

Secure Communication system using Steganography and Cryptography

A MINI PROJECT REPORT

SUBMITTED TO

Computer Science And Engineering Department,
WCE, Sangli

Jadhav Rohit Bhimrao 2012BCS015

Joshi Sarang Rajendra 2012BCS025

Langote Gopinath Tejerao 2012BIT011

T.Y. B.Tech. (CSE)

UNDER THE GUIDANCE OF

Ms. N.L.Mudegol

Assistant Professor

Dept of Computer Science And Engineering
WCE, SANGLI.



Department Of Computer Science And Engineering

WALCHAND COLLEGE OF ENGINEERING

(An Autonomous Institute)

Vishrambag, Sangli - 416415, Dist-Sangli



Department Of Computer Science And Engineering
WALCHAND COLLEGE OF ENGINEERING,SANGLI

Certificate

This is to certify that the Third year B.Tech. project entitled
Secure Communication system using Stenography and Cryptography
Submitted by

Jadhav Rohit Bhimrao 2012BCS015
Joshi Sarang Rajendra 2012BCS025
Langote Gopinath Tejerao 2012BIT011

is a bonafide work carried out by her under the supervision of NAME OF GUIDE and
submitted towards the partial fulfillment of the requirement for the award of the degree of
Bachelor of Computer Science and Engineering of the Walchand College of Engineering,
Sangli is a bonafide work carried out during academic year 2014-15.

GUIDE NAME

Guide

CSE Department

Examiner(s)

1.

2.

Date :

Place: Walchand College of Engineering Sangli.

Dr.B.F.Momin

Head of the Dept

CSE Department

Acknowledgement

T.Y.B.Tech.(Computer Science And Engg.)

Jadhav Rohit Bhimrao 2012BCS015

Joshi Sarang Rajendra 2012BCS025

Langote Gopinath Tejerao 2012BIT011

Date :

Place: Walchand College of Engineering, Sangli.

Abstract

I and when the send button is clicked the message will be encrypted and the frame captured at that moment will be the carrier file. The message then goes to a hiding process and then at receiving station the process backward.

In this project we tried to maximize the level of security needed to send some messages among users. The design of the system includes a four steps process, the first two occur at the sending station and the other two are at the receiving station. The processes are (Encryption, Hiding, Decryption and Revealing) sequentially. The sender will write a message

Index

1 Introduction

1.1 Preface	7
1.2 Existing Techniques	7
1.3 Motivation	7
1.4 Proposed System	7
1.5 Features of proposed system	8
1.6 Mathematical Model	8
1.7 Relevance of project	8

2 Literature Survey

2.1 section 1	10
2.2 section 2	10

3 Software Requirement Specification

3.1 Introduction	11
3.1.1 Purpose	11
3.1.2 Project Scope	11
3.2 System Features	11
3.2.1 Feasibility	11
3.2.2 Efficiency.....	11
3.3 External Interface Requirement	12
3.3.1 User interfaces	12
3.3.2 Hardware interfaces	12
3.3.3 Software interfaces	13
3.4 Non-Functional Requirement	14
3.4.1 Performance Requirement	14
3.4.2 Software Quality Requirement.	14
3.5 Other Requirement	14
3.5.1 Legal Requirements	15

3.6 Analysis Model	15
3.6.1 Data Flow Diagrams	15
3.6.2 System Implementation Plan	
4.system design	
4.1 Flow of Proposed System	16
4.2 Usecase Diagram	16
4.3 Sequence Diagram	17
4.4 Activity Diagram	18
4.5 Project Flow Diagram	19
5 Technical Specification	
5.1 used PL1	20
5.2 used software 1	20
6 Software Implementation	
6.1 Introduction	20
6.1.1 Problem Statement	20
6.2 System Architecture	20
6.2.1 Module 1	21
7 Software Testing	
7.1 Test Cases	27
8 Result Analysis	
8.1 Result Snapshots	28
9 Conclusion And Future Work	
9.1 Conclusion	33
9.2 Future Work	33
References	

Introduction

1.1 Preface

This software is based on the security domain and have the goal to secure transfer of the messages from one client to another. In this project, we used a stenographer and cryptography to complete this purpose.

There are many chatting applications and security hardly available in any of them so objectives are

- 1) security
- 2) efficiency
- 3) low time constraints

This software works fine in autonomous system means in an Ad-hoc network.

1.2 Existing techniques

There are many chatting applications are available like secure chat which also one of the secure chatting application in which different techniques are used than this.

