A PROJECT REPORT

ON

“Image Encryption and Decryption”

IN PARTIAL FULFILLENT OF THE REQUIRMENT

OF THE AWARD OF THE DIPLOMA

IN

COMPUTER ENGINEERING

SUBMITTED BY

1.Miss. Unde P.S.	**(1811640007)**
2.Miss. Haral S.S.	**(1811640009)**
3.Miss. Dabekar R.R.	**(1911640151)**
4. Miss. Phapale S.B.	**(1911640144)**

UNDER THE GUIDANCE OF

Prof.Shinde D.D.

MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION

DEPARTMENT OF COMPUTER ENGINEERING

SONIYA GANDHI POLYTECHNIC
SHRIGONDA-413701
(2020-2021)

SONIYA GANDHI POLYTECHNIC

SHRIGONDA-413701

CERTIFICATE

This is to certify that the project entitled

“Image Encryption and Decryption”

Submitted by

1.Miss. Unde P.S. **2. Miss. Haral S.S.**

3. Miss. Darekar R.R. **4. Miss. Phapale S.B.**

Is the bonafied work completed in the academic 2020-21 under my supervision and guidance in partial fulfillment for award of “**Diploma in Computer Engineering**” by Maharashtra State Board of Technical Education.

Place: Shrigonda

Date:

Prof. ShindeD.D.
[Project Guide]

Prof. ShindeD.D.
[Project Co-Ordinator/HOD]

External Examiner

Prof. Nagwade A.B
Principal
[SGP College, Shrigonda.]

ACKNOWLEDGMENT

We have great interest to develop this project. The project **Image encryption and Decryption** is softwareproduct to encrypt and decrypt the image. Main objective of this application is to provide a secure and secret transmission of text by encrypting it on an image using a key and which can only be decrypted by an authenticated receiver using the same key on the same application.

We are thankful to Prof. Shinde D.D. (Head of Computer Department/ Project Co-Ordinator) to help us & tell us changes in project as required. He every time helps us & also other groups for project & our project guide Prof. Shinde D.D. for supporting us to select topic "Image encryption and Decryption" & help us for our project.

This project is prepared under me and my teams' knowledge, guidance given by our professors and specially Thanks to concerned person, who has helped us to get knowledge on the project.

Miss. Unde P.S.

Miss. Haral S.S.

Miss. Darekar R.R.

Miss. Phapale S.B.

Abstract

Generally, we send many pictures to our friend’s relatives and others. The photos that may contain personal information so keeping them to at most secure is the important thing. So, in this project, we implement the idea of encrypting and decrypting the image using BLOWFISH algorithm. Abstract: In this algorithm we use the concept of random function for encrypt and decrypt the image using blowfish Algorithm. At present the need of information security has become a necessity. Random number generator (RNG) is widely used in cryptographic system as the cryptographic keys generator. These keys are the most important component in the system since the security of the cryptographic system relies entirely on its quality. This algorithm will be used as a variable key size up to 448 bits Latest mitigation techniques proposed at register-transfer level for dependable cryptosystems deal with time redundancy in an active on-line error-detection scheme. Round-based block ciphers are very likely to be hardened with these techniques. With this approach, attackers must face two trouble: dealing alongside on-line error detection and flouting the obligation locale in the round sequence. PRNG will produce disparate repetition sequences for the rounds of the cryptosystem, making extremely tough to associate output data alongside inoculated faults.

INDEX

LIST OF FIGURES

CHAPTER NO. 1 INTRODUCTION

1.1 Introduction Theory

Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. The field of encryption is becoming very important in the present era. Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Many image content encryption algorithms have been proposed. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to another computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, then such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

In this modern technological age, data and information have become key factor of human existence because various works of life are in dare need of data and information. Typically, data and information are stored in different electronic storage medias such as blue ray, smart card, flash drives (USB drives), memory cards, compact disks (CD), digital Video disks (DVD), hard disks, etc. Data and information stored in these various devices could be files, audio, images, text, animations, documents, etc. To ensure the availability of digital data and information to the world, these digital components need to be transmitted over short and long distances through the internet for various usages and applications.

[1] Defines internet as an international network that interconnects computer networks using standard internet protocols such as internet Protocol Suite (TCP/IP) to transmit data and information across the globe to billions of internet users. The internet is a connection of local,

metropolitan to global networks such as public, private, business, government, and academic networks that are joined together by wireless, optical fibers and electronic networking technologies. The use of internet growth geometrically which created the need for internet users to deliberately generate techniques and methods to secure sensitive data and information to deny

unfriendly users from getting unauthorized access. The accelerated use of internet by government, academic, health, science, engineering, agriculture, transport, business activities and applications requires a greater demand for quality data and information service. Based on the increasing use of the internet to meet the world's day – to - day data and information activity needs, there exists the urgency to provide quality data and information service by ensuring standard protocol control measures. Hence data and information security are needful and important when transmitted over the internet.

During data transmission, there are chances of these highly confidential, important data could fall into wrong hands such as hackers, which could lead to dangerous situations such as loss of data (bank information, pin numbers, passwords), shut down of emails, websites, servers, telecommunication system etc. However, providing data and information security is a complex and broad scope of study. Image data has become one of the most frequently shared and stored data in the world at different end – to - end communication channels. An image data may contain highly confidential and valuable information.

There are several types of image data presently in use this modern era. They are applicable in medical research, forensic, military, government sector, multimedia, film division, science research, engineering research, etc. In the cause of image data transmission, hackers do attempt to access the data illegally for malicious use. These illegal actions and troubles mostly occur in the transmission process over the internet

[2]. To courageously safeguard and protect image data, cryptography algorithms can be applied. Today many data encryption algorithms exist such as:

- Data Encryption Standard (DES),
- Advanced Encryption Standard (AES),
- International Data Encryption Algorithm (IDEA),
- Blowfish Algorithm, etc.

This work focused on Blowfish Algorithm. Blowfish Algorithm is a symmetric (64-bits) block cipher algorithm that was used to supersede Data Encryption Standard (DES)

[3]. This algorithm is very effective in securing data and information in this technological jet age. Its advantage lies on the ranging length of variable key from 32-bits to 448-bits with a default 128- bits, making it one of the best algorithms for securing data and information.

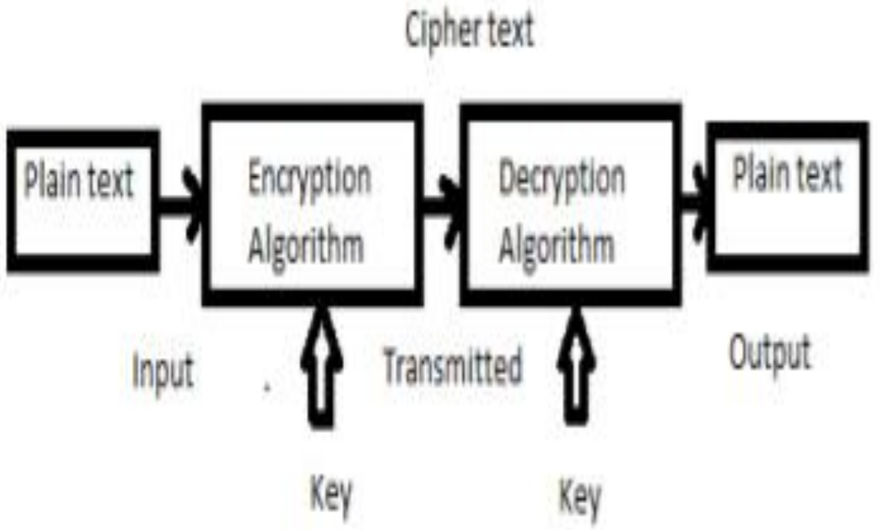


Fig 1.1 : -Encryption / Decryption Process

1.2 PROPOSED SYSTEM

Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of ciphertext efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors

PROPOSED TECHNIQUE: -

In 1993, Bruce Schneider [1993] published the Blowfish block cipher. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date, the security of Blowfish has not been compromised. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data on 32-bit processors. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security. As with DES, Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round’s left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. This operation is different from the permutation function performed in DES.

Encryption Process:

Data image as a plaintext and the encryption key are two inputs of encryption process. In this case, original image data bit stream is divided into the block's length of Blowfish algorithm.

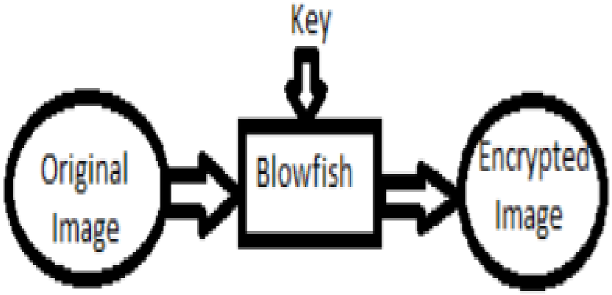


Fig 1.2.1 : -Image Encryption

Image header is excluded to encrypt and the start of the bitmap pixel or array begins right after the header of the file. The byte elements of the array are stored in row order from left to right with each row representing one scan line of the image and the rows of the image are encrypted from top to bottom.

Decryption Process:

The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom.

