A

Project - I Report

on

SECURE TRANSMISSION USING RDH

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Poonam Patil.
Kanchan Tayade.
Pritam Salunkhe
Om Gupta.
Alok Pandey.

Under the Guidance of

Mr.Manoj E.Patil.

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 - I entitled *Secure Transmission Using RDH*, submitted by

Poonam Patil.
Kanchan Tayade.
Pritam Salunkhe
Om Gupta.
Alok Pandey.

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: 10 October 2016
Place: Jalgaon

Mr.Manoj E.Patil.
Guide

Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Contents

List of Figures

Abstract

To maintain image contents confidentiality and to recover original image, there is a need of Reversible Data Hiding scheme.Data hiding is process of hiding the data into cover media. All previous methods embed data by reversibly vacating the room from encrypted images. This may be subject to some error on data extraction and image recovery. This method embed the data by reserving the room before encryption with reversible data hiding algorithm. This is enhanced reversible data hiding technique for colored images. The secrete message is encrypted before actual data embedding process start. Method can achieve data extraction and image recovery with free of error.

Chapter 1

Introduction

In this chapter, "Introduction", the brief review about the project. Data Hiding is the process of hiding the data into cover media. The cover media can be image, audio or video file. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. This method widely used in medical imagery, military imagery and law forensics. Such places do not suffer any distortion of the original cover media. In this paper, the cover media is taken as coloured image. The data is being hidden into the coloured image. There is no any correlation between the cover media and the embedded data. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. To achieve a security, Cryptography is used.Cryptography maintains security of a cover media. As long as image is concerned the technique could be useful in the area of protection and transmission of secret sensitive military and medical images [1].

In next section, Data hiding, is the process of hiding the data into cover media.Compression, It is a technique in information technology by which the same amount of data is transmitted by using a smaller number of bits and Cryptography..Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and store data is cover in section 1.1 Background. Motivation is discuss in section 1.2. Section 1.3 discuss Problem definition. Scope of the project covers in section 1.4. Section 1.5 Objective of project are discuss. Organisation Of The Report are discussed in section 1.6.Summary is describe in last section.

1.1 Background

In this section, overall background of project is discuss [2].

1. **Data Hiding :**Data Hiding is the process of hiding the data into cover media. The

cover media can be image, audio or video file. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data.

2. **Compression :**It is a technique in information technology by which the same amount of data is transmitted by using a smaller number of bits. In simple way, we can say, it reduces the le size up to an extent without compromising the contained data.

   - **Merits :**
     - Reduces le size
     - Improves sharing efficiency
   - **Demerits :**
     - Consumes more cpu time
     - Bit complex

3. **Cryptography :** Cryptography scrambles messages so it cant be understood. It is simply an art and science of converting plain text into cypher text. It is the process that performs the functions of encryption and decryption. When we encrypt data, it means we are converting plain text into cypher text. On the other hand, if we decrypt data, then it means we are converting cypher text into plain text. For our project, here we are employing a special cryptography algorithm i.e. algorithm.It is a popular cryptography technique in recent trend [2].

   - **Merits :**
     - Secure data
     - Easy to implement
     - Fast and flexible
     - Variable bit key for data hiding
   - **Demerits :**
     - Limited for mobile devices only
     - Complex hardware
     - Easy to detect cipher patterns

1.2 Motivation

In this section,motivation of project is discuss. As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and

store data. The security of such systems greatly depends on the methods used to manage, establish, and distribute the keys employed by the cryptographic techniques. Even if a cryptographic algorithm is ideal in both theory and implementation, the strength of the algorithm will be rendered useless if the relevant keys are poorly managed. Also the time factor is important aspect cause it increases the performance ultimately.So the triple layer implementation is more efficient for enhancement of security and performance for secure data transmission [4].
In next section, problem definition of project is cover.

1.3 Problem Definition

Reversible data hiding is technique for hiding the data into colored images. Sender before transmitting message to receiver first hide the message or data into cover media. The cover media can be taken as colored image. Data hiding process links two set of data, a set of embedded data and another set of cover media data. There is no any correlation between the embedded data and cover media. Vacating the room from encrypted images is relatively difficult and inefficient. This method may subject to error on data extraction or on image. Hacker can recover embedding data is placed at particular bit position. For removing this problem Reversible data hiding technique reserves room before encryption at content owner side. Encrypt data before embedding data into reserved room. Image and embed encrypted data are again encrypted for confidentiality. Encrypted image with embed data are transmit by sender to transmission media. Receiver receives the encrypted image. Receiver decrypt the image and recover original image. Using key receiver extract the embed data from image successfully.
In next section, scope of project is cover.

1.4 Scope

In this section, scope of the project is explain. The propose method is the combination of two different approaches together that is, reversible data hiding and color visual cryptography which gives an new improved technique to overcome the limitations of the existing techniques in the area of reversible data hiding(RDH). The proposed methodology gives the new approach for data hiding and image encryption process. Losslessly reserving the room from the encrypted image is difficult and sometimes inefficient so proposed method apply a technique of reserving the room for embedding data prior to the image encryption , thus the

reserved room can be used to hide the secret message.
In next section, objectives of project is cover.

1.5 Objectives

In this section, objectives of the project is discuss. The main reason behind development of this project is enhancement of security and performance in data sharing via different carrier mediums. Here we implement the combination of compression, cryptography and Data Hiding to achieve the required goal. Our system covers most of the existing error in current system along with play ability of the output le.
In next section, organisation of report is cover.

1.6 Organisation Of The Report

This section explains how the entire report is organized. CHAPTER 1, titled Introduction, gives an introduction of the project with background and motivation are discussed. CHAPTER 2, titled System Analysis, gives the feasibility justication, discusses the risk analysis. CHAPTER 3, titled System Requirements and Specication, explains all the requirements before and during the project. All the requirements like hardware, software, functional and non-functional are presented.CHAPTER 4, titled System Design, gives the system architecture and design of the entire project using UML diagrams. CHAPTER 5, titled Conclusion, concludes the documentation.
In next section, summary of project is cover.

