A

Project Report

on

Network Security using StegoCrypt

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

B.E. Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Yogita G. Motiramani
Rudra J. Vivarekar
Nikita J. Kolhe
Darshana A. Mundada

Under the Guidance of

Miss. Priti R. Sharma

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)

2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Project Report entitled by Network Security using StegoCrypt has been satisfactorily completed by,

Yogita G. Motiramani
Rudra J. Vivarekar
Nikita J. Kolhe
Darshana A. Mundada

in partial fulfillment of the degree of *Bachelor of Engineering* in *B.E. Computer Engineering* under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 7, 2016
Place: Jalgaon

Miss. Priti R. Sharma
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgement

We thank GOD almighty for guiding us throughout the Project Report. We would like to thank all those who have contributed to the completion of the project and helped me with valuable suggestions for improvement. Our sincere thanks to principal Dr. Prof. K. S. Wani sir, SSBT's COET for having provided us facilities to complete our seminar. We would like to express my gratitude and appreciation to all those who gave us the possibility to complete this report. A special thanks to Dr. Prof. G. K. Patnaik sir, head of the department, whose help, stimulating suggestions and encouragement, helped us to coordinate our project especially in writing this report. Last but not least, many thanks go to the guide of project, Miss. Priti R. Sharma whose have given her full effort in guiding the team in achieving the goal as well as her encouragement to maintain our progress in track. We thank all Staff members of our college and friends for extending their cooperation during project report. Above all We would like to thank our parents without whose blessings, we would not have been able to accomplish my goal.

Yogita G. Motiramani
Rudra J. Vivarekar
Nikita J. Kolhe
Darshana A. Mundada

Abbreviations

LSB Least Significant Bit

PCC Play Color Cipher

RSA Rivest, Shamir and Adleman,

UML Unified Modelling Language

Contents

List of Figures

Abstract

Information security plays a vital role in communication. The threats to information security have been incrementing at confounding rate. The most influential approaches used against such threats are cryptography and steganography. Cryptography and Steganography are two most popular ways to secure data transmission. However, combination of these two techniques results in appearing a highly secured method for data communication. In the proposed system for cryptography, the algorithm of substitution is based on Play Color Cipher and asymmetric RSA algorithm is used to make Play Color Cipher key in encrypted form. In steganography, encrypted key is hidden using multimedia steganography technique.

Chapter 1

Introduction

Security is main concern regarding data transfer. Integrity of data is important factor for the both sender as well as receiver. In today's times, many techniques are used to ensure the same; those techniques are cryptography and steganography.

Cryptography serves as an important tool for sending information securely in communication system. The cryptography basically takes place between the sender and receiver. The process involved in the communication between the sender and receiver is of two types, encryption and decryption. Encryption is a process where in the ordinary information also called as the plain text is coded into some unrecognizable form which is usually called the Cipher text. The decryption process starts with converting the cipher text which is in the unrecognizable form to ordinary information that is plain text [**?**].

Steganography is data hidden within data. Steganography techniques can be applied to images a video files or an audio files. Typically, however, strganography is written in characters including hash marking, but its usage within images is also common.At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorised viewing. Steganography must not be confused with cryptography. The main goal of steganography techniques is that it is difficult to detect the image and so saved from attack [**?**].

A new technique proposed with combination of cryptography and steganography enhance with new secure feature for generating a new security system. A secure data transmission is made using cryptography and steganography. Combination of this two techniques results in appearing a highly secured method for data communication [1].

In this chapter, section 1.1 Background is described. Motivation is described in section 1.2. In section 1.3 problem definition described. Scope of the project is described in section 1.4. Section 1.5 describes objectives. Organisation of report is described in section 1.6. Finally, last section is of summary.

1.1 Background

The present scenario in the data transmission or communication includes number of cryptography techniques like RSA, DES etc [**?**]. But sometimes there is a possibility of the information, message or our private data which we are sending from sender to receiver in the encrypted form is recognized by the third person that is intruder or hacker. In this the problem is our private data is not protected by the existing cryptographic techniques. The proposed solution is somewhat more efficient than the existing ones. It would be rather more prudent if we can send the secret information, either in plain text or cipher text, by cleverly embedding it as part of a cover media (for example, an image, audio or video carrier file) in such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media. This idea forms the basis for Steganography, which is the science of hiding information by embedding the hidden (secret) message within other, seemingly harmless images, audio, video files or any other media [**?**]. And more secure way is the combination of both techniques i.e. cryptography and steganography.

1.2 Motivation

The existing problem is important to solve because the data or private information which we are sending from sender to receiver is hack by the third party that is intruder or hacker and they are easily understand the information. At that time the confidentiality of the private data is totally lost. The proposed system provides the technique which keeps the information that user wants to send confidential. Because the data is encrypted using Play Color Cipher cryptography technique and Steganography technique.

1.3 Problem Definition

Cryptography and steganography are the key technologies for secure communication over network. This system consists of sender side and receiver side. At sender side, system takes input text from user. This text is substituted with color block by using Play Color Cipher algorithm. This algorithm generates a symmetric key (PCC key). Before transmission, PCC key is encrypted using encryption algorithm and generates cipher key. Then generated cipher key is hidden using multimedia steganography technique. At receiver side, user first recovers the hidden key. After recovering, user decrypt cipher key and generates plain text (PCC key). Using Play Color Cipher algorithm, user decrypts color coded text and generates plain text.

1.4 Scope

- It is the technique of encrypting the data and hide that data in the cover media which is unpredictable for unintended user. It also keep private information confidential, so it is of vital use in forces like Army, Navy and Air force.
- The system provides the security and integrity of data or information.
- It will provide a more clear and non ambiguous description of the functions.
- The system is highly user friendly.
- The software provides clarity in its functionality even to nave.

1.5 Objective

- The objective of the proposed system is to provide a double security to data.
- Confidentiality(the information cannot be understood by anyone for whom it was unintended).
- Integrity(the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected).

