A Project Report on

Color Code Substitution Based Advance Mailing Technique

Submitted in partial fulfillment of the requirements for the award
of the degree of

Bachelor of Engineering

in

Information Technology

by

Chinmay Karangutkar(16204032)
Ankita Gound(16204013)
Ameya Murkute(16204028)
Prapti Nevrekar(16204014)

Under the Guidance of

Prof. Ganesh D. Gourshete

Department of Information Technology
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI

Academic Year 2018-2019

Approval Sheet

This Project Report entitled ***"Color Code Substitution Based Advance Mailing Technique"*** Submitted by ***"Chinmay Karangutkar (16204032)"***, ***"Ankita Gound (16204013)"***, ***"Ameya Murkute(16204028)"***, ***"Prapti Nevrekar(16204014)"***is approved for the partial fulfillment of the requirement for the award of the degree of ***Bachelor of Engineering*** in ***Information Technology*** from ***University of Mumbai***.

Prof. Ganesh D. Gourshete
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Place:A.P.Shah Institute of Technology, Thane
Date:

CERTIFICATE

This is to certify that the project entitled ***"Color Code Substitution Based Advance Mailing Technique"*** submitted by ***"Chinmay Karangutkar(16204032)"***,***"Ankita Gound(16204013)"*** ,***"Ameya Murkute(16204028)"***, ***"Prapti Nevrekar(16204014)"*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering***in ***Information Technology.***,to the University of Mumbai,is a bonafide work carried out during academic year 2018-2019.

Prof. Ganesh D. Gourshete
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place: A.P.Shah Institute of Technology, Thane
Date:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Chinmay Karangutkar (16204032)

Ankita Gound (16204013)

Ameya Murkute(16204028)

Prapti Nevrekar(16204014)

Date:

Acknowledgement

We have great pleasure in presenting the report on **Color Code Substitution Based Advance Mailing Technique.** We take this opportunity to express our sincere thanks towards our guide **Prof. Ganesh D. Gourshete** Department of IT, APSIT thane for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards his constant encouragement, support and guidance through the development of project.

We thank **Prof. Kiran B. Deshpande** Head of Department,IT, APSIT for his encouragement during progress meeting and providing guidelines to write this report.

We thank **Prof. Vishal S. Badgujar** BE project co-ordinator, Department of IT, APSIT for being encouraging throughout the course and for guidance.

We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Student Name 1: Chinmay Karangutkar
Student ID1: 16204032

Student Name 2: Ankita Gound
Student ID2: 16204013

Student Name 3: Ameya Murkute
Student ID3: 16204028

Student Name 4: Prapti Nevrekar
Student ID4: 16204014

Abstract

Lately, exponential growth of technology in every aspect of life is observed. Improvement of technology provides facilities to both users and hackers/intruders too. Advancement in technology that encourages hackers/intruders activities result in lack of security to users confidential data. The most common and popular techniques for data hiding that have been in use since long time are cryptography and steganography. Thus these email systems are also used on very large scale , many social docs are been getting transferred via email systems, so this systems and servers should also be secured from all intruders and hackers as there is confidential data getting transferred via network, so it can be protected in most advanced and secured way i.e: with help of triple encryption and steganography.

Contents

List of Figures

List of Abbreviations

LSB:	Least Significant Bit
AES:	Advanced Encryption Standard
RSA:	Rivest Shamir Adleman
RGB:	Red Green Blue
ERD:	Entity Relationship Diagram
DFD:	Data Flow Diagram
PCC:	Play Color Cipher

Chapter 1

Introduction

The Internet is an innovative technology that has become one of the most important event on modern world history. It contains huge amount of information in different fields. Many techniques are available to prevent unauthorized users from copying information without owner permission. Two of these techniques are cryptography and steganography.

Steganography word is originally from two Greek words Steganos which means Covered and Graptos means writing and which literally means cover writing Steganography means to hide messages existence in a particular medium such as audio, video, image, text communication. It is very different from protecting the actual content of a hidden message. Steganography simply means that is not to be alter the any structure of the secret message, but hides it inside a cover-object which is used as medium for transmitting message. After hiding the message, the process cover object and stego-object which helps to carrying hidden information object.

So, steganography is used to hide information and cryptography is used to protect information are totally different from each another.

1.1 Scope

The main motto of this project is to create a system which will be platform independent, will be efficient in mailing image and videos in encrypted format i.e the confidentiality is been maintained

1.2 Problem statement

To solve the current lack of highly encrypted mail service using triple encryption using steganography and multi language support for highly important or secretive communication.

