A

Major Project Report

on

A CRYPTOGRAPHIC & STEGANOGRAPHIC SYSTEM USING MAGIC RECTANGLE & GENETIC ALGORITHM

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Monali Pawar
Minal Chaudhari
Ankita Wani
Dhiraj Mahajan

Under the Guidance of

Mr.Ashish T. Bhole

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 major project entitled *A Cryptographic & Steganographic system using Magic Rectangle & Genetic Algorithm*, submitted by

Monali Pawar
Minal Chaudhari
Ankita Wani
Dhiraj Mahajan

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 4, 2016
Place: Jalgaon

Mr.Ashish T. Bhole
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

We hereby take this opportunity to express our heartfelt gratitude towards the people whose help is very useful to complete our project work on topic of "A Cryptographic & Steganographic System using Magic Rectangle and Genetic Algorithm ". We would like to express our heartfelt thanks to our project guide Mr. Ashish T. Bhole (Assit.Prof.) whose experienced guidance becomes very valuable for us. We would also greatly thankful to our principal Dr. K.S. Wani, H.O.D. Prof. Dr. Girish K. Patnaik for providing precious help and advice. Finally We would like to thank all our friends and well-wishers who have a very important role in nurturing and strengthening our career.Last but not least thankful to our parents.

Monali Pawar
Minal Chaudhari
Ankita Wani
Dhiraj Mahajan

Contents

Acknowledgements ii

Abstract 1

1 Introduction 2

1.1 Background . . . 2
1.2 Motivation . . . 3
1.3 Problem Definition . . . 3
1.4 Scope . . . 3
1.5 Objective . . . 4
1.6 Organization of the report . . . 4
1.7 Summary . . . 4

2 System Analysis 5

2.1 Literature Survey . . . 5
2.2 Proposed System . . . 6
2.3 Process and Process Modeling . . . 7
2.3.1 Justification for the selected model for our project . . . 7
2.4 Feasibility Study . . . 8
2.4.1 Economic Feasibility . . . 8
2.4.2 Operational Feasibility . . . 8
2.4.3 Technical Feasibility . . . 8
2.5 Risk Analysis . . . 9
2.5.1 Introduction . . . 9
2.5.2 Components . . . 9
2.5.3 Need . . . 9
2.5.4 Software Risk . . . 9
2.5.5 Project Risks . . . 9
2.5.6 Technical risks . . . 10
2.6 Effort Allocation . . . 10

2.7 Project Scheduling 11
2.8 Summary 11

3 System Requirement Specification **13**
3.1 Hardware and Software Requirements 13
3.2 Functional Requirements 14
3.3 Non-Functional Requirements 14
3.4 Summary 14

4 System Design **15**
4.1 System Architecture 15
4.2 E-R Diagrams 16
4.3 Data Flow Diagrams 17
4.4 Interface Design 18
4.4.1 Introduction to Interface Design 19
4.4.2 Component of Interface Design 19
4.4.3 Need of Interface Design 19
4.4.4 The Golden Rules 19
4.5 UML Diagrams 19
4.5.1 Use Case Diagrams 20
4.5.2 Interaction Diagrams 20
4.5.3 Class Diagram 22
4.5.4 State Diagram 23
4.5.5 Component Diagram 24
4.5.6 Deployment Diagram 25
4.6 Summary 25

Conclusion **26**

Bibliography **27**

List of Tables

List of Figures

2.1 Process Model 7
2.2 Effort Allocation Table 11
2.3 Gantt Chart for Project Scheduling 12

4.1 System Architecture 16
4.2 E-R Diagram 17
4.3 Data Flow Diagram(DFD0) 18
4.4 Data Flow Diagram(DFD1) 18
4.5 Usecase Diagram 20
4.6 Sequence Diagram For Encryption Process 21
4.7 Sequence Diagram For Decryption Process 21
4.8 Collaboration Diagram For Encryption Process 22
4.9 Collabration Diagram For Decryption Process 22
4.10 Class Diagram 23
4.11 State Diagram 24
4.12 Component diagram 25
4.13 Deployment Diagram 25

Abstract

For many years, people were concerned with the secure transmission of data. The encryption is used to securely communicate data in open networks. As each type of data has its own structures, different techniques should be used to protect confidential data. The existing algorithms used for encryption in cryptography have some flaws such as easily data can be retrieved using ASCII values for numerical representation. The proposed system combines cryptographic algorithm with steganography to protect data or message over network thereby enhancing the data security.

Chapter 1

Introduction

For many years, people have debated about the various cryptography techniques for secure transmission or sharing of data. Secure transmission of data plays a very vital role in today's era. There are various cryptography techniques for such secure transmission. Among the various algorithms and concepts, the Adi Shamir's secret sharing scheme, is the securest one. The Adi Shamir's secret sharing scheme depends on Lagrange's polynomial for dividing the secret into number of shares. People have failed to notice, however, an adversary or intruder may obtain the secret without any valid share.This creates loss of data security problem. Therefore to overcome this drawback this system is proposed.

The sections of the chapter are organized as follows. Section 1.1 presents background. Motivation is discussed in section 1.2. Section 1.3 presents Problem Definition. Scope of the project is discussed in section 1.4. Section 1.5 presents objective of the project. Finally,summary of the chapter is given in the last section.

1.1 Background

The parameters used in encryption and decryption process of the algorithm plays a vital role for speed. For instance, key streams in one time pad, the secret key in DES algorithm,the prime p and q in RSA plays an important role etc. In RSA, the secret key is derived from the public key and by choosing very large size of p and q. Even though the parameters of RSA are considered carefully, it is not fully secured because of using ASCII character. The same cipher text will be produced if the same character is repeated more than one place in the plain text. To overcome this, the proposed system tries to develop a method with different algorithms Magic Rectangle,Fisher Yates algorithm and genetic algorithm.

1.2 Motivation

The existing in RSA, the secret key is derived from the public key and by choosing very large size of p and q. Even though the parameters of RSA are considered carefully, it is not fully secured because of using ASCII character. The same cipher text will be produced if the same character is repeated more than one place in the plain text. To overcome this, the proposed system tries to develop a method with different algorithms Magic Rectangle,Fisher Yates algorithm and genetic algorithm.