1.6 Organization Of Report

This chapter involves the basic introduction to the Proposed System, Problem Statement, Problem Definition, Objective, and Future Scope. The system analysis is done in second chapter, which includes Literature Survey, Existing System, Proposed System, Feasibility Study, Risk Analysis. Chapter 3 talks about the system requirements and specifications which includes Software Requirement, Functional Requirement, Non Functional requirement. The system designing concepts are involved into chapter 4 including Proposed System Flow, Data Flow Diagram, UML Diagram, Advantages and Limitations.

1.7 Summary

This chapter focuses on the basic introduction towards the system including Problem Statement, Problem Definition, Objective, and Scope. The next chapter will focuses on analysis of the proposed system.

Chapter 2

System Analysis

Analysis is a software engineering task that bridges the gap between system level requirements engineering and software design. Requirements engineering activities result in the specification of softwares operational characteristics (function, data, and behavior), indicate software's interface with other system elements, and establish constraints that software must meet. Requirements analysis allows the software engineer (sometimes called analyst in this role) to refine the software allocation and build models of the data, functional, and behavioral domains that will be treated by software.

This chapter is organized as follows. In section 2.1 Literature Survey is described. Proposed System is described in section 2.2. In section 2.3 Feasibility is described. Risk Analysis is described in section 2.4. In section 2.5 Project Scheduling is described. Effort Allocation is described in section 2.6. Finally, the last section is of summary

2.1 Literature Survey

Many studies on data hiding in images,audio and video have been performed recently.The Internet has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life. As of September 2009, approximately 1.73 billion people worldwide use Internet for various purposes ranging from accessing information for educational needs to financial transactions, procurement of goods and services [1]. As the modern world is gradually becoming paperless with huge amount of information stored and exchanged over the Internet, it is imperative to have robust security measurements to safeguard the privacy and security of the underlying data.

There are different types of approaches for preventing the security attacks. The most useful approaches are

1. Cryptography

2. Steganography

3. Digital Watermarking

2.1.1 Cryptography

The word cryptography is derived from two Greek words which mean "secret writing".Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others.Cryptography is an effective way to protect the information that is transmitting through the network communication paths [**?**].

- **RSA:** RSA was first developed in 1977. RSA functions depend upon the large prime numbers of public and private keys. The security is also based on the difficulty of prime numbers. The RSA algorithms are used in public key encryptions as well as in digital signatures. It allows the sender to encrypt the message using public key and decrypt the message using private key by receiver. So,the security will be high using RSA in public key encryption [**?**].

- **DES:** The Data Encryption Standard (DES) was jointly developed in 1974 by IBM and the U.S. government (US patent 3,962,539) to set a standard that everyone could use to securely communicate with each other. It operates on blocks of 64 bits using a secret key that is 56 bits long. The original proposal used a secret key that was 64 bits long. It is widely believed that the removal of these 8 bits from the key was done to make it possible for U.S. government agencies to secretly crack messages [**?**].

2.1.2 Steganography

Steganography in Greek means "covered writing". Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganographic techniques available to hide the data depending upon the carriers we use.Steganography and cryptography both are used for the purpose of sending the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption and secret key. In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption.Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object the suitable formats are used. "Redundancy? is the process of providing better accuracy for the object that is used for display by the bits of object [**?**].

- **LSB:** LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding message into the image. The Least Significant Bit insertion varies according to number of bits in an image. For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message. For 24 bit image, the colours of each component like RGB (red, green and blue) are changed. LSB is effective in using JPG images [**?**].

2.1.3 Existing System

The literature survey results that, there exists many system that work for the same purpose but do not meet the whole requirements. Some of thy system are as follows,

- Many years ago communication through "Letters"
- Communication through "Cryptography"
- Now a days communication through "Steganography"

2.2 Proposed System

To protect data or information from unauthorized access we are implementing this project. We are using combination of cryptography and steganography to hide private data in multimedia using various algorithms such as Play Color Cipher(PCC) and RSA Algorithm [**?**].

Play Color Cipher Algorithm is used to encrypt the message and generates color cipher text. For the encryption of keys RSA Algorithm is used. The encrypted keys are hidden using multimedia steganography.

2.3 Feasibility Study

The proposed system is built in order to provide more secured communication system. It also emphasizes on combination of Cryptography and Steganography which makes the system complicated to understand for intruders. The existing system possessed has many security threats in communication. The idea behind the proposed system is to solve the drawbacks of the existing communication system which includes simple cryptographic algorithm such as RSA and DES.

2.3.1 Economical Feasibility

This is the main factor in the feasibility study. When product is economically affordable then it can be used. So project must be cost saving. Establishing the cost effectiveness of the proposed system i.e. if the benefits do not outweighs the costs then it is not worth going ahead. The project involves the utilization of software and Jdk 1.6.0. The proposed system is economically feasible which will help reduce the security threats.

2.3.2 Operational Feasibility

Operational Feasibility deals with the human factors. It checks the impact of the proposed system on the staff. Since this system is being developed for the company's software consultants who computer survey is already. The consultants of the company benefit a lot from the proposed system. As there would be less paper work and they will find it very easy to use also, since the system will be computerized, Retrieved of information will be easier as all information will be stored in a file. As the system is developed for the security purpose the user whose is using the system to access the data must only know the method to decrypt the data. The system will also be user friendly. Hence the new system is operationally feasible.

2.3.3 Technical Feasibility

It is concerned with hardware and software feasibility. In this study, one has to test whether the proposed system can be developed using existing technology or not. As per client requirements the system to be developed should have speed response because of fast exchange of information, reliability, scalability, integration and availability.

2.4 Risk Analysis

Risk analysis and management are a series of steps that help a software team to understand and manage uncertainty. Many problems can plague a software project. A risk is a potential problem might happen, it might not. But, regardless of the outcome, it is really a good idea to identify it, assess its probability of occurrence, estimate its impact, and establish a contingency plan should the problem actually occur. Everyone involved in the software process, managers, software engineers, and customers participate in risk analysis and management.

