1. Introduction

# 1.1 Introduction to Cryptography:

In the era of information technology, the possibility that the information stored in a person’s computer or the information that are being transferred through network of computers or internet being read by other people is very high. This causes a major concern for privacy, identity theft, electronic payments, corporate security, military communications and many others. We need an efficient and simple way of securing the electronic documents from being read or used by people other than who are authorized to do it. Cryptography is a standard way of securing the electronic documents.

### 1.1.1 Basic idea of Cryptography:

Basic idea of cryptography is to mumble-jumble the original message into something that is unreadable or to something that is readable but makes no sense of what the original message is. To retrieve the original message again, we have to transform the mumble-jumbled message back into the original message again.

### 1.1.2 Basic Terminologies used in Cryptography:

Data that can be read and understood without any special measures is called plaintext or cleartext. This is the message or data that has to be secured. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

Cryptography is the science of mathematics to “encrypt” and “decrypt” data. Cryptography enables us to store sensitive information or transmit it across insecure networks like Internet so that no one else other the intended recipient can read it. Cryptanalysis is the art of breaking Ciphers that is retrieving the original message without knowing the proper key. Cryptography deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.



### 1.1.3 Cryptographic Algorithms:

Cryptographic algorithms are mathematical functions that are used in the encryption and decryption process. A cryptographic algorithms works in combination with a key (a number, word or phrase), to encrypt the plain text. Same plain text encrypts to different cipher texts for different keys. Strength of a cryptosystems depends on the strength of the algorithm and the secrecy of the key.

### 1.1.4 Two Kinds of Cryptography Systems:

There are two kinds of cryptosystems: symmetric and asymmetric. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Symmetric cryptosystems are also called as private key cryptosystems and asymmetric cryptosystems are also called as public key cryptosystems.

# 1.1.5 Overview of Private Key Cryptography:

In private-key cryptography, the sender and recipient agree beforehand on a secret private key. The plaintext is somehow combined with the key to create the ciphertext. The method of combination is such that, it is hoped, an adversary could not determine the meaning of the message without decrypting the message, for which he needs the key. The following diagram illustrates the encryption process:

Message to be encrypted or plain text

Encryption Algorithm

Encrypted message or Cipher text

Private Key known only to sender and receiver

The following diagram illustrates the decryption process:

Message to be decrypted or cipher text

Decryption Algorithm

Decrypted message or Plain text

Private Key known only to sender and receiver

To break a message encrypted with private-key cryptography, an adversary must either exploit a weakness in the encryption algorithm itself, or else try an exhaustive search of all possible keys (brute force method). If the key is large enough (e.g., 128 bits), such a search would take a very long time (few years), even with very powerful computers.  
  
Private-key methods are efficient and difficult to break. However, one major drawback is that the key must be exchanged between the sender and recipient beforehand, raising the issue of how to protect the secrecy of the key. When the President of the United States exchanges launch codes with a nuclear weapons site under his command, the key is accompanied by a team of armed couriers. Banks likewise use high security in transferring their keys between branches. These types of key exchanges are not practical, however, for e-commerce between, say, amazon.com and a casual web surfer.

1.1.6 What is the use of Cryptography in project?

-Provide security to the object.

-High performance of encryption where encrypted data should not be unless and until correct login should not be done

2.STYGANOGARPHY:

2.1 Introduction to Styganography

Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio file.

Where cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography’s role is gaining prominence.

What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a password.

2.2 Where Hidden Data hides?

It is possible to alter graphic slightly without losing their overall viability for the viewer and listener. With graphic images, you can remove redundant bits of color from the image 7 and still produce a picture that looks intact to human eye and is difficult to discern from its original.

It is in those bits that stego hides its data. A stego program uses an algorithm, to embed data in an image or sound file, and a password scheme to allow you to retrieve information.

2.3 What does the project do?

- Hiding the text message in an image file.

- Encryption of the same message, so as to support more secure steganography.

- The decoding of the message, decryption and source message retrieval are also supported.