1.7 Summary

In this chapter,Background of project is discussed, which is include Data Hiding ,Compression and Cryptography.As computer systems become more pervasive and complex, security is increasingly important,so Motivation are discussed. Problem definition is discussed. Scope of the project,Objective of project, Organisation of the project are discussed.

In the next chapter, System Analysis of the project,which is include literature survey, proposed system, feasibility study, project scheduling, effort allocation.

Chapter 2

System Analysis

In this section we present system analysis and design of proposed systems. System analysis model defines user requirements, establishes basis of system design and defines set of validation requirements needed for testing implemented system. System design is the technical kernel of System engineering and is applied regardless of the System process model that is used. beginning once system requirements have been analyzed and specified, System design is the first of three technical activities design, code generation, and test?that are required to build and verify the system. Each activity transforms information in a manner that ultimately results in validated proposed system [1].

Section 2.1 present Literature Survey of project,the purpose of a literature survey is to, as the name suggests, 'survey' the literature surrounding a certain topic area. The Proposed System is made up of image encryption, data embedding and data-extraction/image-recovery phases discussed in section 2.2. Feasibility Study is discuss in section 2.3. Section 2.4 Project Scheduling distributes estimated effort across the planned project duration by allocating the effort to specific task. Effort Allocation presents how to manage our project i.e. it presents process and project matrices,the basis for effective management decision making discussed in section 2.5. Finally Summary is discussed in last section.

2.1 Literature Survey

In this section, Literature Survey is discuss. Reversible data Hiding in Encrypted Images by reserving Room before encryption. Wei Zhang and Xianfeng Zhao have propose the system that maintains the reversibility. This paper defines the reversible data-hiding in encrypted image by using spare space as reserving room before encryption. Here more attention on RDH technique which maintains the reversibility that means original cover recovered after embedding additional data. It provides the security and confidentiality to

user.The advantages of this proposed system is to maintain the extra space for embedding data in data hider module. This system achieves excellent performance without any loss of data [1].
In next section, proposed system of project is cover.

2.2 Proposed System

In this section, propose system is discuss. The propose scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version2 8hen using both of the encryption and data-hiding keys, the embedded additional data can be successfully e9tracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image [1].
In next section, feasibility study of project is cover.

2.3 Feasibility Study

Once scope has been identified (with the concurrence of the customer), it is reasonable to ask: Can we build software to meet this scope? Is the project feasible? Feasibility is the second stage in system development life cycle. It is always essential to evaluate the various aspects before we developed a system. Evaluation should always justify the cost and benefits are less as compared to project. The feasibility of the software development of the projects may be view from 3 angles:

1. Operational Feasibility
2. Technical Feasibility
3. Economical Feasibility

In next section, operational feasibility of project is cover.

2.3.1 Operational Feasibility

In this section, operational feasibility is discuss. It was decided that the proposed protect could be created as a windows based application system that will meet the operating environment of various people for browsing the internet.The reasons for this conclusion are:

- Business method adopted is acceptable to all users.
- The end users have been involved in the planning and development.
- Manual errors will be reduced.
- It is a user friendly browser and any person having moderate knowledge of computers, internet and protect handling can operate it.
- it is an operationally feasible protect considering both the hardware and software.

In next section, technical feasibility of project is cover.

2.3.2 Technical Feasibility

The system must be evaluated from the technical point of view first. The assessment of this feasibility must is based on an outline design of the system requirement in the terms of input, output, programs and procedures. Having identified an outline system, the investigation must go on to suggest the type of equipment, required method developing the system, of running the system once it has been designed. Technical issues raised during the investigation are:

1. Does the existing technology sufficient according to customer requirements?
2. Can the system expand if developed ?

In next section, economical feasibility of project is cover.

2.3.3 Economical Feasibility

Automation leads to cost reduction and beneficial to cost analysis of the system. It yields the following results:

1. Extra cost required to purchase the software is very less. Various reports can be obtained by running the proposed system.

2. Automation results in the reduction of the manpower and processing time.

3. Even though small changes are made it is economically feasible as lot of advantage is achieved by using the proposed system.

In next section, project scheduling of project is cover.

2.4 Project Scheduling

In this section, how project is scheduled is discuss. Software project scheduling distributes estimated effort across the planned project duration by allocating the effort to specific task. Scheduling for projects can be viewed from two different perspectives. In the first view, an end-date for release of a computer-based system has already been established and fixed. In the second view, assume that rough chronological bounds have been discuss but that the end-date is set by the software engineering organization.

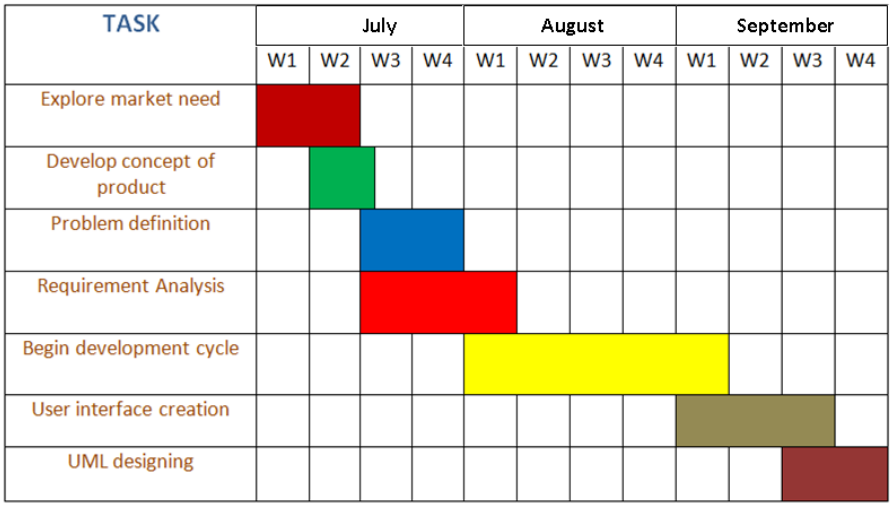

Figure 2.1: Project Scheduling

In next section, effort allocation of project is cover.