2.4.1 Software Risk

Although there has been considerable debate about the proper definition for software risk, there is general agreement that risk always involves two characteristics.

1. Uncertainty-the risk may or may not happen; that is, there are no 100.

2. Loss-if the risk becomes a reality, unwanted consequences or losses will occur.

When risks are analyzed, it is important to quantify the level of uncertainty and the degree of loss associated with each risk. To accomplish this, different categories of risks are considered.

2.4.2 Project Risk

Threaten the project plan. That is, if project risks become real, it is likely that project schedule will slip and that costs will increase. Project risks identify potential budgetary, schedule, personnel (staffing and organization), resource, customer, and requirements problems and their impact on a software project. In our project, project risk occurs if our requirement of technical member means technical team is unavailable according to our project plan and estimation and if our project is not completed within time in this situation project risk can occurs.

2.4.3 Technical Risk

Threaten the quality and timeliness of the software to be produced. If a technical risk becomes a reality, implementation may become difficult or impossible. Technical risks identify potential design, implementation, interface, verification, and maintenance problems. In addition, specification ambiguity, technical uncertainty, technical obsolescence, and "leading edge" technology are also risk factors. Technical risks occur because the problem is harder to solve than we thought it would be. In our project if any module of our web site is not worked properly according to our expectation then technical risk may occur.

2.5 Project Scheduling

Software project scheduling is an activity that distributes estimated effort across the planned project duration by allocating the effort to specific software engineering tasks. It is important to note, however, that the schedule evolves over time. During early stages of project planning, a macroscopic schedule is developed. This type of schedule identifies all major software engineering activities and the product functions to which they are applied. As the project gets under way, each entry on the macroscopic schedule is refined into a detailed schedule. Here, specific software tasks (required to accomplish an activity) are identified and scheduled. Scheduling for software engineering projects can be viewed from two rather different perspectives. In the first, an end-date for release of a computer-based system has

already (and irrevocably) been established. The software organization is constrained to distribute effort within the prescribed time frame. The second view of software scheduling assumes that rough chronological bounds have been discussed but that the end-date is set by the software engineering organization. Effort is distributed to make best use of resources and an end-date is defined after careful analysis of the software. Unfortunately, the first situation is encountered far more frequently than the second.

Task Name		July				August				September			
Requirement Gathering	S	✓	✓	✓									
	C	✓	✓	✓									
Analysis of Project	S				✓	✓	✓						
	C				✓	✓	✓						
Design of Project	S							✓	✓	✓			
	C							✓	✓	✓			
Documentation	S									✓	✓	✓	✓
	C									✓	✓	✓	✓

S: Schedule C: Completion

Figure 2.1: Gantt Chart

2.6 Effort Allocation

Project means team work; Project is developed by combination of effort of team. So whole project is divided into modules and number of modules is allotted to team members. After completion of each module, it will be link from one module to another module to form a complete project. This effort allocation should be used as a guideline only. The characteristics of each project must dictate the distribution of effort. Work expended on project planning rarely accounts for more than 23 percent of effort, unless the plan commits an organization to large expenditures with high risk. Requirements analysis may comprise 10 to 25 percent of project effort. Effort expended on analysis or prototyping should increase in direct proportion with project size and complexity. A range of 20 to 25 percent of effort is normally applied to software design. Time expended for design review and subsequent

iteration must also be considered.

Network Security Using StegoCrypt	Darshana A. Mundada	Yogita G. Motiramani	Rudra J. Vivarekar	Nikita J. Kolhe
Identification of Project and Requirement Gathering	✓	✓	✓	✓
Study of Existing System	✓	✓	✓	✓
Selection of Process Model and Effort Allocation	✓	✓		
Identification of functional and Non-functional requirement			✓	✓
Data Modelling		✓	✓	
Functional Modelling	✓			✓
Behavioural Modelling		✓		✓
Data Design	✓		✓	
Interface Design		✓	✓	
Component Level Design	✓		✓	

Figure 2.2: Effort Allocation Table

2.7 Summary

This chapter focuses on the system analysis.Including proposed system, process and process modeling, feasibility study, risk analysis, effort allocation and project scheduling. The next chapter will focuses on requirement gathering.

Chapter 3

System Requirement Specification

The chapter focuses on the various requirements of the system.Section 3.1 describes the hardware requirements of the system. The software requirements of the system are discussed in section 3.2. Section 3.3 describes the functional requirements of the system. Non-functional requirement of system are discussed in 3.4. Finally the last section is of summary.

3.1 Hardware Requirements

The hardware requirement includes a system with following configurations:

- Processor: Intel core i3
- Hard Disk: 500GB
- RAM: 4GB DDR3 RAM
- Monitor: 15 VGA color
- Mouse: optical

3.2 Software Requirements

The various software requirements of the system are summarized here:

- Operating system : Ubuntu 14.04
- Front end : Java
- Java version : Jdk 1.6.0

3.3 Functional Requirement

Requirement Analysis is dependent on three aspects (Data, Function and Behavior).Requirement Analysis of data is a process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making. Data analysis has multiple facts and approaches, encompassing diverse techniques under a variety of names, in different business, science, and social science domains. Requirement Analysis of function is providing services to user as they expect in the sense of Java Integrated Environment. Function Analysis is one of important aspect of any project to determine project efficiency, integrity, user friendliness etc.

3.4 Non-functional Requirement

In Nonfunctional Requirements of this project implements those functions which does not effect on function and behavior of project for desired goal and objective of project. Non-functional Requirement just provides user friendliness and notifications that are not most necessary for this project .The non-functional requirements of the proposed system include the basic input given by the user which includes the plain text. Authentication factor is also considered during the development of the system. User friendliness is also maintained in the proposed system.