1.3 Problem Definition

Today, to transmit confidential information over the network, security is essential. Cryptographic algorithms play an important role to provide the data security against malicious attacks. Many people think that the efficiency of cryptographic algorithm depends only on its time taken for encryption and decryption. However, the efficiency of cryptographic algorithm also depends on number of stages used to obtain cipher text to maintain data secrecy. The algorithms such as Magic Rectangle, Fisher Yet Shuffle algorithm and Genetic algorithm are designed separately to maintain data secrecy. If one continues to use these algorithms individually, data may be lost as security provided by these algorithms can be easily compromised. To overcome the problem, proposed system combines Magic Rectangle, Fisher Yates Shuffle algorithm and Genetic algorithm to enhance the security by increasing complexity of the encryption process.

As sender gives input, the magic rectangle is constructed based on some constraints such as seed value, min start, max start, column sum. To enhance data security, Fisher Yates shuffle algorithm is applied on constructed Magic Rectangle to shuffle the data. The genetic algorithm hides shuffled data into an image for generating a complex cipher text which send to receiver.

1.4 Scope

The present scope of the proposed system involves secure transmission of data in the form of numbers, text, special characters or the combination of any or all of these. It may be further extended towards secure transmission of data in the form of image,audio and video too.

1.5 Objective

The main objective of the proposed system is to provide a more secure transmission of data. Along with secure transmission of data, the proposed system also focuses to avoid attacks on data, so that an attacker will not be able to retrieve data.

1.6 Organization of the report

First Chapter presents introduction of the project.System analysis is discussed in the second chapter. In the addition to that literature survey, proposed system and feasibility study,these btopics are also described in second chapter.In the third chapter, System requirement specifications are elaborated. Study of various system designs like ER diagrams, DFDs and UML diagrams is also done in the fourth chapter. In the last chapter, Conclusion and the future scope of the project is described.

1.7 Summary

In this chapter, an introduction of the project topic with the background, motivation, problem definition has been discussed. Scope and objective of the project has been also discussed in this chapter. Next chapter presents system analysis of the project.

Chapter 2

System Analysis

The main purpose behind the development of proposed system is to increase the complexity of encryption process and to improve the efficiency of cryptographic algorithm by increasing number of stages used to obtain cipher text from plain text to maintain data secrecy. This leads to more secure transmission of data.

Section 2.1 describes the literature survey for the proposed system that is developed. The proposed system is described in Section 2.2. Section 2.3 includes the Feasibility study of the system . Risk analysis is done in Section 2.4. Section 2.5 includes the effort allocation study. Project scheduling is described in Section 2.6. Section 2.7 describes the summary.

2.1 Literature Survey

The content of the report focusses on the research and contributions of various sources. These sources help for the proposed work [7, 8].

These papers focus on how the Security is a major concern in wired communication. Various techniques are given in papers for providing the security for the transmitting data. Most commonly used cryptographic algorithms are advanced encryption standard (AES), data encryption standards (DES), triple data encryption standards T-DES for symmetric cryptography and Diffie Hellman key exchange and Rivest Shamir and Adleman (RSA) algorithm for the Asymmetric cryptography, in which RSA is the most commonly used algorithm.

These papers also describes the different algorithm used in network in order to provide security to the confidential data transmission.The working of algorithms are also given in detail.

The paper proposes an innovative algorithm, namely, Magic Rectangle which is helpful to enhance the security on account of its complexity of the encryption process. The singly even magic rectangle is constructed based on the seed number, start number, row sum and column sum which is very difficult to trace these values because of their randomness [2].

New architecture is designed of shuffling of data based on Fisher Yates Shuffle algorithm to maintain secrecy of data [4].To enhance data security iterative fisher Yates shuffle algorithm (IFYS) is designed in which, third order shuffling is carried out. IFYS-algorithm shuffles the elements in NMMR randomly,which potentially increase data security. These cipher texts are transmitter in channels through modulation techniques. This process ensures that data transfer with confidentially and integrity of the data can be improved effectively [4].

The paper uses cryptographic algorithm along with Steganography For pleasing the defense of data hiding and communication over network. In order to hide the information over the image in complex manner the genetic algorithm based technique is implemented in paper which is used to evaluate the valuable pixels where the data can be hide in a secure manner.

2.2 Proposed System

Security is a major concern in wired communication. Various techniques are used for providing the security for the transmitting data.Most commonly used cryptographic algorithms are advanced encryption standard (AES), data encryption standards (DES), triple data encryption standards T-DES for symmetric cryptography and Diffie Hellman key exchange[1] and Rivest Shamir and Adleman (RSA), MR, Genetic algorithm.

All these algorithm are prone of hacking if they are separately used to encrypt the data. As all these algorithm are single stage encryption algorithm.

The proposed system is a solution to this problem. Proposed system designed by merging Magic Rectangle, Fisher Yates Shuffle algorithm and Genetic algorithm to enhance the security by increasing complexity of the encryption process. The magic rectangle is constructed from input data based on some constraint. To enhance data security fisher Yates shuffle algorithm (FYS) is applied on Magic Rectangle in which, shuffling of data is carried out. At last in order to hide the shuffled data within the image in complex manner the genetic algorithm based technique is implemented. So unbreakable cipher text is obtained.