2.5 Effort Allocation

In this section, effort allocation is discuss. Under this, we study how to manage our project i.e. it presents process and project matrices,the basis for effective management decision making. It includes cost and resource equipment and also establishes an effective project plan. It mainly consists of the three P's: People , Product and Process.

Activity	Poonam Patil	Kanchan Tayade	Pritam Salunkhe	Alok Pandey	Om Gupta
Project Planning	25 %	25 %	25 %	20 %	5 %
Requirement Gathering	30 %	15 %	15 %	20 %	20 %
Design	35 %	20 %	25 %	10 %	10 %

Figure 2.2: Effort Allocation

2.5.1 People

People factor is required to enhance the readiness of organization to undertake increasingly complex applications by helping to attract, grow, motivate, deploy and retain the talent needed to improve their application development capability. This project has been carried by group of five people. People: User-Employee Developer: 5 Group Members.

2.5.2 Product

It includes the objectives and the scope that should be established, alternatives solutions that should be considered and technical and management constraints should be identified. The projects objective is very clear, that is to provide performance and security to highly secure data while transmission in secure aspects. We will be using Microsoft .NET Framework for doing this project as it is user friendly. The major problem here is that since information security is a major concern in today's digitized arena. Also if highly secure data is accessed by unauthenticated user then it may cause severe problems.

2.5.3 Process

Process for building the project provides a framework from which a comprehensive plan for its development can be established. The framework for this includes: The availability of software such as Microsoft .NET framework 4.5 and Microsoft Visual Studio 2008. The process model that we are using is incremental model. This is because it provides systematic, sequential approach for software development that begins at system level through analysis, design, coding and testing phases. As the requirements for the project are not specified completely during initial stages hence in such cases incremental model fits best for the software development process.

- User can select the data file which is to be send securely.
- Now user can perform compression and encryption or decryption and decompression operation on it.
- Data file is now ready for attaching behind audio file.

In next section, summary of project is cover.

2.6 Summary

In this chapter, System Analysis include, Literature survey of project,the purpose of a literature survey is to, as the name suggests, 'survey' the literature surrounding a certain topic area.The propose scheme is made up of image encryption, data embedding and data extraction/image-recovery phases are discussed . Software project scheduling distributes estimated effort across the planned project duration by allocating the effort to specific task are discussed. Effort allocation ,how to manage our project i.e. it presents process and project matrices,the basis for effective management decision making are discussed.

In next chapter, system requirement specification, which is include Software and hardware specification, functional requirement of the project.

Chapter 3

System Requirement Specification

Requirement Analysis is a software engineering task that bridges the gap between system level software allocation and software design. Requirement analysis enables the system engineer to specify software function and performance indicates software interface with other system elements and establish constraints that software must meet. Requirement Analysis provides the software designer with models that can be translated into data, architectural, interface, and the user with means to assess quality once the project is built.

This chapter species all the requirements for the project. Section 3.1 describes Hardware Requirements. Software Requirements is described in section 3.2. Section 3.3 describes Specication. Functional Requirements is described in section 3.4. Finally, Summary of the chapter is given in the last Section.

3.1 Hardware Requirements

In this section,discussed, which hardware requirements are required for project.

- Processor : Pentium 4
- RAM : 512 MB
- Carrier Medium

In next section, software requirement of project is cover.

3.2 Software Requirements

In this section,discussed, which software requirements are required for project.

- Operating system : Windows 7,8
- Technologies : Java
- Front End : Java

In next section, specification of project is cover.

3.3 Specification

In this section, specication of project is discuss. The term specication means different things to different people. A specication can be written document, a graphical model, a formal mathematical model, a collection of using scenario, a prototype, or any combination of these states. The system specication is the nal work product produced by the system and requirements engineer. It serves as a foundation for software engineering, database engineering, and human engineering. It describes the function and performance of a computer based system and the constraints that will govern it deployment. The specication bound each allocated system elements. The system also describes the information i.e. input to and output from the system. It starts from the size and capacity requirements.
In next section, functional requirements of project is cover.

3.4 Functional Requirements

In this section,discussed, which functional requirements are required for project.

- Image Selection
- Image Encryption
- Data Hiding
- Extracting the data/ Obtain the image

In next section, summary of project is cover.

3.5 Summary

In this chapter, overall detail of this project like hardware requirement,software requirement,functional requirements are discussed.

In the next chapter, System design, describes the module to system architecture. E-R diagrams are described. Data flow diagrams are discussed. UML diagrams are discussed.

Chapter 4

System Design

Design is the first step into the development phase for any engineered product or system. Design is a creative process. A good design is the key to effective system. The term "design" is defined as "the process of applying various techniques and principles for the purpose of defining a process or a system in sufficient detail to permit its physical realization". It may be defined as a process of applying various techniques and principles for the purpose of defining a device, a process or a system in sufficient detail to permit its realization. Software design sits at the technical kernel of the software engineering process and is applied regardless of the development paradigm that is used. The system design develops the architectural detail required to build a system or product.

Section 4.1 describes the module to System Architecture. E-R diagram are described section 4.2. Section 4.3 describes Data flow diagrams. UML diagrams are described in section **??**. Last section describes Summary.

4.1 System Architecture

In this section, describes the module to system architecture. Losslessly vacating room from the encrypted image is relatively difficult and sometimes inefficient. These methods may subject to some errors on data extraction and/or image. Hacker can recover embedding data because data is placed at particular bit position. Hence there is a need to reserve a room before encryption at content owner side using key encryption technique. Reversible data hiding is technique to embed the additional message in the some distortion unacceptable cover media. This is the technique that is mainly used for the authentication of data like images, videos, electronic documents. This system proposes designing of reversible data hiding mechanism that can losslessly recover original image and can extract embedded data. It will protect the image contents confidentiality [1].