- Simple look and feel
- Fast response time
- Easy enhancement

3.5 Summary

In this chapter, System Requirement Specification is provided. In the next chapter, Design of the project is presented.

Chapter 4

System Design

Design is an activity concerned with making major decisions, often of a structural nature. It shares with programming a concern for abstracting information representation and processing sequences, but the level of detail is quite different at the extremes. Design builds coherent, well planned representations of programs that concentrate on the interrelationships of parts at the higher level and the logical operations involved at the lower levels.Software design is the first of the three technical activities-designs, Coding and test which are required to build and verify the software [**?**].

Section 4.1 describes the system architecture of the proposed system. Section 4.2 describes the database design of the project.Data flow diagrams are discussed in section 4.3. Section 4.4 describes the various interface design. The UML diagrams are discussed in section 4.5. Finally, the last section is of summary.

4.1 System Architecture

Proposed system consists of sender side and receiver side. At sender side, system takes input text from user. This text is substituted with color block by using Play Color Cipher algorithm. This algorithm generates a symmetric key (PCC key). Before transmission, PCC key is encrypted using encryption algorithm and generates cipher key. Then generated cipher key is hidden using multimedia steganography technique. At receiver side, user first recovers the hidden key. After recovering, user decrypt cipher key and generates plain text (PCC key). Using Play Color Cipher algorithm, user decrypts color coded text and generates plain text. [**?**]

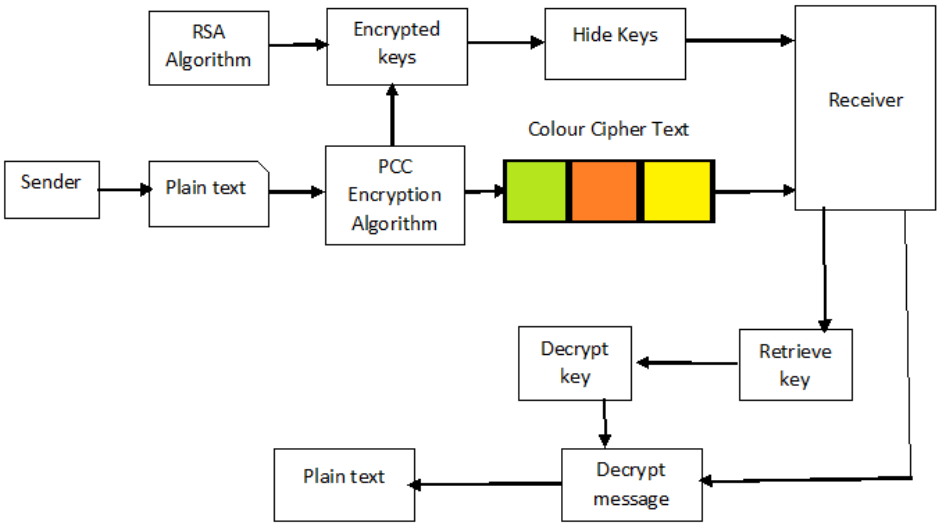

Figure 4.1: System Architecture

4.2 Database Design

The data design is the first of the four activities that are conducted during software engineering. The impact of data structure on program structure and procedural complexity causes data design to have a profound influence on software quality. The concept of data encryption, hiding and data abstraction provide the foundation for an approach to data design.

4.3 Data Flow Diagram

A DFD is a graphical technique that depicts the information flow and the transformation that we have applied as the data moves from input to output. The data flow diagram also known as data flow graph or bubble chart. A data flow diagram may be used to represent a system or software at any level of abstraction. The data flow diagram can be completed using only four simple notations i.e. special symbols or icons and the annotation that with a special system. A data flow diagram (DFD) is a graphical technique that describes information about flow and that are applied as data moves from input to output. The DFD is also called as data flow graph or bubble chart. Named circles show the processes in DFD or named arrows entering or leaving the bubbles represent bubbles and data flow. A rectangle represents a source or sink and is not originate or consumer of data. Data flow diagrams are the basic building blocks that define the flow of data in a system to the particular destination and difference in the flow when any transformation happens. It makes whole procedure like a good document

and makes simpler and easy to understand for both programmers and non-programmers by dividing into the sub process. The data flow diagram serves two purposes:

- To provide an indication of how data are transform as the moves through the system.
- To depict the function that transforms the data flow.

A level 0 DFD, also called a fundamental system model (FSM) or a context model. It represents the entire s/w elements as a single bubble with input and output data indicated by incoming and outgoing arrows respectively. Figure 4.2shows the Level 0 DFD of the system.