1.3 Motivation

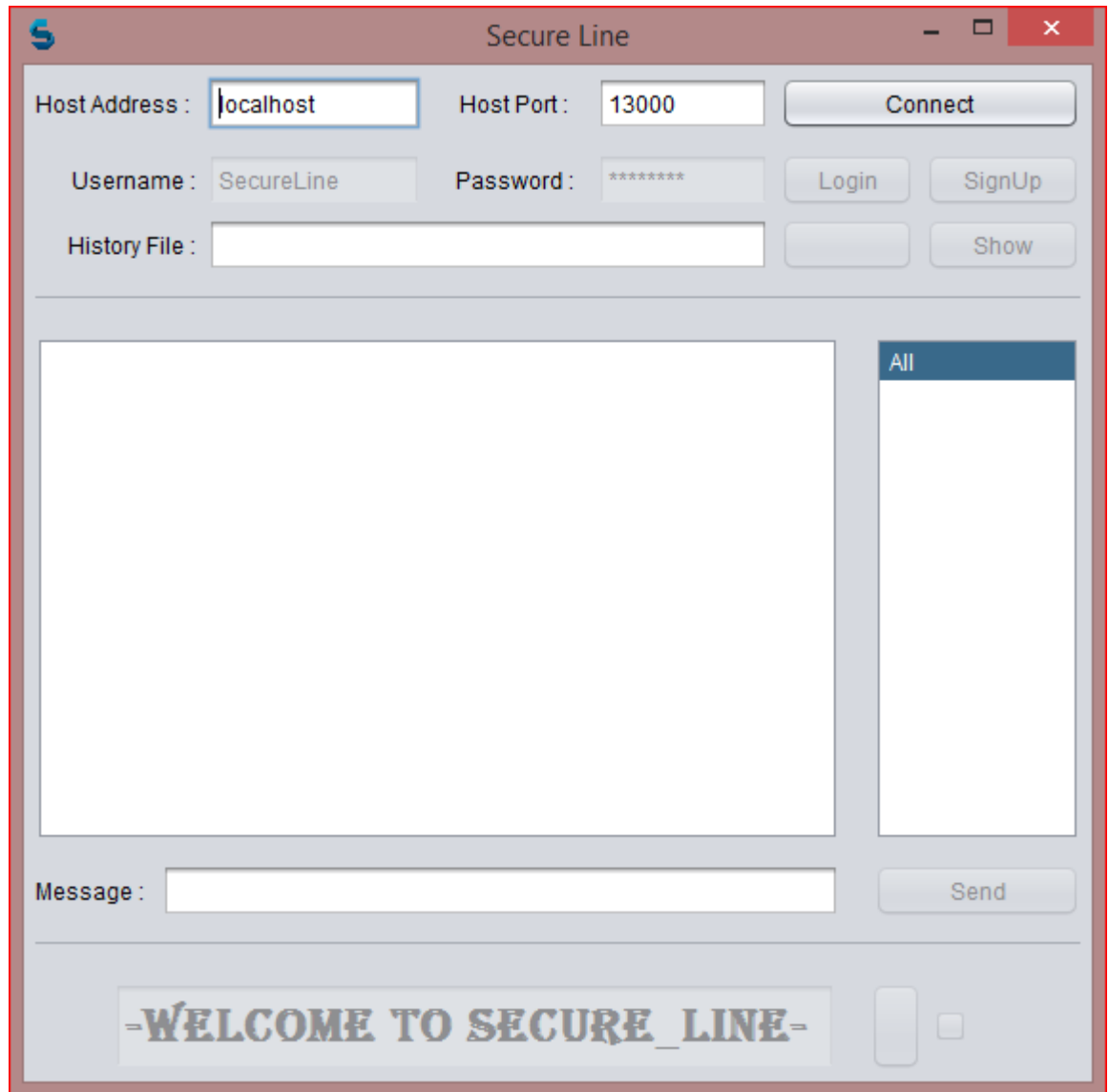
1) Now-a-days hacking from the internet stream has been increased on the large scale and if any two person want to communicate it will be risk for sharing important data so security is really important.

2) There is need of software which is easy to use and efficient and also secure for sharing important data.

3) In particular Ad-hoc network, like institution or company needs to communicate real fast and securely.

1.4 Proposed system

To fulfill above requirements we build the chatting application, called "Secure-line" which is secure, user-friendly and efficient.



1.5 Features of proposed system:

1. It is easy to install
2. It is Secure by using Steganography and Cryptography
3. It is Efficient
4. It is fast.

1.6 Mathematical Model

It is Dynamic model where we can create many users as we want and can

communicate with any of them.

Here consider

S = Stenographic,

C = Cryptography,

N = Network,

I = Input,

O = Output,

E = Encrypted message,

D = Decoded message

$$E=(I \cup S \cup N) \text{_____} (1)$$

$$D=(E \cup C \cup S \cup N) \text{_____} (2)$$

$$O=(D \cup N)$$

1.7 Relevance of project

This software is very efficient and it can send big message within a second so time

Literature Survey

Victor Grigoras¹ , Carmen Grigoras “Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems”

Chaos Encryption algorithm is based on this paper for Large Signal Modulation in Additive Nonlinear Discrete-Time Systems”

E. N. Lorenz, “ Deterministic non periodic flow,”

This is paper used for the Deterministic non periodic flow, which form very useful for finding the non repeating numbers

Software requirement specification

3.1 Introduction

3.1.1 Purpose

Now-a-days hacking from the internet stream has been increased on the large scale and if any two person want to communicate it will be risk for sharing important data so security is really important. There is need of software which is easy to use and efficient and also secure for sharing important data. In particular Ad-hoc network, like institution or company needs to communicate real fast and securely.

3.1.2 Project scope

It works in Ad-hoc network and it can be work with public IPs.

