difference will be that administrator interface will be having an interface for granting access to the users.

CHAPTER 4

# DESIGN

## 4.1 ARCHITECTURAL DESIGN

This system will consist of three parts: one cryptography module ,one steganographic module and one watermarking module.

By using Netbeans IDE, java graphics API for Watermarking, Crypto classes for cryptography and AWT in Swing classes for Steganography we will implement following three techniques:

i. The cryptographic module will be implemented using secret key, public key and hash functions. Cryptography is based on mathematical algorithms which need prior knowledge of algebra, algebraic geometry, number theory, probability theory and statistical inference. Cryptanalysis is the science of analyzing and breaking cryptographic secured communication by using combination of analytical reasoning, mathematical tools pattern findings etc.

ii. Stenographic techniques are implemented by steganographic module ;either is spatial domain using Lease Significant Bit' insertion like algorithms or in frequency domain using various transforms like discrete Cosine transform, discrete Wavelet transform etc. The attempt of finding presence of secret content by visual analysis or statistical by algorithmic analysis is called 'stegnalysis'. In actual implementation, secret message processing (text processing) and original cover processing (image processing) phases are applied before applying to 'stegosystem encoder' to increase number of security levels.

iii. Watermarking module includes 'embedding algorithm' and 'extraction algorithm'. The embedding algorithm embeds watermark logo into cover image to from 'watermarked image'. The 'extraction algorithm' extracts watermark logo from 'watermarked image'. Robustness against various attacks, perceptual transparency, high embedding information hiding capacity and number of security levels combinely determines quality of watermarking technique.

## 4.2 DECOMPOSITION DESCRIPTION

**DFD Level-0**


Figure 4.2.1 DFD Level-0

**DFD Level-1**

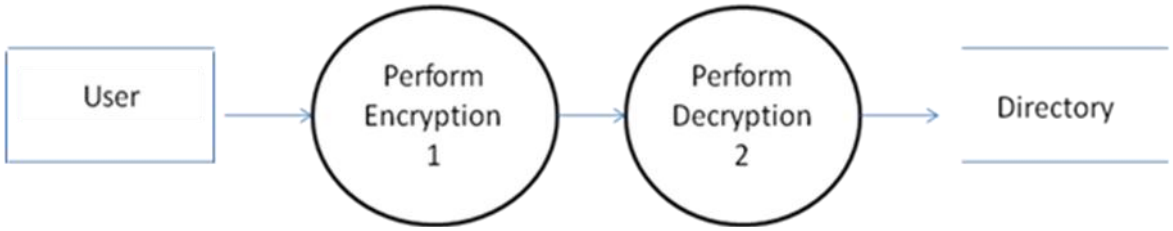


Figure 4.2.2 DFD Level-1

**DFD Level-2**

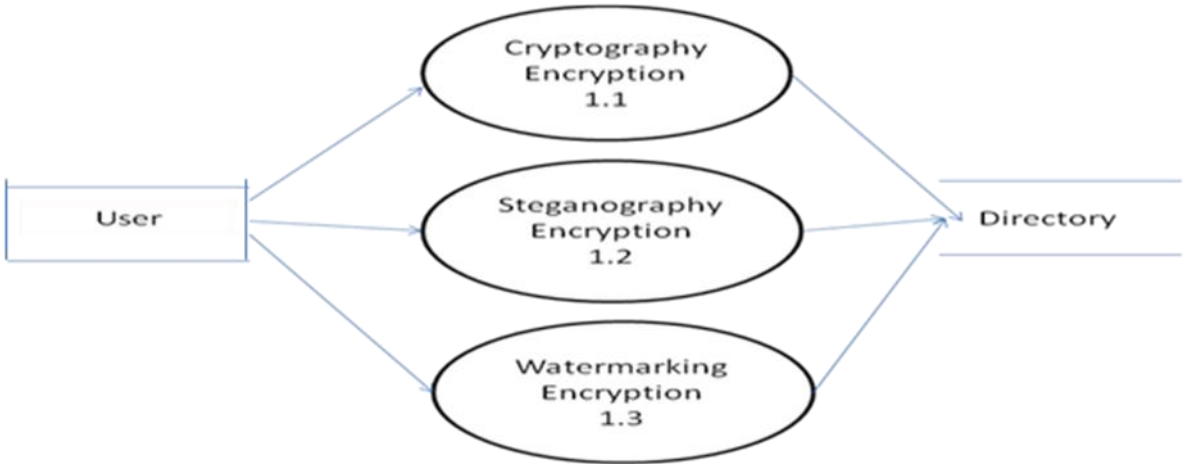


Figure 4.2.3 DFD Level-2

**DFD Level-2**


Figure 4.2.4 DFD Level-3

**DFD Level-3**

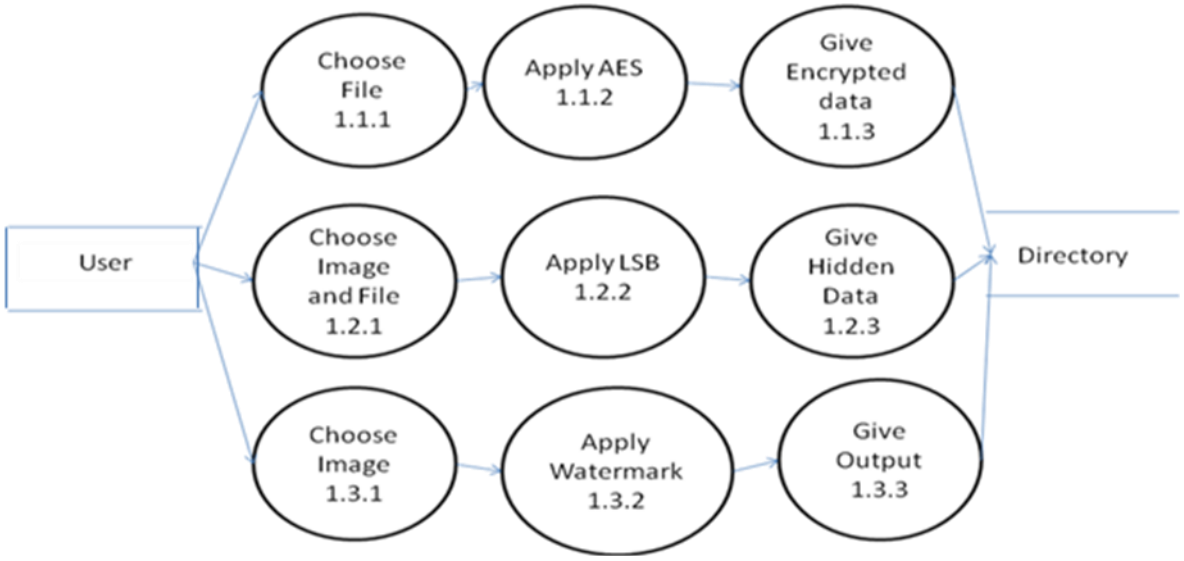


Figure 4.2.5 DFD Level-4

**DFD Level-3**

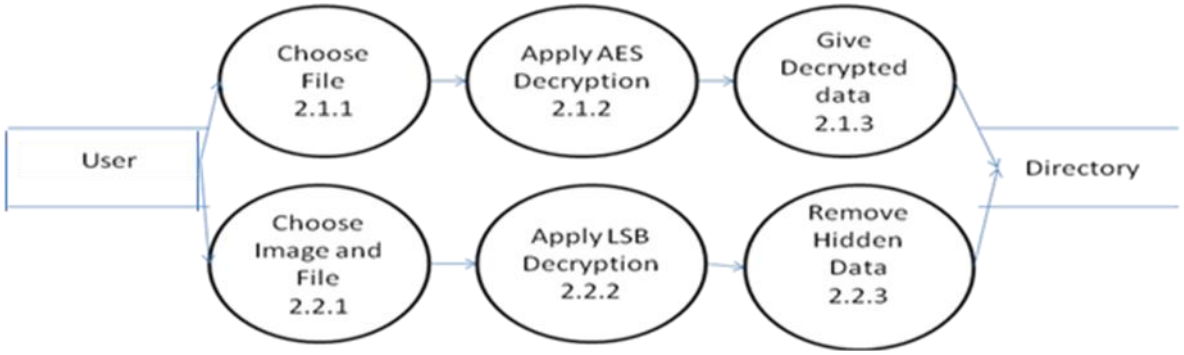


Figure 4.2.6 DFD Level-5

## 4.3 DATA DESIGN

### i. Data Description

Application consist of three techniques: steaganograpy, cryptography and water marking. User need to select which technique to use by clicking the check boxes accordingly. User can also select 2 techniques or all the three techniques to increase security level.

### ii. Data Dictionary

Data Dictionary of our application consists of:

- Cryptograpgy module.
- Steganography module.
- Watermarking module.
- Directory Used.