Project Profile:-

|  |  |
| --- | --- |
| Project Title | “CRYPT-BOX” |
| Develop For | All the user |
| Developed At | Government Polytechnic, Ambad |
| Objectives | To provide, combine security & functional utility tool |
| Front End | JAVA |
| Back End | SQL SERVER 2008 |
| Developed By | 1.MR.SHUBHAM LAKHMALE(CO-6G)  2.MR. ONKAR SOLANKE(CO-6G)  3. MR. SIDHESHWAR KALE(CO-6G)  4. MR.SHUBHAM HAZARE (CO-6G) |

CHAPTER 3: IMPLEMENTATION

CRYPTOGRAPHY:

### IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Main Modules:-

MODULES:

* Homophonic Cryptographic IDE
* Encr yption Module with Key Generation
* Decryption Module

Cryptographic Process Basic Process

M is the original message

K enc is encryption key

M' is the scrambled message

K dec is decryption key

It is “difficult” to get M just by knowing M'

E and D are related such that

E(K enc , M) = M'

D(K dec , M') = M

D(K dec , E(K enc , M)) = M

Plaintext—M Cipher text—M' Original

Plaintext—M

Decryption function—D Encryption

function—E

So how does cryptographic process work?

The idea is rather simple. Let's say you have plaintext

M. By providing the encryption key and the encryption

function you get cipher text, M'.

The cipher text can bedecrypted using a decryption function and decryption key and the result is the original text. In cryptographic process the mathematical property is

such that it is practically impossible to derive M from M' unless the key is known.

Key Process Techniques

*  Symmetric-Key Encryption: One Key Symmetric-key encryption, also called shared-key encryption or secret-key cryptography, uses a single key that both the sender and recipient possess.This key, used for both encryption and decryption, Is called a secret key (also referred to as a symmetric key or session key). Symmetric-key encryption is an efficient method for encrypting large amounts of data. But the drawback is to transfer the Key to Receiver as it is prone to security risks.
*  Public-Key Encryption: Two Keys

Two keys—a public key and a private key, whichare mathematically related—are used in public-keyencryption. To contrast it with symmetric-key encryption, public-key encryption is also sometimes called asymmetric-key encryption. In public-keyencryption, the public key can be passed openly between the parties or published in a public repository, but the related private key remains private.Data encrypted with the public key can be decrypted only using the private key. Data encrypted with the private key can be decrypted only using the public key. In Figure 1, a sender has the receiver's public key and uses it to encrypt a message, but only the receiver has the related private key used to decrypt the message.

Private Key Method

Public Key Method

Encryption is done with Public Key and Decryption with another key called Private Key. This is called Public Key Cryptography.

HASH functions

An improvement on the Public Key scheme is the addition of a one way hash function in the process. A one-way hash function takes variable length input. In this case, a message of any length, even thousands or millions of bits and produces a fixed-length output; say, 160-bits. The hash function

ensures that, if the information is changed in any way even by just one bit an entirely different output value is produced.

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key Instead; a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are

typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems so encrypt passwords. Hash functions, then help preserve the integrity of a file. As long as a secure hash function is used, there is no way to take someone's signature from one document and attach it to another, or to alter a signed message in any way. The slightest change in a signed document will cause the digital signature verification process to fail.

3.1 STYGANOGRAPHY

IMPLEMRNTATION

Implementation:

- Technical Details:

o Using java.awt.Image, ImageIO

o The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

- The Encoding Process:

- The steganography technique used is LSB coding.

- The offset of the image is retrieved from its header.

- That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process.

- For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.

- Creation of User Space:

o User Space is created for preserving the original file, so that all the modifications are done in the user space.

o In the object of BufferedImage, using ImageIO.read method we take the original image.

o Using createGraphics and drawRenderedImage method of Graphics class, we create our user space in BufferedImage object.

- The text file is taken as input and separated in stream of bytes.

- Now, each bit of these bytes is encoded in the LSB of each next pixel.

- And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using ImageIO.write method.

- This completes the encoding process.

- The Decoding Process:

- The offset of the image is retrieved from its header.

- Create the user space using the same process as in the Encoding.

- Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes. The data of image is taken into byte array.

- Using above byte array, the bit stream of original text file, is retrieved into the another byte array.

- And above byte array is written into the decoded text file, which leads to the original message.

4.2 Platform

Provided using: Java Cryptographic Extension (JCE)

The Java Cryptography Extension (JCE) provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. Support for encryption includes symmetric, asymmetric, block, and stream ciphers. The software also supports secure streams and sealed objects.