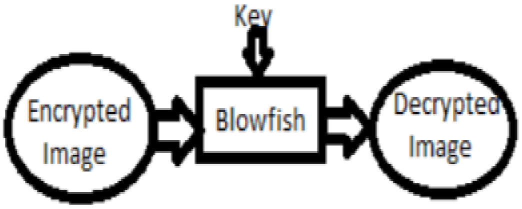


Fig 1.2.2: - Image Decryption

The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom

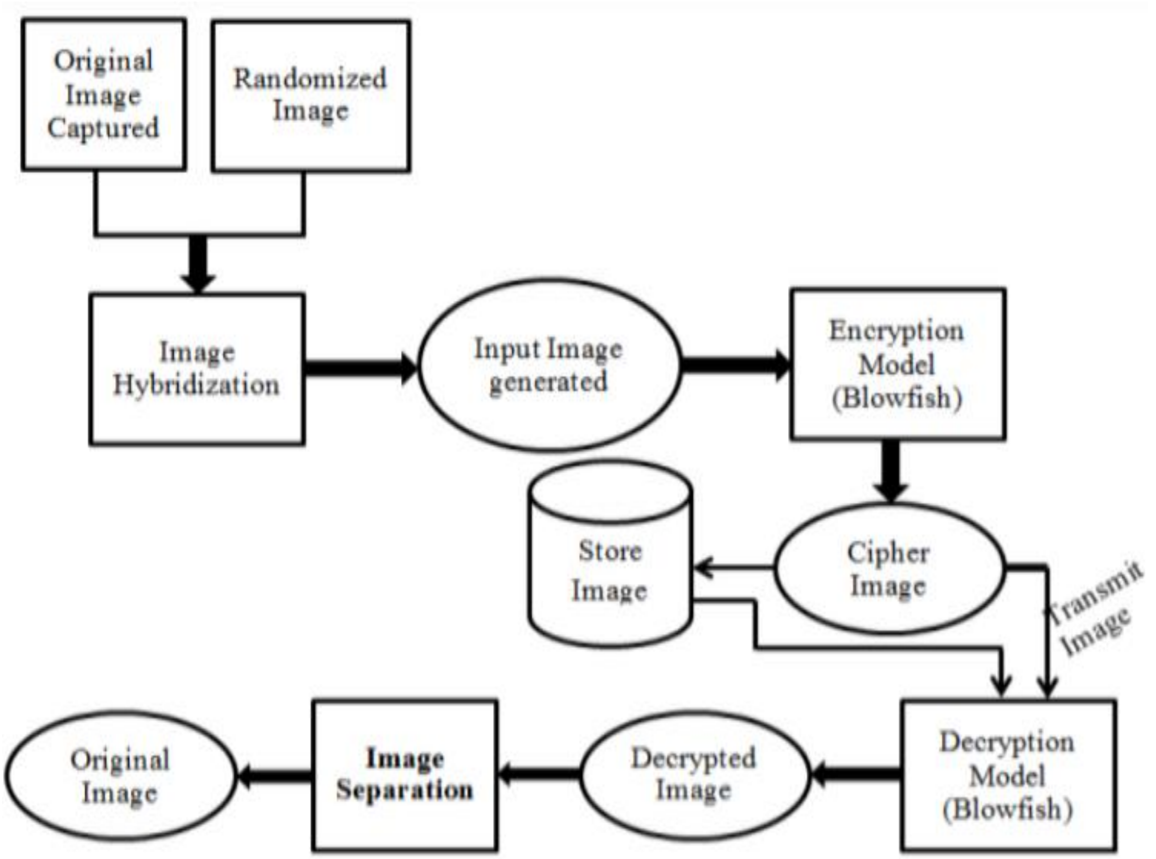


Fig1.2.3: - Proposed Architecture

1.3 Need and Scope of System

- Blowfish is a 64-bit block cipher and is suggested as a replacement for DES.
- Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors.
- security of Blowfish has not been compromised.
- Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes).
- To successfully transmit two confidential images.
- To encrypt and decrypt the images so that no intruder can access the data over a network while transmitting.
- Our project(system) can do the cryptography by encrypting and decrypting data.
- We are dependent on other mailing systems Like - gmail, yahoo etc. for information transfer.
- In future we can add the information transfer module so that after encryption users can transfer information by the same software.

1.4 Problem Definition

Information Security is the most common word uttered by any man, any device or any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most complex Cryptography. The advancements of digital revolution were not achieved without drawbacks such as illegal copying and distribution of digital multimedia documents. In order to provide data security and protection, different encryption methods must be used.

1.5 Background

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Encryption is the process of transforming the information for its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private.

The security of images has become more and more important due to the rapid evolution of the internet in the world today. The security of images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

In 1993, Bruce Schneier published the Blowfish block cipher. At this time, the current Data Encryption Standard (DES) was known to be vulnerable to crypto analysis and brute-force attacks. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date, the security of Blowfish has not been compromised. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a symmetric block cipher that encrypts data in 8-byte (64-bit) blocks.

The algorithm has two parts, key expansion and data encryption. Key expansion consists of generating the initial contents of one array (the P-array), namely, eighteen 32-bit sub keys, and four arrays (the S boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish can have a key that ranges from 32 to 448-bits. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a cipher based on Feistel rounds. No attack is known to be successful against this. It is suitable for applications where the key does not change often, like a communications link or an automatic file encrypt or. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one.

Chapter 2: - LITERATURE SURVEY

2.1 Survey of Literature: -

After the survey of various methods used for image encryption, we came through a few of these like Image encryption using AES, DES.

2.1.1

DES algorithm using Transportation Cryptography Techniques Data encryption standard (DES) is a private key cryptography system that provides the security in communication system but now a days the advancement in the computational power the DES seems to be weak against the brute force attacks. To improve the security of DES algorithm the transposition technique is added before the DES algorithm to perform its process. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So, the security is approximately double as compared to a simple DES algorithm.

2.1.2

Image Encryption Using Block-Based Transformation Algorithm Here a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish is used. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique.

2.2 Basic project ideas

- Caesar Cipher – Encryption/Decryption. ...
- Keystroke logger
- Hash Function(s)
- Packet Sniffing
- SQL Injection Vulnerability Assessment
- Online Fund Transfers Using Des Encryption
- Image Encryption
- Credit Card Fraud Detection

Chapter 3 Software Requirement Specification

3.1 Requirement Analysis

3.1.1 Software Requirements:

1) Language: - JAVA

2) Operating System: - Windows 10 onwards.

3) Editor: - Eclipse

3. 1.2 Hardware Requirements:

1) RAM: - 256 MB onwards.

2) HDD: - 10 GB onwards.

3) Processor: - Intel Pentium onwards.

4) Processor Speed: - 2.4GHZ onwards

3.2 System Features

1) Multiple Recipients & Documents. Senders can attach multiple documents with the email and send them to multiple recipients by a simple click.
2) Secure
3) Easy-to-use
4) Documents Support
5) No Capturing of Personal Details
6) Web based Decryption

7) Email Client Independent
8) No Security Keys Required

3.3 User interface

The graphical user interface is a form of user interface that allows users to interact with electronic devices through graphical icons and audio indicator such as primary notation, instead of text-based user interfaces, typed command labels or text navigation. GUIs were introduced in reaction to the perceived steep learning curve of command-line interfaces (CLIs).

Chapter 4 SYSTEM IMPLEMENTATION PLAN

4.1 Existing System

The existing system for this project the text information is encrypted by ASCII values or any special characters. In the existing system, didn't use the safely sent the encrypted information into the mail. The hackers easily access that information. The encrypted text is didn't restrict any secret key. So that information easily decrypted. Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each shared image and the small contrast of the recovered secret image

EXISTING TECHNIQUES: -

There are many image encryption algorithms which are available such as Baker's Transformation, in this Baker's map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc. But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

- **DATA ENCRYPTION STANDARD (DES):** DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997. DES is a 64-bit block cipher under 56-bit key.
  The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

- **TRIPLE DES (TDES):** The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. TDES uses three round message This provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming.

- **ADVANCED ENCRYPTION STANDARD (AES):** AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds.

- **BLOWFISH:** Bruce Schneier designed blowfish in 1993 as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64-bit block cipher and is suggested as a replacement for DES. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors.

