

# Hiding Information within Picture



Project Advisor: Dr. Rafi Ullah Habib

Presented by:

Student Name	Number
Hamad Ali al name	342101728

**College of Science**

## Table of Contents:

### Chapter 1.....

#### 1.1 Abstract

#### 1.2 Introduction

### Chapter2.....

#### 2.1.Literature review

#### 2.2 Acknowledgements

### Chapter3.....

#### 3.1 implementation

### Chapter4.....

#### 4.1 Results

#### 4.2 Different techniques

#### 4.3Project Plan

### Chapter5.....

#### 5.1 List of Figures

#### 5.2 block diagrm

#### 5.3 use case digram

#### 5.4 Context Digram

#### 5.5 Class diagram

#### 5.6 Sequence diagram for admin

#### 5.7 Sequence diagram for USER

#### 5.9 deployment diagram

#### 5.10 Acteve daigrm

#### 5.11 State Diagram

## 1.1 Abstract

Steganography is the popular security method that provides complete security for Communicating secret details. Image steganography is a very interesting field because of The imperceptible way of hiding data in images, since small distortion in the images Cannot be identified by a human eye. This is the main idea to develop image Steganography algorithms for secure communication..

Because some of the information and data bear the stamp of secrecy, hoping people at all levels, both companies and government institutions to find appropriate solutions to provide a secure and confidential data being transferred, either on the Internet or on a different level and means of data transfer, such as flash memory.

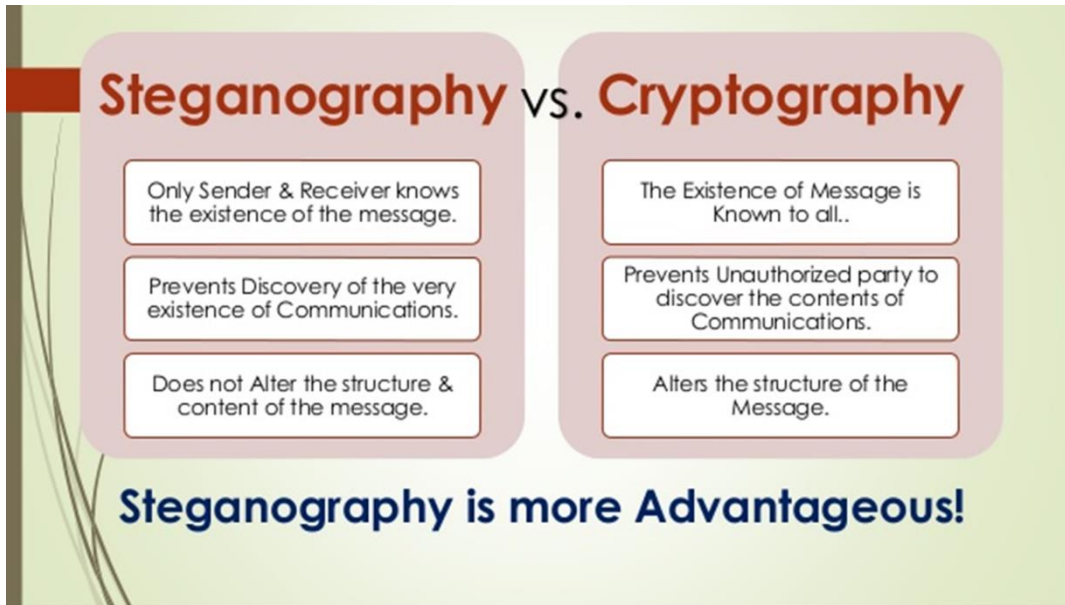
From this point I was born the idea to work on this project to provide confidentiality and protection for all correspondence exchanged between the Different areas of interested

## 1.2 Introduction

Steganography simply takes one piece of information and hides it within another.[1, 2] Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend. A recording of a short sentence might contain your company's plans for a secret new product. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

## 2.1.Literature review



{1} Cryptography and Steganography. Since the advent of computers there has been a vast dissemination of information, some of which needs to be kept private, some of which doesn't. The information may be hidden in two basic ways (Cryptography and Steganography). The methods of Cryptography does not conceal the presence of secret information but render it unintelligible to outsider by various transformations of the information that is to be put into secret form, while methods of Steganography conceal the very existence of the secret information. The following table has shown the comparison between Cryptography and Steganography (Al-Dieimy, 2002; D2000).