4.2 Algorithm Used

The project uses an encryption algorithm called Data Encryption Standard (DES). Whenever a text file is selected to be encoded in the Image or the Audio file, it is first encrypted using the DES Algorithm and then that file is sent to the receiver. The receiver in turn decrypts it using the same key, and thus gets the appropriate message. In a nutshell, the reason that we encrypt the message is :

Cryptography + Steganography = Secure Steganography

About DES:

Fundamentally DES performs only two operations on its input, bit shifting, and bit substitution. The key controls exactly how this process works. By doing these operations repeatedly and in a non-linear manner you end up with a result which cannot be used to retrieve the original without the key. DES works on 64 bits of data at a time. Each 64 bits of data is iterated on from 1 to 16 times (16 is the DES standard). For each iteration a 48 bit subset of the 56 bit key is fed into the encryption block represented by the dashed rectangle above. Decryptiothe is inverse of the encryption.

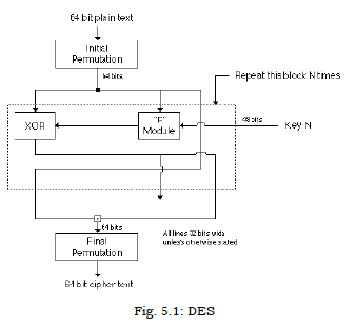


figure 5.1 is the heart of DES. It actually consists of several different transforms and non-linear substitutions.

Fig. 5.1: DES

Implementation:

Following are the steps to generate Secret keys and encryption:

1. Create an interface of the SecretKey interface. This interface contains no methods. Its only purpose is to group secret keys.

2. KeyGenerator Class: Class provides functionality of symmetric key generator. They are constructed using one of the getInstance class methods.

3. To generate key of the DES algorithm we use:

KeyGenerator getInstance(String algorithm) method with

KeyGenerator key=KeyGenerator.getInstance(―DES‖).getInstance();

4. The getInstance method generates a KeyGenerator object for the specified key algorithm from the specified provider. Some of the standard algorithms available with Java Cryptography Architecture API Specification are:

AES, DES, Blowfish, DESede, RSA.

4.0 SYSTEM ANALYSIS

SYSTEM ANALYSIS:

User Characteristics:

* CRYPT-BOX offers the following data protection features to cater to each specific user need:
* Casual Users: If you want to lock, hide and password-protect your personal pictures, videos, private files, from family and friends who would share your computer or have a prying eye on you, you need to drag and drop those files in ‘cryptbox-encrypt the files'.
* Technical Users: If you want to encrypt your project files, source codes, company documents, trade secrets, plans, copyrighted material and secret information from colleagues, employees, technical and administrators and from accidental deletion and theft.
* Network Users: If you want to protect and block your personal files and folders from shared home, public or company network, wfi, ad-hoc or blue-tooth connection.
* Company Employees: If you want to maintain a server to keep files encrypted and give limited access to the Lockers to all employees in your company.
* To prevent data-theft: If you want to secure a notebook computer so that if it gets misplaced, lost or stolen, all your important files and personal folders are inaccessible.

Definition:-

* CRYPT-BOX is a revolutionary concept in data security that allow you to lock, hide and password protect with encrypting
* your files, folders and drives, encrypt your files and folders and keeping your data synced at all times so that you won't have to worry about confidentiality of your data as well as data loss.
* Besides locking, encryption.
* STYGANO IMAGE is the modern concept in which we can hide a image into another.
* Information or a file is hidden inside a carrier file, the data is usually encrypted with a password.

6.0 SYSTEM STUDY

6.1 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

* ECONOMICAL FEASIBILITY
* TECHNICAL FEASIBILITY
* SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only ++minimal or null changes are required for implementing this system.

* Front-end- JAVA
* IDE - NET BEANS 2008

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Schedule Feasibility:

It is a measure of how reasonable the project timetable is

Implementation Feasibility: As far the implementation is concerned, there would not be any problem. All the user of it gets its service by only operate this system.

6.0 PROBLEM ANALYSIS

Problem Analysis:-

* We are asked some question for good requirement those are as follow :-

1] What is additional functionality you want in the system?

2] What are the expectation from the system?

3] How do you manage to do this work manually?

4] Is there anything else that wants to specify?

5] What are problems you face in existing system?