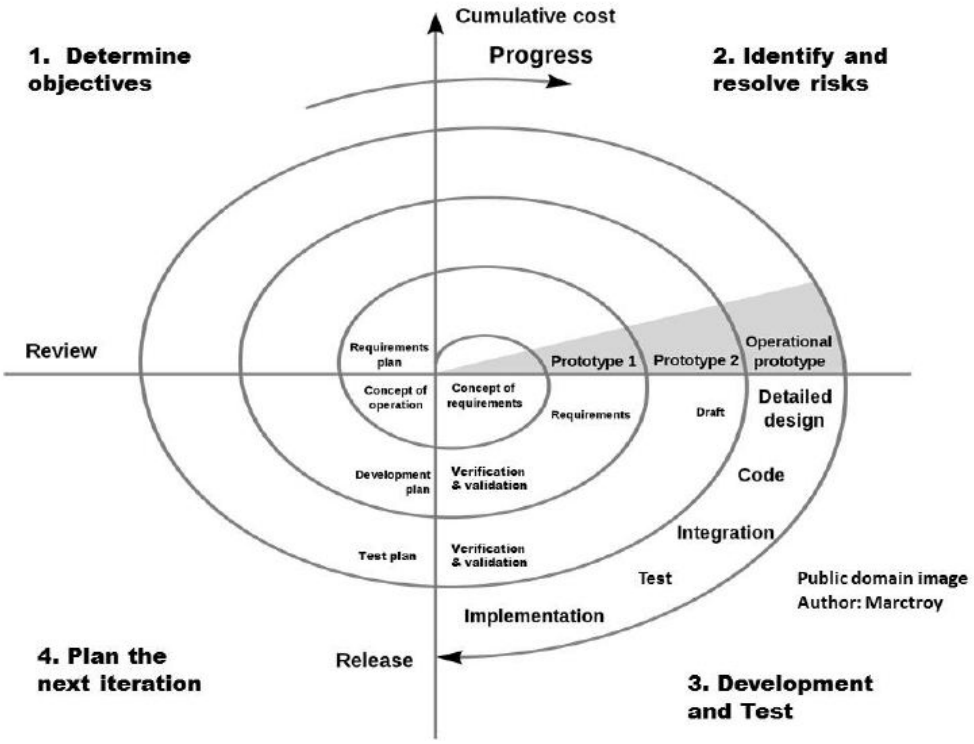

Figure 2.1: Process Model

2.3 Process and Process Modeling

To solve actual problems in an industry setting, a software engineer or a team of engineers must incorporate a development strategy that encompasses the process, methods, and tools layers described. This strategy is often referred to as a process model or a software engineering paradigm.

A process model for software engineering is chosen based on the nature of the project and application, the methods and tools to be used, and the controls and deliverables that are required. There are no of process models in software engineering which has its own specialization and each model is required in different conditions like as RAD model is used when deadlines are too short, Iterative model is choose when customer is not satisfied with proper requirements.

2.3.1 Justification for the selected model for our project

There are many process models in the software engineering, but we have chosen Water Fall Model because the project is totally dependent on previous modules. Another Reason for choosing this model is to provide better user satisfaction.

2.4 Feasibility Study

The proposed system is built in order to enhance the security of confidential Data.several attacks are introduced to break the existing algorithm due to their limitations like single stage encryption.Also, it may not be guaranteed that the cipher text is fully secured.Hence the need is arised to develope such system which can use multistage encryption so that it become very defficult to break the security.

Proposed system involve three algorithm Magic rectangle,fisher Yates shuffle algorithm (IFYS) and Genetic algorithm.The proposed work introduces one more level of security in public key algorithms such as RSA, ElGAMAL.In proposed system single even magic rectangle is formed based on the seed number, start number, row sum and column sum. The value of row sum and column sum is very difficult to be traced.Shuffling process is done for improving the complexity of data that is needed to be transmitted.Genetic Algorithm is used for pixel selection of image where data is to be hide so that finding of clandestine information become very difficult.

2.4.1 Economic Feasibility

The project involves the utilization of softwares like and Jdk1.6.0. The proposed system is economically feasible which will help enhance the security of the existing Secret Sharing Scheme.

2.4.2 Operational Feasibility

The proposed system provides more and better security to the data transmission scheme. The concept of multistage encryption increased the complexity of encryption process. Thus, the security of the confidentional data is enhanced.

2.4.3 Technical Feasibility

The project involves coding in Java which is platform independent. Hence further utilization of the code can be done to enhance the performance of the system. Newer technologies including IDEs like Ecllipse can be used in future for better performance and code optimization of the system.

2.5 Risk Analysis

2.5.1 Introduction

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 .It might happen, it might not. But, regardless of the outcome, its a really good idea to identify it, assess its probability of occurrence, estimate its impact, and establish a contingency plan should the problem actually occur.

2.5.2 Components

Everyone involved in the software process managers, software engineers, and customers participate in risk analysis and management.

2.5.3 Need

Think about the Boy Scout motto: Be prepared. Software is a difficult undertaking. Lots of things can go wrong, and frankly, many often do. Its for this reason that being prepared understanding the risks and taking proactive measures to avoid or manage them is a key element of good software project management.

2.5.4 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.

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

2.5.5 Project Risks

Project risks 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 the 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 occur.

2.5.6 Technical risks

Technical risks 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 the module of share generation or share reconstruction is not working properly according to the expectations, then technical risk may occur.

- *List of technical risk in the project*
  Network failure: The proposed system involves the network connections through hub. If some failure occurs in the working of the switch, then the network may fail and the secret may not be transmitted to the clients. This problem of network failure can be solved by using a switched network.

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 is link from one module to another module to form a complete project. The 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 comprise1025 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 25percent of effort is normally applied to software design. Time expended for design review and subsequent iteration must also be considered.

The Effort Allocation Table for the proposed system is shown in the following Table 2.2

Phases	Activity	Monali G. Pawar	Minal S. Chaudhari	Ankita K. Wani	Dhiraj S. Mahajan
Requirement Gathering	Identification of project and Requirement Gathering	✓	✓	✓	✓
	Study of Existing System	✓	✓	✓	✓
	Study of Process Model and Effort Allocation	✓	✓		
Analysis	Identification of Functional and Non-Functional Requirements			✓	✓
	Data Modelling	✓		✓	
	Functional Modelling		✓		✓
	Behavioral Modeling	✓	✓		✓
Design	Data Design		✓	✓	
	Architecture Design	✓		✓	
	Interface Design	✓			✓
	Component Level Design		✓	✓	✓

Figure 2.2: Effort Allocation Table

2.7 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. The 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. The Gantt Chart for project scheduling is shown in Figure 2.3.

2.8 Summary

In this chapter, the analysis of the proposed system is described. In the next chapter, System Requirements Specification is discussed.

Task Name		Jully				August				September				October			
		w1	w2	w3	w4	w1	w2	w3	w4	w1	w2	w3	w4	w1		w2	
Requirement Gathering	S	#	#	#													
	C	#	#	#													
Analysis of Project	S			#	#												
	C			#	#												
Design of Project	S				#	#	#	#	#								
	C									#	#						
Documentatio-n of Project	S											#	#	#	#		
	C															#	#

S: Schedule , **C:** Completion

Figure 2.3: Gantt Chart for Project Scheduling

Chapter 3

System Requirement Specification

System Requirements specification involves the description of all the hardware and software requirements of the proposed system. The functional and non-functional requirements also play an important part of the system requirements.

Section 3.1 describes the software requirements of the system. The functional requirements of the system are discussed in Section 3.2. Section 3.3 describes the non- functional requirements of the system. Summary is described in Section 3.4.

3.1 Hardware and Software Requirements

Software and hardware requirements are the base for the development of the project. The proposed system involves various software and hardware requirements. The system is developed using the minimal available resources. The various software and hardware requirements of the system can be summarized here:

- Operating system : Windows 7/8
- Processor : Intel(R) Core(TM) i3 CPU
- Installed Memory (RAM) : 3GB or more
- System Type : 64-bit/32-bit operating system
- Front end : Java
- Java version : Jdk1.6.0
- Hardware : Ethernet Switch 802.3

3.2 Functional Requirements

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 faces and approaches, encompassing diverse techniques under a variety of names, in different business, science, and social science domains. Function analysis is one of important aspect of any project to determine project efficiency, integrity, user friendly etc.