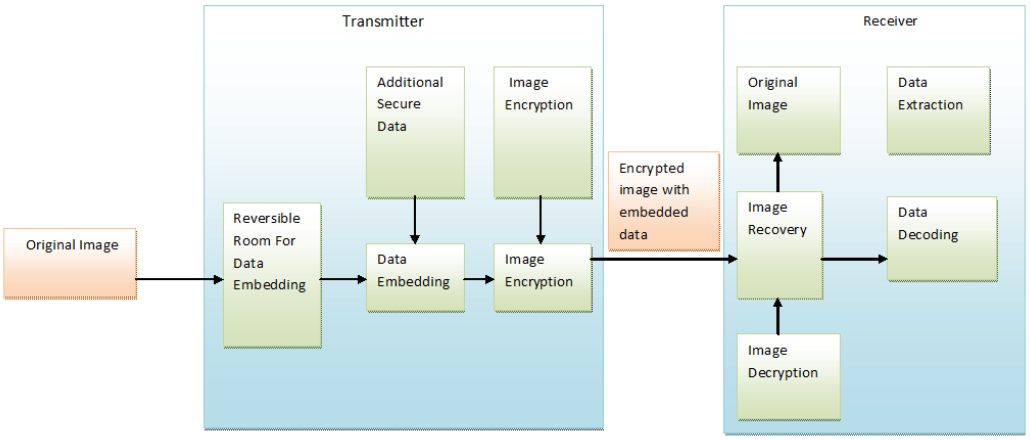

Figure 4.1: Reversible Data Hiding by Reserving Room before Encryption with key

The propose method combines the benefits of two different approaches together. Those are Reversible Data Hiding and using key encryption of an image. Reversible Data Hiding, by using keyless approach is shown in Figure 4.1. The proposed system has designed and implemented with the following modules:

1. Reserving Room for Data Embedding
2. Data Hiding
3. Key Image Encryption
   - Filtering
   - Division
   - Shuffling
4. Image Decryption
5. Data Extraction

The content owner selects the cover media as an image. From an original image space for embedding the secret data is found out. Then the image is encrypted with key image encryption methodology. Upon receiving receiver decrypts image using the keyless approach and extracts the data and recovers original image.

4.1.1 Reserving Room for Data Embedding

The common approach for high capacity data embedding is to find the room for embedding data. The scheme involves partitioning the image logically. The goal of image partition

is to construct a smoother area, on which RDH algorithm can achieve better performance.

4.1.2 Data Hiding

The data hiding module separates Red, Green and Blue component of the image. Then each component of the colour is considered separately. By considering each separate colour component, the data is added into it. This increases the data embedding capacity of an image. The data hiding algorithm:

1. Find separate Red, Green and Blue components of an image. We will have three different matrices of three different colour components like R-Matrix, G-Matrix, Bmatrix.

2. Then apply the process of difference expansion for hiding data bits. Here pixel from blocks, which are having f-value lies below f-avg are used for embedding process. These blocks are smoother than others. After using all possible pixels of R-component of a block, G-component is considered then B-component is used. In this way data is being added into the different colour components.

3. Convert the message text into binary form. Then consider bits from the binary data one by one and hide it.

4. If certain block is completely used then the other block is taken under consideration. Likewise complete data file is hidden in the image blocks.

4.1.3 Key Image Encryption

The keyless approach of image encryption can be implemented with following steps:

1. **Splitting** : The splitting step includes distributing the combined RGB components into individual R, G and B components. The granularity of the sieve depends on the range of values that R/G/B component may take individually.

2. **Division** : After converting the original image into the Red, Green and Blue components, the next step is to divide the Red, Green and Blue components into z parts or shares each. R -¿ (RA, RB, RC, ————————-, RZ) G -¿ (GA, GB, GC, ————————-, GZ) B -¿ (BA, BB, BC, ————————-, BZ) While performing division, it should be get confirmed that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection. For example, if x = 8,then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (RA, RB, RC, ———————— RZ) should regenerate R and similarly for G and B components.

3. **Shuffling** RA-Z, GA-Z and BA-Z shares are generated after performing division. Next is to perform the shuffle operation. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary colour. RB decides how RA is shuffled, RC decides how RB is shuffled, ———— RZ decides RZ-1 is shuffled and RA decides how RZ is shuffled. After performing above three operations, the final generated share is combined and final Z-random shares are generated. The final z random shares are (RS). RSA - ¿ (RA- shuffle, GA- shuffle and BA- shuffle) RSB -¿ (RB- shuffle, GB- shuffle and BB- shuffle)- - - - RSZ -¿ (RZ- shuffle GZ- shuffle and BZ- shuffle) If we consider individual shares, then these individual shares does not predict any valid information. So to have original image, all shares are required.

4.1.4 Image Decryption

The process of retrieving the original image involves following process:

1. Filtering the random shares and retrieving R/G/B (Ashuffle) and R/G/B (B-shuffle)
2. Then, from the individual shuffled shares generate the original RA, GA, BA and RB, GB.
3. Using these, original image is then generated. The retrieved image is same as original and there is no loss of picture quality occurs.

4.1.5 Data Extraction

For performing the data extraction, the new pixel values of the image are considered. The difference of the neighbouring pixels is calculated. The LSB of the difference is the bit which was hidden. For this, the data retrieval method require the index position of those blocks which were considered in hiding process and the pixel pairs position where the data is hidden as the input. Data Extraction Algorithm:

1. Separate the Red, Green and Blue components matrices of the image blocks.
2. First, calculate the average and the difference of the Pixels(a,b).
3. The embedded data is least significant bit of y, and the original difference y is calculated.
4. The original pixels can be restored.