7.0 SYSTEM DEVELOPEMENT STRATEGY

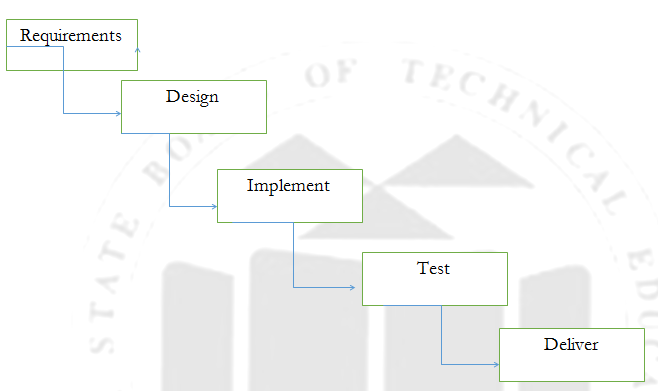
System development strategies:

* There are three distinct approaches to the development of any good system as the point of view system analysis and design.
* System development life cycle method.
* Structure analysis development method.
* System proto type method.
* Here, starting with 1st system development life cycle method.

Which has the following activities of any system?

* Preliminary investigation.
* Determination of system.
* Development of software.
* System testing.
* Implementation and evolution.

8.0 SYSTEM ENGINEERING PARADIGM APPLIED



9.0 INFORMATION GATHERING

INFORMATION GATHERING:

* Information from field
* The information is collected from non-Technical users by interviewing to them and took suggestion from end user as per there requirement .
* By asking possible question to the user during interview.
* The system mainly developed for providing high security to important data.
* Other detail are given to us from lecturer of our institute.
* Information from books

The detail designing and coding of this application are viewed from the “The complete reference:

V. K. Pachghare, Cryptography and Information Security, Prentice-hall Of India Pvt Ltd ”

10.0 SYSTEM REQUIREMENT

System Requirements:

Hardware Requirements:

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 256 Mb.

Software Requirements:

* Operating system :- Windows XP Professional
* Front End :- JAVA, Swing(JFC)
* Tool :Eclipse 3.3

11.0 SYSTEM TESTING

### 11.1 SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the

Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS:-

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

11.2 Unit Testing:

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach

Field testing will be performed manually and functional tests will be written in detail.

Test objectives

* All field entries must work properly.
* Pages must be activated from the identified link.
* The entry screen, messages and responses must not be delayed.

Features to be tested

* Verify that the entries are of the correct format
* No duplicate entries should be allowed
* All links should take the user to the correct page.

# 6.2 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results:

All the test cases mentioned above passed successfully. No defects encountered.

11.3 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results:

All the test cases mentioned above passed successfully. No defects encountered.

12.0 SYSTEM FLOW DIAGRAM

Stop

Start

Main Window

Login Form

Registration Form

13.0 SYSTEM DATA FLOW DIAGRAM

User\_Name

Password

Enter Data

D User

About

Fun Utility

General Utility

Security Tool

Exit

Main Window

14.0 TABLE OF DATABASE

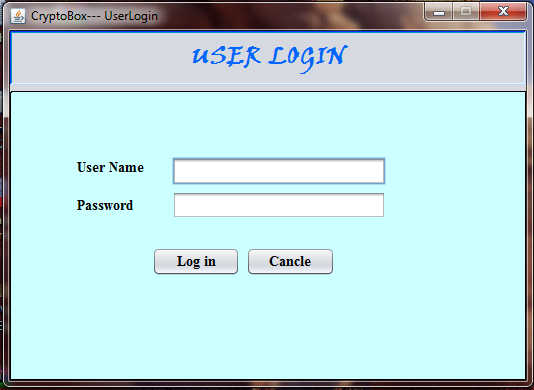
|  |  |  |
| --- | --- | --- |
| Column Name | Data Type | Null-able |
| User-Name | VARCHAR2(100) | NO |
| Password | NUM,VARCHAR2 | NO |

14.1 PROCESS ALGORITHM

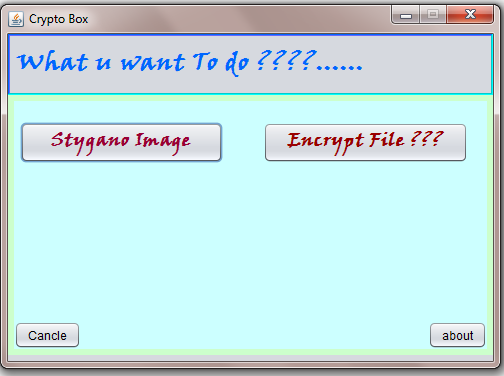
* Step1:- Start
* Step2:- Click on crypto-box application.
* Step3:- Log into application by putting user name and password.
* Step4:-Select appropriate tool.
* Step5:- For next time running. application, repeat step 2 & step 4.
* Step6:- Exit