4. 2 Flow Chart

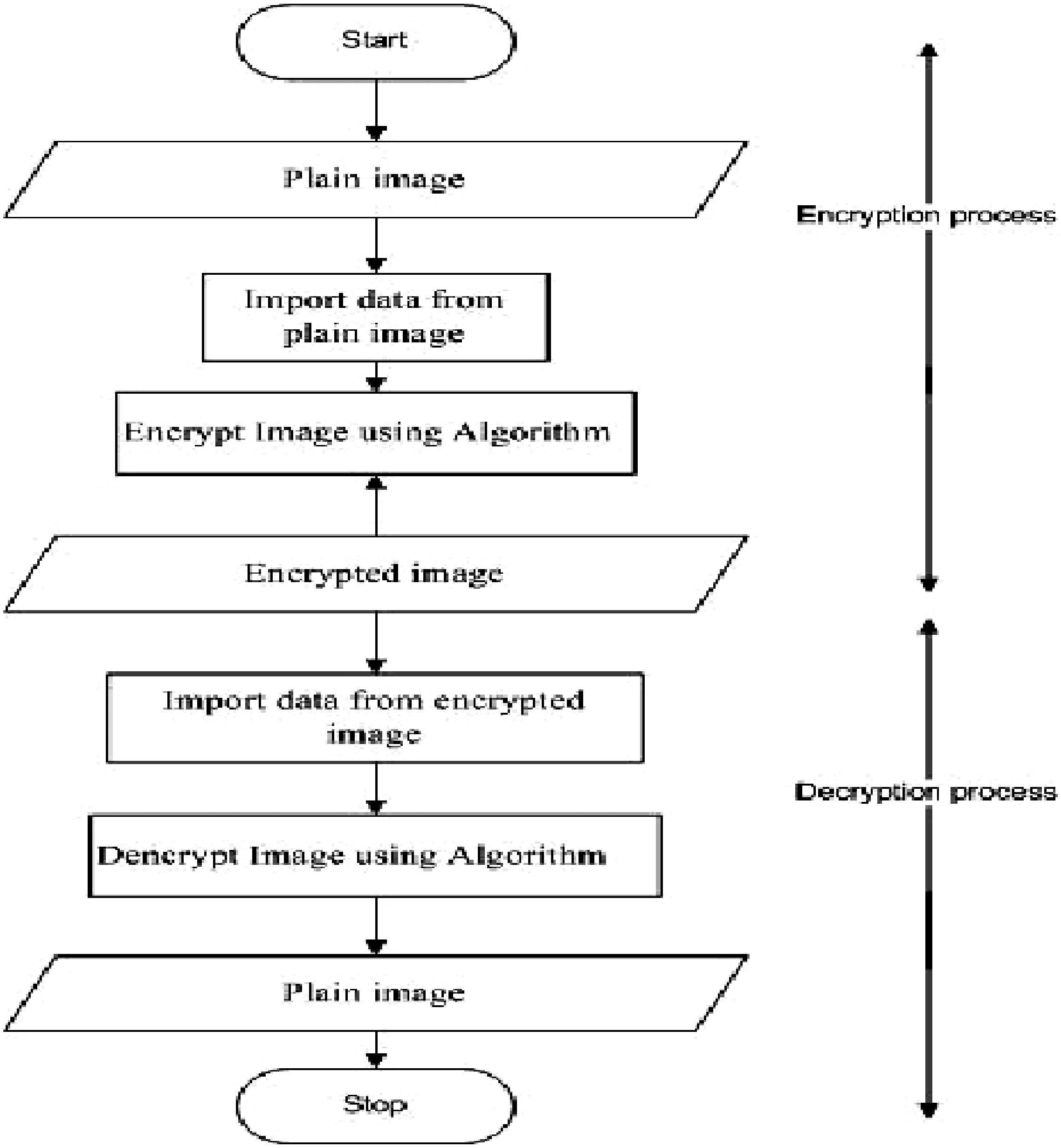

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Denecrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Fig 4.2 : -flowchart

4.3 ER- Diagram

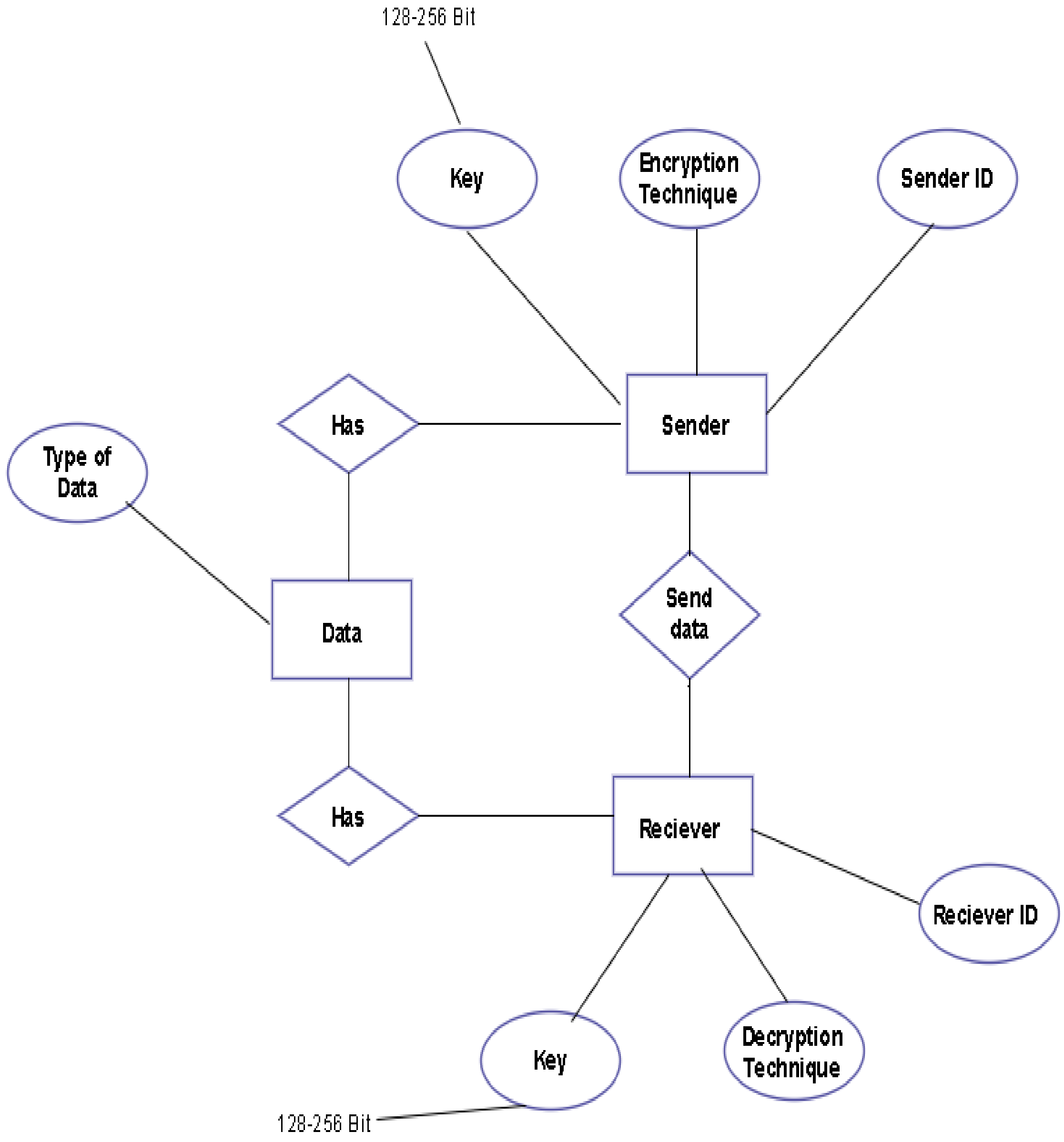


Fig4.3: - ER- Diagram

Chapter 5 System Design

5.1 System architecture

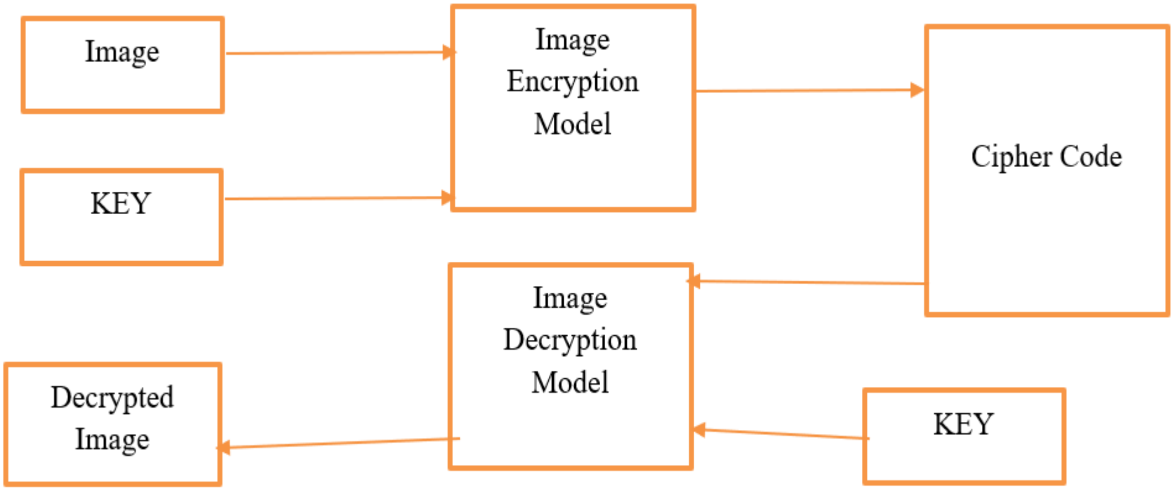
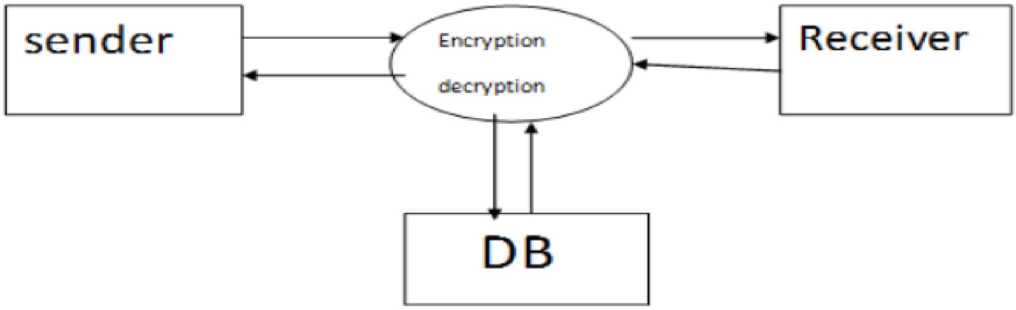