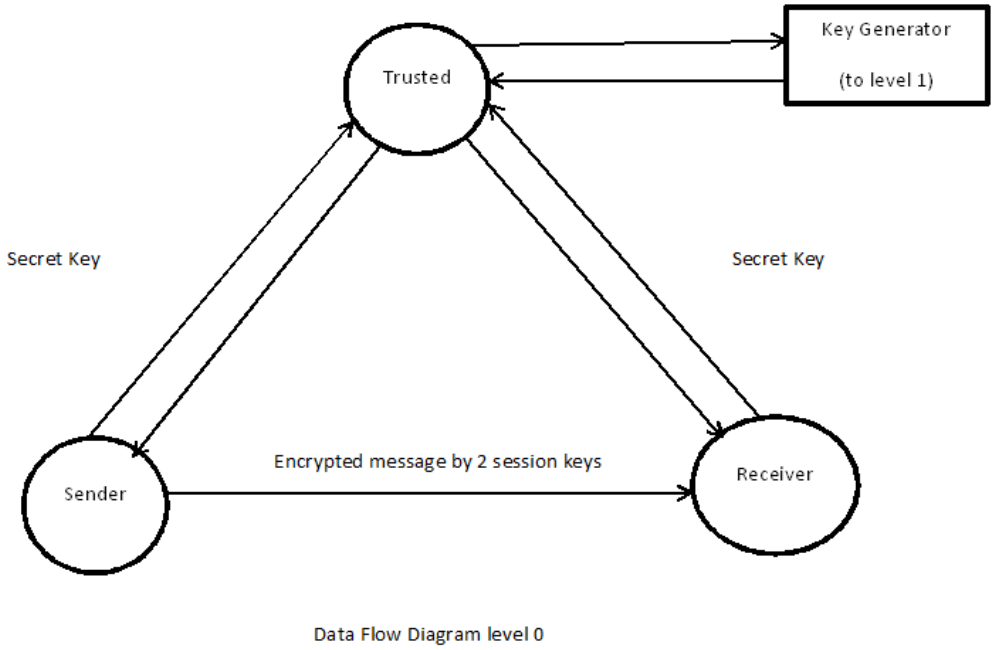

Figure 4.2: Data Flow Diagram Level 0

Level 1 DFD contains additional processes and information ow paths, as the level 0 DFD is partitioned to reveal more detail. Level 1 DFD might contain 5 - 6 bubbles with interconnecting arrows.Figure 4.3 shows the Level 1 DFD of the system.

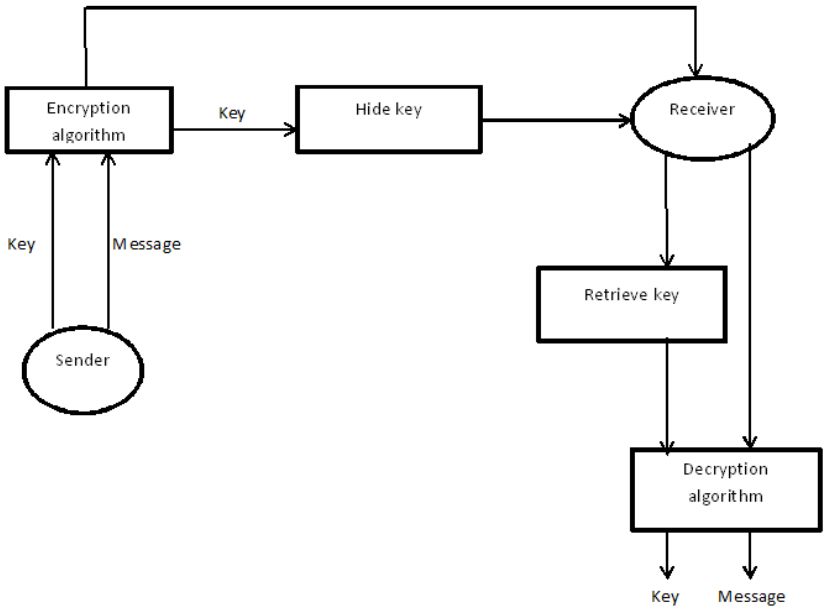

Figure 4.3: Data Flow Diagram Level 1

4.4 Interface Design

The interface design describes how the software communicates within itself, with systems that inter operate with it, and with humans who use it. An interface implies a flow of information (e.g., data and/or control) and a specific type of behavior. Therefore, data and control flow diagrams provide much of the information required for interface design.

4.4.1 User Interface Design

The overall process for designing a user interface begins with the creation of differen models of system function (as perceived from the outside). The human- and computer-oriented tasks that are required to achieve system function are then delineated; design issues that apply to all interface designs are considered; tools are used to prototype and ultimately implement the design model; and the result is evaluated for quality.

4.5 UML Diagrams

The UML is a language for [**?**]: **Visualizing:** Structures which are transient can be represented using the UML **Specifying:** The UML addresses the specification of all the important analysis, design and implementation decisions that must be made in developing and deploying a software intensive system. **Constructing:** The UML is not a visual programming language, but its models can be directly connected to a variety of programming languages.

Documenting: The UML addresses the documentation of a system's architecture and all of its details.

4.5.1 Use Case Diagram

A Use case diagram shows a set of use cases and actors and their relationships. Use case diagrams address the static use case view of a system. These diagrams are especially important in organizing and modeling the behaviors of a system [**?**]. The Use Case diagram of the proposed system is shown in figure 4.4.

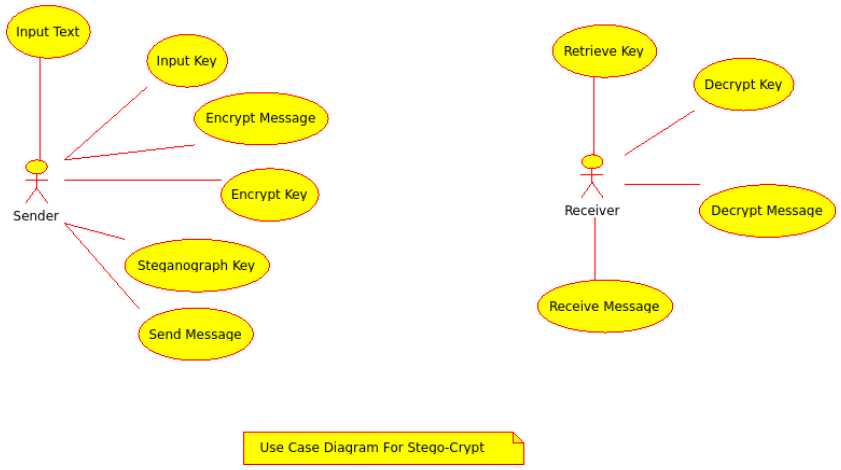

Figure 4.4: Use Case Diagram for StegoCrypt

4.5.2 Class Diagram

A Class diagram shows a set of classes, interfaces and collaborations and their relationships. These diagrams are the most common diagram found in modeling object-oriented systems. Class diagram address the static design view of a system [**?**]. Figure 4.5 shows the class diagram for the proposed system.