## 4.4 OBJECT ORIENTED APPROACH

### i. Use Case Diagram

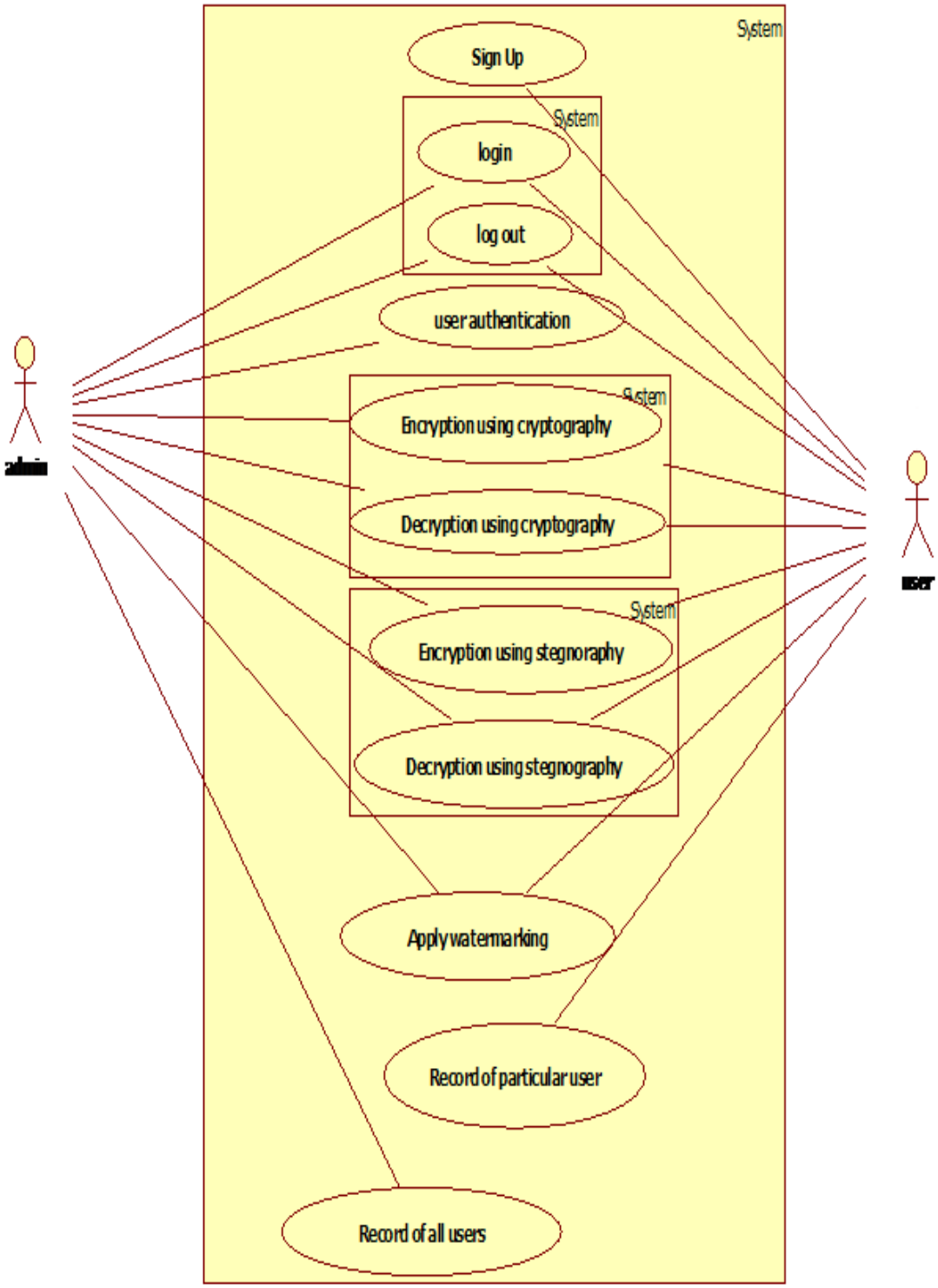


Figure 4.4.1 Use Case Diagram

**ii. Activity Diagram**

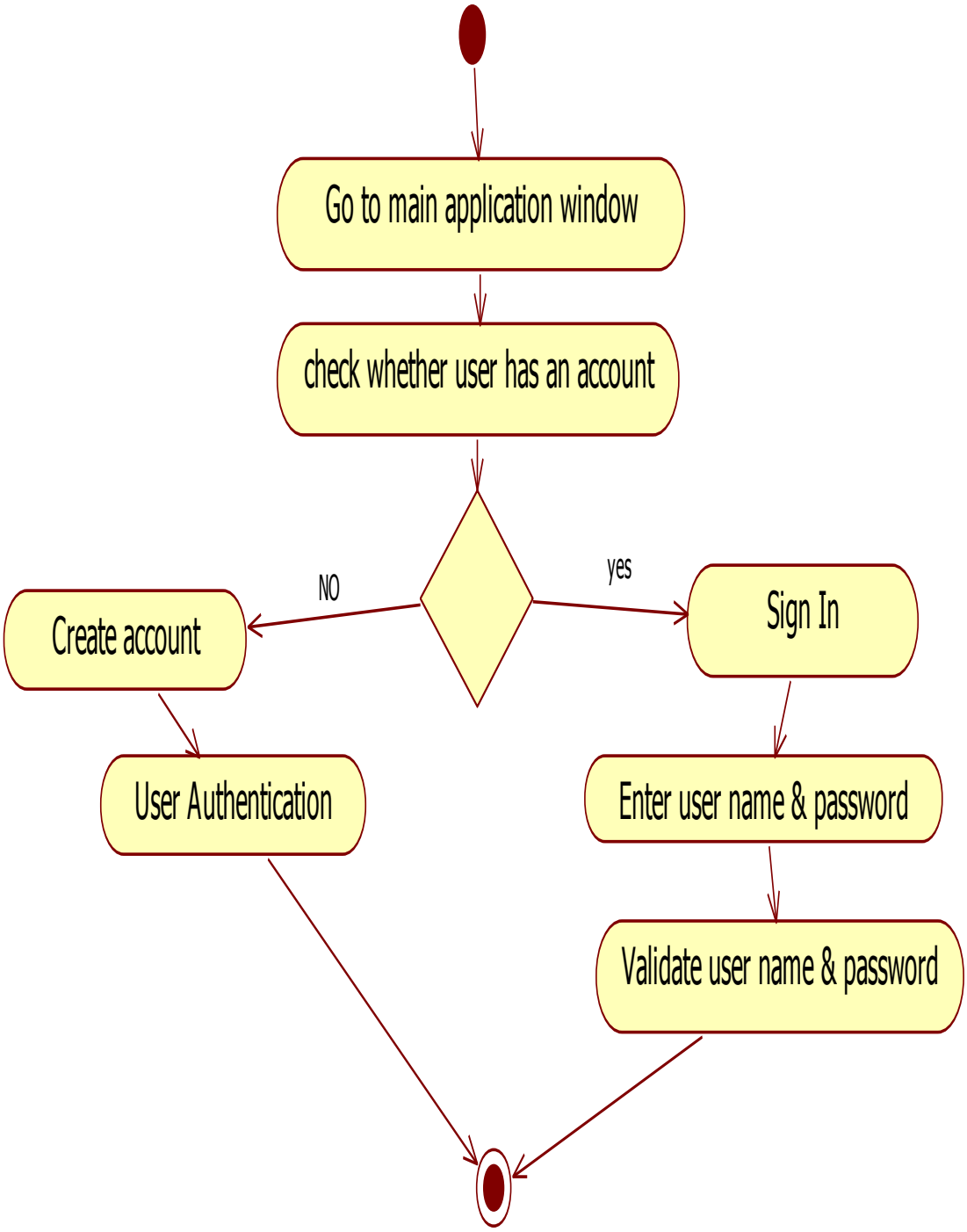


Figure 4.4.2 User Account Creation

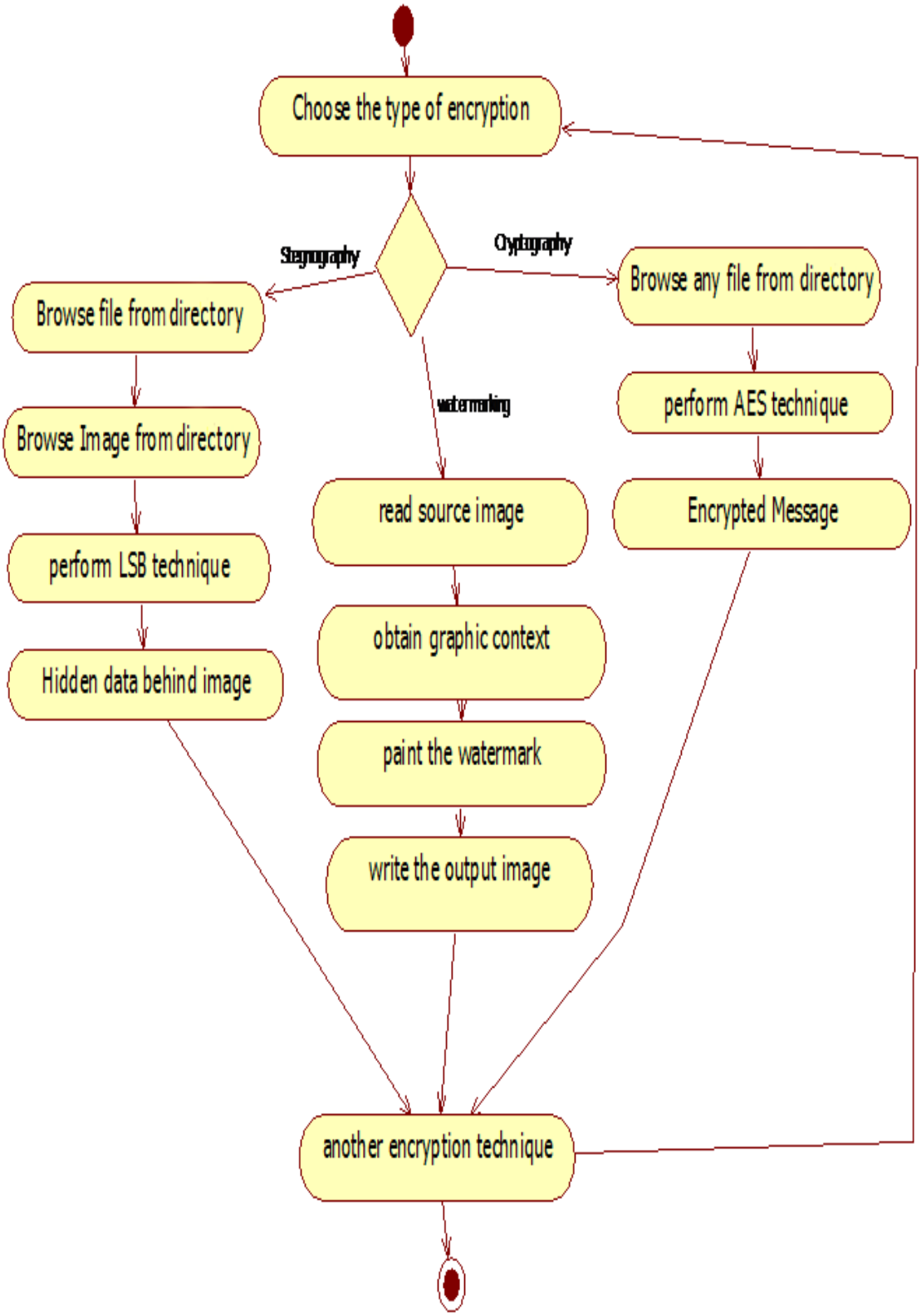


Figure 4.4.3 Encryption

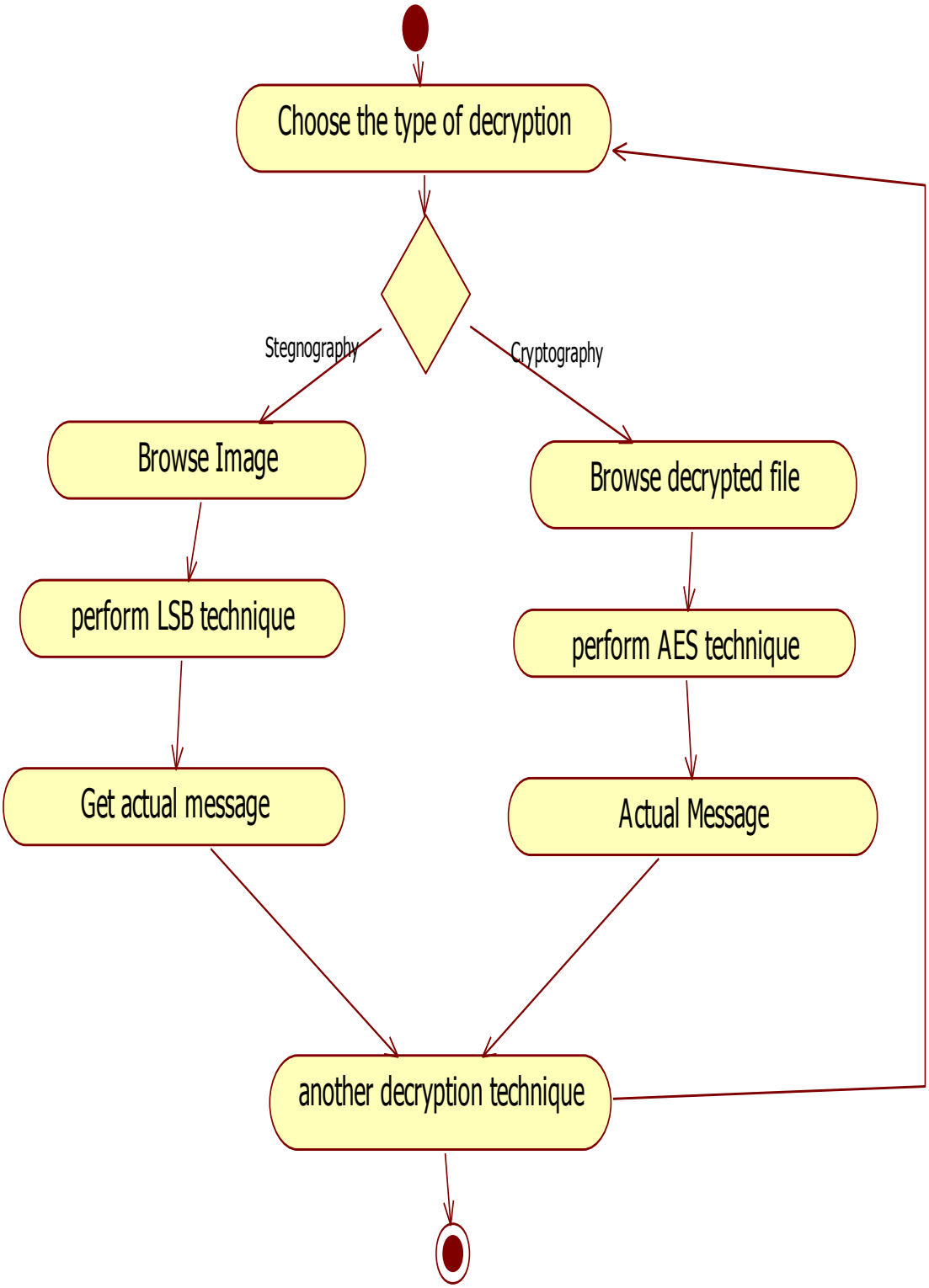


Figure 4.4.4 Decryption

### iii. Class Diagram

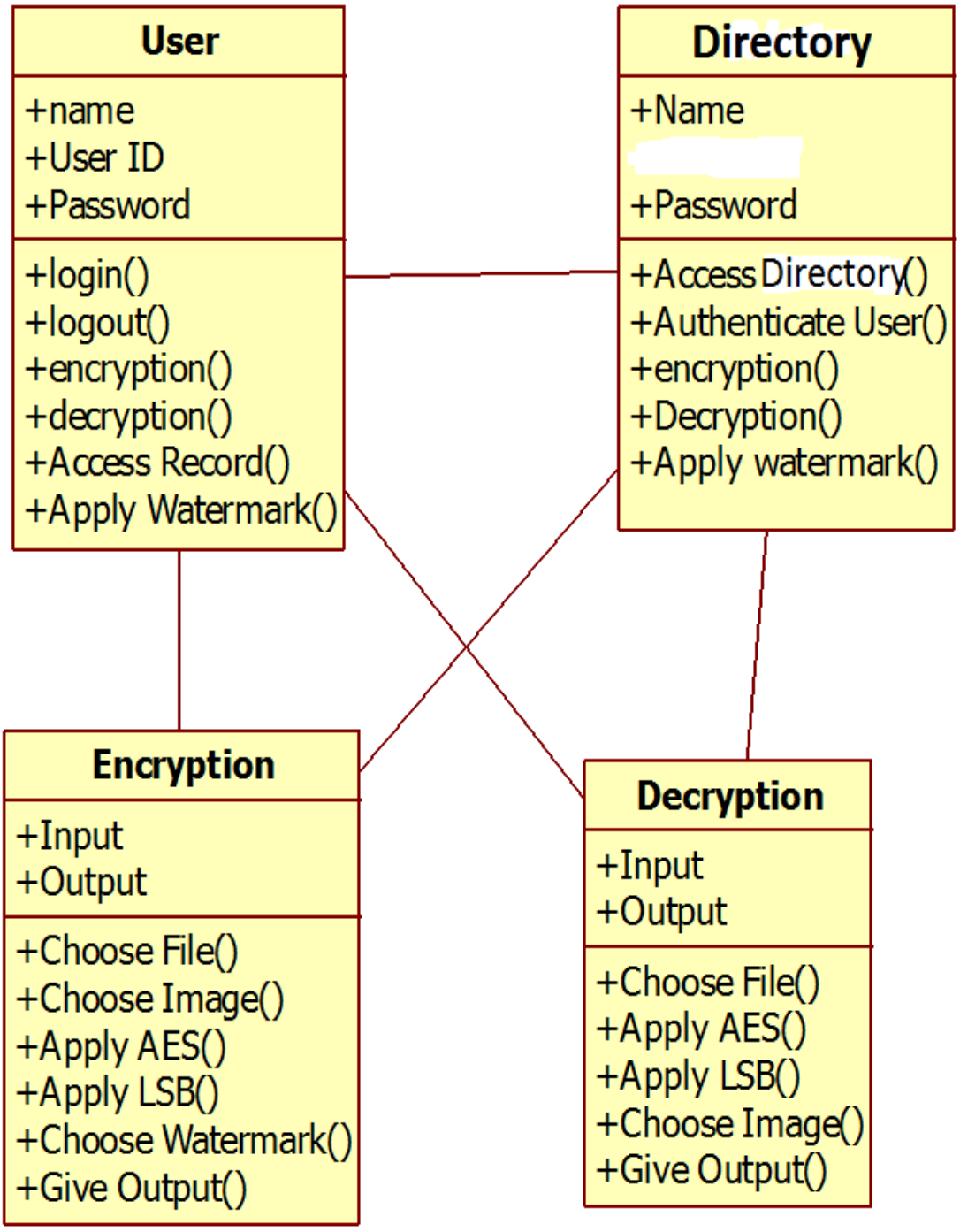


Figure 4.4.5 Class Diagram

### iv. Sequence Diagram

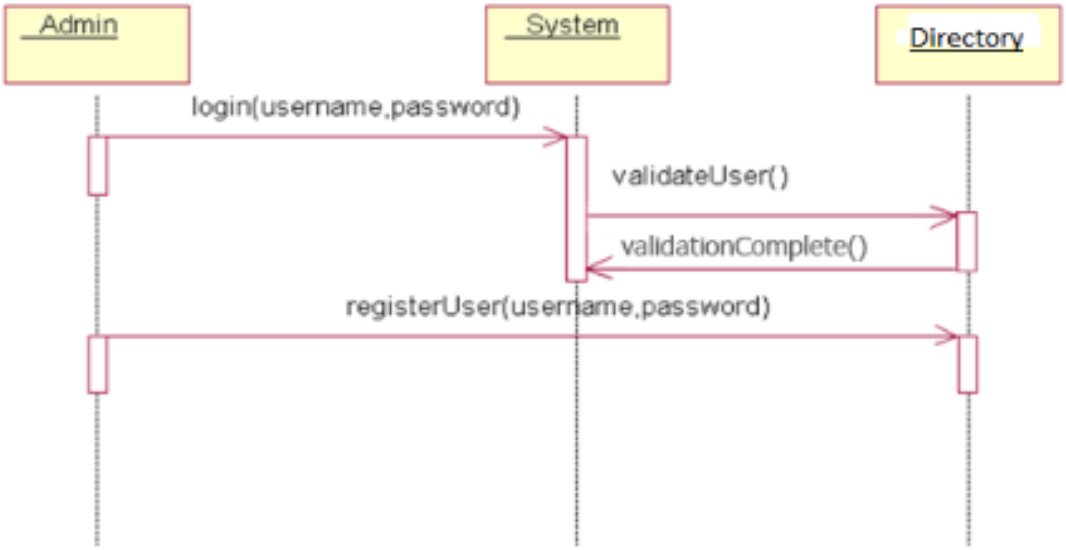


Figure 4.4.6 Add User

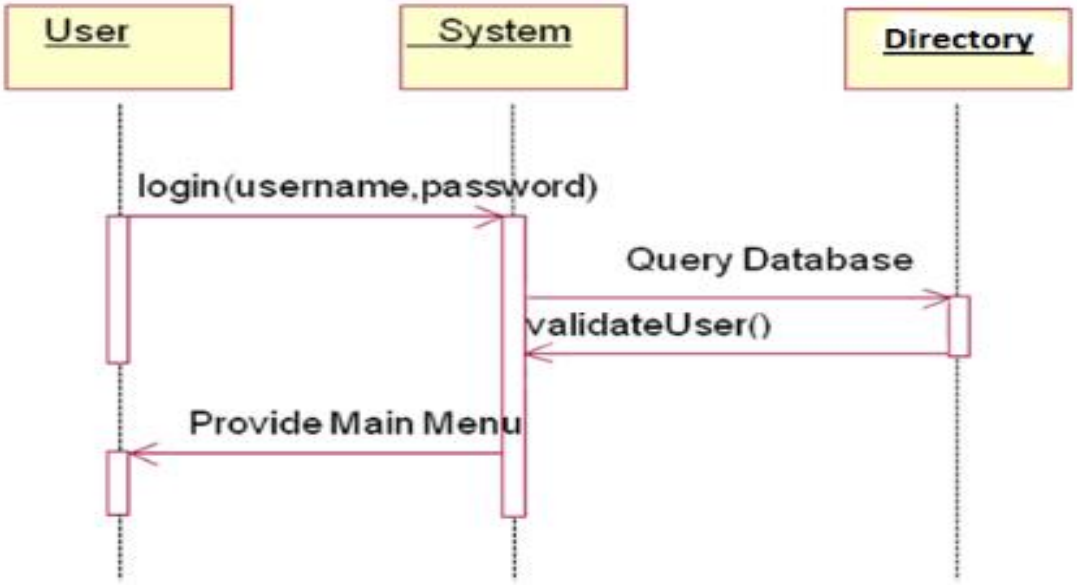


Figure 4.4.7 User Authentication

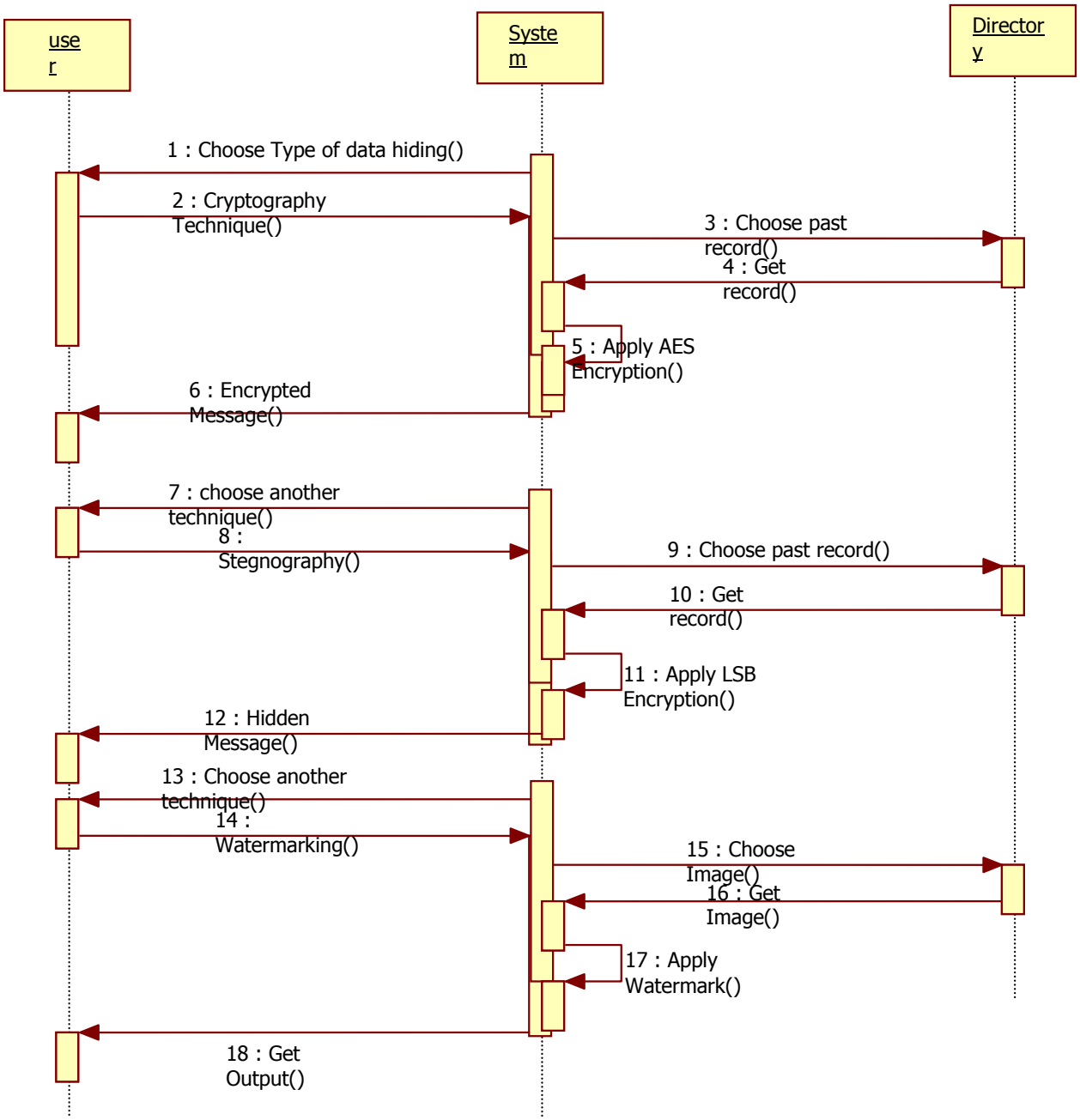


Figure 4.4.8 Encryption

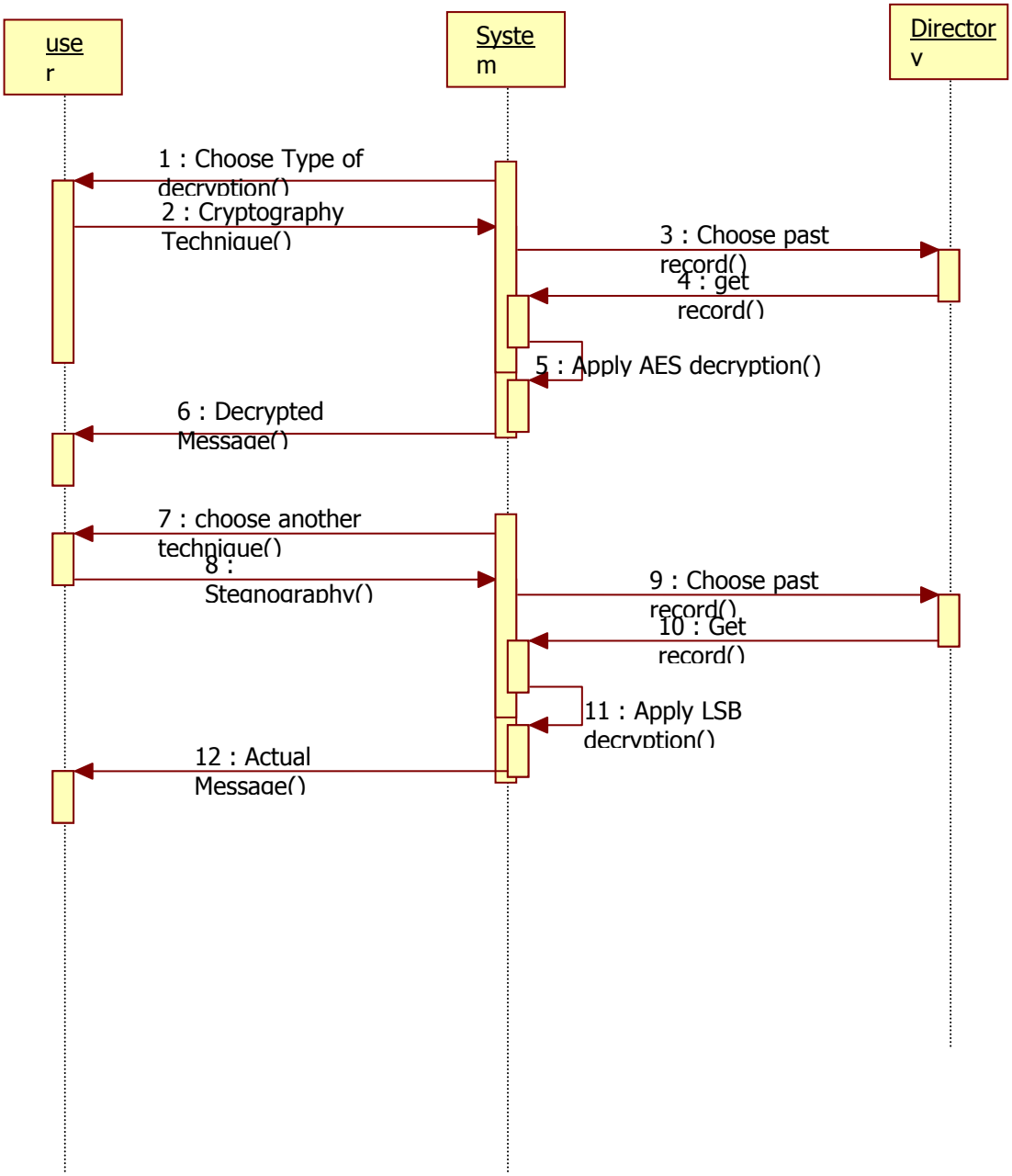


Figure 4.4.9 Decryption

### v. State Chart Diagram

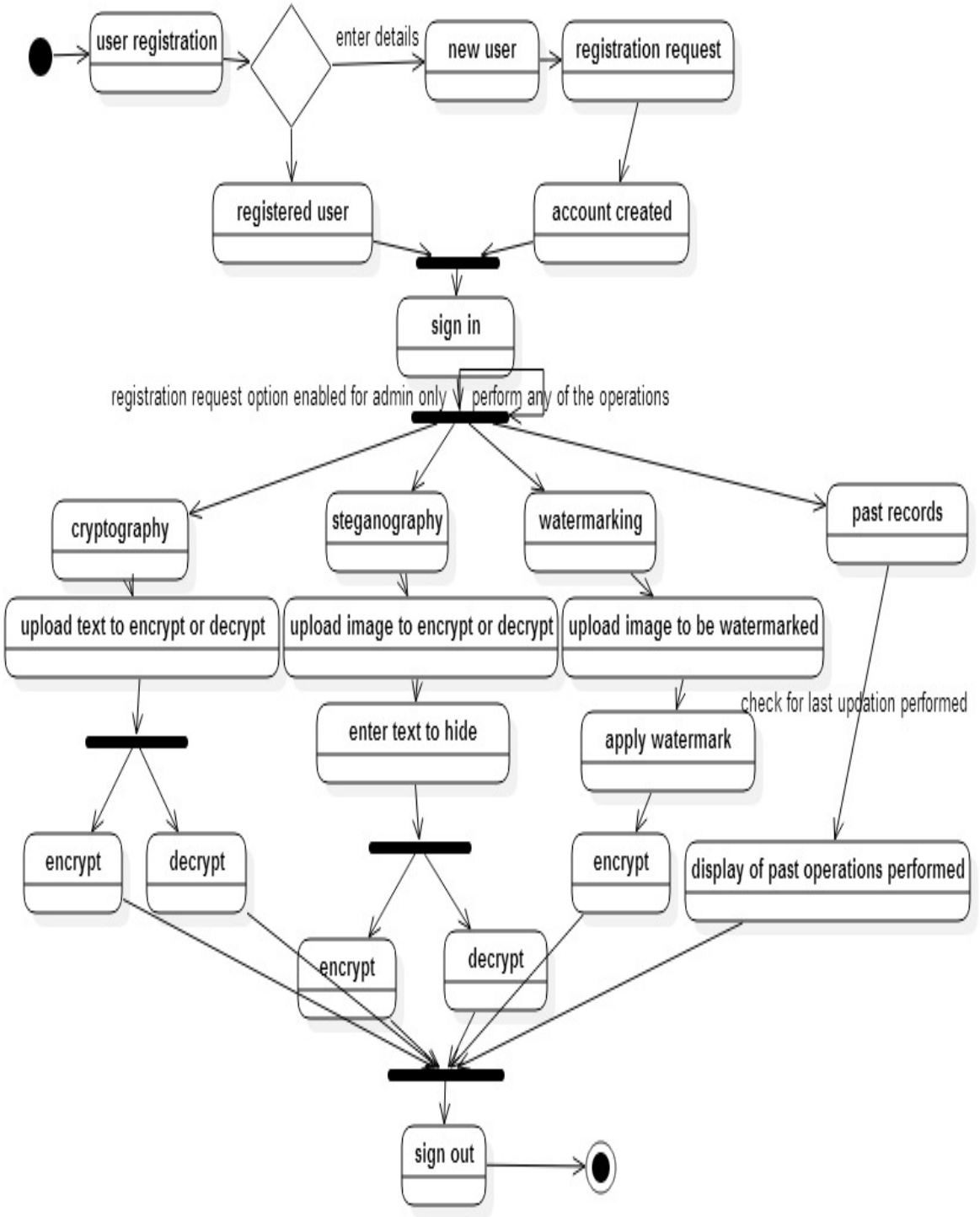


Figure 4.4.10 State Chart

CHAPTER 5

# RESULT ANALYSIS : SNAPSHOTS

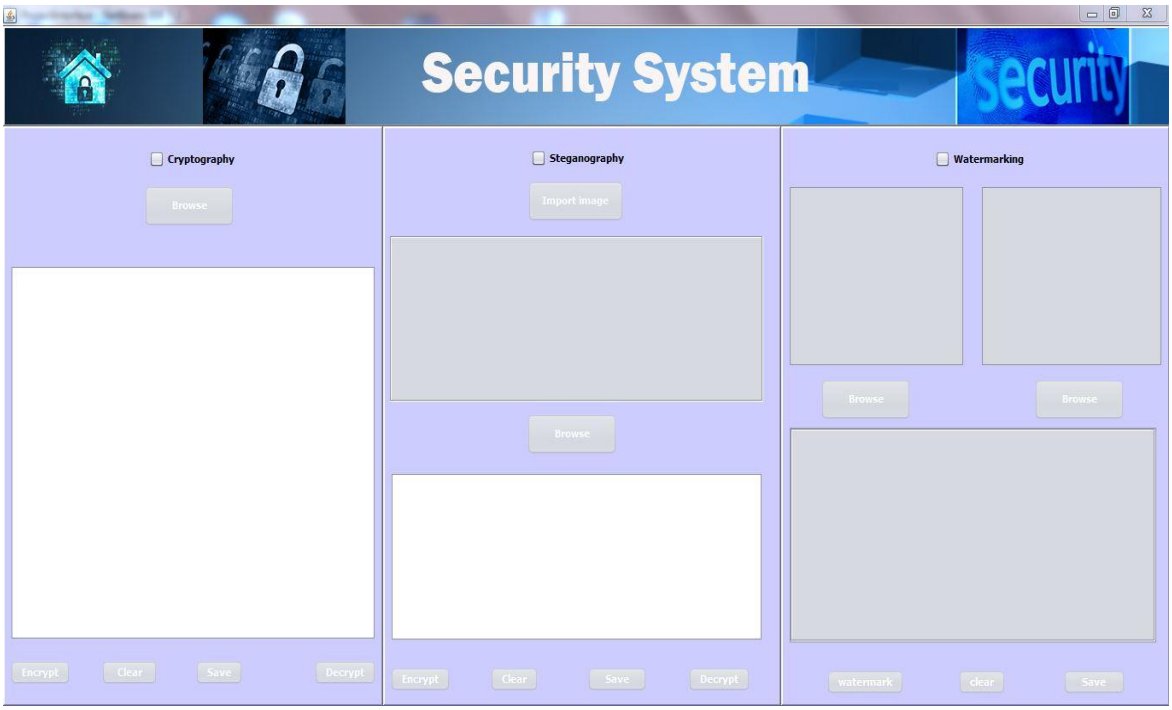


Figure 5.1 Opened output screen

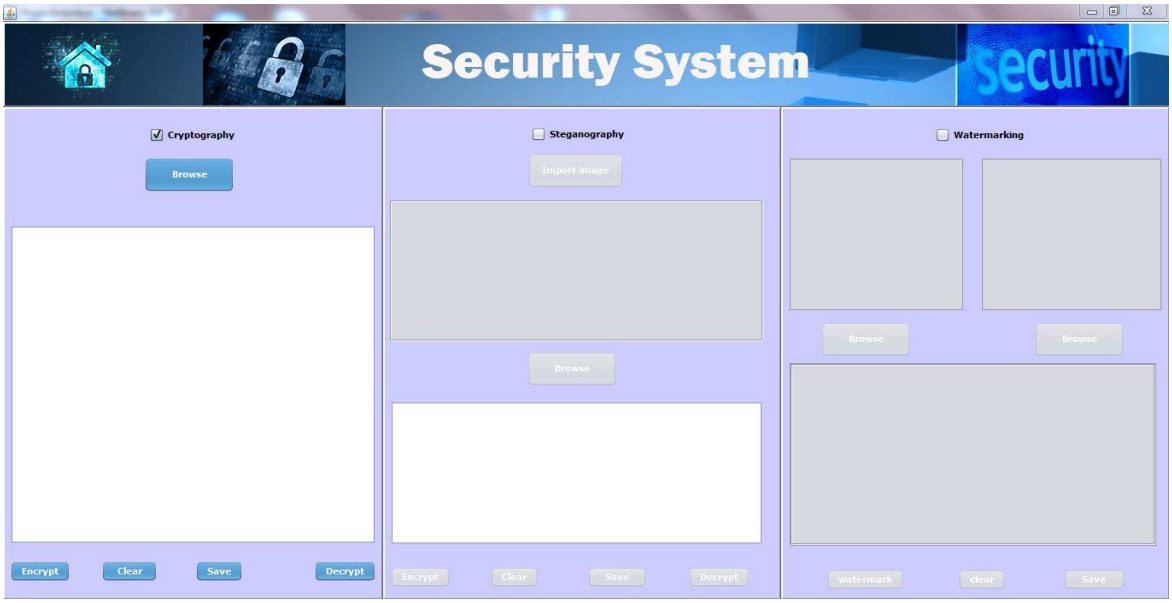


Figure 5.2 Cryptography selected

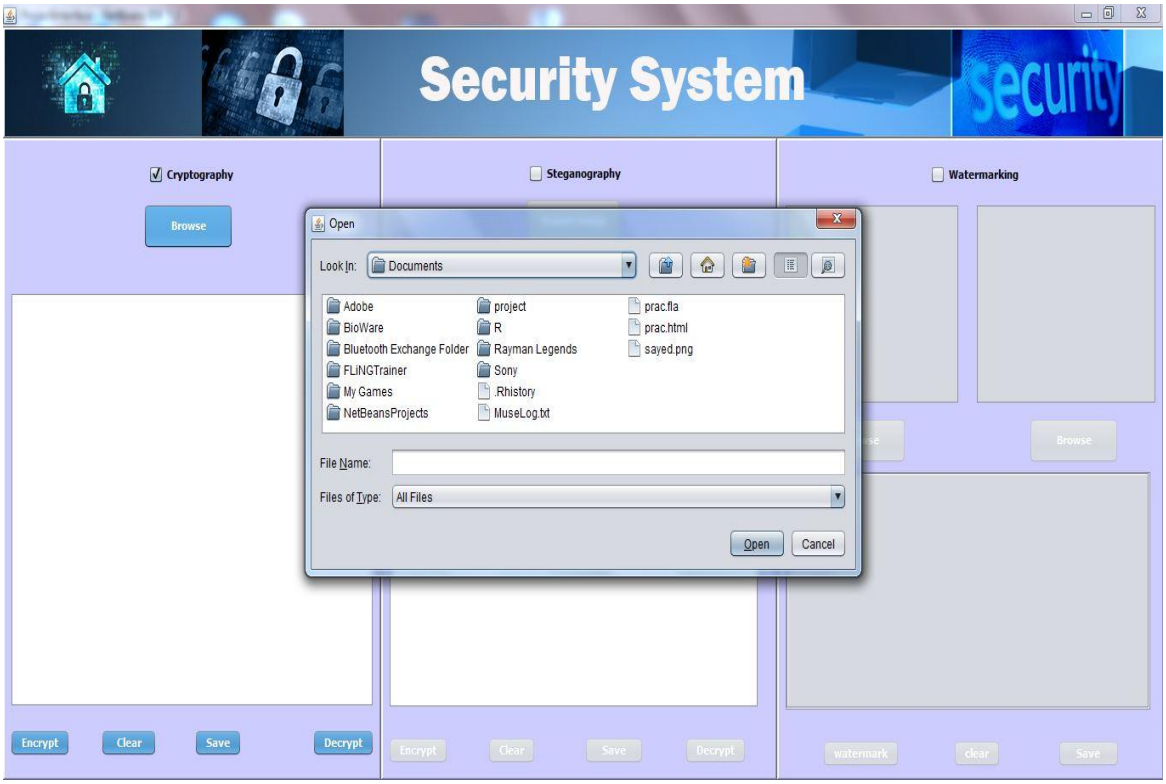


Figure 5.3 Browse a text file to encrypt

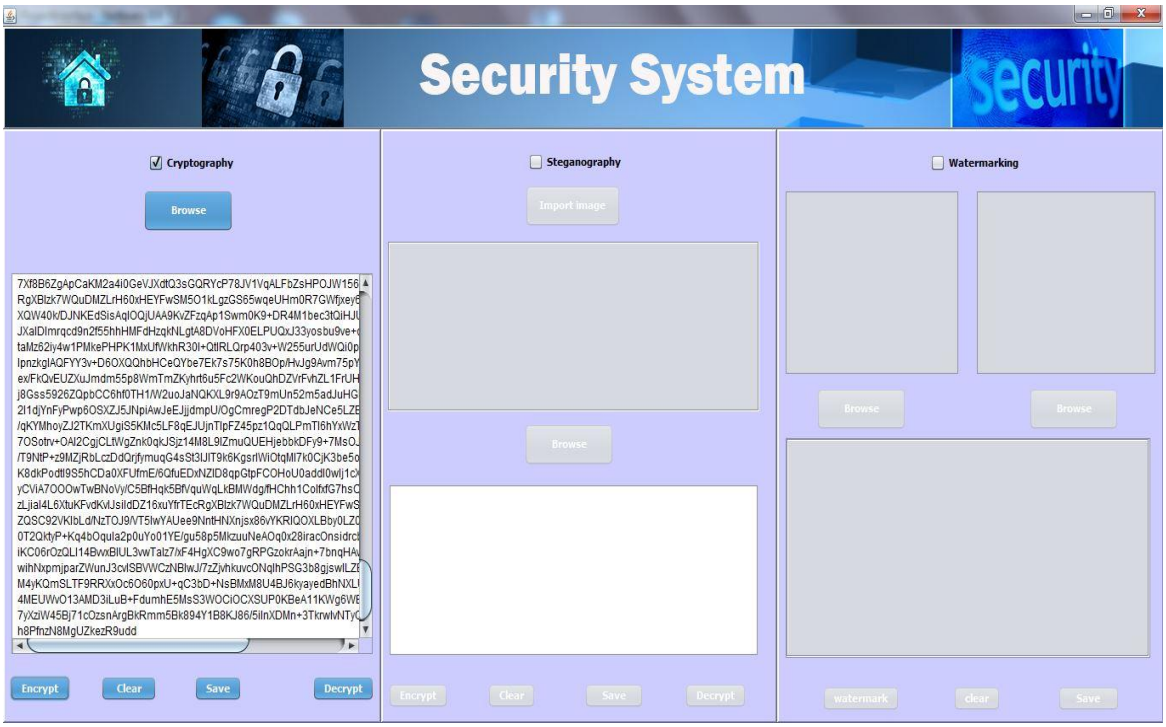


Figure 5.4 Encrypted text file

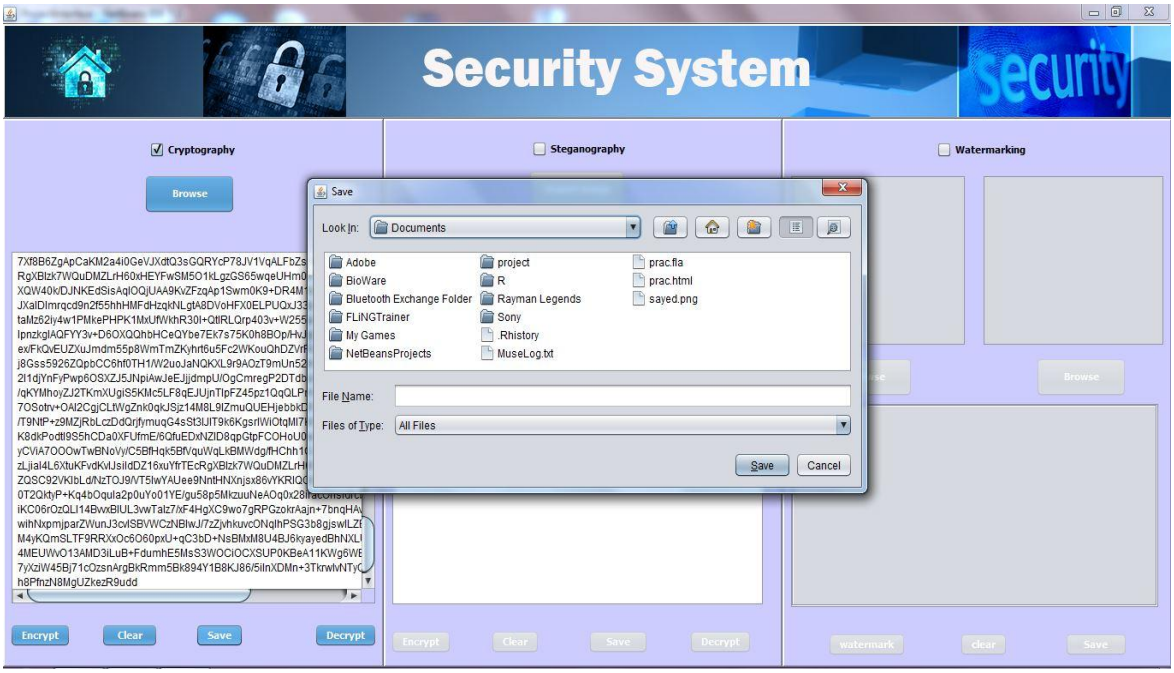