5. With the help of above process, one by one each bit will be extracted from the pixel pairs.

6. To find the hidden data, use and apply proper decoding technique. And extract binary data.

In next section, E-R diagram of project is cover.

4.2 Entity - Relationship Diagram

In this section, E-R diagram related to project is describe . Diagram depicted data at rest, data being stored. It also implies how data is implemented, created modified, use and deleted. Data relationship is the relationship between the entities. All relationship is further described by words of symbol that indicates the number of occurrence of the related entity and vice versa. In the entity relationship diagram rectangle are use to display entities and relationship is described with in diamond shape boxes.

The overall logical structure of a database can express graphically by an E-R diagram. The entity relationship diagram enables a software engineer to fully specify the data object that are input for a system the attributes that define the properties if these object.

The E-R diagram model is one of the several semantic data models the semantic aspect of the model lies in the attempt to represent the meaning and interaction of real word enterprise into a conceptual schema.Please note that the concept of E-R diagram is totally different from DFD.

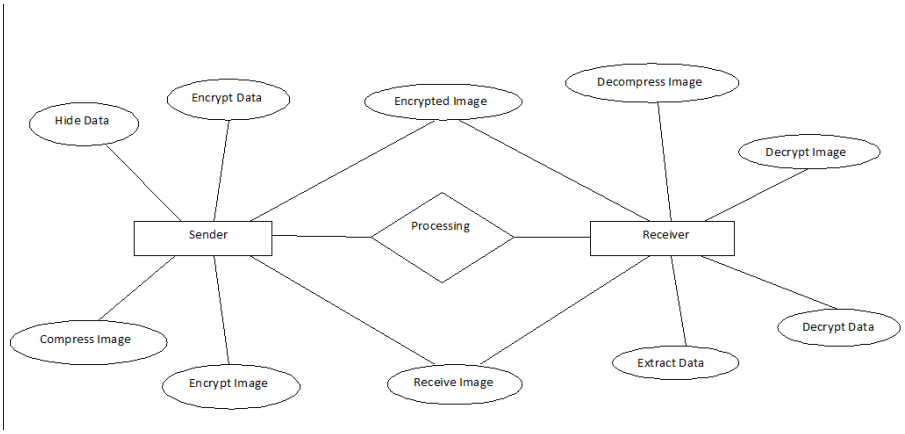

Figure 4.2: E-R Diagram

In next section, data flow diagrams of project is cover.

4.3 Data Flow Diagram

In this section, Data Flow Diagrams shows the overall flow of the project. The takes an input-process-output view of a system i.e. data objects ow into the software, are transformed by processing elements, and resultant data objects ow out of the software. The DFD enables the software engineer to develop models of the information domain and functional domain at the same time. As the DFD is refined into greater levels of details, the analyst perform an implicit functional decomposition of the system. At the same time, the DFD refinement results in a corresponding refinement of the data as it moves through the process that embody the applications. Data Flow analysis studies the use of data in each activity. It documents these findings in data flow diagrams. Which graphically show the relation between processes and data. Data flow analysis examines the use of data to carry out specific business processes within the scope of system investigations. You might think of it as viewing of the system from the viewpoint of data where they originate, how they are used or changed, and where they go including the stops along the way from their to their destination.

Figure 4.3: Level 0 DFD

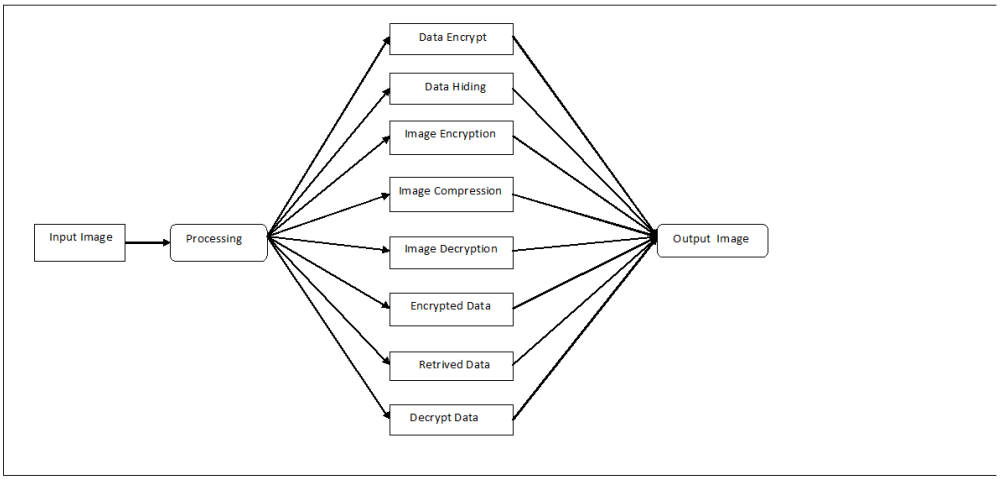

Figure 4.4: Level 1 DFD

In next section, UML diagrams of project is cover.

4.4 UML Diagrams

In this section, UML diagrams related to project is describe. The is a language that defines the industry's best engineering practices for the modeling systems. The goal of UML is to be a ready-to-use expressive visual modeling language that is simple and extensible.

4.4.1 Use Case Diagram

Use case diagram shows a set of use cases, 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 behaviour of the system.Figure 4.5 illustrates use case diagram for Secure Data Transmission using RDH.