## REFERENCES

[1] Anas Majed Hamid, Miss Laiha Mat Kiah, Hayan .T. Madhloom, B.B Zaidan, A.A Zaidan, " Cryptography and Steganography", International Journal of Engineering and Technology (IJET) , Published by: Engg Journals Publications, ISSN:0975-4042, Vol.1,NO.2,P.P 63.

## 2.2 Acknowledgements

I have to plan for my project because I studying at the university and try to Overcoming the problems that affect information security, where we are Some secret sections miss when transferring data and many other problems Affects data security when transferred from one location to another. So I am I decided to design a program to hide the text inside the images is trying to me Overcome this problem after the system began to analyze all and put the audience Visualization of it.

### 3.1 implementation

- **Algorithms:**
- **LSB:**

#### Algorithm to embed text message:

Step 1: Read the cover image and text message which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixels of cover image.

Step 4: Replace LSB of cover image with each bit of secret message one by one.

Step 5: Write stego image.

#### Algorithm to retrieve text message:

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixels of stego image.

Step 3: Retrieve bits and convert each 8 bit into character.

Step 6: Calculate LSB of each DCT coefficient.

Step 7: Retrieve and convert each 8 bit into character

## 4.1 Results

- The objective of the project is to hiding the text within the image and returned it in an easy way for allowed people only. Other projects do not have a database for keeping those images hiding so this making it difficult summoned and storing in a database, but my project will create its database. All hiding text in images are saved within the database. The images can be decrypted only password
- I have to plan for my project because I study at university and try to overcome the problems that affect the security of information, where we miss some secret passages when transferring data and many other problems that affect the security of the data when transferring how to find the start of adventure in com move. So I decided to design a program to hide the text inside the images is my attempt to overcome this problem after the system began to analyze everything and visualize the audience it.

## 4.2 Different techniques:

### a) Digital Steganography:

Modern steganography entered the world in 1985 with the advent of the personal computer being applied to classical steganography problems. Development following that was slow, but has since taken off, going by the number of "stego" programs available. Digital steganography techniques include:

- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within Hiding data or within random data. The data to be concealed is first Hiding before being used to overwrite part of a much larger block of Hiding data or a block of random data (an unbreakable cipher like the one-time pad generates cipher texts that look perfectly random if you don't have the private key).
- Chaffing and winnowing.
- Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a cipher text-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in key presses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Changing the order of elements in a set.
- Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.
- Blog-Steganography. Messages are fractionalized and the (Hiding ) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.
- Modifying the echo of a sound file (Echo Steganography).
- Secure Steganography for Audio Signals.
- Image bit-plane complexity segmentation steganography

## 4.3Project Plan

--

## References

[http://www.programmer2programmer.net/live\\_projects/project\\_7/steganography.aspx](http://www.programmer2programmer.net/live_projects/project_7/steganography.aspx)

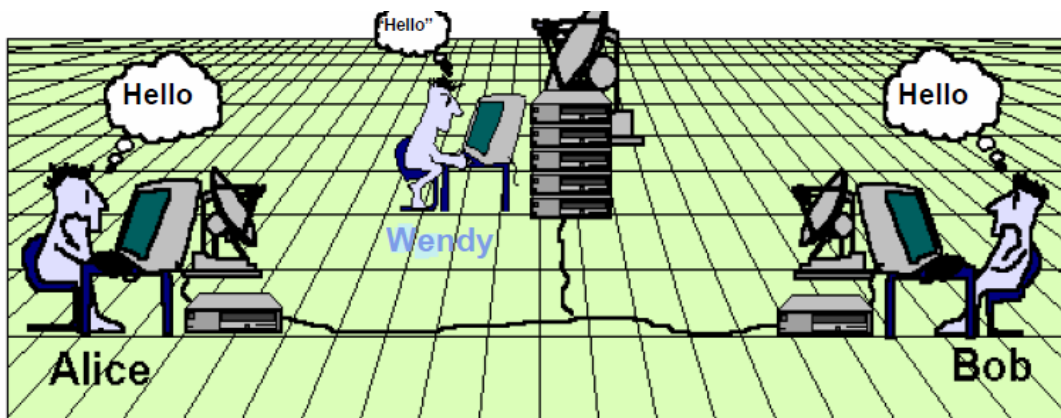
[www.slideshare.net](http://www.slideshare.net)

IEEE Paper titled: “A steganography implementation” by Mehboob, Faruqi.