Fig5.1: -System Architecture

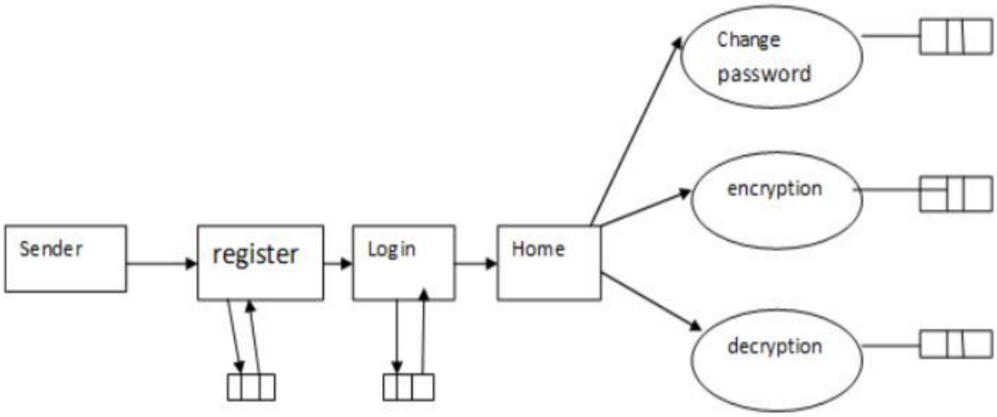
5.2 Analysis Model

5.2 .1 Data Flow Diagram

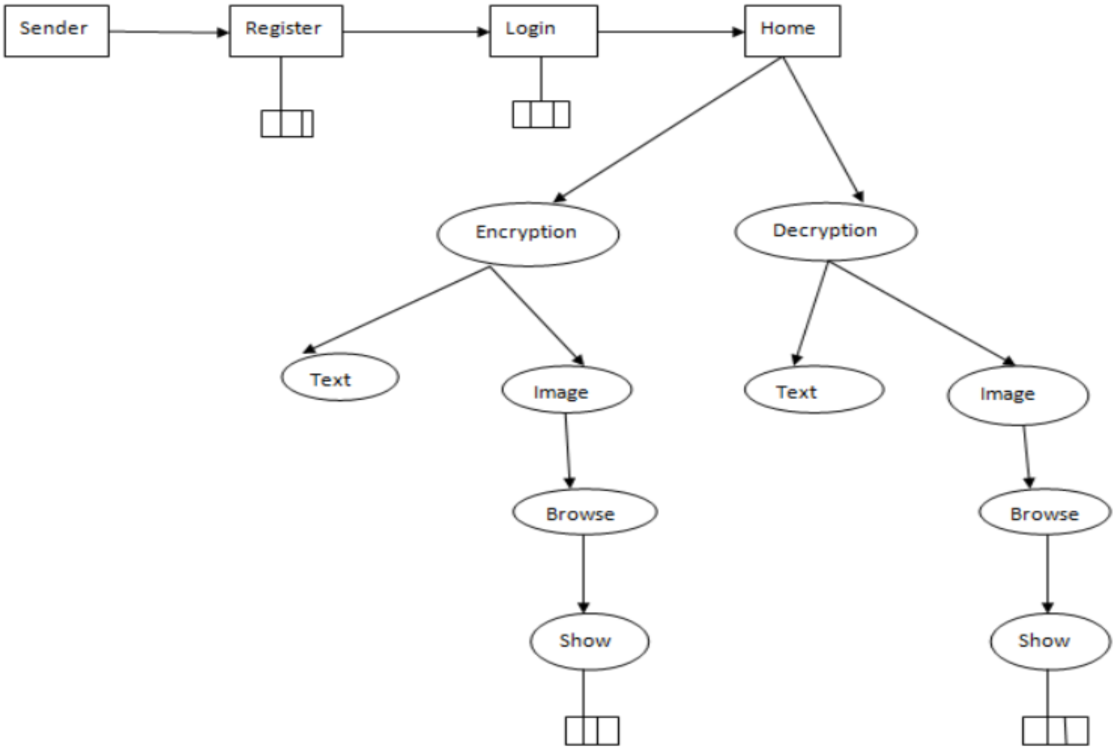
Level 0 Diagram: -



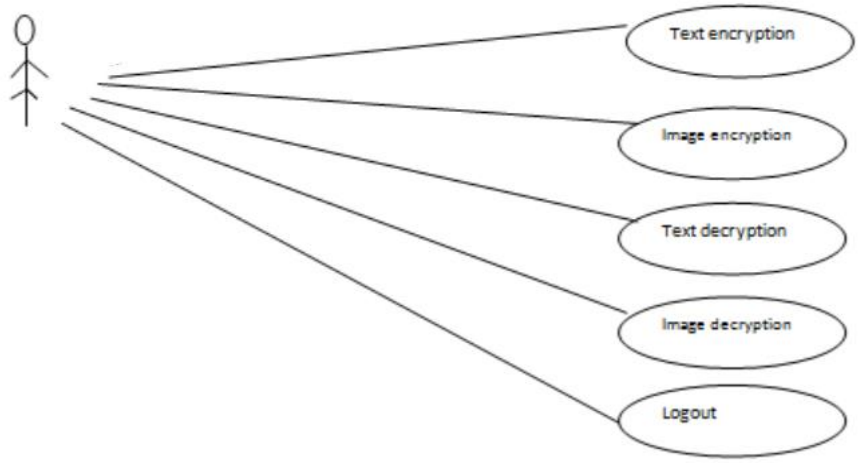
Level 1 Diagram: -



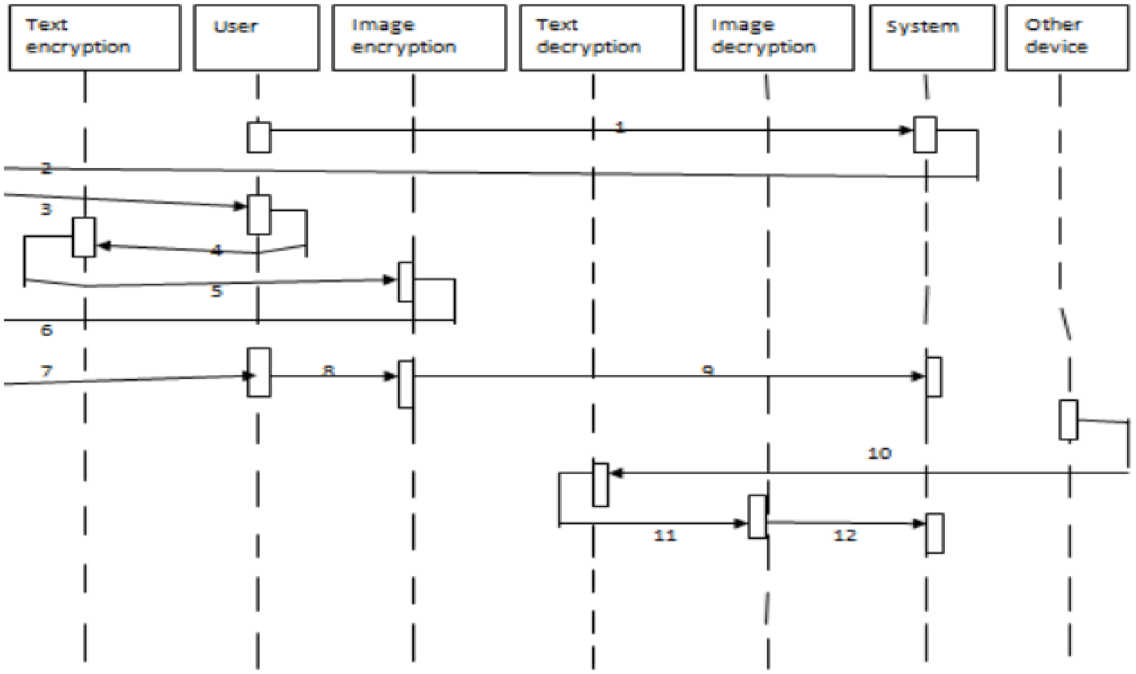
Level 2 Diagram: -



5.2.1.1 Use Case Diagram: -



5.2.1.2 Sequence Diagram: -



1.login(fill details)