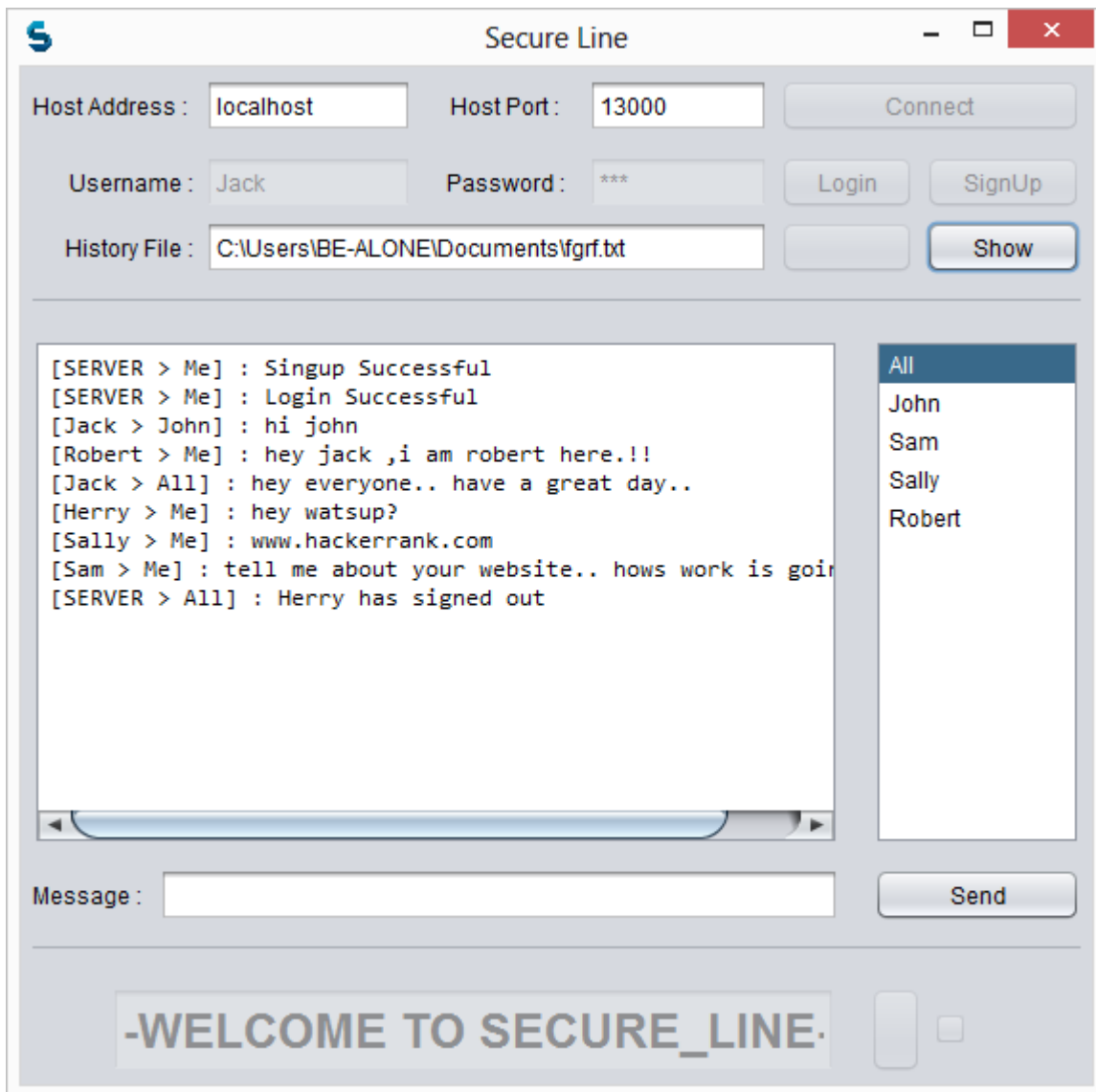
3.2 System Features:

1. Efficiency
2. Fast
3. Secure
4. User Friendly

3.3 External Interface Requirement

User interfaces:

1. It is basically developed through java.
2. By click on send button we can send it to the specific client which we have selected.



Hardware Interfaces:

Requirements:

1. It requires network topology
2. It runs on Intel dual core and above versions of processors.

Switches:

A **network switch** is a computer networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device. A network switch is considered more advanced than a hub

because a switch will only forward a message to one or multiple devices that need to receive it, rather than broadcasting the same message out of each of its ports.



Software Interface:

Requirements:

1. JVM, JRE 1.0 and above for running
2. Runs on windows 98 and above i.e. specifically windows platform.

3.4 Non Functional Requirements

3.4.1 Performance Requirements:

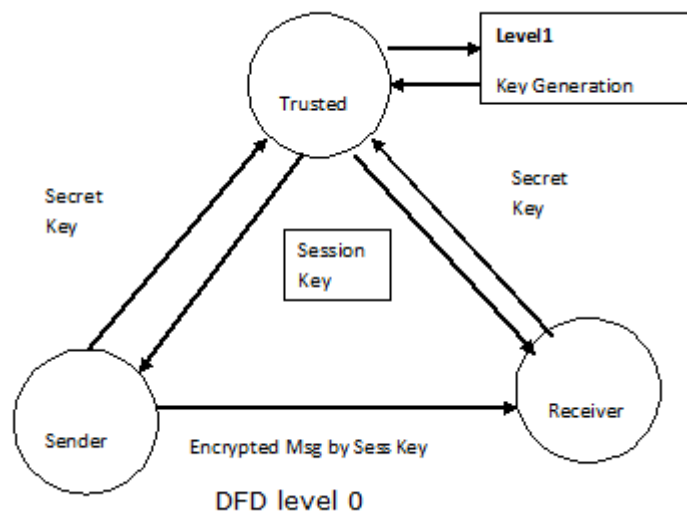
1. RAM is above 256 MB
2. Internet speed must be high i.e. the speed of message delivering is also depends on your internet speed.
3. Server must be on.