Figure 5.5 Save the encrypted text file

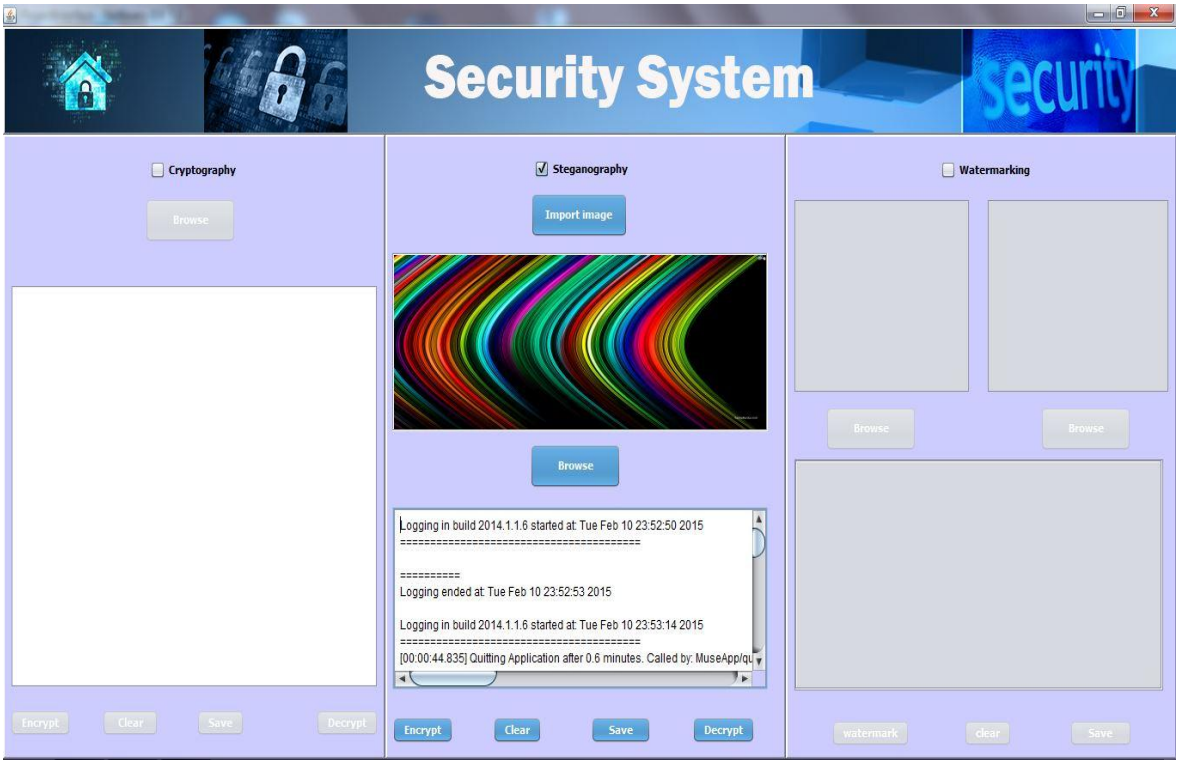


Figure 5.6 Browsing of text and image

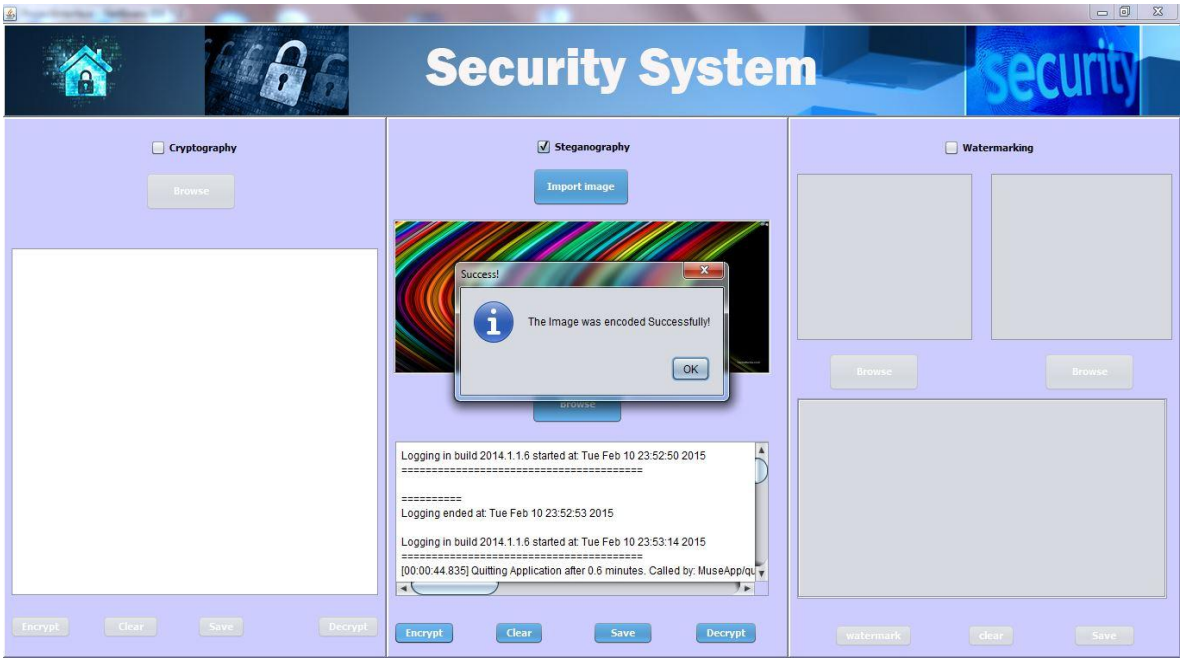


Figure 5.7 Hiding of text behind image

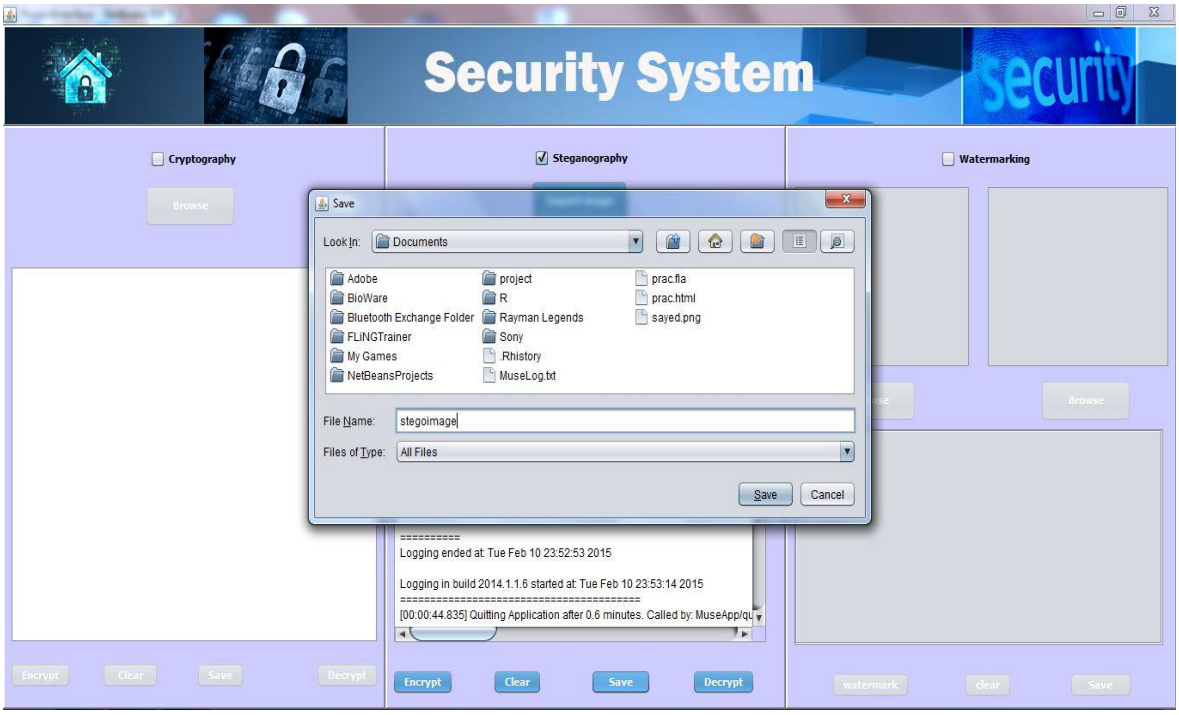


Figure 5.8 Saving of encoded image

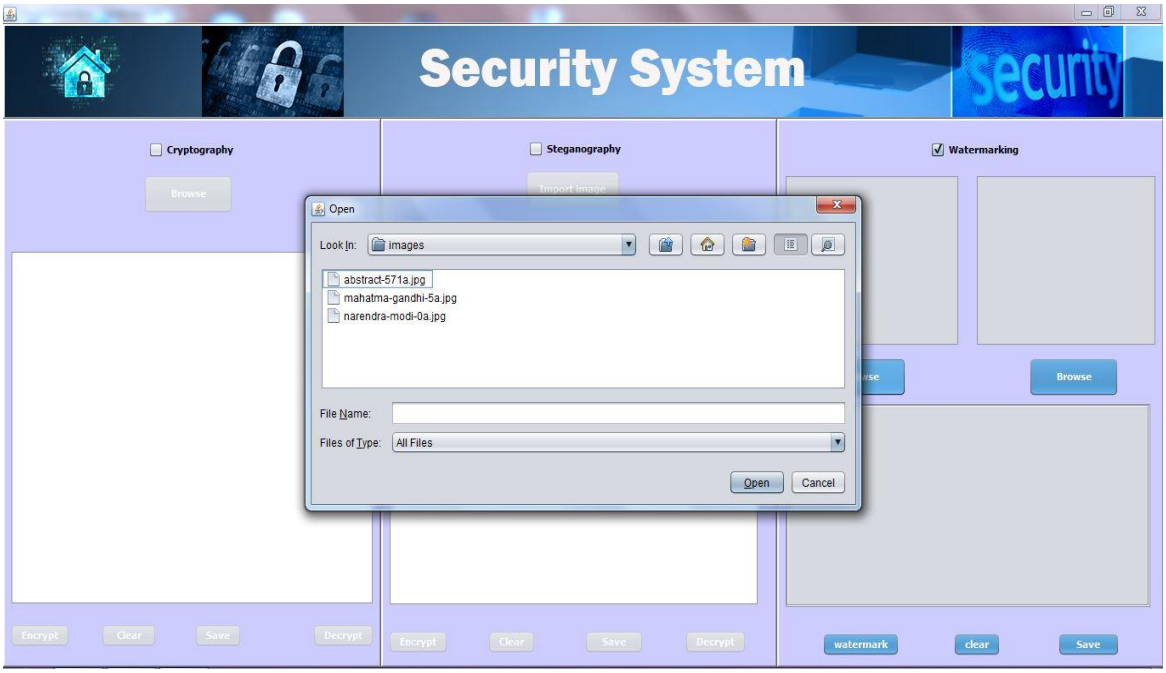


Figure 5.9 Browsing of original image

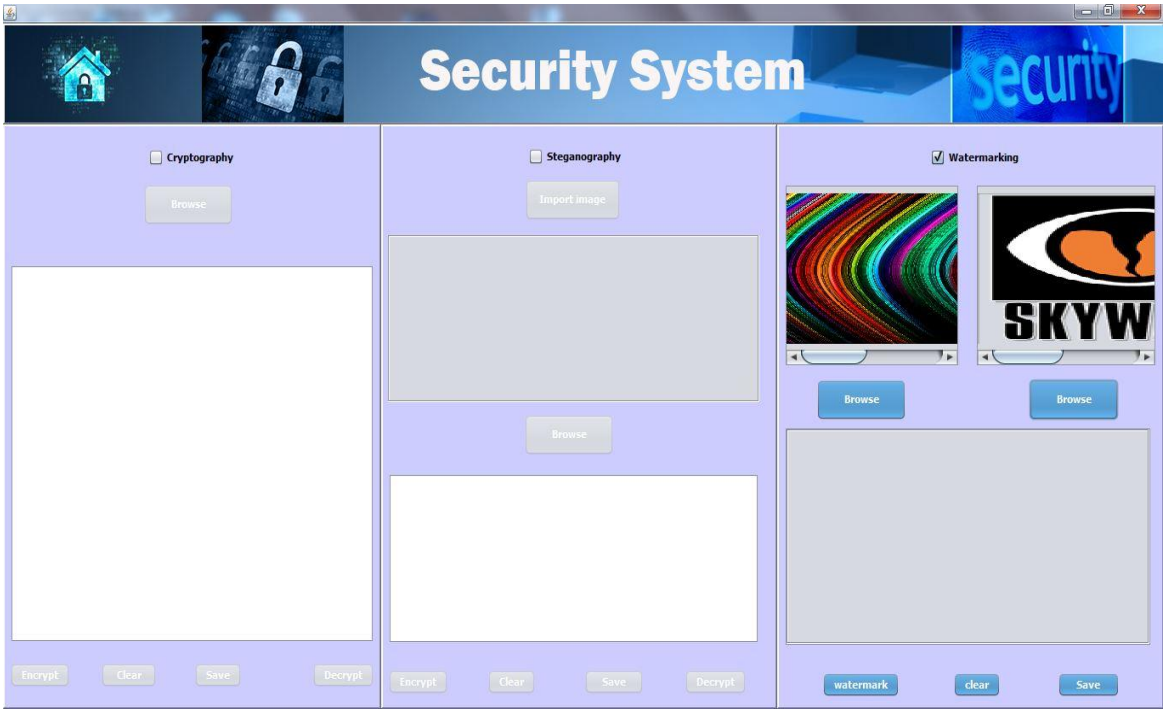


Figure 5.10 Browsing of image used for watermarking


Figure 5.11 Watermarking is performed

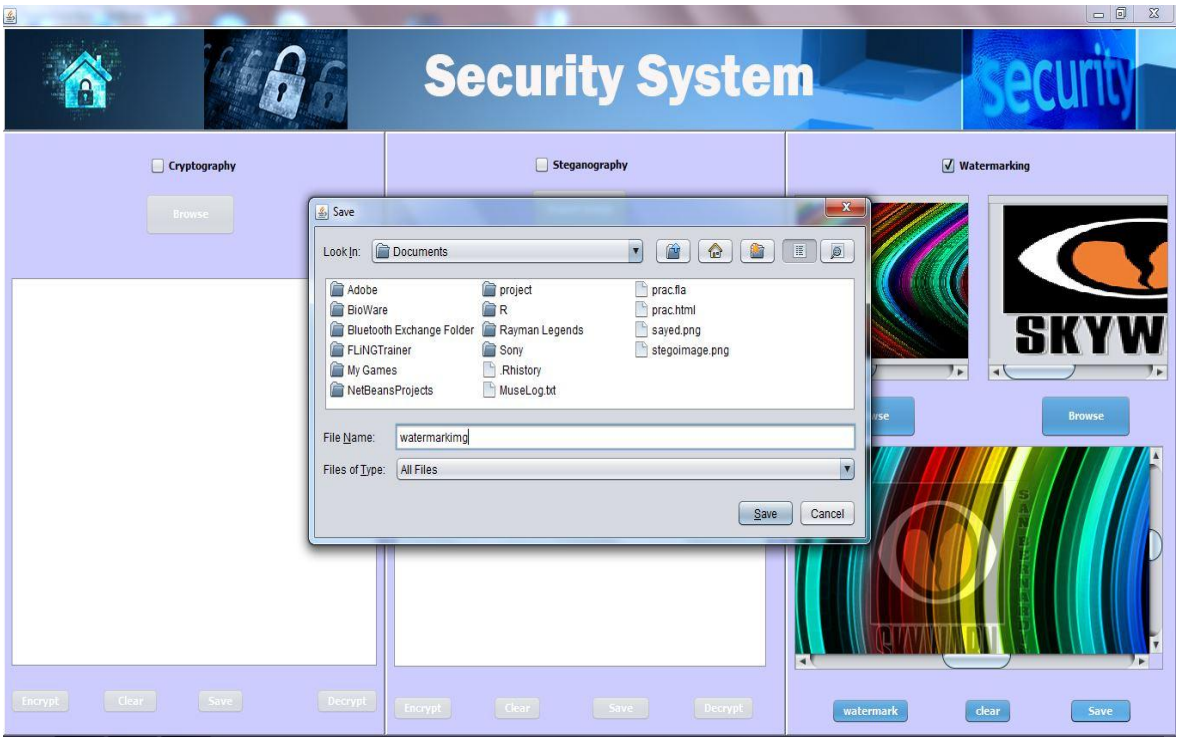


Figure 5.12 Save the watermarked image

CHAPTER 6

# TESTING

## 6.1 ACCEPTANCE TESTING

In engineering and its various sub disciplines, **acceptance testing** is a test conducted to determine if the requirements of specification or contract are met. It may involve chemical tests, physical tests, or performance tests.

In systems engineering it may involve black-box testing performed on a system (for example: a piece of software, lots of manufactured mechanical parts, or batches of chemical products) prior to its delivery.

Software developers often distinguish acceptance testing by the system provider from acceptance testing by the customer (the user or client) prior to accepting transfer of ownership. In the case of software, acceptance testing performed by the customer is known as user acceptance testing (UAT), end-user testing, site (acceptance) testing, or field (acceptance) testing.