15. INPUT AND OURTPUT DESIGN  
15.1 INPUT DESIGN

LOGIN WINDOW:

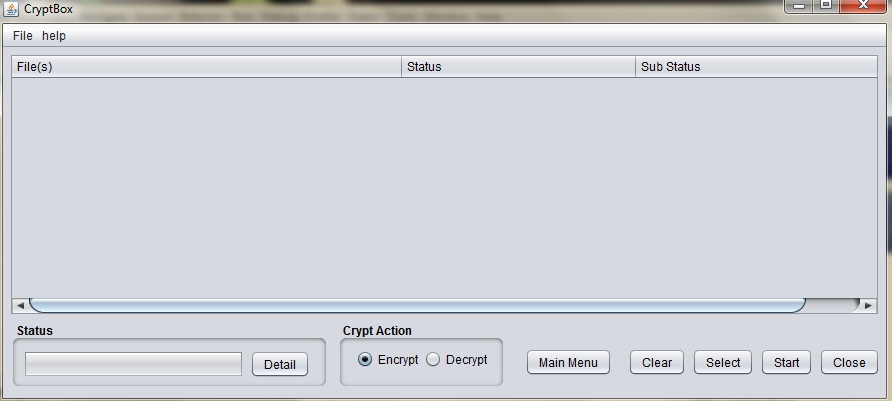


TOOLS SELECTION WINDOW:

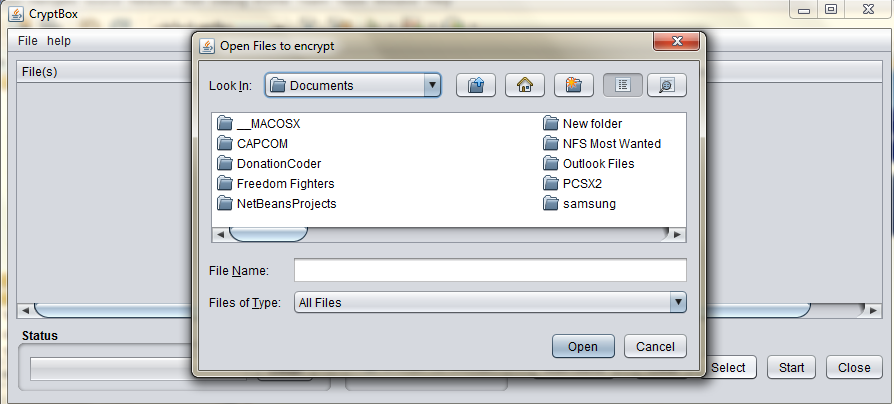


15.2 OUTPUT DESIGN

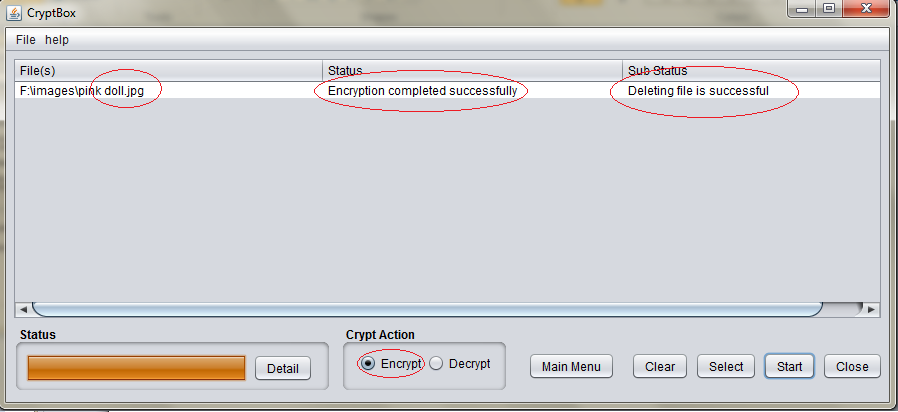
15.1 AFTER SELECTING CRYPTO-BOX TOOL:



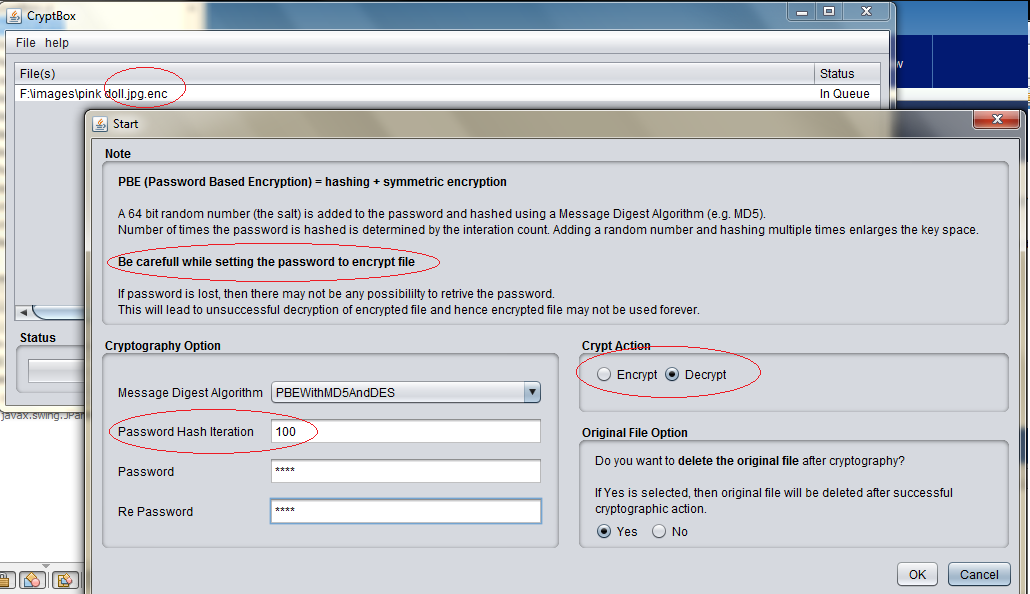
15.2 CRYPTO-TOOL FOR FILE SELECTION ENCRYPTION:



15.3 AFTER SELECTING FILE FOR ENCRYPTION:



15.4 PROVIDING SECURITY TOOL:

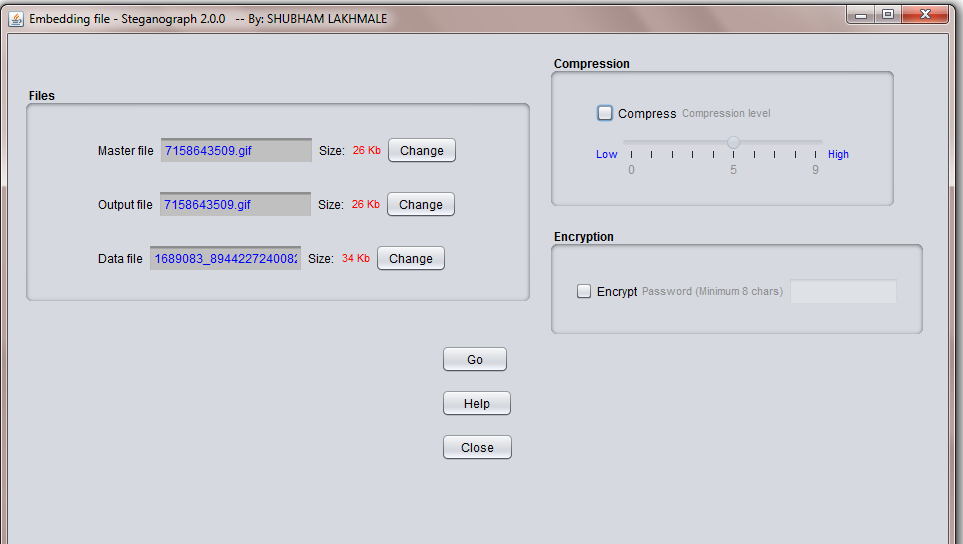


15.3 STYGANOGRAPHY OUTPUT DESIGN

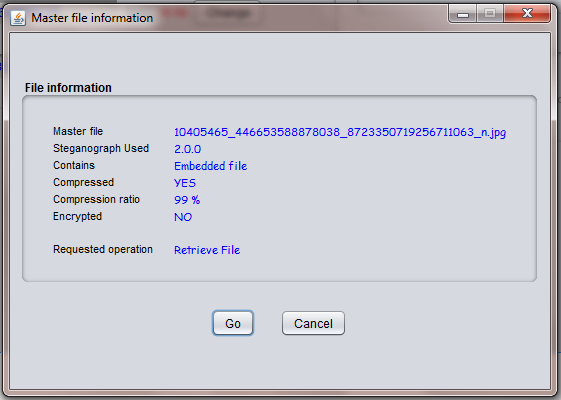
STYGANO-IMAGE main window:



15.2.2 embedding file window:



15.2.3 MASTER FILE INFORMATION:

In this phase we perform all possible test cases some of them are :-

16.0 TEST CASE

Registration/ Log-in Form :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Testing registration form | \* Application must be in running state. | \*Click on add  \*enter  User information | The entered information must be saved | The entered information is saved | pass |
| 2 | To test the login form | \* Application must be in running state. | \*enter id & password | (correct UI UP)  The login must be successfully | The login is successfully | Pass |

**Lock/Unlock Desktop Form :-**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Lock desktop | Application must be in running state. | -Security tools-lock desktop | Desktop must be locked | Desktop is locked | pass |
| 2 | Unlock desktop | Application must be in running state. | Security tools-lock desktop | Desktop must be unlocked | Desktop is unlocked | Pass |

Lock/Unlock Drive Form :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Lock unlock drives | Application must be in running state. | Security tools –lock unlock drive | Selected drive must be locked | drive is locked | Pass |
| 2 | Lock unlock drives. | Application must be in running state. | Security tools –lock unlock drive | Selected drive must be unlocked | Drive is unlock | Pass |

Folder-Locker Form :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Folder locker | Application must be in running state. | Security tools folder locked/ unlocked | Selected folder must be locked/ unlocked | folder must be locked/ unlocked | pass |
| 2 | Folder  Locker | Application must be in running state. | Security tools folder unlocked | Selected folder must be unlocked | folder must be unlocked | pass |

System Volume Cleaner:-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | System volume | Application must be in running state. | General utility-System volume cleaner | System volume must be cleaned | System volume is cleaned | Pass |

Temporary File Remover :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Temporary file remover | Application must be in running state. | General utility-temporary file remover | Temperary file  Must be deleted | Temporary file is deleted | Pass |

Start Up Program :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Start up program | Application must be in running state. | General utility-System volume cleaner | program must be start when reboot | Program is start when reboot | Pass |

Show/Hide Notify:-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sr no | Objective of test case | Pre-requisites | Steps | Expected result | Actual Result | Status |
| 1 | Hide notify | Application must be in running state. | Functionality-hide notify | Notification must be hidden | Notification is hidden | Pass |
| 2 | Show notify | Application must be in running state. | Functionality-show notify | Notification must be display | Nonfiction is display | Pass |

17.0 FURTHER ENHANCEMENT OF SYSTEM

17.1 Future Scope:

 This module can be further extended to have support for the Video files.

 Currently, for encoding, we use this software and for transmission we use some other medium. So the current software can itself be used to transmit the files also.

 Currently , the length of the message file has some limitations for the Audio Steganography, so for the same, we can have support for a wider size of files.

 Can be implemented as a plugin to a web browser

17.2 CRYPTOGRAPHIC FUTURE SCOPE:

This module can further extended for security puroposes also can be used in most significant purposes.

Currently most algorithm used in this is hashing MDA5

And can be more chances developing as per the requirements also in critical conditions

Now the currently used algorithm is MDA5 ,after the MDA4 algorithm i.e Message Digest Algorithm.

18. Reference:

* Microsoft .Net Framework 4.0 Windows Form Development.
* Vb.Net Black Book.
* Introduction to MICROSOFT Access
* [www.Vb.net.com](http://www.Vb.net.com)
* [www.vbtutorial.com](http://www.vbtutorial.com)
* [www.google.com](http://www.google.com)
* www.freeproject.c

19. Conclusion:

* This was our Project of System tool for various

Application “CRYPTO-BOX”.

* We Think this application gave lot of satisfaction

to the user.

* Every Program is never said to be Perfect & Bug free, same for our Application, there may be some more improvement are possible.
* We learn so many things & lot of Knowledge about developing the software. even it is basic of

development.

* We hope this will proved faithful to us

**20.0 Future Scope:-**

* Cryptography.
* Image Extractor.
* Data Recovery.
* Password on Mobile.
* Direct login on lock directory.

THANK YOU…..