The functional requirements of the proposed system include the data in the form of number, text,or combination of these. The data is encrypt using algorithm and data is shuffled and finally then that data is hidden into the image. The shares along with the token are then given to the shareholders.

3.3 Non-Functional Requirements

The Nonfunctional requirements of the proposed system includes 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 the project.

3.4 Summary

In this chapter, the various requirements of the proposed system are described. In the next chapter, System Design is discussed.

Chapter 4

System Design

System Design describes the system architecture which includes the overall structure of the proposed system. The E-R diagrams, data ow diagrams, UML diagrams play an important role in the system designing of the project.

Section 4.1 describes the system architecture of the proposed system. E-R Diagrams are discussed in Section 4.2. Section 4.3 describes the data flow diagrams. Interface design is discussed in Section 4.4. Section 4.5 describes the UML diagrams. Summary is described in the Section 4.6.

4.1 System Architecture

Software architecture is the development work product that gives the highest return on investment with respect to quality, schedule and cost. Software architecture alludes to the overall structure of the software and the ways in which that structure provides concep- tual integrity for a system. In its simplest form, architecture is the hierarchical structure of program components (modules), the manner in which these components interact and the structure of data that are used by the components the architectural design representation defines the components of a system (e.g., modules, objects, filters) and the manner in which those components are packaged and interact with one another. The architectural design description should address how the design architecture achieves requirements for performance, capacity, reliability, security, adaptability, and other system characteristics.The architecture of our system is as shown in fiq4.1.

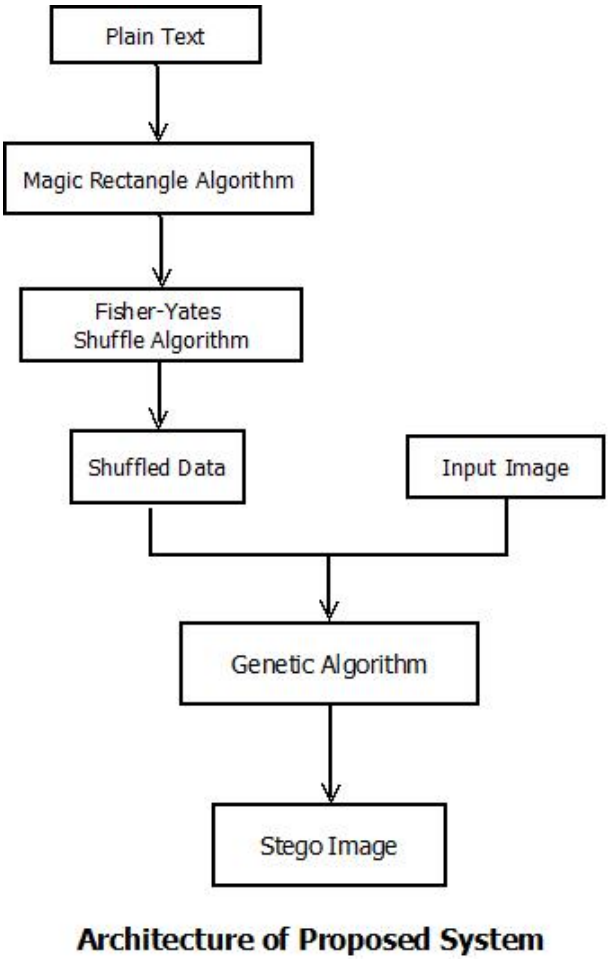

Figure 4.1: System Architecture

4.2 E-R Diagrams

The entity relationship data model is based on a perception of a real world that consist of a collection of basic objects called entities, and relation among these objects.

Figure 4.2 shows the E-R Diagram for the Proposed System.