<http://www.peterindia.net/SteganographyLinks.html>

Paper titled “Information Security through Image Steganography” by Nani Koduri M.S. in Information Security and Computer Forensic.

## 5.1 List of Figures



Modern Steganography the presoner's

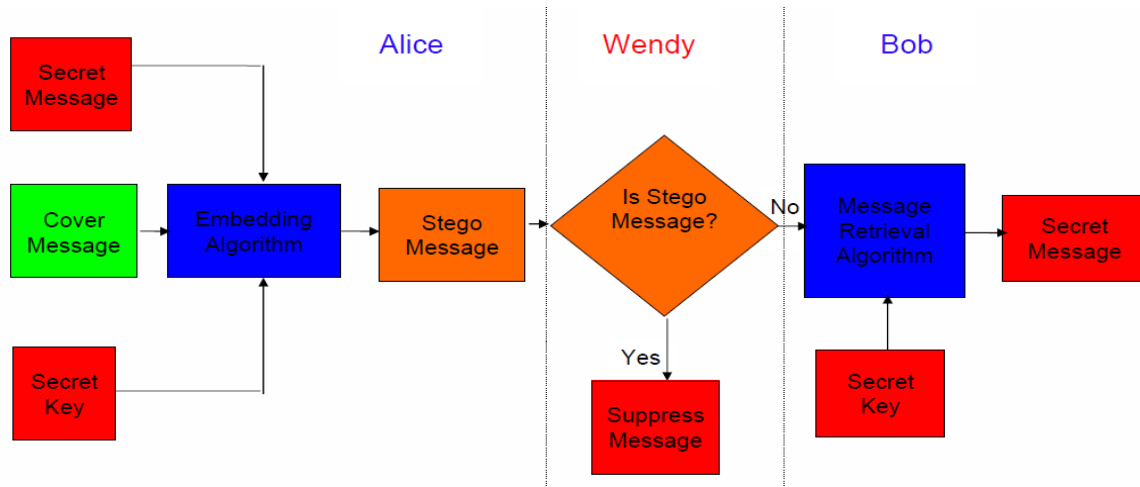
### Problem:

Alice and Bob are communicating with each other using secret message exchanging.