3.5 Other Requirements

You must be authorized user of the “Secure-line”to use the service of this software.

3.6 Analysis model

3.6.1 Data Flow Diagram



It shows the the actual data flow of the software or system. and it explained in system implementation plan.

3.6.2 System Implementation plan:

Basically, we divided our system in three different parts

1. Networking
2. Cryptography
3. Steganography

In networking, how multiple clients can be handled with the single server using threading concepts in java.

Staganography is used for embedding message into the image and for that specific algorithm is used.

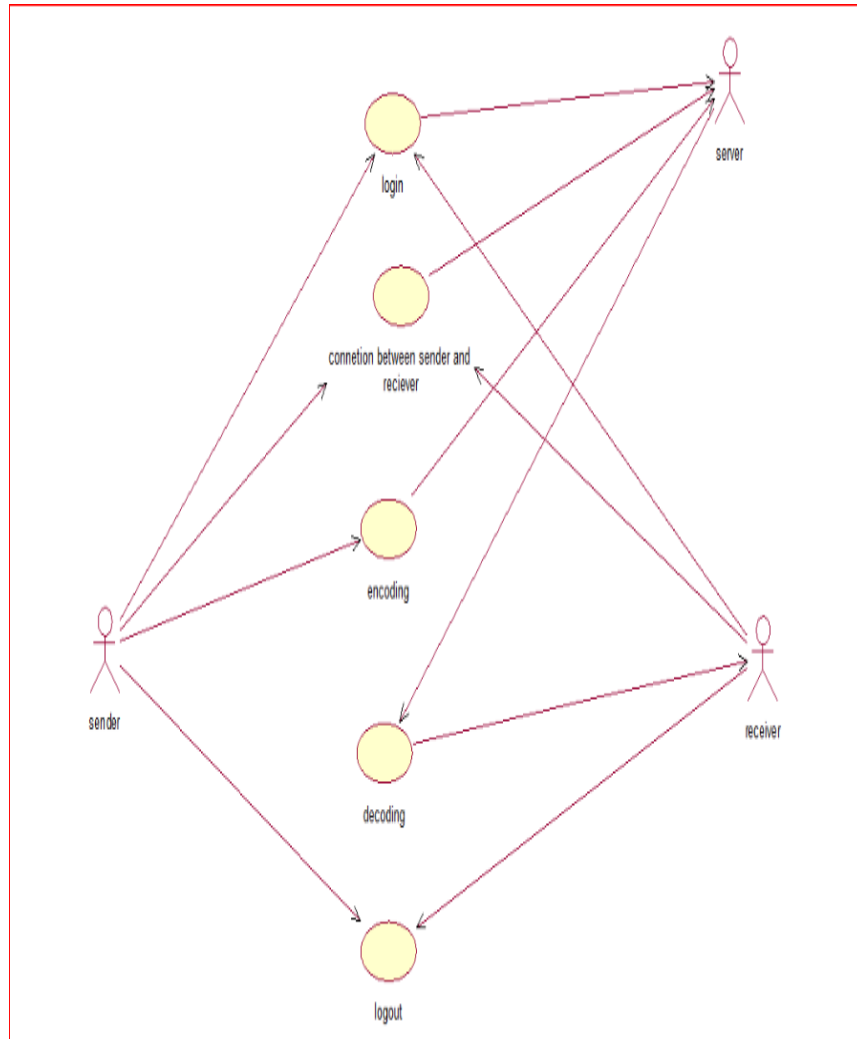
In cryptography, the embedded image is made diffused using the pixel swapping algorithm.

In networking, how multiple clients can be handled with the single server using threading concepts in java.