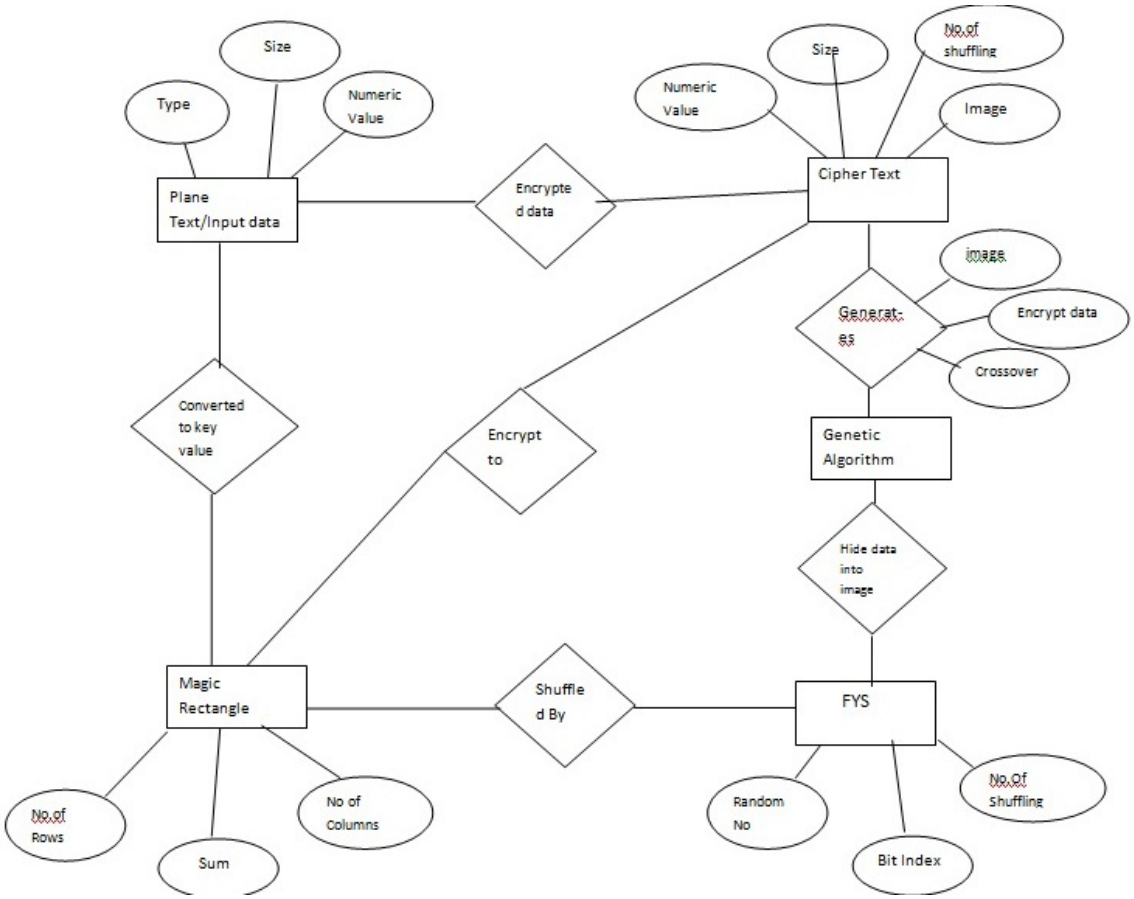

Figure 4.2: E-R Diagram

4.3 Data Flow Diagrams

A DFD is a graphical technique that depicts the information ow and the transformation that we have applied as the data moves from input to output. A data ow 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 specific system.

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. 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.

The level 0 DFD of the system is shown in Figure 4.3. Figure 4.4 shows the level 1 DFD of the system.

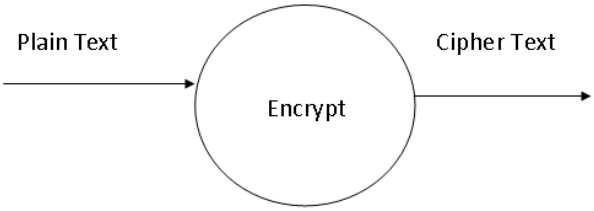

Figure 4.3: Data Flow Diagram(DFD0)

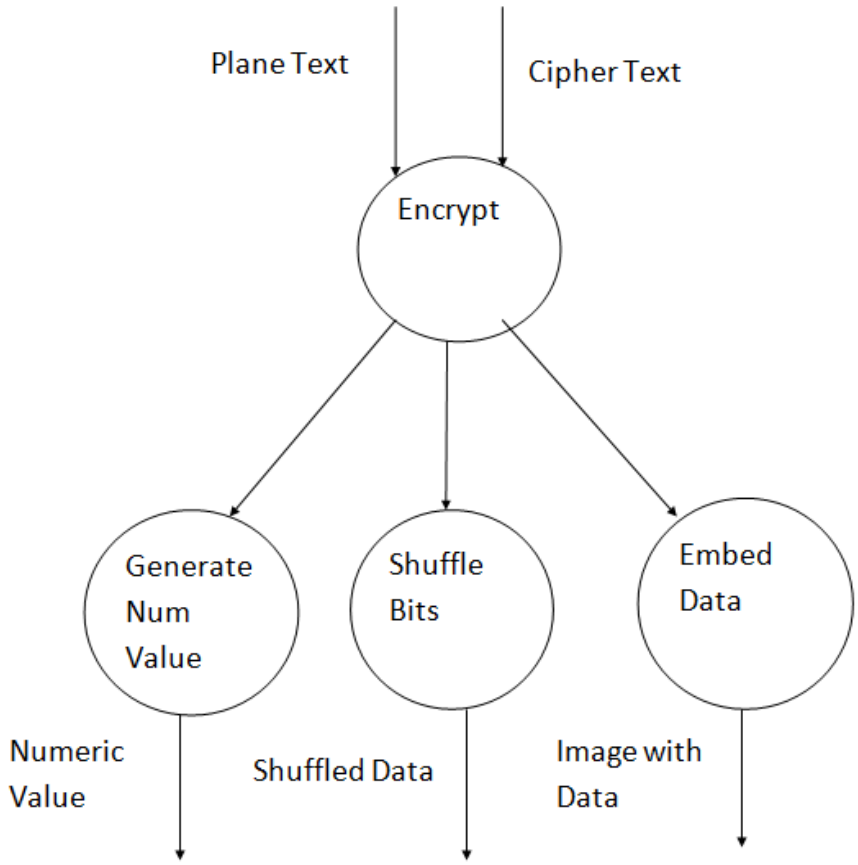

Figure 4.4: Data Flow Diagram(DFD1)

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.Interface design focuses on three areas of concern:

- The design of interfaces between software components.
- The design of interfaces between the software and other non human producers and consumers of information (i.e., other external entities).

- The design of the interface between a human (i.e., the user) and the computer.

4.4.1 Introduction to Interface Design

User interface design creates an effective communication medium between a human and a computer. Following a set of interface design principles, design identifies interface objects and actions and then creates a screen layout that forms the basis for a user interface prototype.

4.4.2 Component of Interface Design

A software engineer designs the user interface by applying an iterative process that draws on predefined design principles.

4.4.3 Need of Interface Design

If software is difficult to use, if it forces you into mistakes, or if it frustrates your efforts to accomplish your goals, you wont like it, regardless of the computational power it exhibits or the functionality it offers. Because it molds a users perception of the software, the interface has to be right.

4.4.4 The Golden Rules

The golden rules actually form the basis for a set of user interface design principles that guide this important software design activity.

- Place the user in control.
- Reduce the users memory load.
- Make the interface consistent.

4.5 UML Diagrams

The UML is a language for

- ***Visualizing***-The 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 & 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. The various structural and behavioural diagrams are discussed in the chapter.

4.5.1 Use Case Diagrams

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 4.5.

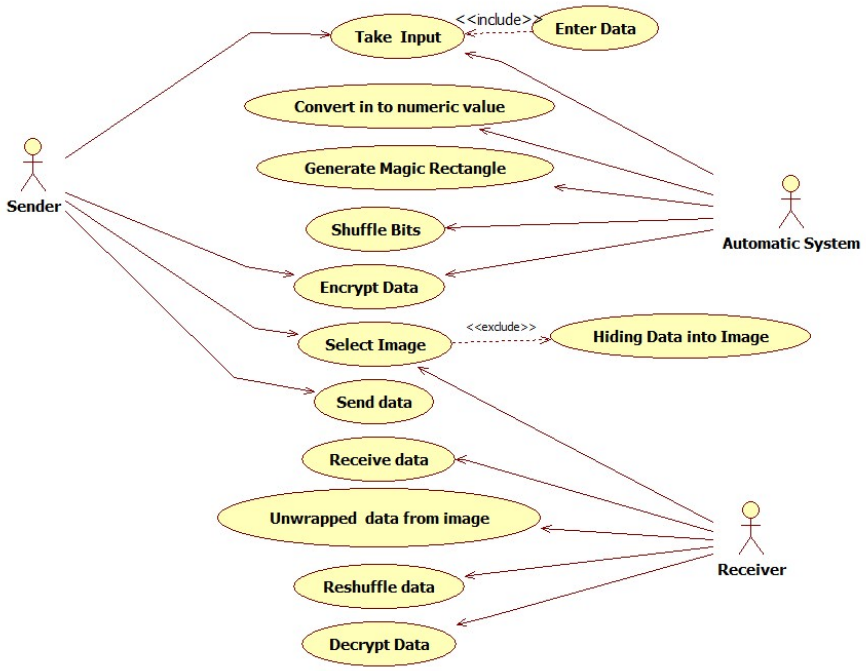

Figure 4.5: Usecase Diagram

4.5.2 Interaction Diagrams

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. Figures **??** and **??** are the sequence and collaboration diagrams of the system respectively.