1.3 Objective

The main objective of our project is to provide security to the communication medium used by email server which includes many sub-objectives :

1. To pass unnoticed text information in Image format.
2. To pass unnoticed image information into stegnographed image .
3. To provide a easy to access system for the user.
4. To provide a support for multiple languages
5. To surpass the attacks led by any attacker while communication is been in process.
6. To make this system portable on all Operating Systems Platforms.

Chapter 2

Motivation

Now-a-days, the steganography is used to hide a secret data in a file, so that an intruder who want to controls the communication does not remark in hidden message behind the file. This motivates the researches to continue with the research work and get their work appreciated through the standard journals. The search of relevant papers is based on the lists of citation and the mostly visited reference list. Thus the importance of the citation sites is growing and the number of citation an author receives is becoming more important than the size of his list of publications. Also every publisher has its own specific style of citation/ reference representation style.

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Encrypt a message using cryptography, and hide the encryption within an image using steganography.

Different search engines led to exchange the information between world on the web. The web based search engines enabled to search and analysis of scientific literature and calculation of citation indexes. Scientific paper search engines enable analysis of relationship between papers, authors, research groups.

Chapter 3

Literature Review

Cryptography based on Color Substitution for plain text was done for English Language. In Symmetric-key ciphers, the sender sends the plain text which is encrypted using a shared secret key. The receiver decrypts it using the same shared key. These ciphers consist of Substitution and Transposition ciphers.

Sofyane Ladgham Chikouche, Noureddine Chikouche[1],has proposed an improved method based on the combination of the Pseudo-random LSB (Bit Substitution Technique) and the cryptographic algorithm. There comparsion was approach in terms of histogram of the original image and the image-stego and the percentage of change between the original image and the stego-image.The publication [1] is in October, 2017 and 5th International Conference on Electrical Engineering- Boumerdes (ICEE-B). The advantage of [1] is the picture quality of cover-image is hardly affected hiding capacity is good, and it is very simple in implementation. The disadvantage of [1] is robustness is less the hidden data is subject to alternation due image manipulation.

Advance Encryption Technique using Color Code Based Substitution with Multiple Language Support[2], has proposed System has proposed advance cryptographic technique with Multi-language support which consist of various techniques that are clubbed together to develop the system. The system uses play color cipher to encrypt and decrypt the plain text. The color code substitution will be used for encryption and decryption of the data using the algorithm play color cipher.The translator is used to convert Hindi language into English language. The publication [2] is in June,2017. The advantage [2] is To increase the security of the data and making it more robust, asymmetric encryption technique is used on the data for multiple language. The disadvantage [2] is the block size of encrypted image is fixed.

AES Cryptography in Color Image Steganography By Genetic Algorithms [3],has proposed work incorporates the AES cryptography algorithm, to improve the hidden data security in two methodologies for steganography:- genetic algorithm and path relinking. This [3] Paper published in October,2015. The advantage [3] is once a picture is transformed into mathematical representation it can be shuffled anyway you like until you have the right key to decrypt it. The disadvantage [3] is if the size of the original file is already known or estimated then that could be a potential threat to the excess of the memory that it would show in its properties.

Chapter 4

Proposed System

System has proposed advance cryptographic technique with Multi language support which consist of various techniques that are clubbed together to develop the system. The system proposed uses play color cipher to encrypt and decrypt the plain text. The key which is the backbone of any cryptographic technique is symmetric for PCC. In order to make this more robust, the key is encrypted using RSA algorithm which is an asymmetric cryptography technique. The google translator is used to ensure Multilanguage support. RSA algorithm has been used to encrypt and decrypt the message into the plain text.

Implementation for Text

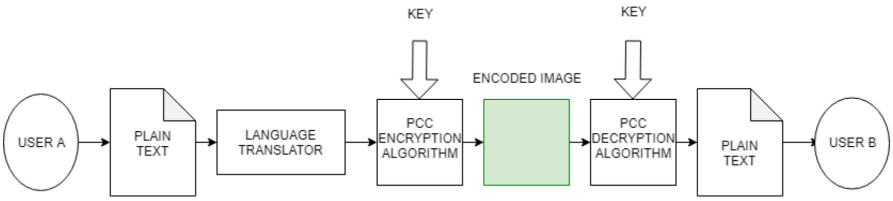


Figure 4.1: Process Of Text

- User A: In this figure 3.1,the user A is a sender which used to send the plain text to user B.
- Plain text: Plain text usually refers to data that is transmitted or stored unencrypted.The process of transforming cipher text back into plain text.
- Language Translator: Translation is the communication of the meaning of a source-language text by means of an equivalent target-language text. Translate text from one language to another.
- PCC Encryption:The algorithm of substitution is based on Play Color Cipher. This is a symmetrical system which is implemented by encryption of text by converting it into colors. Each character of the plain text is encrypted into a block of color. To produce the original text inverse process is used using color block.