## 5.2 Block Diagram

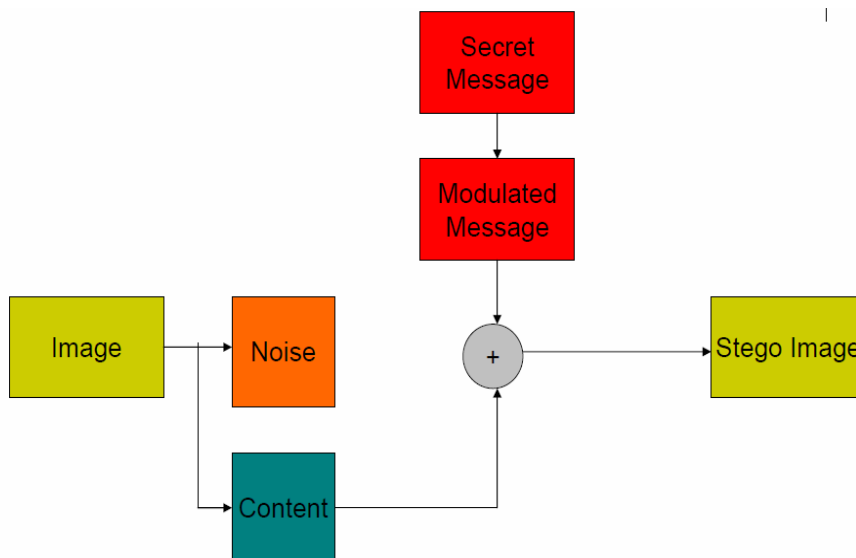


## Hiding information within Picture



Block Diagram

## Steganography in practice:

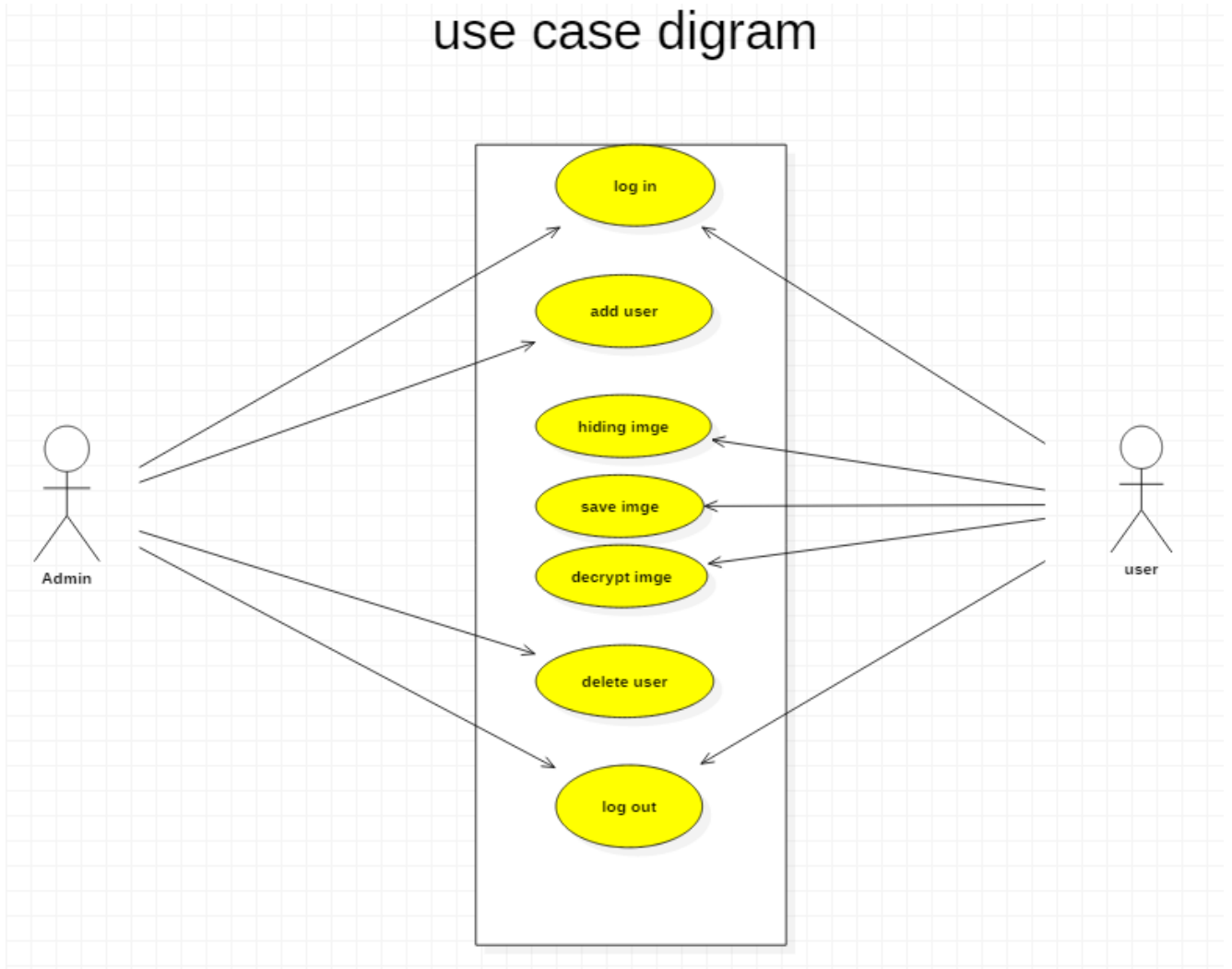


Steganography in practice

.