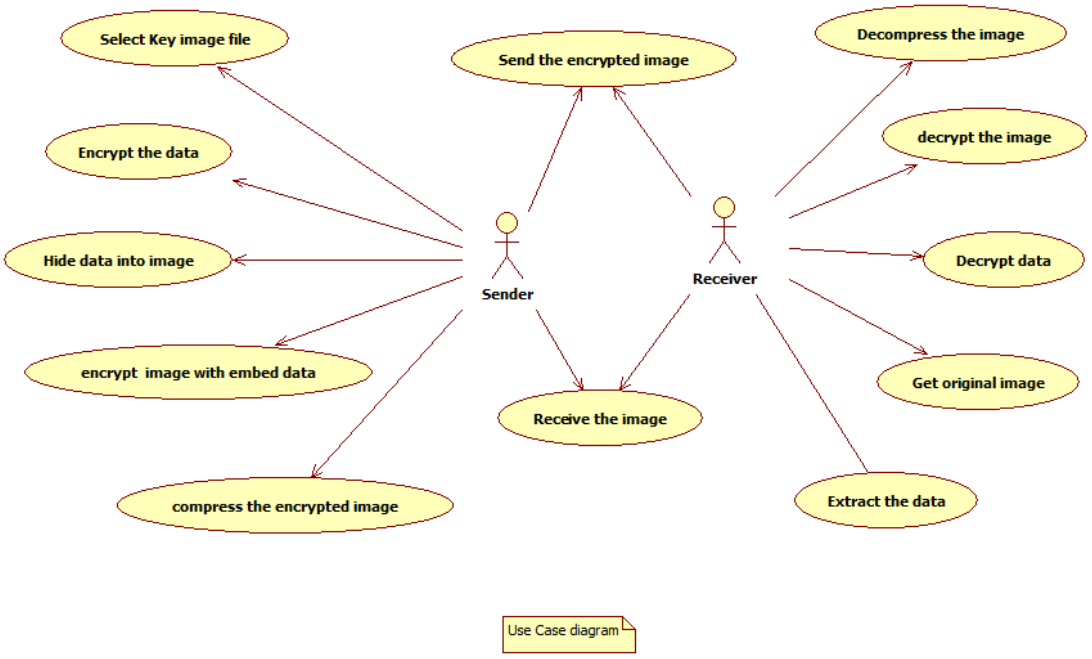

Figure 4.5: Use Case Diagram

4.4.2 Class Diagram

A class diagram is an Structural diagram that emphasizes the structural organization of Classes and there representation. Class diagram also shows relationship between different classes. Figure 4.6 illustrates class diagram.

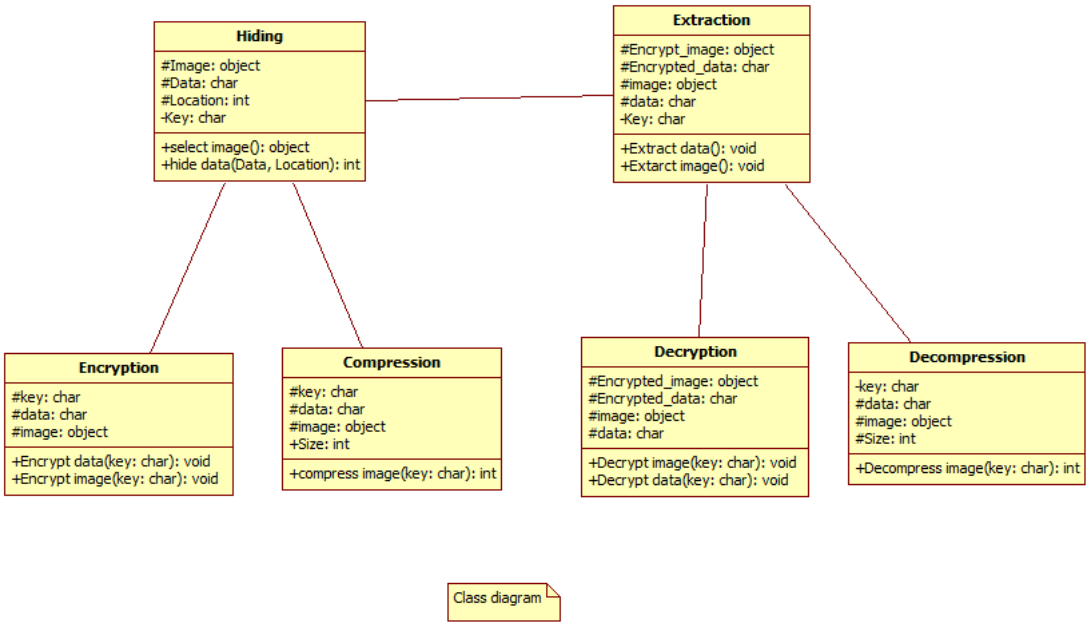

Figure 4.6: Class Diagram

4.4.3 Sequence Diagram

A sequence diagram is an interaction diagram that emphasizes the time ordering of messages. Sequence diagram is isomorphic means that we can take one and transform it into the other.Figure 4.7 illustrates sequence diagram.