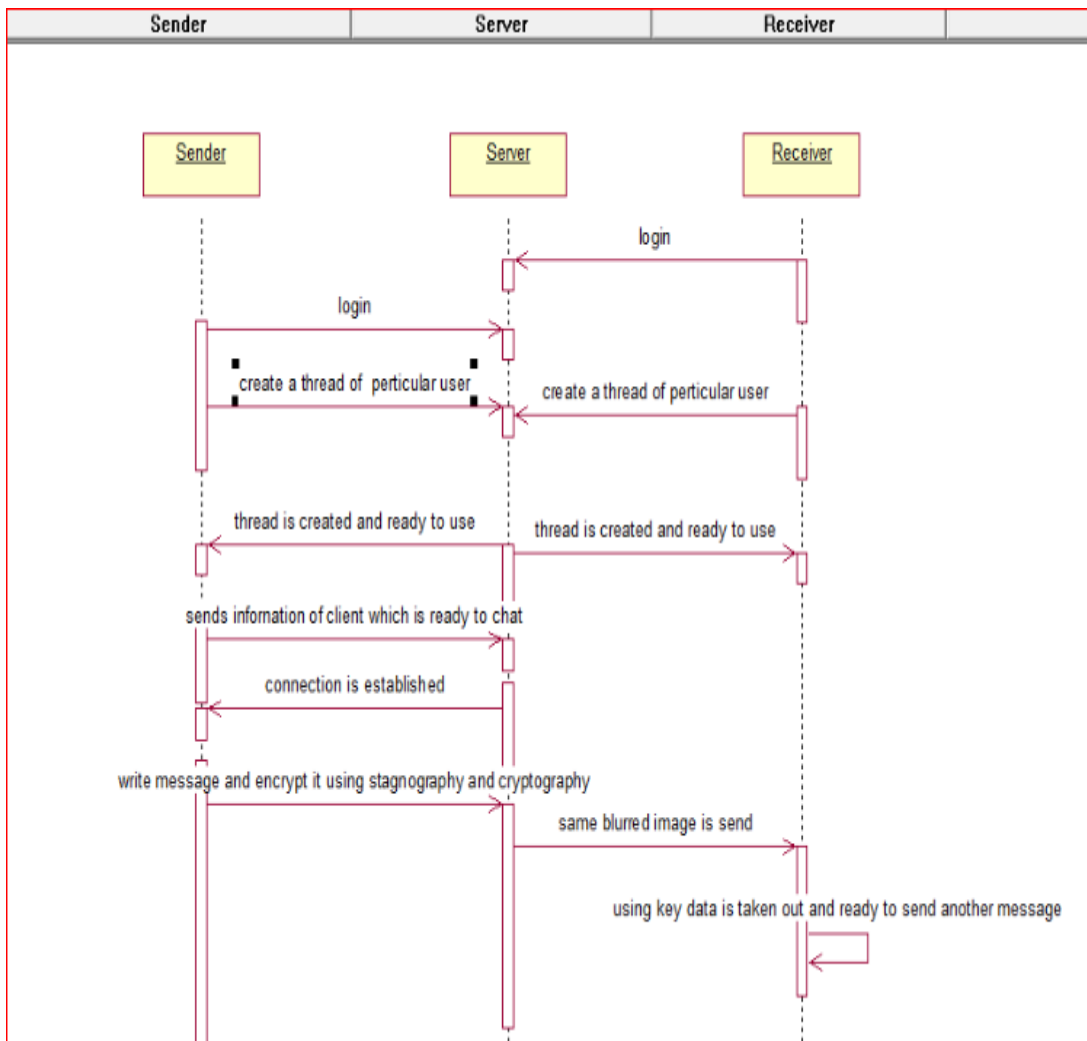
Firstly, message will embed into the image then it will send for encryption and then it will send into the network. And at recipient it is correctly opposite i.e receive from network, decryption and the revealing message from image.

System Design

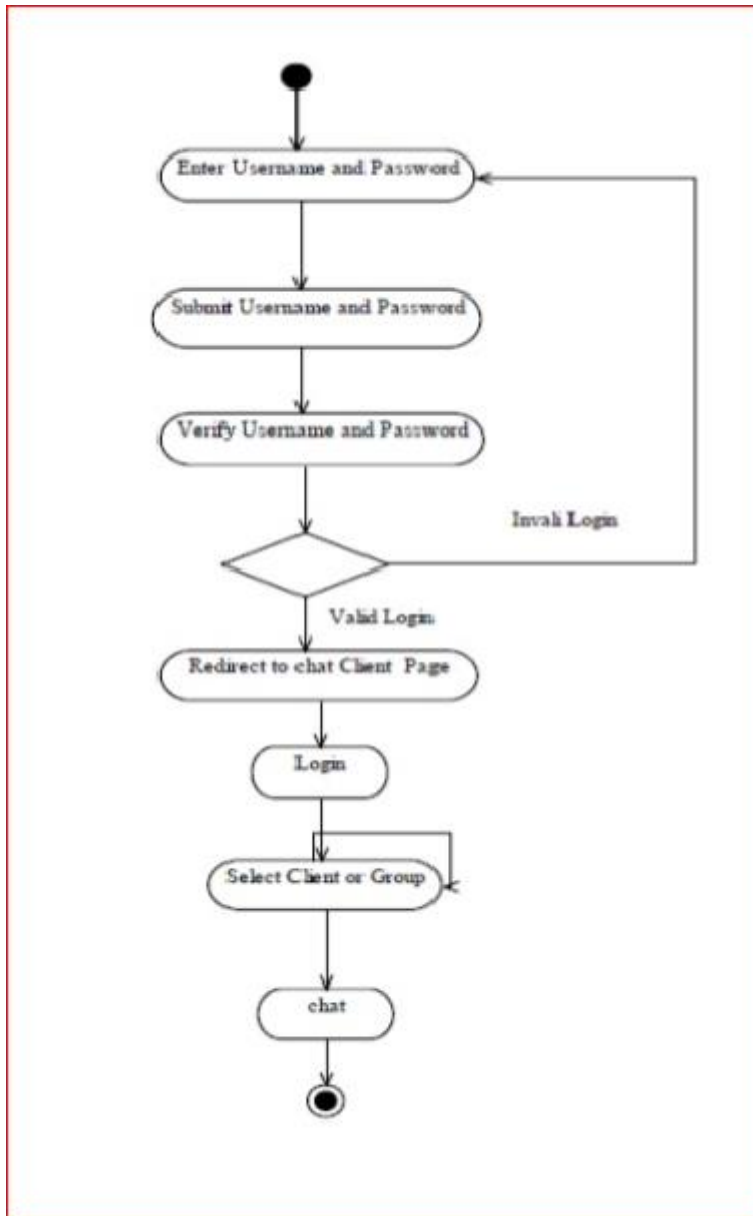
4.1 Use case diagram:



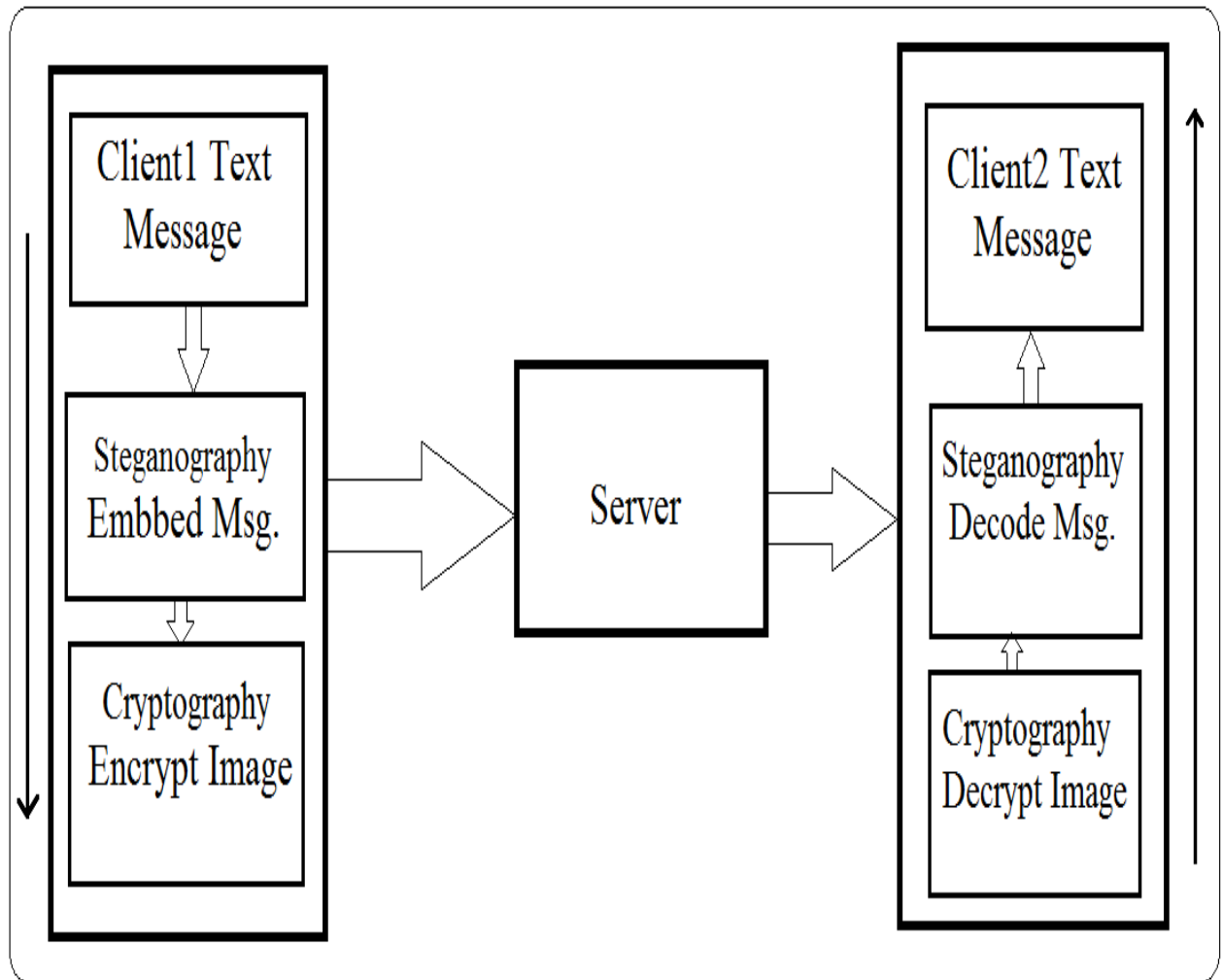
4.2 Sequence diagram



4.3 Activity diagram



4.4 project Flow Diagram



Technical Specification

5.1 used PL

Project is basically developed through the “java” programming language and different available packages are used.

5.2 used software:

EditPlus and Eclipse are used for the core programming and “Net Beans” for GUI.

Software Implementation

6.1 Introduction

6.1.1 Problem Statement

Chatting application within clients using ad-hoc network using concepts of Multithreading, RMI, steganography and cryptography. For implementation of all concepts standard algorithms should be used.

6.2 System architecture

1. Networking

2. Steganography

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word *steganography* combines the Ancient Greek words *steganos* meaning "covered, concealed, or protected",

and *graphein* meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other *cover text*. For example, the hidden message may be invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Image before Embedding message:



Image after embedding message:



Cryptography:

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that block adversaries various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Cryptology-related technology has raised a number of legal issues. In the United Kingdom, additions to the Regulation of Investigatory Powers Act 2000 require a suspected criminal to hand over his or her decryption key if asked by law enforcement.