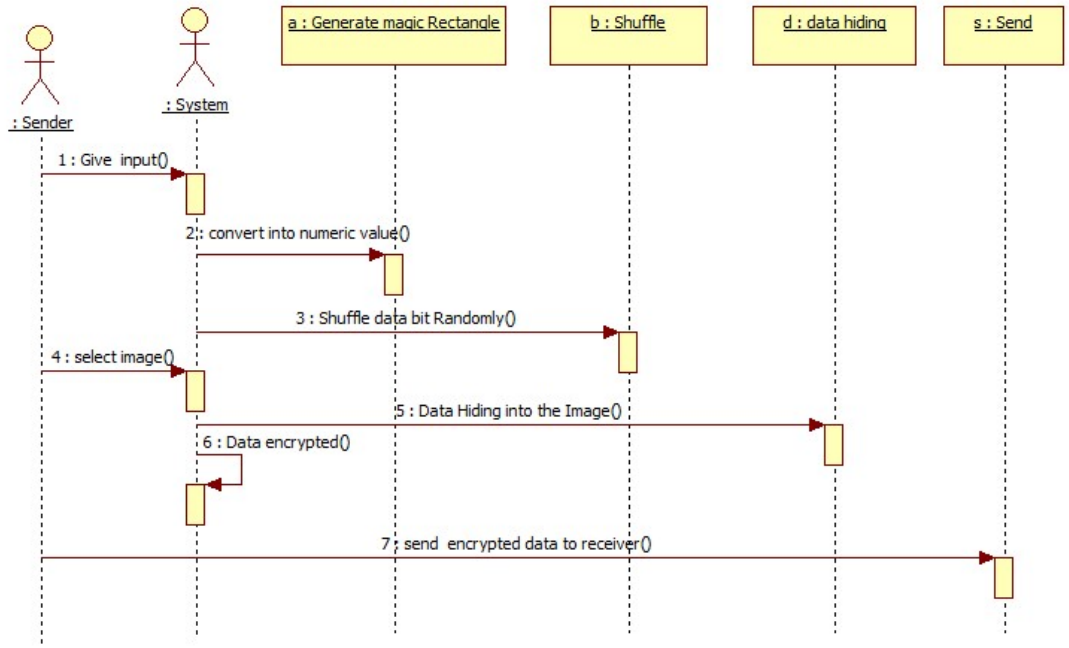

Figure 4.6: Sequence Diagram For Encryption Process

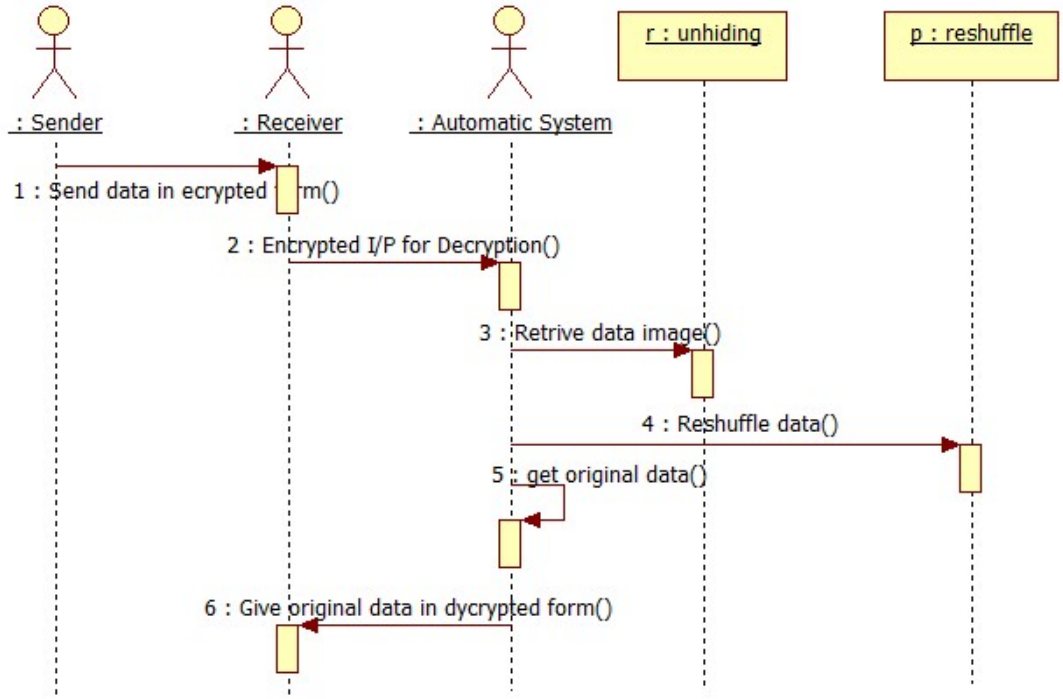

Figure 4.7: Sequence Diagram For Decryption Process

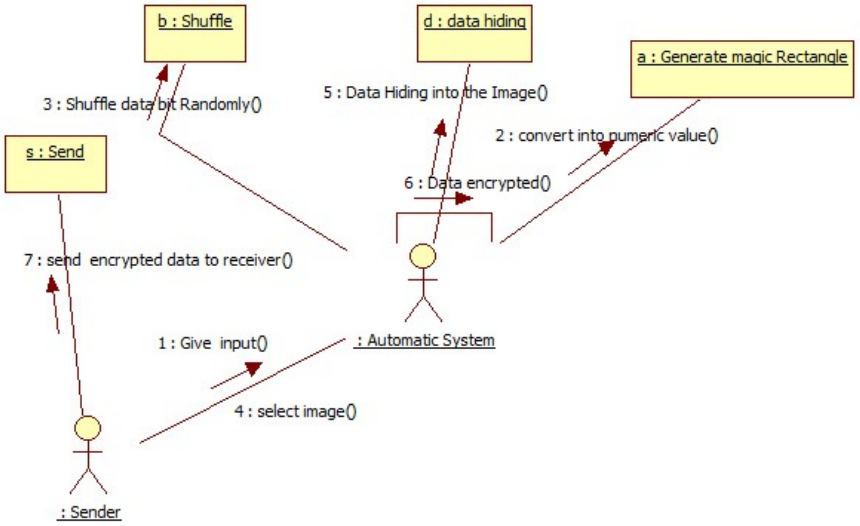

Figure 4.8: Collaboration Diagram For Encryption Process

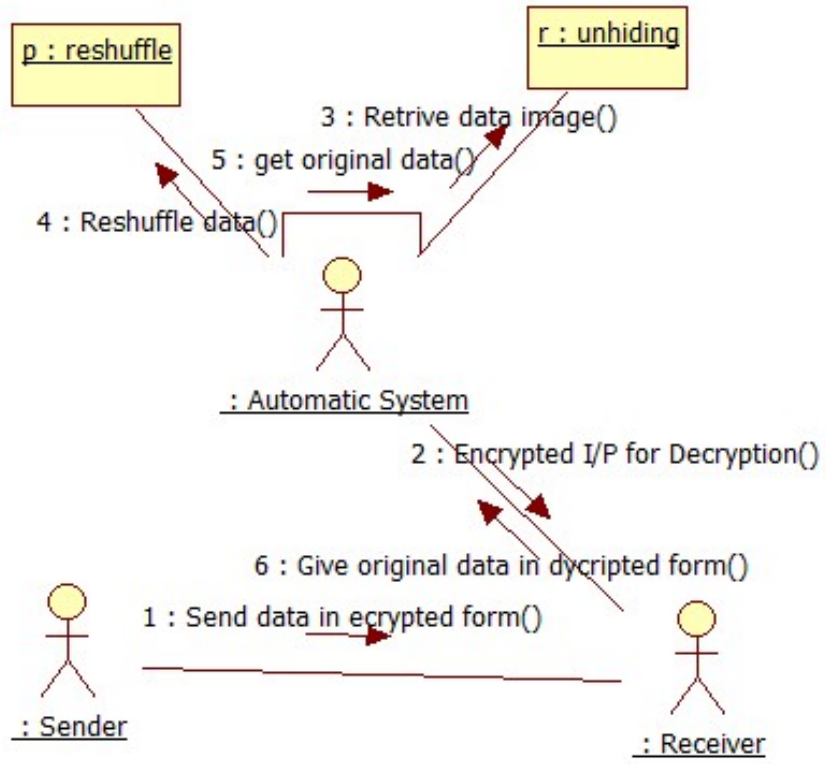

Figure 4.9: Collabration Diagram For Decryption Process