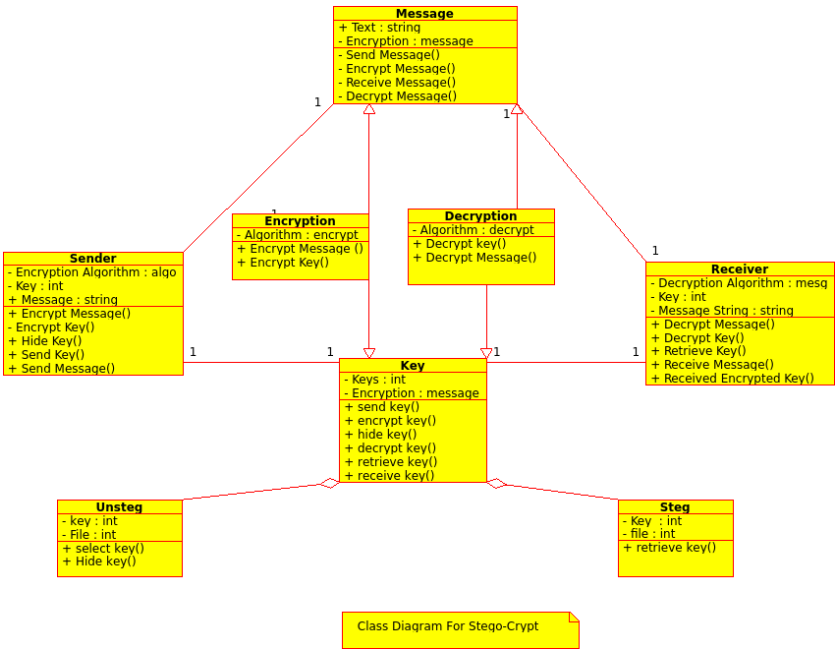

Figure 4.5: Class Diagram for StegoCrypt

4.5.3 Sequence Diagram

Both sequence and collaboration diagrams are kinds of interaction diagrams. An interaction diagram shows an interaction, consisting of a set of objects and their relationships. They address the dynamic view of a system [**?**].

- A sequence diagram is an interaction diagram that emphasizes the time-ordering of messages.
- A collaboration diagram is an interaction diagram that emphasizes the structural organization of the objects that send and receive massages.

Sequence diagram and collaboration diagrams are isomorphic i.e one can be transformed into other.

Figure 4.6 shows sequence diagram for encryption of message.

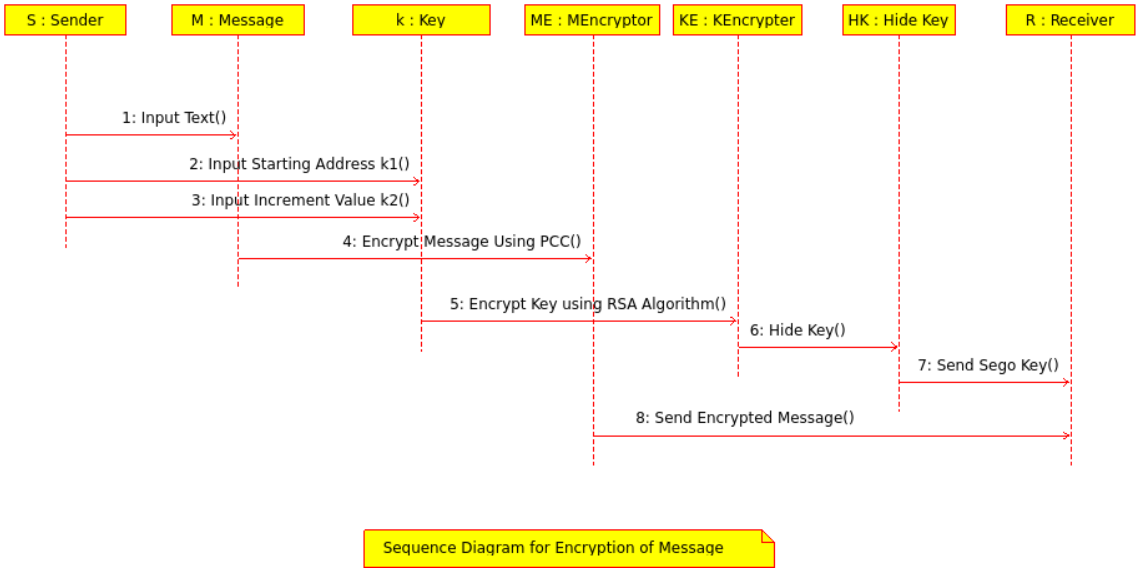

Figure 4.6: Sequence Diagram for Encryption of Message

Figure 4.7 shows sequence diagram for decryption of message.

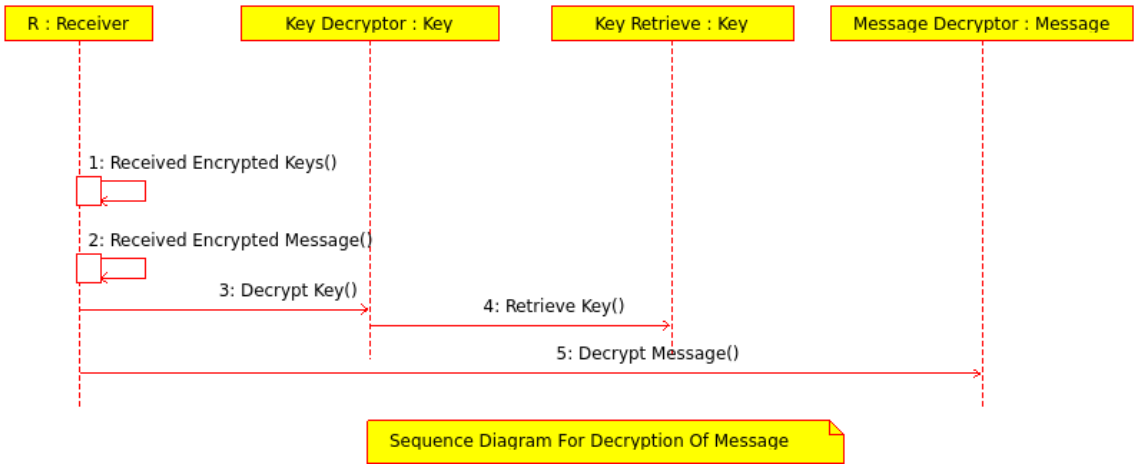

Figure 4.7: Sequence Diagram for Decryption of Message

Figure 4.8 shows collaboration diagram for encryption of message.