2.Check data base

3.Valid/Invalid

4.Choose text and encrypt

5.Choose image

6.check data base for images

7.Image available

8.encryption done

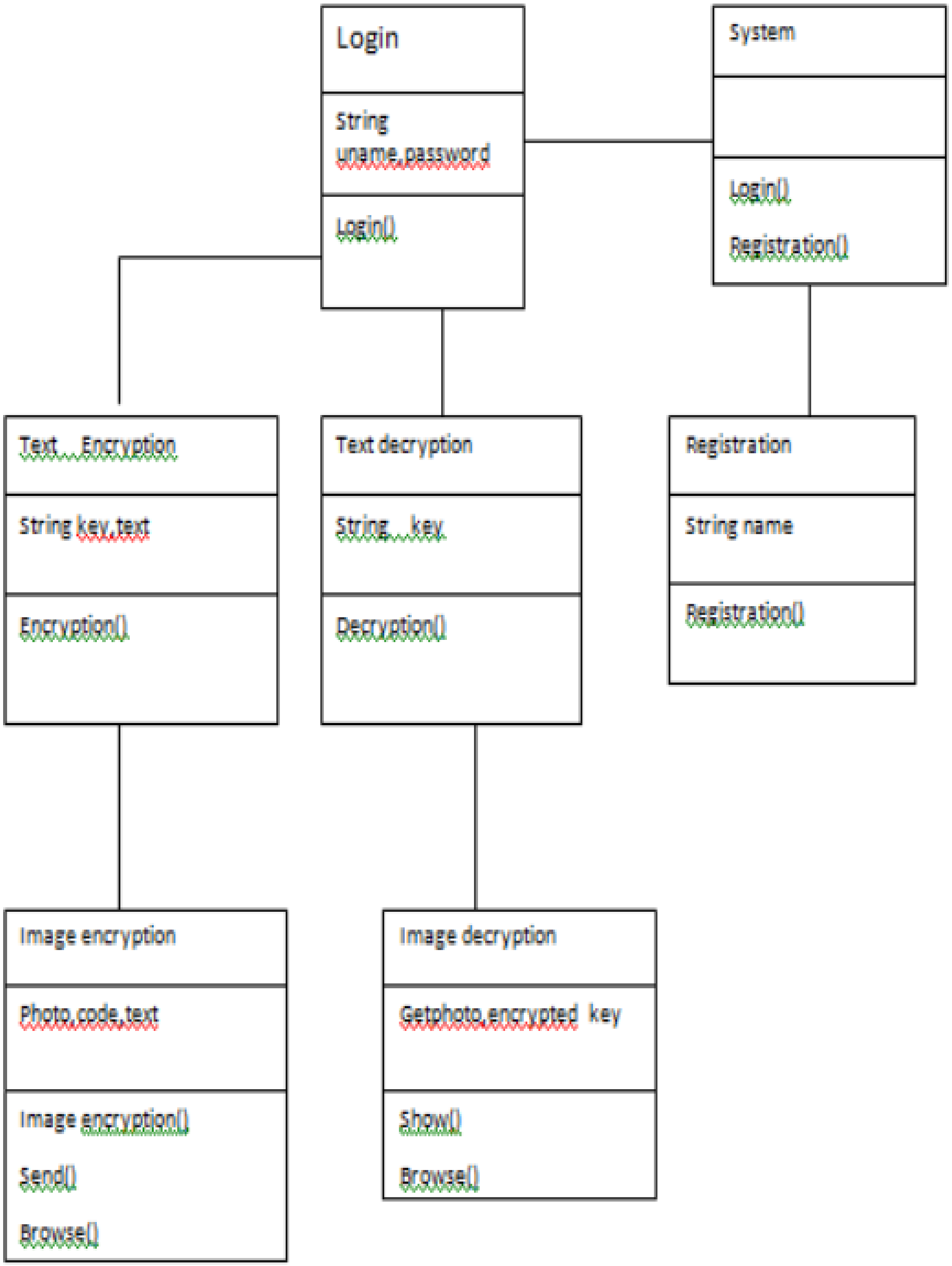
9.Send to receiver

10.Receiver decrypts the text with a key

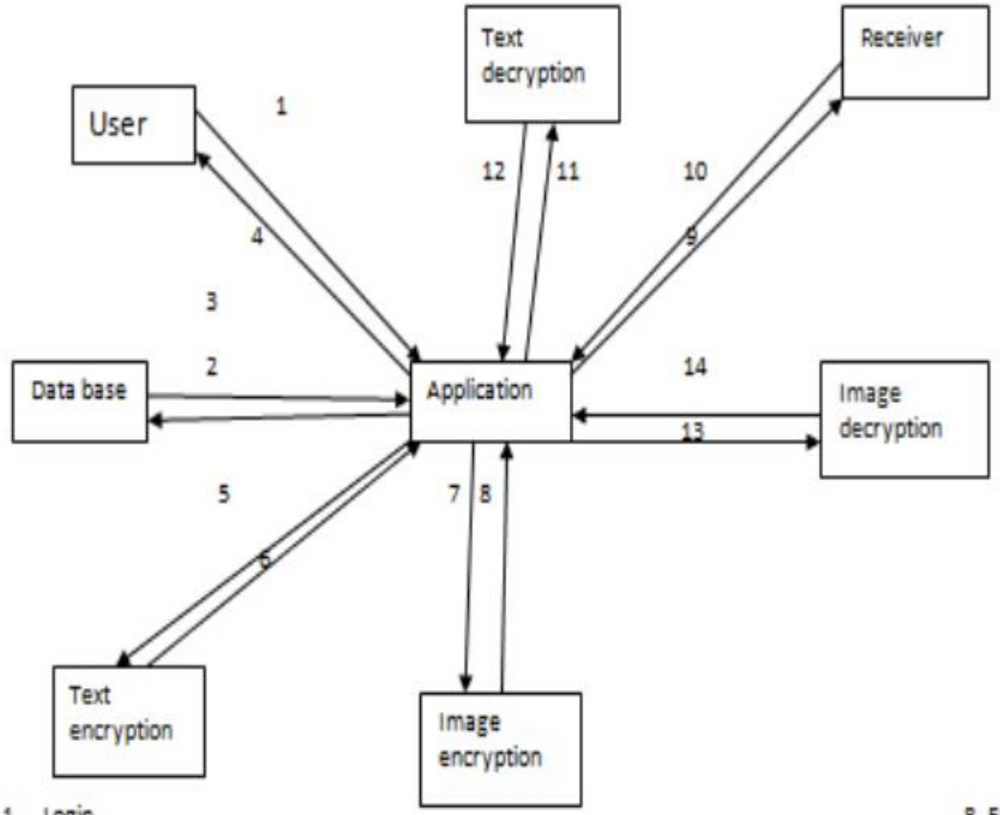
11.Decrypts the image

12.System shows text

5.2.1.3 Class Diagram: -

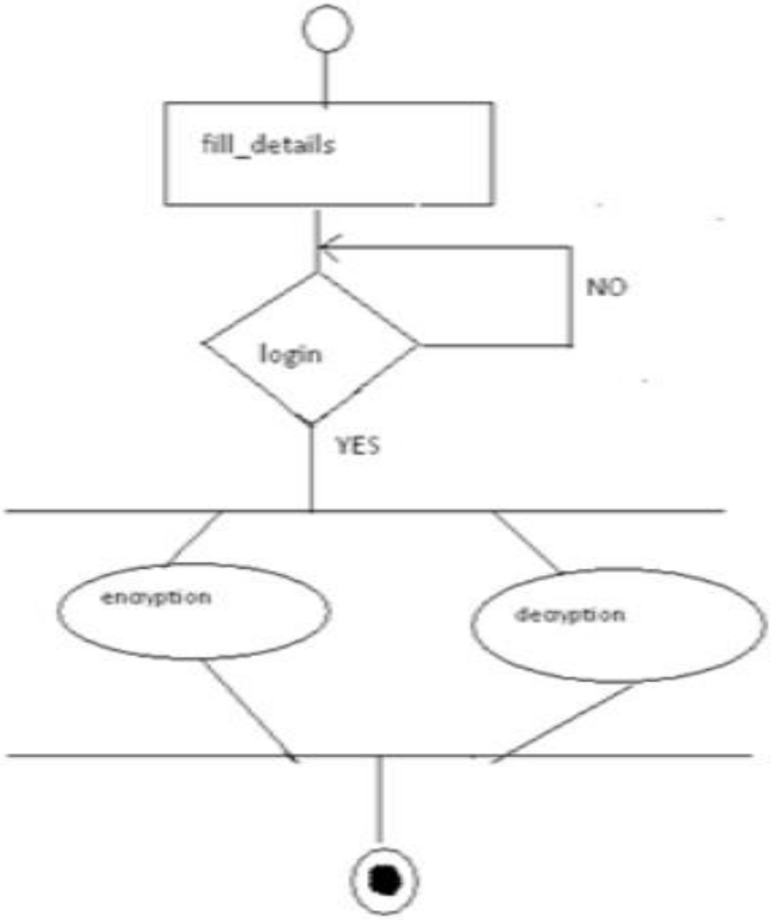


5.2.1.4 Collaboration diagram: -



1. Login
2. Check data
3. Response
4. Valid /invalid
5. Choose text
6. Encrypted text
7. Choose an image
8. Encrypted image
9. Send
10. Response
11. Request key
12. Decrypted key
13. Browse the received image
14. Decrypted image

5.2.1.5 Activity Diagram



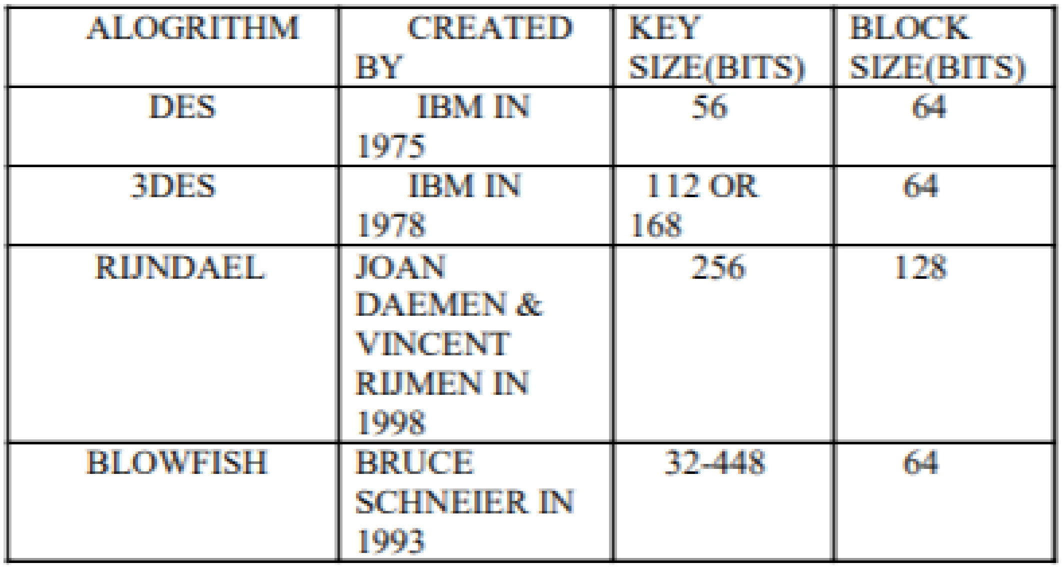
CHAPTER NO.6 IMPLEMENTATION DETAILS

6.1 Algorithmic Strategy used mathematical model

The basic algorithm for Blowfish is illustrated as follows:

```
Divide X into two 32-bit halves XL and XR
For i =1 to 16:
XL = XL Pi
XR = F (XL) XR
Swap XL and XR
End for
Swap XL and XR
XR = XR P17
XL = XL P18
Recombine XL and XR
Output X (64-bit data block: cipher text)
```

For decryption, the same process is applied, except that the sub-keys Pi must be supplied in reverse order. The nature of the Feistel network ensures that every half is swapped for the next round.



ALOGRITHM	CREATED BY	KEY SIZE(BITS)	BLOCK SIZE(BITS)
DES	IBM IN 1975	56	64
3DES	IBM IN 1978	112 OR 168	64
RIJNDAEL	JOAN DAEMEN & VINCENT RIJMEN IN 1998	256	128
BLOWFISH	BRUCE SCHNEIER IN 1993	32-448	64

Table: -Comparison of Various Algorithm

6.1.1 Algorithm

Phase 1: Input Image Generation

1. Generate a random image (.jpg)

2. Get the original image (.jpg) to be encrypted

3. Hybridize original and randomly generated images to form one image (input image)

Phase 2: Image Encryption

1. 16 rounds of Feistel Network iterations
2. Applying Blowfish Algorithm on the input image
3. Generate Encrypted Image (Cipher Image) and store it.