The first step of testing of any application is acceptance testing in which we first define what we are making and the things mentioned below:

vi. Use cases – define what the user will do and the expected result/outcome.

vii. Non-functional requirements – define expectations for performance, upgrades, reliability, etc.)

viii. Target devices and OS versions – define what devices and OS versions the service shall work on

ix. The Acceptance Criteria will be used for the final User Acceptance Testing (UAT) below.

So we planned each and every point mentioned above before starting our project precisely. Our application will work on every windows system. Application will help all the users to use our application properly. Our application will never crash and will always work properly and robustly on each and every PC's.

## 6.2 INTEGERATION TESTING

**Integration testing** (sometimes called **integration and testing**, abbreviated **I&T**) is the phase in software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before validation testing. Integration testing takes as its input modules that have been unit tested, 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.

Integration testing is usually performed as soon as access to all the modules at the same time are available. Integration testing ensures that all modules such as cryptography, steganography and watermarking work as expected, that all areas of the system communicate with each other correctly and that there are no gaps in the data flow. The final integration test proves that the system works as an integrated unit when all the fixes are complete.

In this testing we integrated each and every module with each other. At the end we got a whole application we required.

## 6.3 USER ACCEPTANCE TESTING (UAT)

Finally the service is ready to go live, but before this there is one final step. The customer (external or internal) of the project goes through the Acceptance Criteria one final time to ensure that the agreed minimum criteria are met. Depending on the preparations prior to this it can be a formality or it can go on for months with additional iterations with development and testing above. Once the UAT is completed the service is ready to go live.