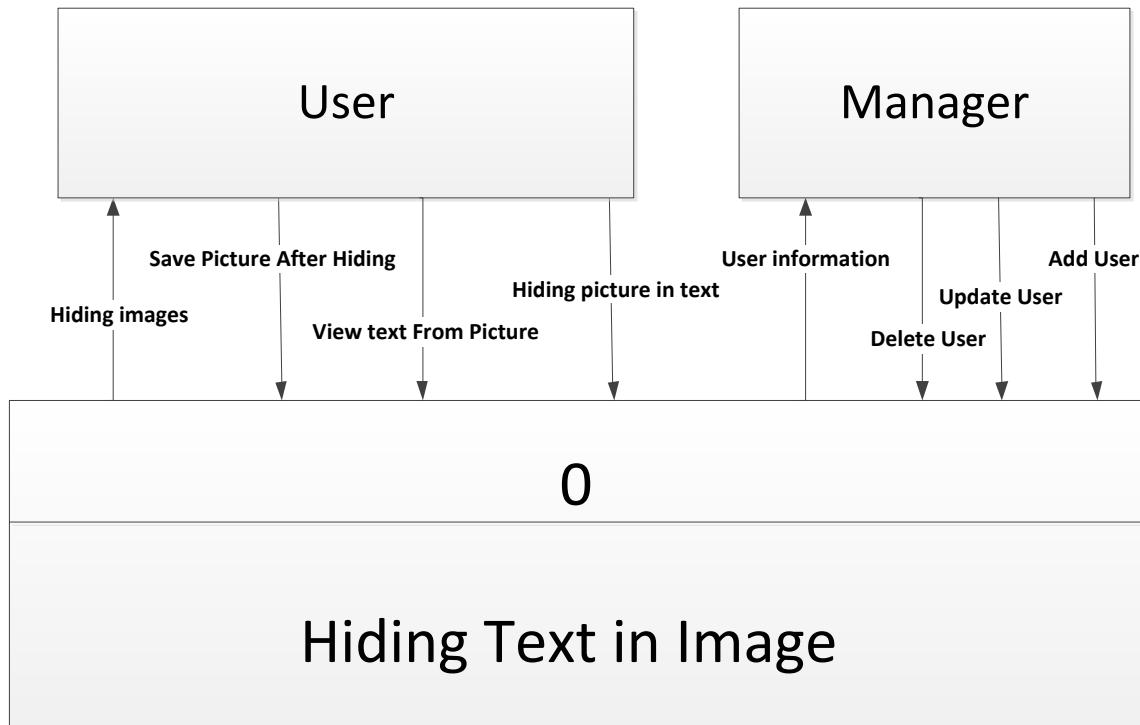
## **5.3 Use case**

## use case digram



## 5.4 Context Diagram

### Context Diagram



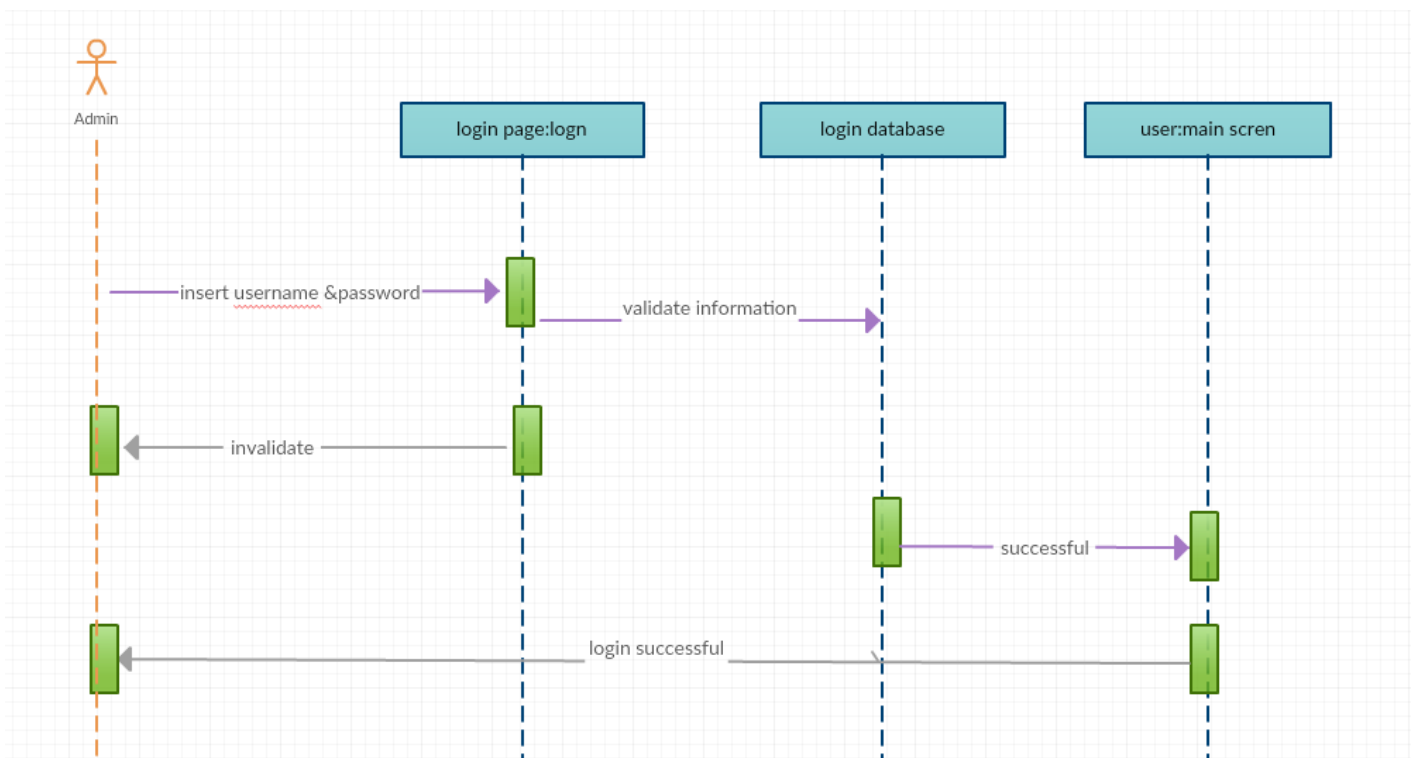
## 5.5 Class diagram

a **class diagram** in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.