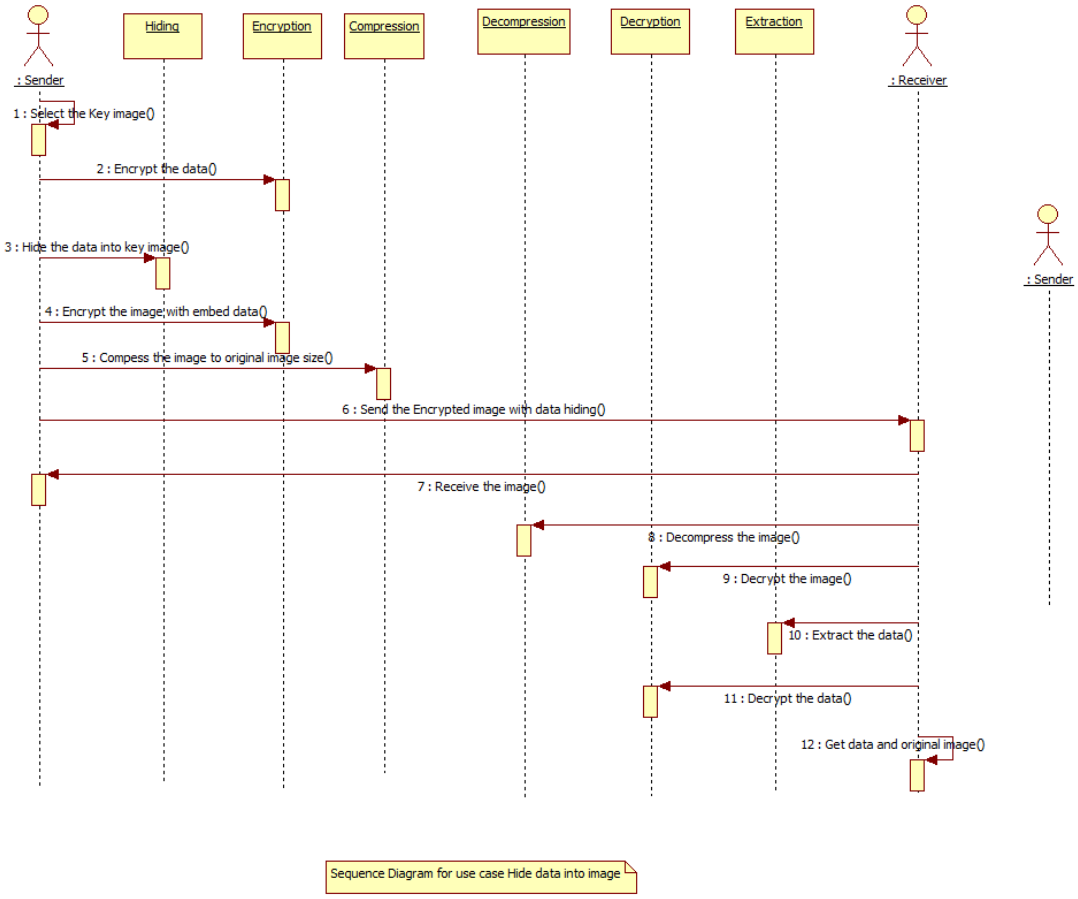

Figure 4.7: Sequence Diagram

4.4.4 Activity Diagram

A Activity diagram is a graphical representation of executed set of procedural system activities and considered a state chart diagram variation.It describes parallel and conditional activities,use cases and system function at detailed level.This diagram is used to model large activities sequencial work flow by focusing on action sequence and respected action initiating conditions.Figure 4.8 illustrates activity diagram.

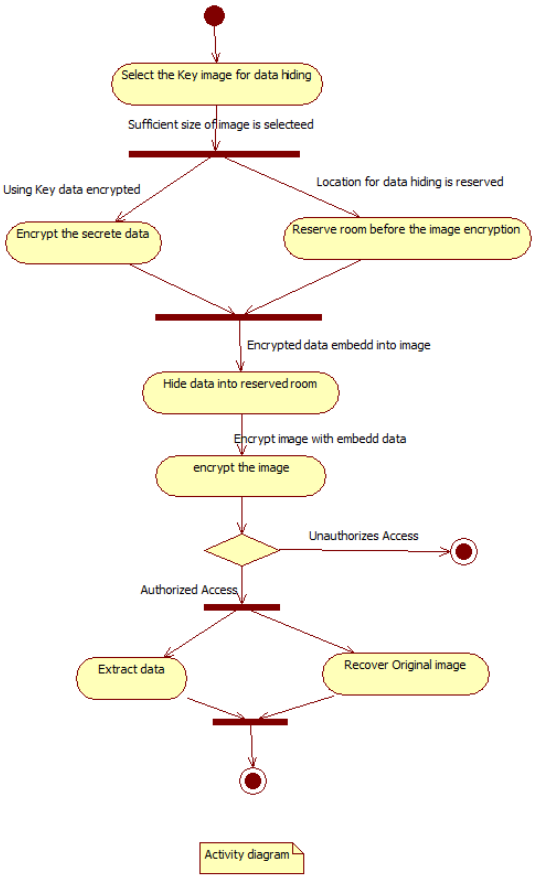

Figure 4.8: Activity Diagram

4.4.5 Component Diagram

A component diagram shows the organizations and dependencies among a set of components.Component diagram address the static implementation view of a system. They are related to class diagram in that a component typically maps to one or more classes, interfaces or collaborations. Figure 4.9 illustrates component diagram.

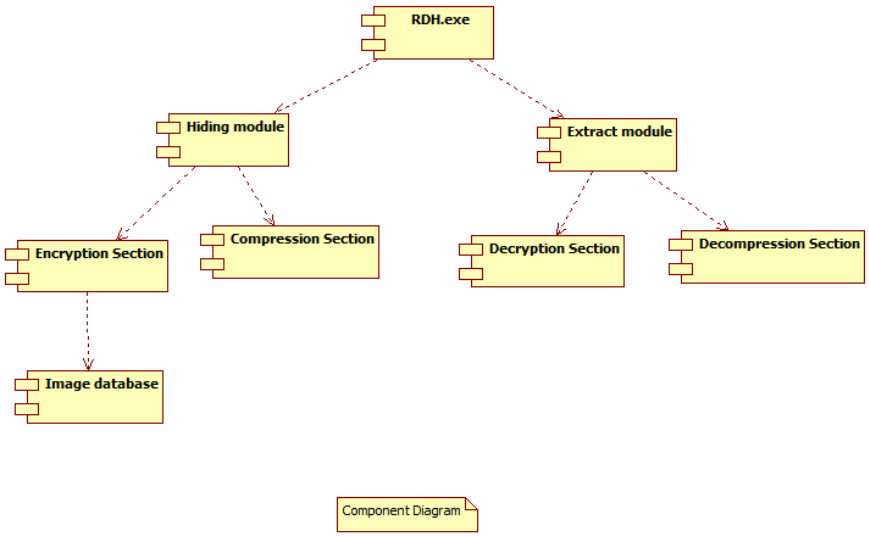

Figure 4.9: Component Diagram

4.4.6 Deployment Diagram

A deployment diagram shows the configuration of runtime processing nodes and the components that live on them. Deployment diagram address the static deployment view of an architecture. They are related to component diagram in that a node typically encloses one or more components. Figure 4.10 illustrates deployment diagram.