4.5.3 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 4.10 shows the class diagram for the proposed system.

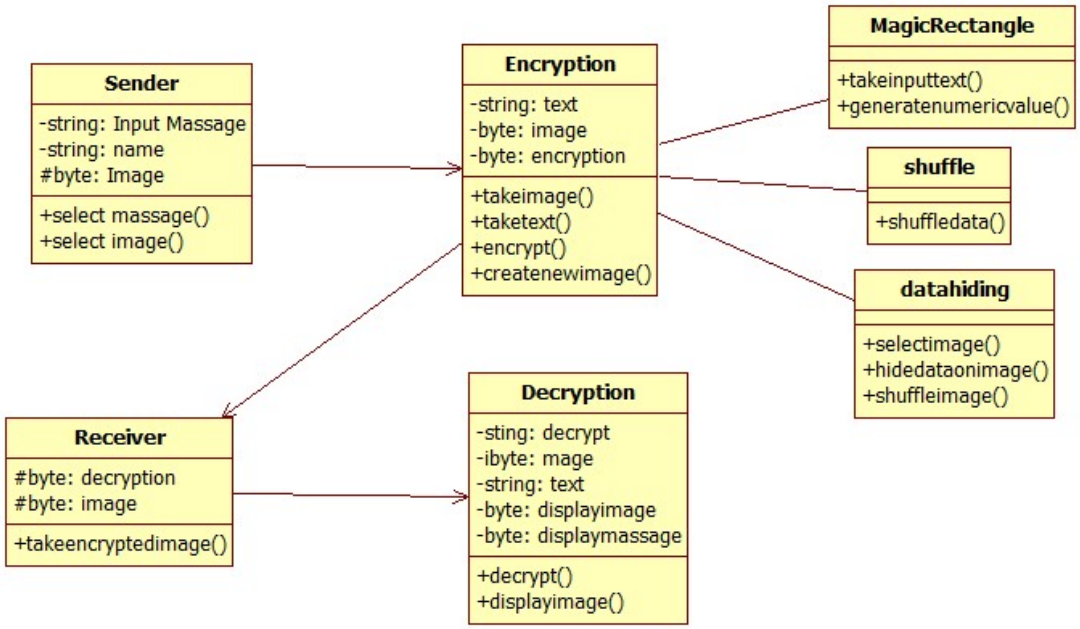

Figure 4.10: Class Diagram

4.5.4 State Diagram

A State diagram shows the dynamic ness of the system.It is used to add dynamic ness into sequence diagram.The state diagram for the proposed system is shown in Figure 4.11.