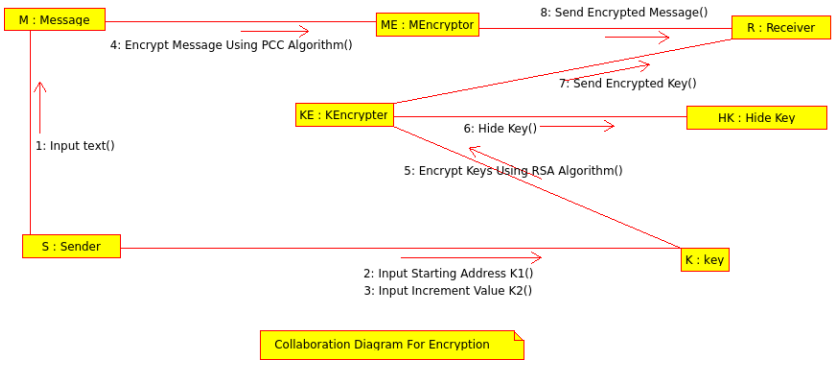

Figure 4.8: Collaboration Diagram for Encryption of Message

Figure 4.9 shows collaboration diagram for decryption of message.

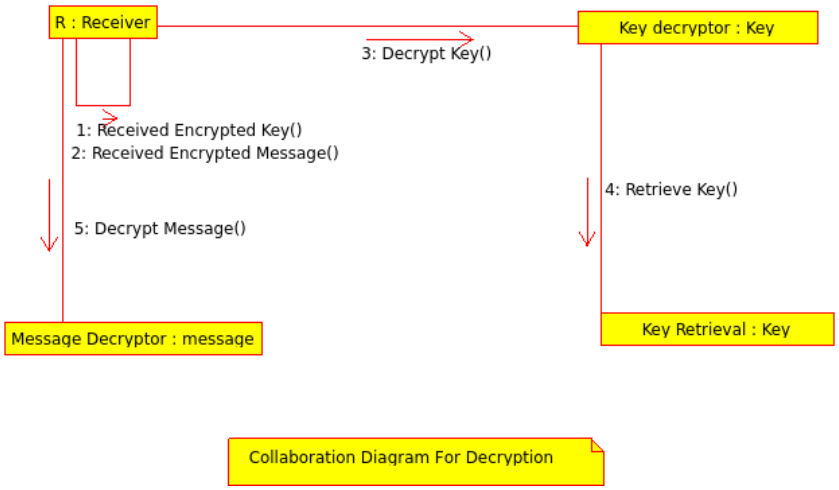

Figure 4.9: Collaboration Diagram for Decryption of Message

4.5.4 Component Diagram

A component diagram shows the organization and dependencies among a set of components. Component diagrams address the static implementation view of a system [**?**]. The component diagram for the proposed system is shown in figure 4.10.

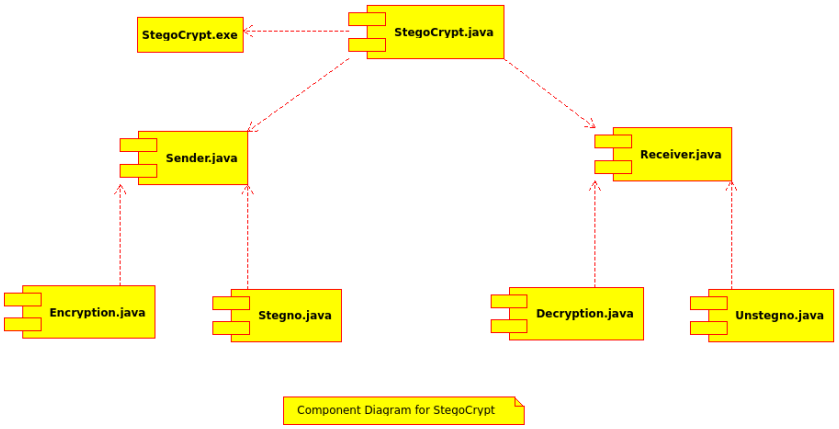

Figure 4.10: Component Diagram for StegoCrypt

4.5.5 Deployment Diagram

A deployment diagram shows the configuration of run-time processing nodes and the components that live on them. Deployment diagram address the static deployment view of an architecture [**?**]. Deployment diagram for the proposed system is shown in figure.