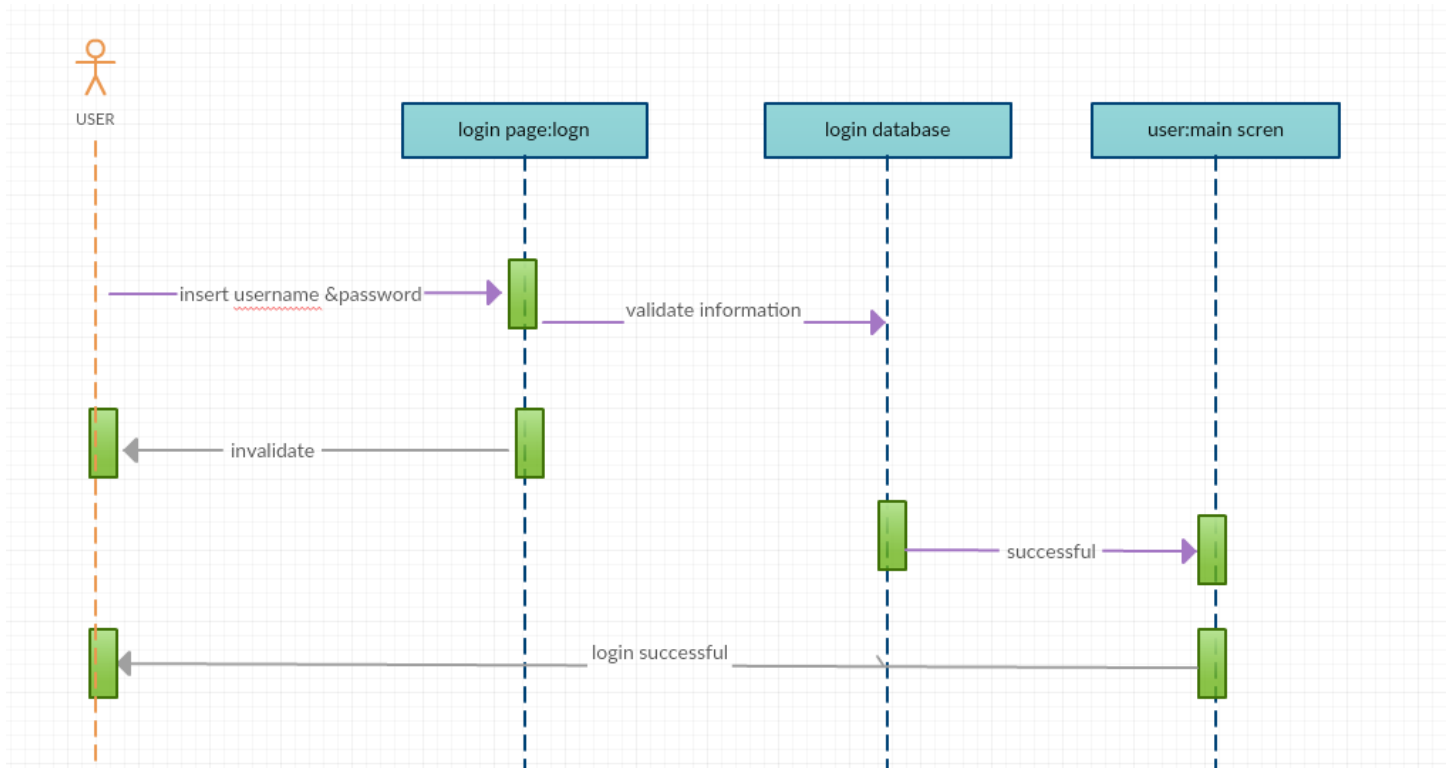
# Class Diagram



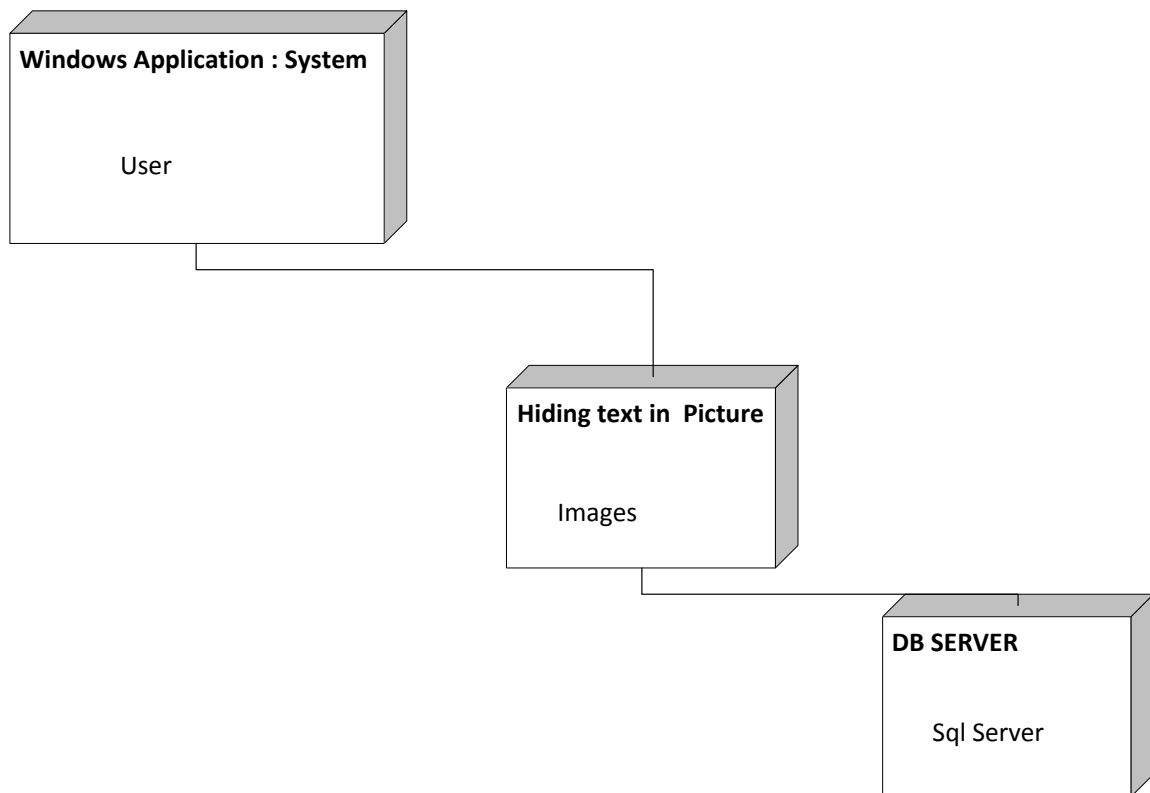