In this we take our application on one user personal computer and asked him to run the application. Then the application will be of system's administrator and then he has to open the application in the netbeans ide. After opening the application he will see the GUI with three different parts such as "Cryptography" ,"Steganography",and "Watermarking" , there is a checkbox in front of every field which are set disabled and to be selected by user randomly any box and any operation. The checkbox is for selecting the fields for encryption and decryption. We have provided both the

encryption and decryption facility to the user so that the user can choose whether to encrypt or decrypt the data(text/image) as shown in Screenshot. Now after selecting the required checkbox by user then he/she has to select the data whether text file or an image file according to the technique selected. After the completion of the process user has to click on save button to save the application according to the user mentioned place for further use of that data. Now user has to go through another technique and browse the file either encrypted with previous technique or a fresh file to work on and perform the operation related to encryption and similarly for decryption. By clicking on encrypt button user will be able to encrypt the required file and similarly by clicking the decrypt button he will be able to decrypt the encrypted file and get the original file. So the application works perfectly fine and our application is now ready to get deployed.

CHAPTER 7

# CONCLUSION AND FUTURE WORK

## 7.1 Conclusion

Steganography, especially combined with cryptography and watermarking is a powerful tool which enables people to keep their information secure without interruption of possible eavesdroppers and increase the level of security. The main advantage of this System is to provide high security for sensitive information and providing three layer of security by addressing loss of integrity, loss of confidentiality and unauthorized sender.

## 7.2 Future Work

In future we would like to work more on AES 256 to include features like providing more security for the data, implement audio and video steganography in the application and address Authentication problem in this application. Furthermore, we would like to make our application work on client-server platform rather than single standalone system and to work on decryption of the watermark images.

# REFERENCES

[1]. B. P Fitzmann, “Trials of traced traitors.” Information hiding, first international work shop, Lecture notes in computer science R. Anderson, Ed. Berlin, Germany: Springer Verlag 1996, vol. 1, pp= 49-64.