Otherwise the user will face a criminal charge.[5] The Electronic Frontier Foundation (EFF) was involved in a case in the United States which questioned whether requiring suspected criminals to provide their decryption keys to law enforcement is unconstitutional. The EFF argued that this is a violation of the right of not being forced to incriminate oneself,

Image Before Swapping the pixel:



Image After Swapping the pixel:



After Rearranging the pixel:



Here we use the chaos theorem for cryptography

This theorem is as follows:

Consider an image (I_o) with dimension $M \times N \times P$, Where, P represents color combination (3 for a color image); M, N represents rows and column of intensity level. Separate R,G, B matrix of Image and convert each R,G,B matrix into single array ($1 \times mn$). For example, Lena image which is one of the common image used for image processing algorithms has a dimension of $225 \times 225 \times 3$ and after separation of R,G,B and converting it in to single array vectors, we get 3 vectors of dimension 1×50625 .

For encryption we first generate elements from chaos map equal to the dimension of $3 \times M \times N$ matrix. In our example of Lena image $225 \times 225 \times 3 = 151875$ elements are generated with Henon map. The Henon map can be generated using the equation given below which is iterated for $n=1$ to 151875 times to generate the required elements.

$$x(n+1)=1-a*x(n)^2+y(n); y(n+1)=b*x(n);$$

We used the following values for the constants 'a' and 'b' to get a random sequence.

$$a=1.76, b=0.1 \text{ and } y(n)=1$$

The same procedure is repeated with Lorentz map. Following equations describes Lorentz map.

$$\begin{aligned} X(1) &= s*(y(i-1,2)-y(i-1,1)); \\ X(2) &= r*y(i-1,1)-y(i-1,2)-y(i-1,1)*y(i-1,3); \\ X(3) &= y(i-1,1)*y(i-1,2)-b*y(i-1,3); \\ y(i,:) &= y(i-1,:)+h*X; \end{aligned}$$

For this map, we used the following values for the constants 's', 'y', 'h', 'b' and 'r' to get a random sequence.

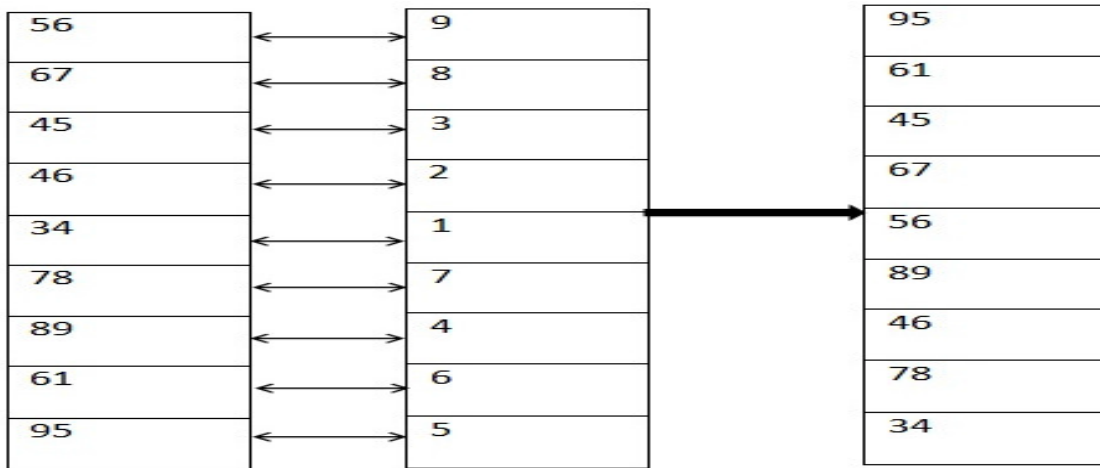
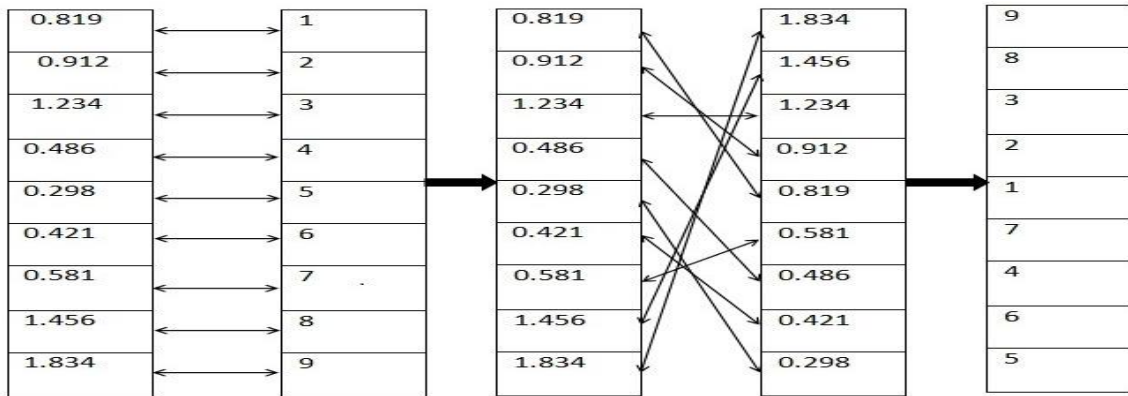
s=10,b=3,r=30,h=0.01 and y=[0.1,0.1,0.]