## 5.6 Sequence diagram for admin



## 5.7 Sequence diagram for USER

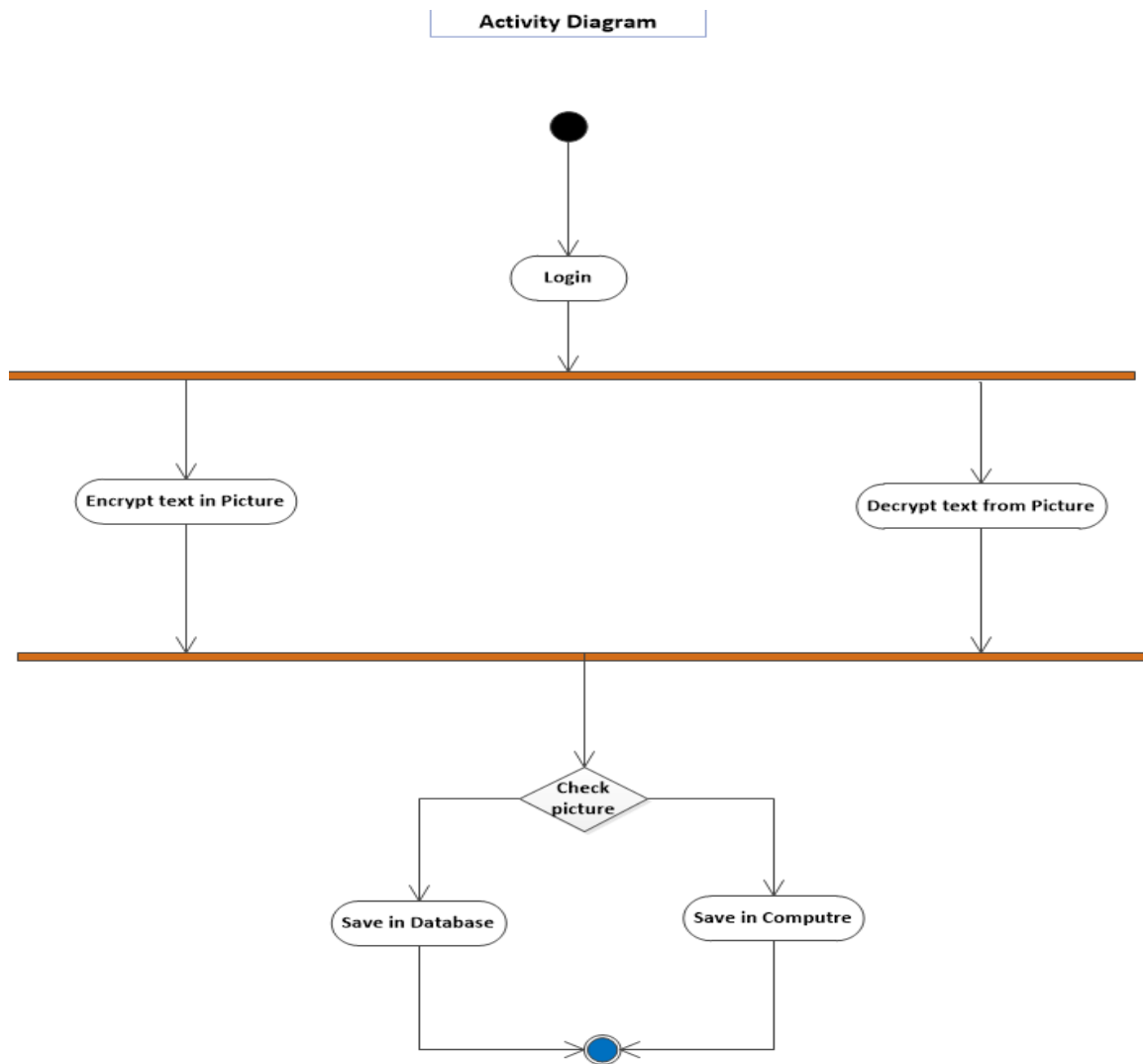


## 5.10 deployment diagram





## 5.11 Activity diagram



## 5.11 State Diagram