Phase 3: Image Decryption

1. Input Cipher Image
2. Applying inverse of Blowfish Algorithm to decrypt cipher image.
3. Generate decrypted Image (.jpg) to produce the hybridized image.

Phase 4: Generate Original Image

1. Get the decrypted image (i.e. the hybridized image).
2. Get the random image
3. Separate the random image from decrypted image to generate original image

6.2 Implementation details for every model

6.2.1 Encryption Process:

Data image as a plaintext and the encryption key are two inputs of the encryption process. In this case, original image data bit stream is divided into the length of the block of Blowfish algorithm.

6.2.2 Decryption Process:

The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom. The first block is entered to the decryption function and the same encryption key is used to decrypt the image but the application of subkeys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

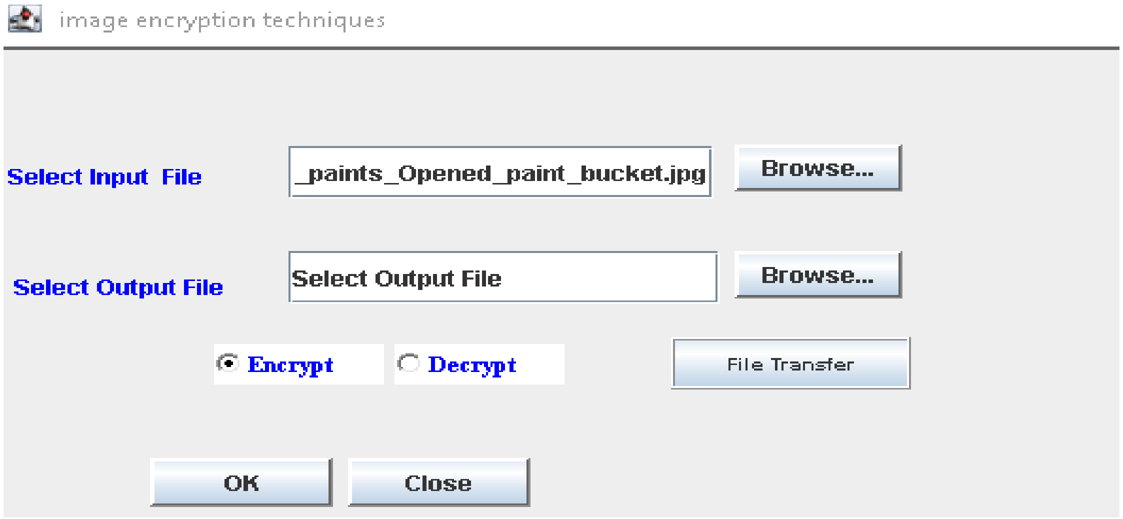
6.2.3 User:

In this application user will register and log in with the username and password, after logging in the user will upload the image which is to be encrypted and then after encrypting the user will get a secret key to the user registered email id using the key and encrypted image.

CHAPTER NO.7 Output Screen

- **Process to encrypt Image:**

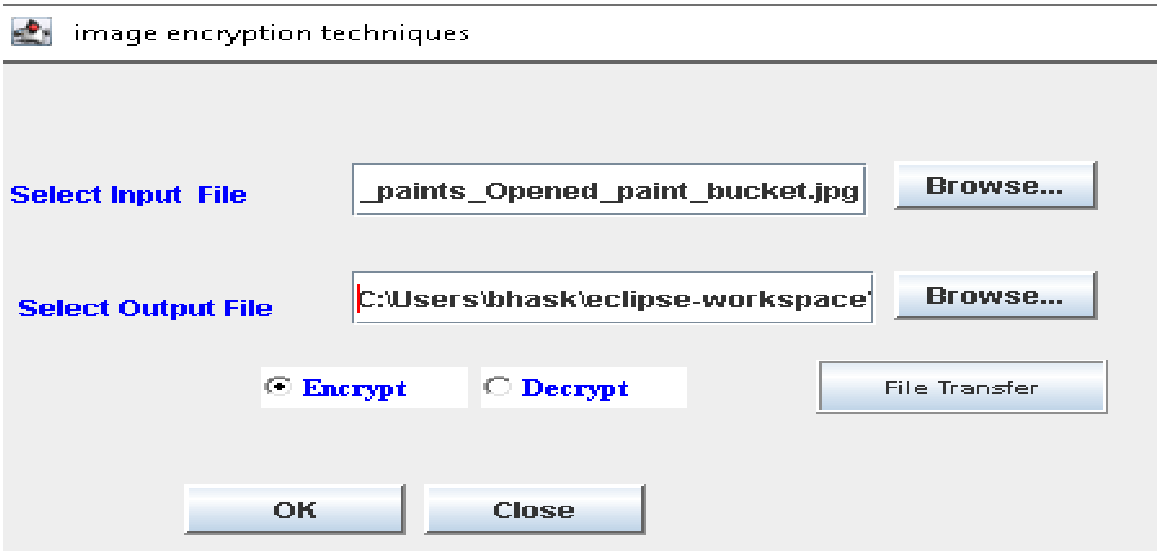
Step 1: - Select the input path of the image of the which is you want to encrypt.


Select Input File: _paints_Opened_paint_bucket.jpg

Select Output File: Select Output File

● Encrypt ○ Decrypt

Step 2: - Select the output path of the image of the which is you want to encrypt. After Selecting the path click on “Encrypt”

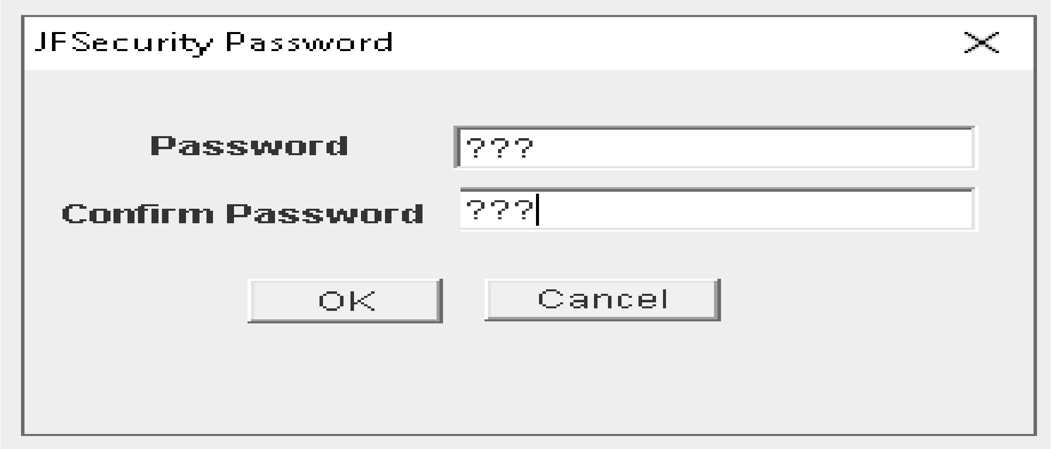

Select Input File: _paints_Opened_paint_bucket.jpg

Select Output File: C:\Users\bhask\eclipse-workspace\

● Encrypt ○ Decrypt

Step 3: - Press on “OK” button. After pressing the “OK “button,

Enter the “password” and “confirm password”. Press on “OK” button.



JFSecurity Password

Password: ???

Confirm Password: ???

Step 4: -This window will be Displayed on screen.