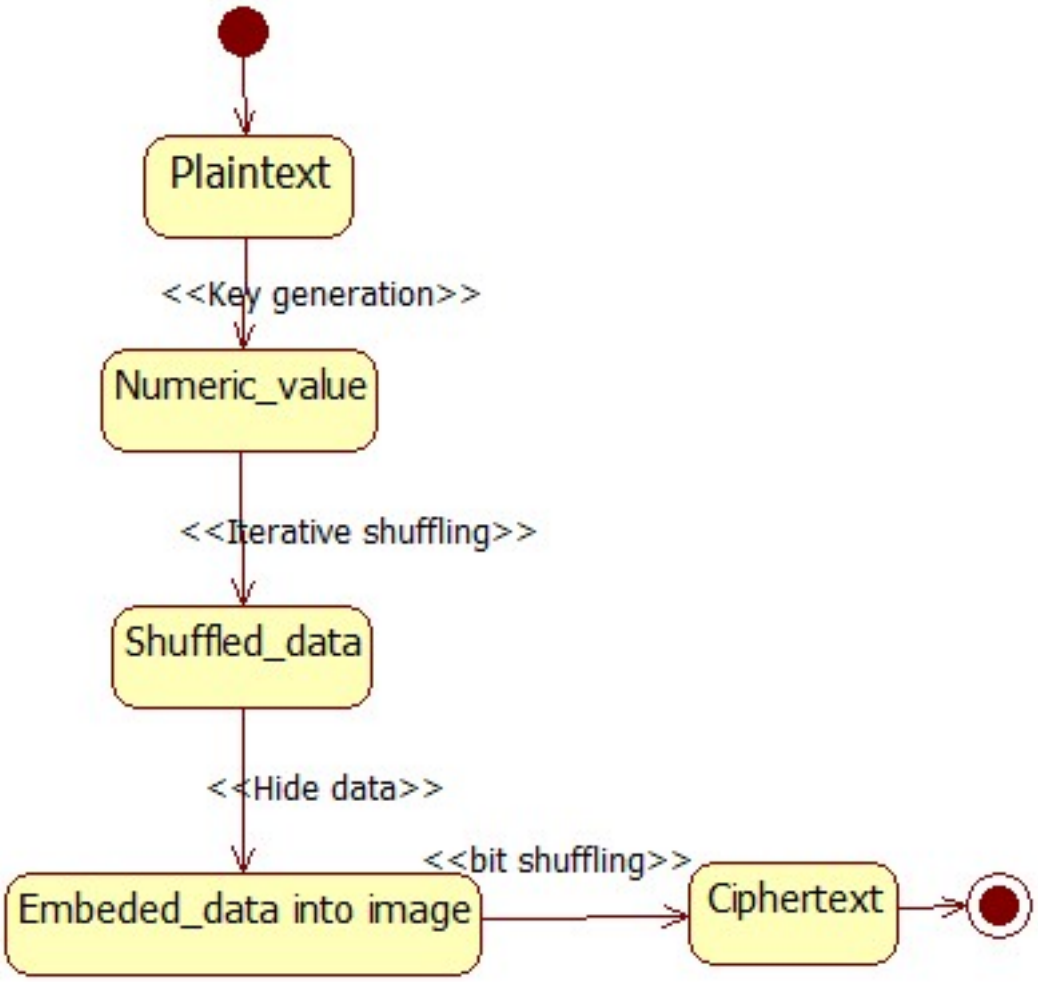

Figure 4.11: State Diagram

4.5.5 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 is Figure 4.12.

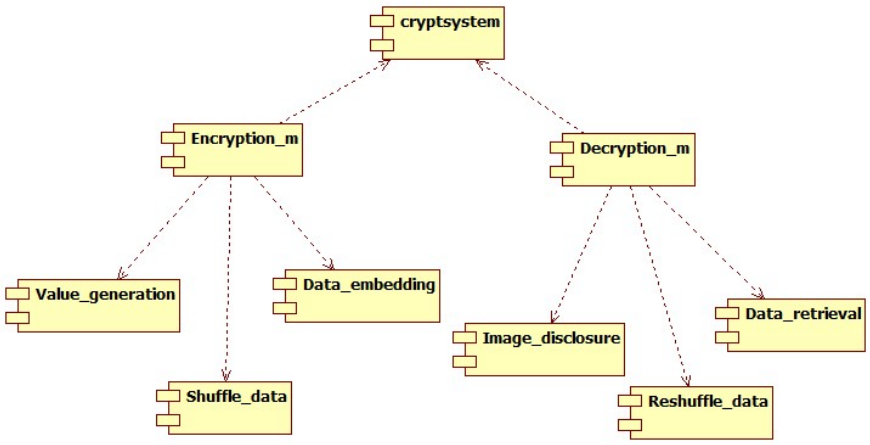

Figure 4.12: Component diagram

4.5.6 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 4.13.

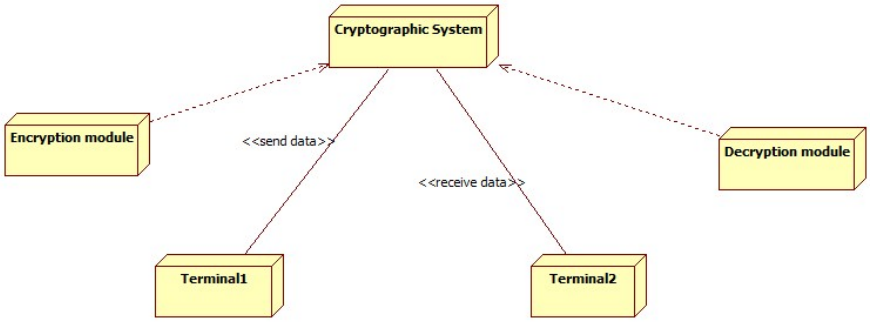

Figure 4.13: Deployment Diagram

4.6 Summary

In this chapter, the proposed system design is described. In the next chapter, Implementation is discussed.

Conclusion

In proposed system,the efficiency of cryptographic algorithm is increased.Number of stages are added into encryption and decryption processes of data to increase it's complexity.As single algorithm can not provide as much efficient result as provided by combination of algorithms in proposed system.The proposed system is used to prevent the sensitive data from different attacks.

Bibliography

[1] Pratiksha Sethi,V. Kapoor,"A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography",International Journal of Computer Applications-June 2016.

[2] Dr. D.I. George Amalarethinam and J.Sai Geetha,K.Mani,"Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting",International Journal of Computer Applications (0975 8887)Volume 96 No.14, June 2014.

[3] Dr. D.I. George Amalarethinam and J.Sai Geetha,"Enhancing Security level for Public Key Cryptosystem using MRGA",IEEE 2014.

[4] "Novel Architecture for Data Shuffling Using Fisher Yates Shuffle Algorithm",C. Aishwarya, J. R. Beny,30 December 2015.

[5] Roza Afarin,"Image Encryption Using Genetic Algorithm",2013

[6] Pratiksha Sethi,V.Kapoor's "A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography" International Journal of Computer Applications (0975 8887) Volume 144 No.9, June 2016

[7] B.Alomair and P.poovendran, E-MACs:toward more secure and more efficient construction of secure channels IEEE transaction on computers, vol 63, No.1, January 2014.

[8] Dr.Mamta sood, Manohar Wagh, and Monika Cheema A review on various data security techniques in wireless communication system journal of engineering research and applications (IJERA) vol.3, issue 2, April 2013.

Index

Introduction, 2

System Design, 15

System Requirement Specification, 13