[2]. K. Tanaka, Y. Nakamura and K. Matsui, “Embedding Secret Information in to a Dithered Multi Level Image,” in Proc IEEE Military communications conf., Monterey, CA, 1990, pp-

[3]. Neil F. Johnson and sushil Jajodia Exploring Steganography: seeing the unseen IEEE computer, 31(2) 26-34, 1998.

[4]. N. Proros and P. Honeyman. “Hide and seek: An Introduction to Steganography “, IEEE: security & Privacy, vol. 10, pp. 32-44, 2003.

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

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

[7] M. Ramkumar & A.N. Akansu. “Some Design Issues For Robust Data hiding Systems”, http://citeseer.nj.nec.com/404009.html.

[8] N.F. Johnson, S. Jajodia, “Staganalysis: The Investigation of Hiding Information”, IEEE, pp. 113-116, 1998.

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

[10] Ahsan, K. & Kundur, D.(2002). Practical Data Hiding in TCP/IP. Proceedings of the Workshop on Multimedia Security at ACM Multimedia.

[11] Naor .M and Pinkas .B (1997), “Visual authentication and identification,” in Proc. CRYPTO’97, vol. 1294, pp. 322–336, Springer-Vela LNCS.

[12] Nakajima .M and Yamaguchi .Y (2002), “Extended visual cryptography for natural images,” in Proc. WSCG Conference pp. 303–412.