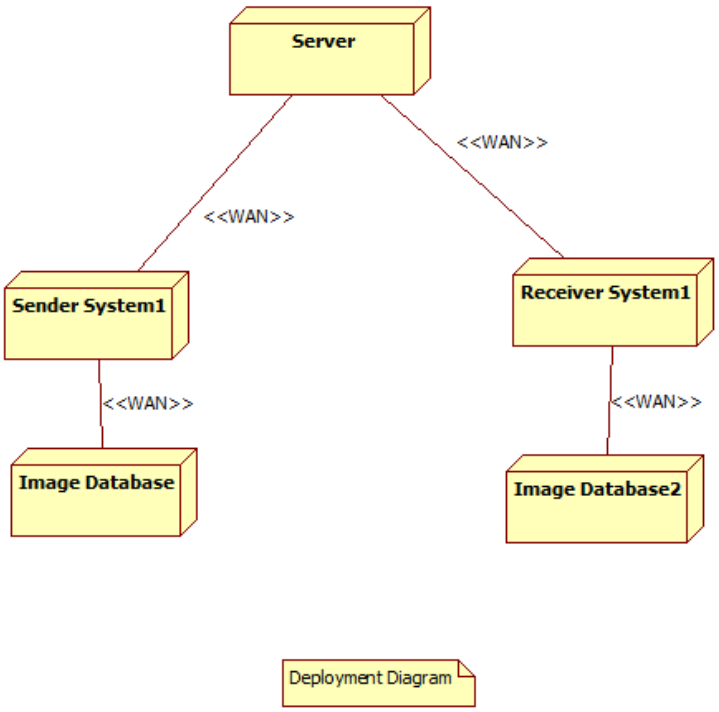

Figure 4.10: Deployment Diagram

4.4.7 State Diagram

A state chart diagram shows a state machine, consisting of states, transitions, events and activities. State chart diagram address the dynamic view of a system. It is especially important in modeling and behaviour of an interface, class or collaboration and emphasize the event ordered behaviour of a object which is especially useful in modeling reactive systems.Figure 4.11 illustrates state chart diagram.

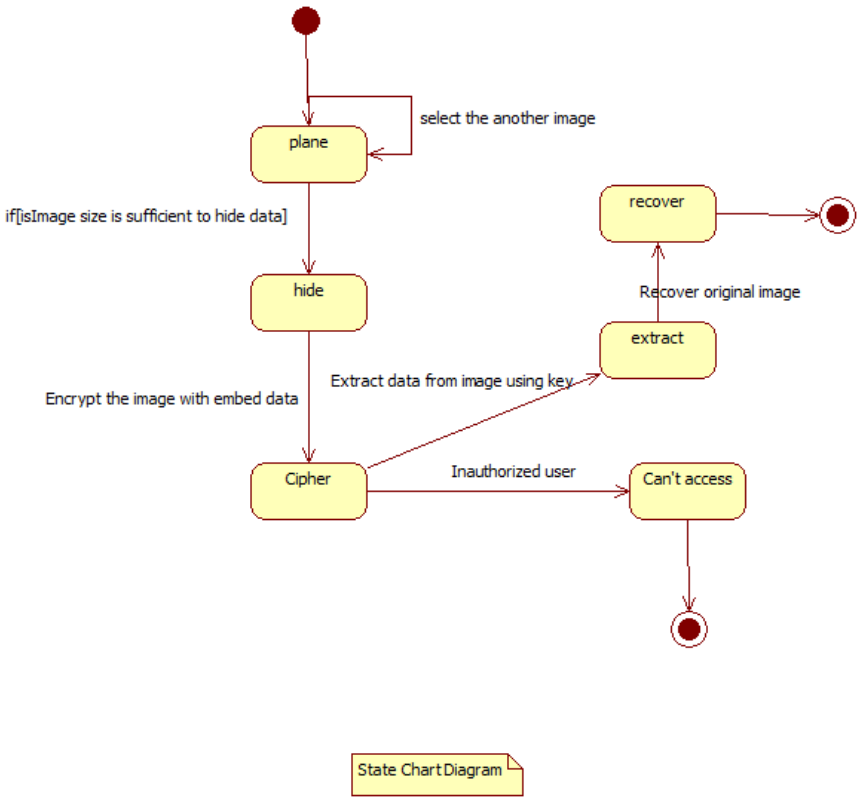

Figure 4.11: State Diagram

4.5 Summary

In this chapter,System design,gives overall detail of this project like system architecture, E-R diagram, data flow diagram, UML diagrams.

In the next chapter,Conclusion of the project are discussed.

Chapter 5

Conclusion

An enhanced Reversible data hiding schemes for encrypted colored image is proposed, which consists of image encryption, data hiding, data extraction and image recovery phases. As the secure data transmission using colored image is the medium to transfer secure data quickly to the user it uses secure key and that key will know to the receiver only, so the secure data transmission is the most powerful medium for sharing the data. In future the original images will encrypt by a keyless image encryption strategy. A data hider does not need to know the original content. He can embed the secret data into the image by using difference expansion method. And at the receiver side, he can extract the data and also image can be decrypted using keyless image decryption method.

Bibliography

[1] Ms. Nilam N. Shaikha, Prof. Amit B. Chougule, Xianfeng Zhao , An Enhanced Reversible Data Hiding Technique for Coloured Images, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 4 Issue: 5, 2016.

[2] International Journal of Scientific Engineering and Applied Science (IJSEAS),International Journal of Scientific Engineering and Applied Science (IJSEAS), 2016.

[3] M. Manju and Dr.V.Kavitha, Survey on Reversible Data Hiding Techniques, IEEE Transactions on Information Forensics and Security, 2014.

[4] Athira Mohan,Ms.Nasseena, An Efficient Joint Data Hiding And Compression Technique, International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016.

Index