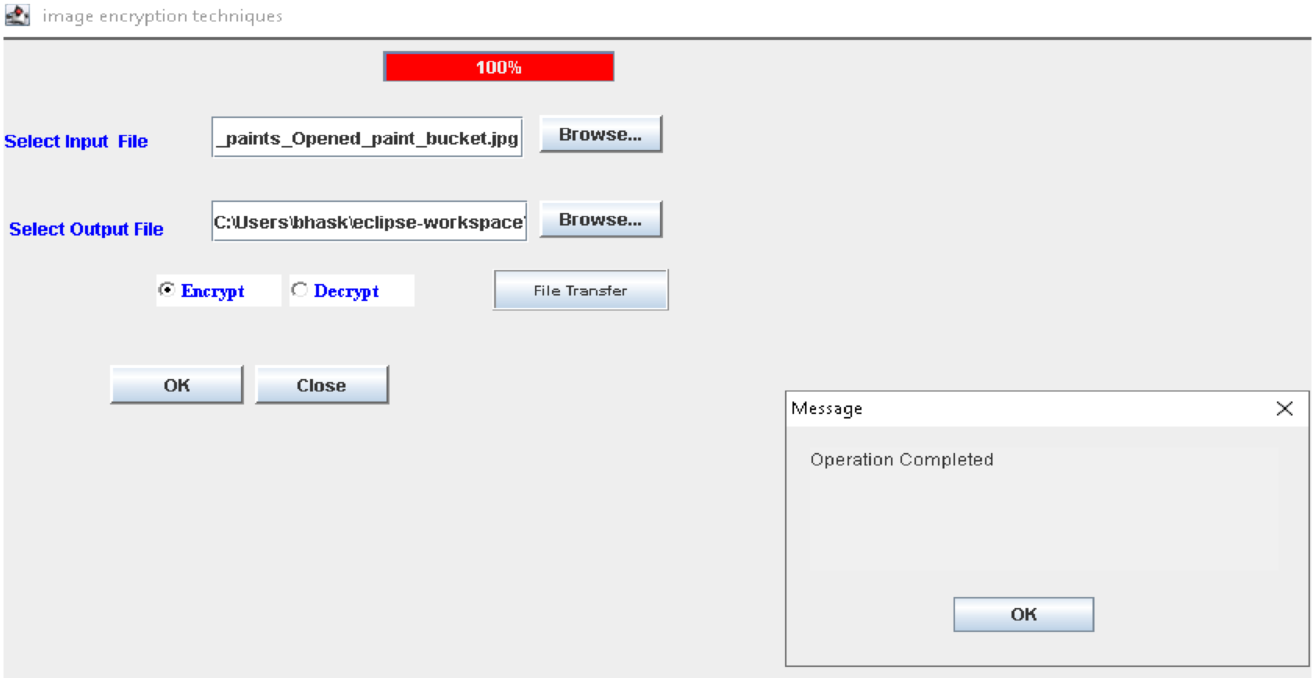


image encryption techniques

100%

Select Input File: _paints_Opened_paint_bucket.jpg

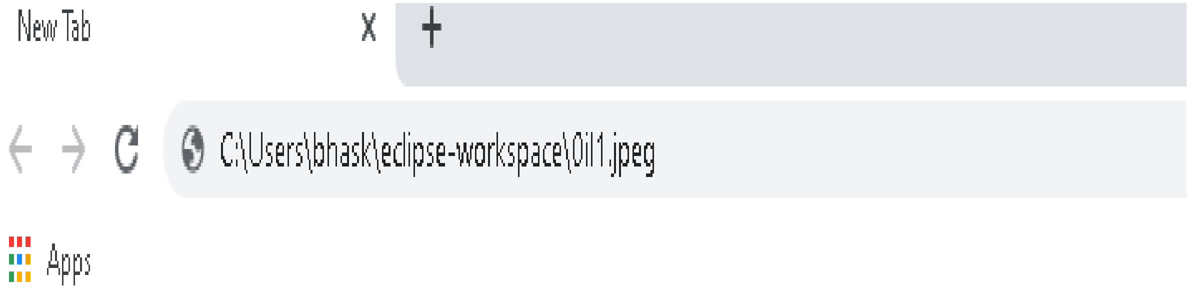
Select Output File: C:\Users\bhask\eclipse-workspace

● Encrypt ○ Decrypt

Message

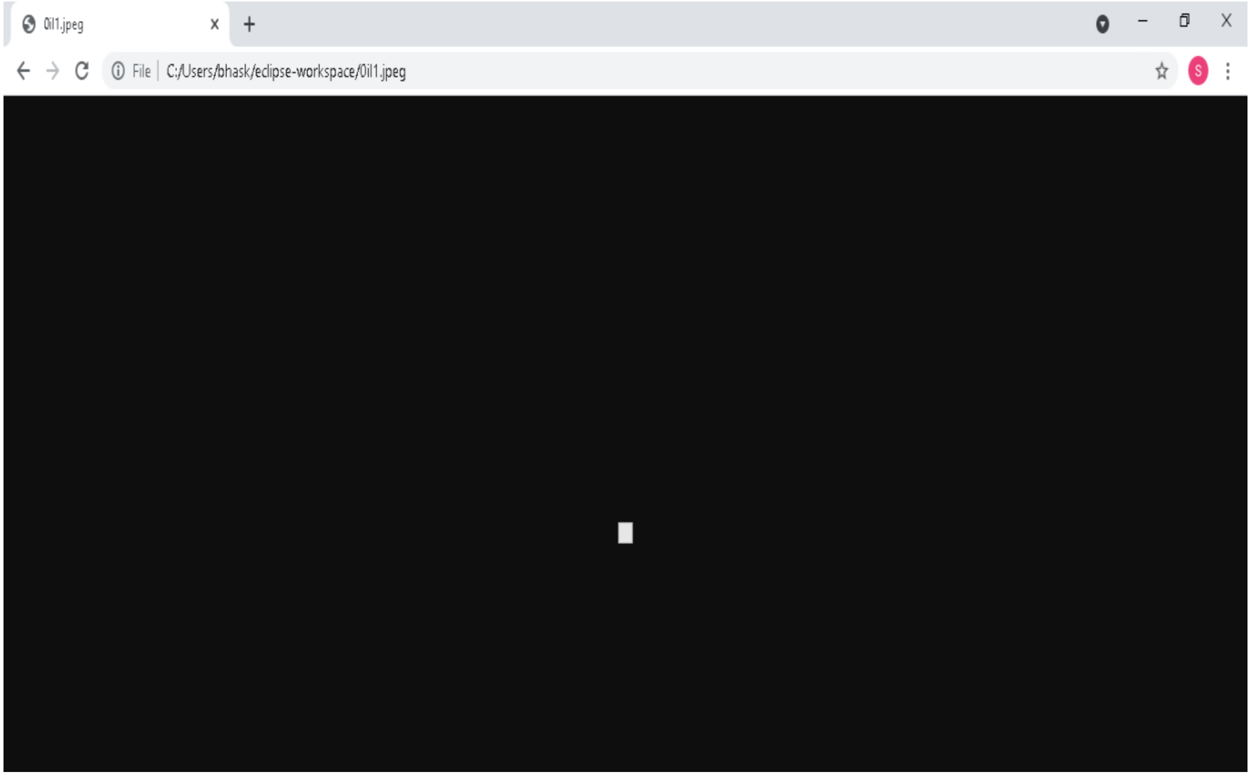
Operation Completed

Step 5: - Now copy output path and paste it on any browser.



C:\Users\bhask\eclipse-workspace\0il1.jpeg

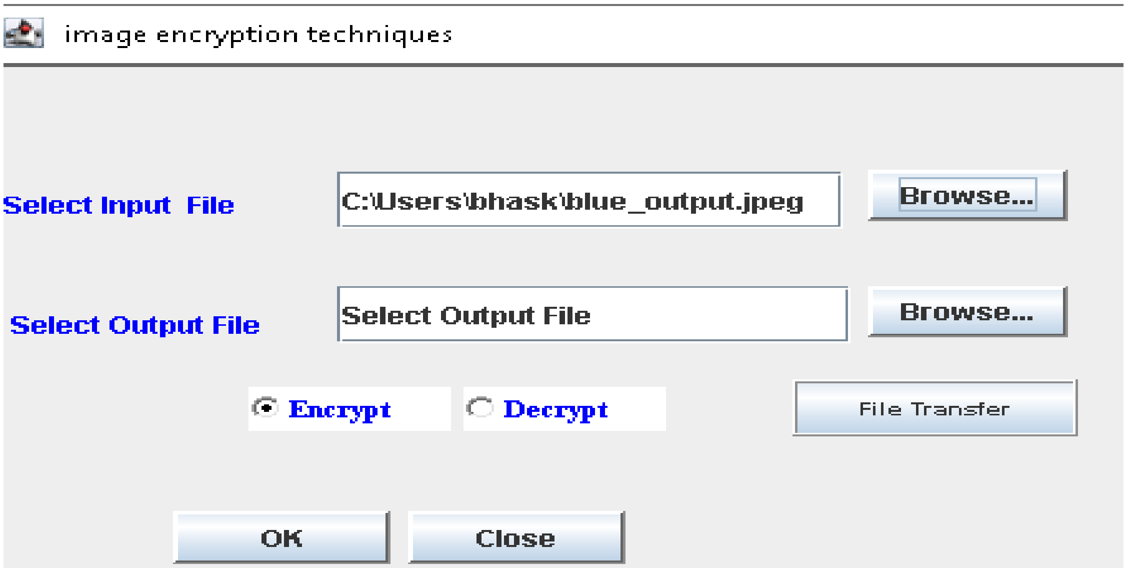
Step 6: - Now, this window will be displayed on screen. This is the Encrypted Image.



C:/Users/bhask/eclipse-workspace/0il1.jpeg

- **Process to Decrypt Image:**

Step 1: - Select the input path of the image of the which is you want to Decrypt.

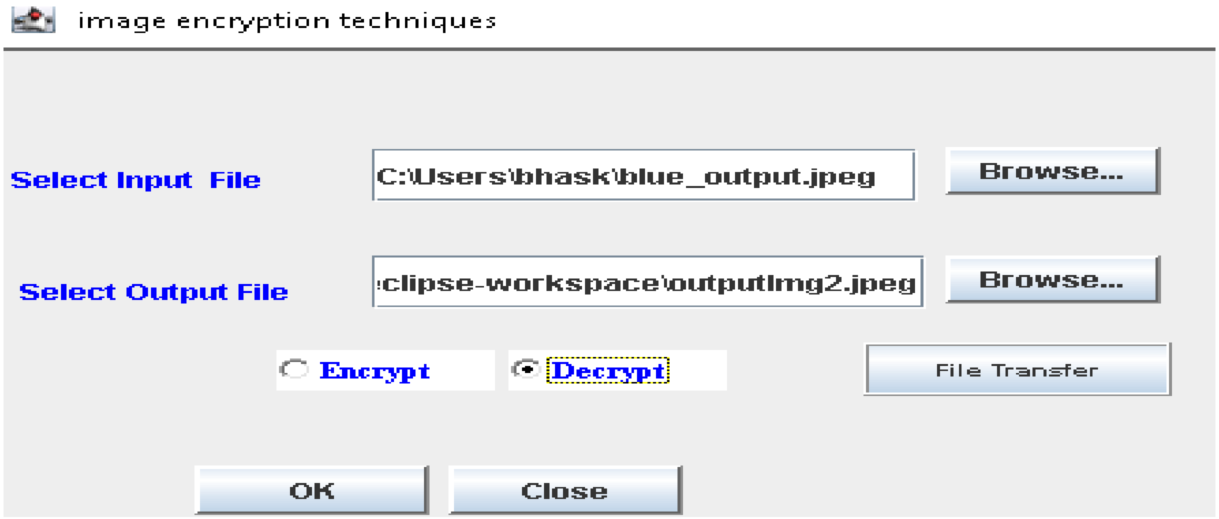


Select Input File C:\Users\bhask\blue_output.jpeg

Select Output File Select Output File

● Encrypt ○ Decrypt

Step 2: - Select the output path of the image of the which is you want to decrypt. After Selecting the path, click on “Decrypt” button.