65	36	96	---	---
12	97	34	--	--
98	78	98	--	--
45	54	88	-	--
--	--	--	--	--
--	--	--	--	--

Here care should be taken to see that the generated elements are unique; there shouldn't be any repetition. Now divide the generated elements into three blocks of each equal to $M \times N$. In our example of Lena image each block is of dimension 1×50625

65	98	98	---	---
78	80	78	--	--
55	45	67	--	--
97	76	87	-	--
--	--	--	--	--
--	--	--	--	--

Now sort the elements of each block in ascending or descending order and compare the disorder between the original and sorted elements of each block and tabulate the index change. We have got three series of index change values in according to three blocks. For example consider the first array from the previous table.



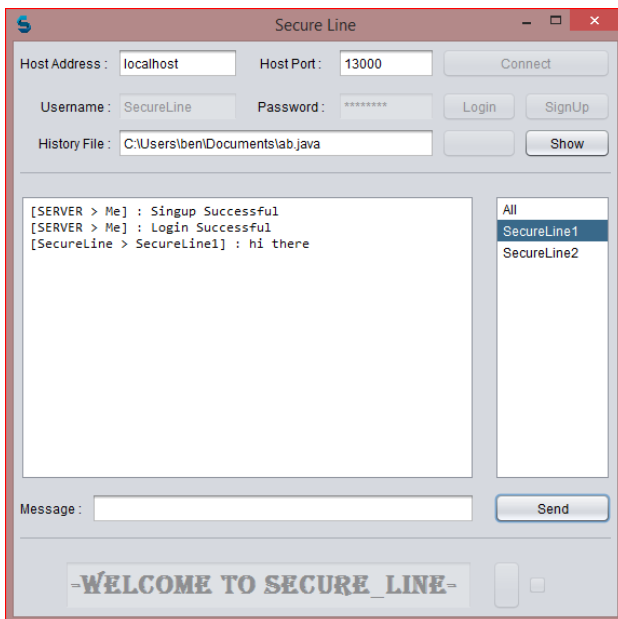
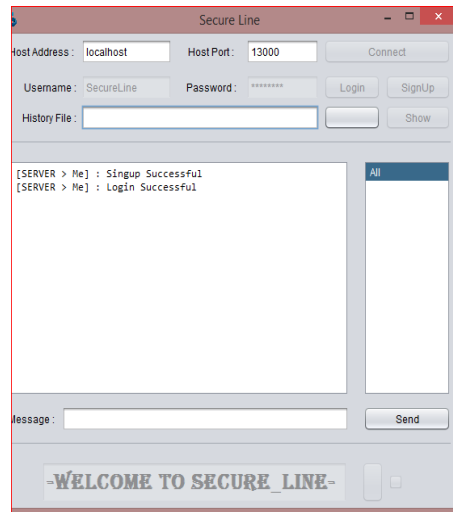
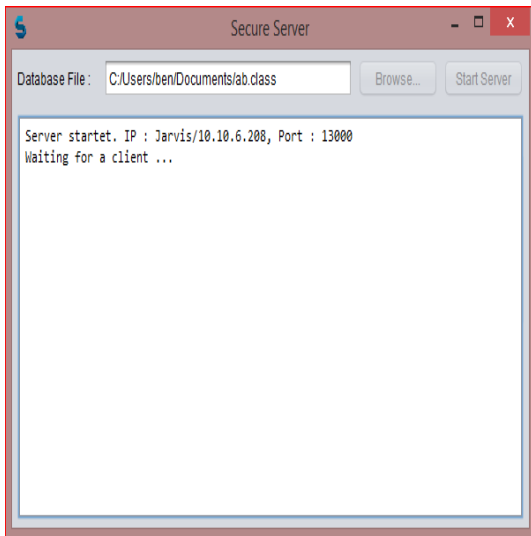
Software Testing


7.1 Testing

Test cases	Excepted	Result
Whether login can be done if server is not available?	NO	NO
Whether login and logout can be done when sever Is available?	YES	NO
Whether allow duplicate user?	NO	NO
Can it work with global IP?	YES	NO
Whether message is delivered to specific user?	YES	YES
Can Message Securely be send?	YES	YES
Whether image is reusable?	YES	YES

Result Analysis

Result Snapshots:




Secure Line

Host Address :
Host Port :

Username :
Password :

History File :

```

[SERVER > Me] : Signup Successful
[SERVER > Me] : Login Successful
[SecureLine > Me] : hi there

```


All

SecureLine

SecureLine2

Message :

=WELCOME TO SECURE_LINE=


Chat History

History :

Sender	Message	To	Time
Me	hi there	SecureLine1	Tue Dec 09 ...

Conclusion and Future Work

9.1 Conclusion:

Whether image is reusable?

Hence we have developed chatting application through which we can chat securely and developed using different algorithms of steganography and Cryptography

9.2 Future work

1. Try to make it work on Global IP
2. Try to Send multimedia data
3. Try to improve efficiency i.e. speed

References:

- [1] Victor Grigoras¹ , Carmen Grigoras “Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems” Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18, 2006.

- [2] Mintu Philip, Asha Das “Survey: Image Encryption using Chaotic Cryptography Schemes” IJCA Special Issue on “Computational Science - New Dimensions & Perspectives” NCCSE, 2011.

- [3] E. N. Lorenz, “ Deterministic nonperiodic flow,” J.Atmospheric Sci. 20 (1963) 130.

- [4] Chen Wei-bin; Zhang Xin; “Image encryption algorithm based on Henon chaotic system” Image Analysis and Signal Processing, 2009. IASP 2009. International Conference, Publication Year: 2009, Page(s): 94 – 97.