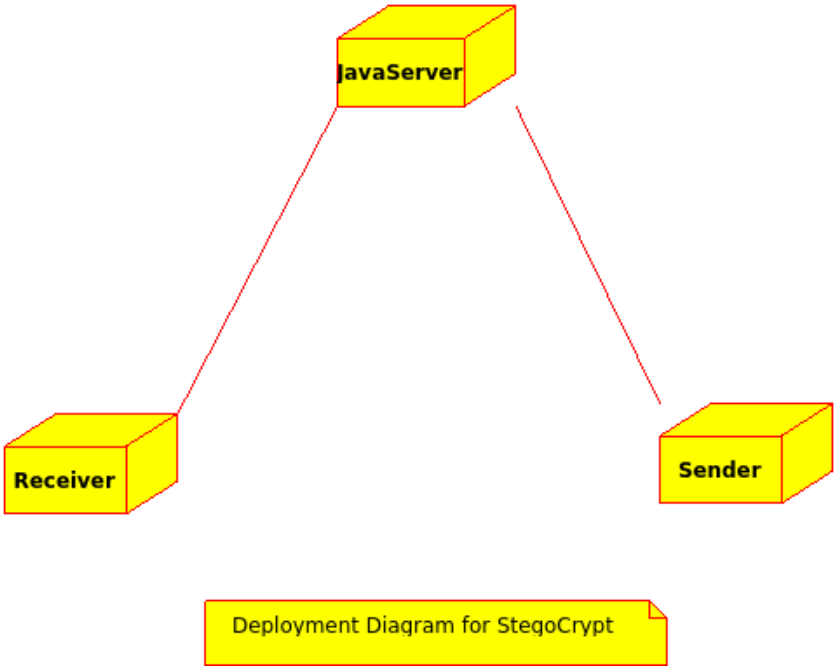

Figure 4.11: Deployment Diagram for StegoCrypt

4.5.6 State Diagram

A statechart diagram shows a state machine, consisting of states, transitions, events, and activities. Statechart diagrams address the dynamic view of our system. They are especially important in modeling the behavior of an interface, class, or collaboration and emphasize the event-ordered behavior of an object, which is especially useful in modeling reactive to our system [**?**] as shown in figure 4.12.

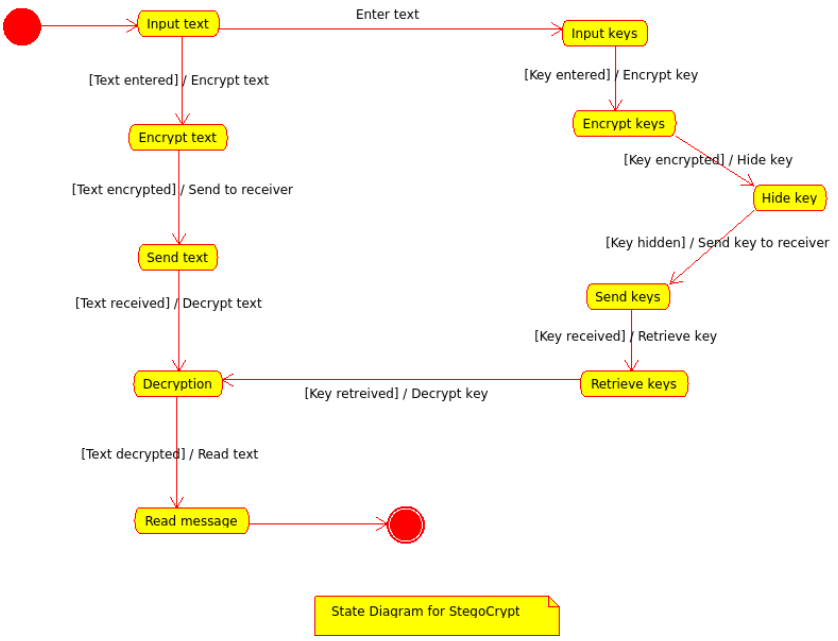

Figure 4.12: State Diagram for StegoCrypt

4.6 Summary

In this chapter, Design of project is provided. In the next chapter, expected result and conclusion is presented.

Chapter 5

Expected Result and Conclusion

This chapter consist of expected result and conclusion. Section 5.1 describes expected result. Conclusion is described in section 5.2.

5.1 Expected Result

After executing, it would be expected that, Play Color Cipher is comfortably converting plain text into cipher text with two encrypted session keys and further they are hidden in a media file. Then these hidden keys and encrypted message reached at the receiver side. Then hidden keys are retrieved and decrypted. Further cipher text is converted into plain text by reverse Play Color Cipher Algorithm.

5.2 Conclusion

Comparing the StegoCrypt with cryptography and steganography (Exiting technique) then it is to be found that the cryptography was only for the encrypting the particular secret data, and steganography was only for the hiding data, so it was easy to detect that something is secret, while in steganography the secret message is hidden into another cover media that is data into other data which can be predicted by naked eyes easily. Using both these techniques together, the cipher has great potential as it eliminates major attacks like brute force, man in the middle, known plain text and known cipher text attacks. In proposed system, implementation of encryption-decryption scheme is done using symmetric and asymmetric techniques and steganography scheme for securing the transmission of data.

Bibliography

[1] Pye Pye Aung and Tun Min Naign. A novel secure combination technique of steganography and cryptography. International journal of information technology, modelling and computing, University of Technology, Pyin Oo Lwin, Myanmar, 2014.

[2] Mamta Juneja and Parvinder S. Sandhu. An improved lsb based steganography technique for rgb color images. International journal of computer and communication engineering, July 2013.

[3] Dr. A.Vinaya Babu K. Ravindra Babu, Dr .S.Udaya Kumar and Dr. Thirupathi Reddy. A block cipher generation using color substitution. International journal of computer applications, Research Scholar (JNTUH),HOD CSE and IT, Aizza College of Engineering and Technology, Mancherail, A.P, India, 2014.

[4] Sunguk Lee. Unified modeling language (uml) for database systems and computer applications. International journal of database theory and application, Research Institute of Industrial Science and Technology Pohang, Korea, March 2012.

[5] Avinash Shah Monica Kanchan. Advance cryptography using color code based substitution with multi-language support. International journal of computer applications, the national conference on role of engineers in national building, Viva Institute of technology, 2015.

[6] Priyanka V. Deshmukh Netra R. Bujad Prof. Sachin Sonawane. *Secure Encryption and Decryption using Play Color Cipher*. National conference on technological advancement and automatization in engineering, Atharva College of Engineering, Mumbai University,Mumbai, India, January 2016.

[7] Ravindra Gupta Vishwa gupta, Gajendra Singh. Advance cryptography algorithm for improving data security. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2, January 2012.

[8] WenLong Fu Xinyi Zhou, Wei Gong. An improved method for lsb based color image

steganography combined with cryptography. Ieee icis, Neuroscience and Intelligent Media Institute, Communication University of China, June 2016.

Index