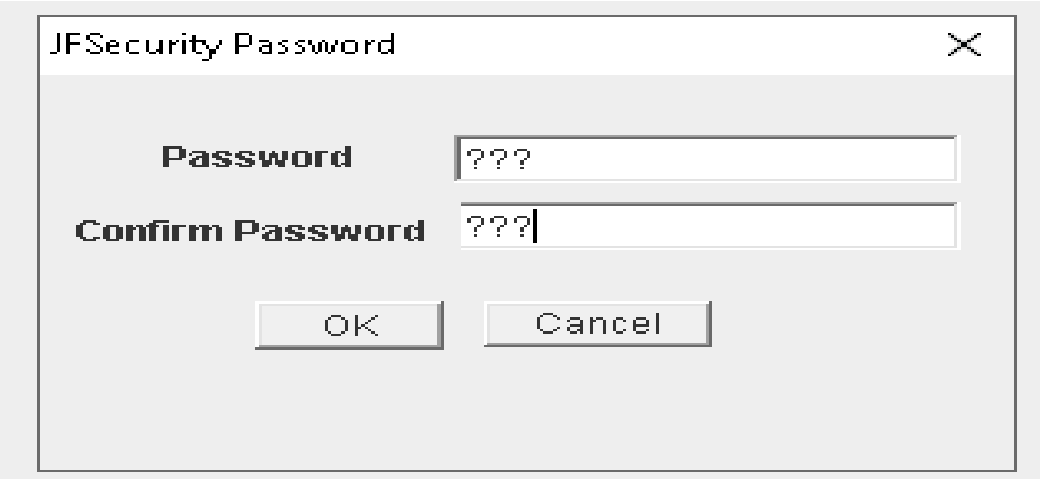


Select Input File C:\Users\bhask\blue_output.jpeg

Select Output File :clipse-workspace\outputImg2.jpeg

○ Encrypt ● Decrypt

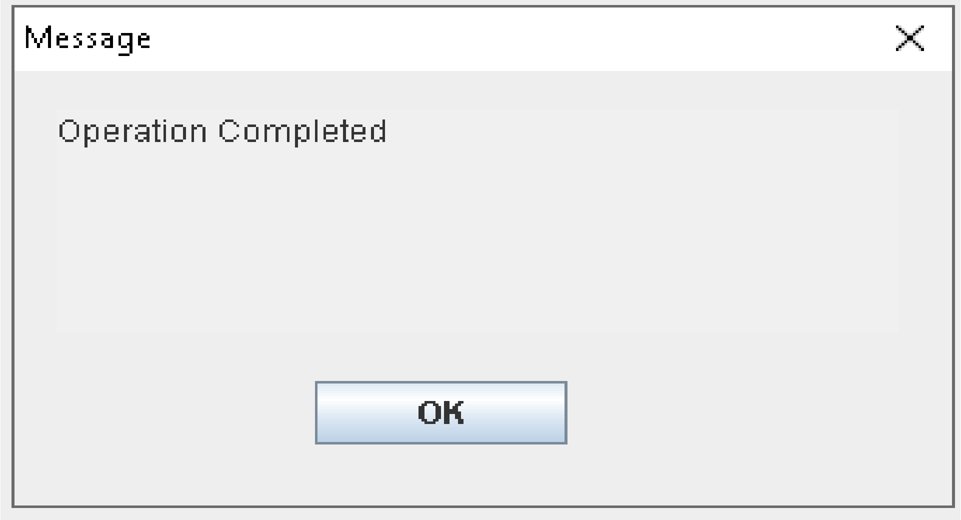
Step 3: - Press on “OK” button. After pressing the “OK “button, Enter the “password” and “confirm password”.



Password ???

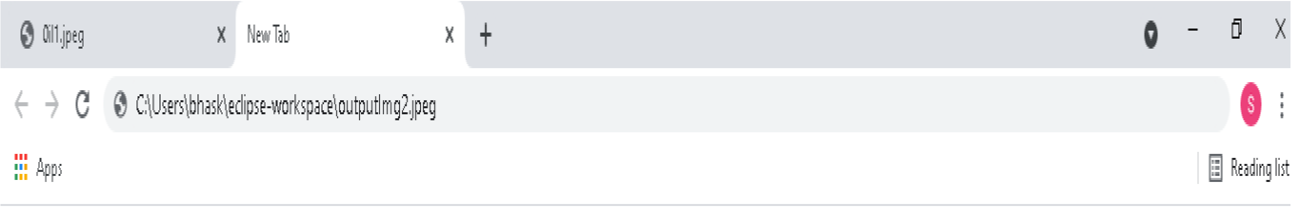
Confirm Password ???

Step 4: -This window will be Displayed on screen.



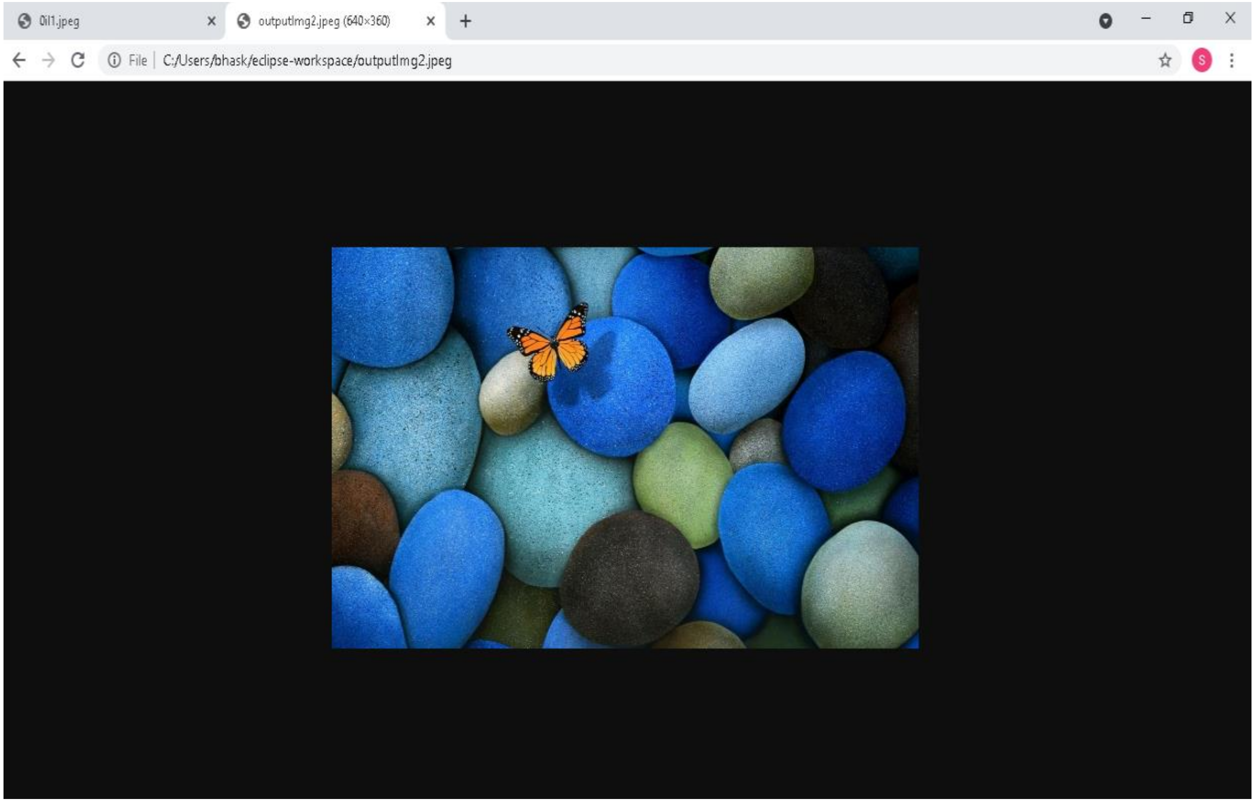
Operation Completed

Step 5: - Now copy output path and paste it on any browser.



C:\Users\bhask\eclipse-workspace\outputImg2.jpeg

Step 6: - Now, this window will be displayed on screen. This is the Decrypted Image.



C:/Users/bhask/eclipse-workspace/outputImg2.jpeg

CHAPTER NO.8 ANALYSIS OF RESULTS

The results of the new model were analyzed and compared using performance measurement factors: i. Time complexity Tables and charts below illustrate time (speed) complexity performance measure in terms of seconds. Images presented are results of encryption and decryption process of the system with relation to time taken for execution

.

Sr. No.	File Name	Image Size (kb)	Encryption Time (s)	Decryption Time(s)
1	Blue_output.jpg	31.80	0.56	0.59
2	Oil_paints.jpg	28.50	0.52	0.50
3	Soil_texture.jpg	21.90	0.44	0.41
4	Sample_test.jpg	16.90	0.33	0.32

Table -1: Comparing encryption and decryption time of system test images.

CHAPTER NO. 9 CONCLUSION

This research work enhanced image encryption system using blowfish and randomization methods provided a double protection of the plain image, reduces encryption and decryption time, require minimal memory to execute and prevent pixel value loss during encryption and decryption.

CHAPTER NO. 10 FUTURE SCOPE

We are very excited by the vast future possibilities that our project has to offer. Possible improvements include getting back the decrypted image in color. We are also looking forward to encrypt videos by extracting each frame and encrypting the images simultaneously. We know that all the videos have sound. So, we are planning to encrypt frames and sound simultaneously. Finally, after achieving all of the above, we are planning to create an app which will do all of the above. With two people having the app, one will become the sender and other the receiver at a time, based on the requirements of either of the two.

CHAPTER NO. 11 REFERENCES

1. Singhal, Nidhi and Raina, J P S. “Comparative Analysis of AES and RC4 Algorithms for Better Utilization”, International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011.
2. Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005. Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http:// www. schneier.com/ blowfish.html.
3. W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology. Vol. 2.
4. H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.
5. C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.
6. M. Ali BaniYounes and A. Jantan, 2008, Image encryption using block-based transformation algorithm, in IAENG International Journal of Computer Science, Volume 35, Issue 1.
7. Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).

Websites

- www.java.sun.com
- www.google.com
- www.yahoo.com