- Key: A Key is a piece of information that determines the output of a cryptographic algorithm.A key specifies the transformation of plain text into cipher text.
- Encoded image: A picture can be encrypted in the same way that text is encrypted by software.
- PCC Decryption: The Block of colors are decrypted into Plain text to transmit to the user B. Each block of color is converting into plain text.
- User B: The user B is a receiver which used to receives original plain text.

Working

The working of the proposed concept is the input given by the user is rst determined whether its in English or not. If the language is used for encryption is determined to be in English, RSA algorithm is applied. One color channel from RGB is chosen. The next step is that the block size for encryption in Play Color Cipher(PCC) is chosen. The play color cipher algorithm is applied on this to obtain the cipher text. This cipher text is then sent to the receiver side thus completing encryption.

Implementation for Image

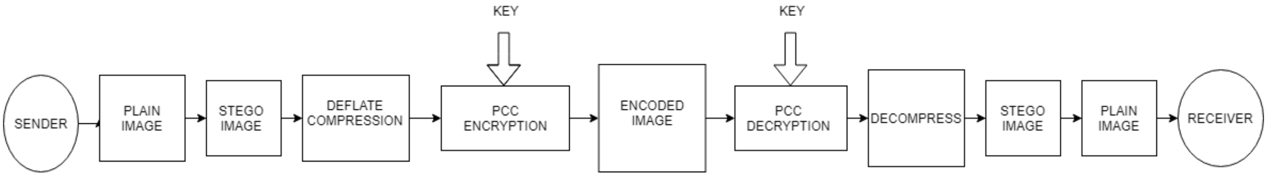


Figure 4.2: Process Of Image

- Sender: The Sender sends the original image to receiver in a secure way.
- Plain image: Plain image usually refers to image data that is transmitted or stored unencrypted.The process of transforming cipher image back into plain image.
- Stego Image: Stego image contain the hidden message in pixel values.Stego image is the output of the embedding process.
- Deflate Compression: In computing, Deflate compression is a loss-less data compression algorithm and associated with file format.
- PCC Encryption:The algorithm of substitution is based on Play Color Cipher. This is a symmetrical system which is implemented by encryption of image by converting it into colors. Each character of the plain text is encrypted into a block of color. To produce the original text inverse process is used using color block.
- Key: A Key is a piece of information that determines the output of a cryptographic algorithm. A key specifies the transformation of plain image into cipher image.

- Encoded image: A picture can be encrypted in the same way that text is encrypted by software.
- PCC Decryption: The Block of colors are decrypted into Plain image to transmit to the receiver. Each block of color is converting into plain image.
- Receiver: The Receiver receives the original image which has been send by sender.

Working

The working for image is the input given by the user will be in plain image form then that image message will be encrypted in stego-image using the deflate algorithm conversion. The encryption will be done by the Play Color Cipher(PCC) encryption key and then at sender side using same key, it will be decrypted.

4.1 Methodologies

4.1.1 RSA Algorithm

RSA is an algorithm used to encrypt and decrypt the messages.It is an asymmetric cryptographic algorithm.Asymmetric means that there are two different keys.RSA involves a public key and private key.The public key can be known to everyone; that helps to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.

Algorithm

- A basic principle behind RSA is the observation that it is practical to find three very large positive integers e, d and n such that with modular exponentiation for all integers m and that even knowing e and n or even m it can be extremely difficult to find d.
  $m^{e^(d)}$ $\equiv$m (mod n)
- In addition, for some operations it is convenient that the order of the two exponentiation can be changed and that this relation also implies:
  $m^{d^(e)}$ $\equiv$m (mod n)

4.1.2 Deflate Play Color Cipher

Algorithm

- To generate the key table, one would first fill in the spaces in the table with the letters of the keyword.
- Then fill the remaining spaces with the rest of the letters of the alphabet.
- The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center.

- The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

4.2 Resource Requirements

4.2.1 Hardware Requirement

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as Hardware.

- Processor: Intel(R) Core(TM) i7-7500U CPU @ 2.70 GHZ 2.90 GHZ.
- RAM: 16.0 GB.
- Hard Disk: 8 GB.

4.2.2 Software Requirement

Software Requirement is a field within software engineering that deals with establishing the needs of stakeholders that are to be solved by software. The Software Requirements are description of features and functionalities of the target system. Requirements convey the expectations of the users from the software product.

- Operating System: Windows 10
- Environment: Visual Studio
- Language: C
- Back End: SQL Server

Chapter 5

Detailed Life Cycle Of The Project

5.1 Class Diagram

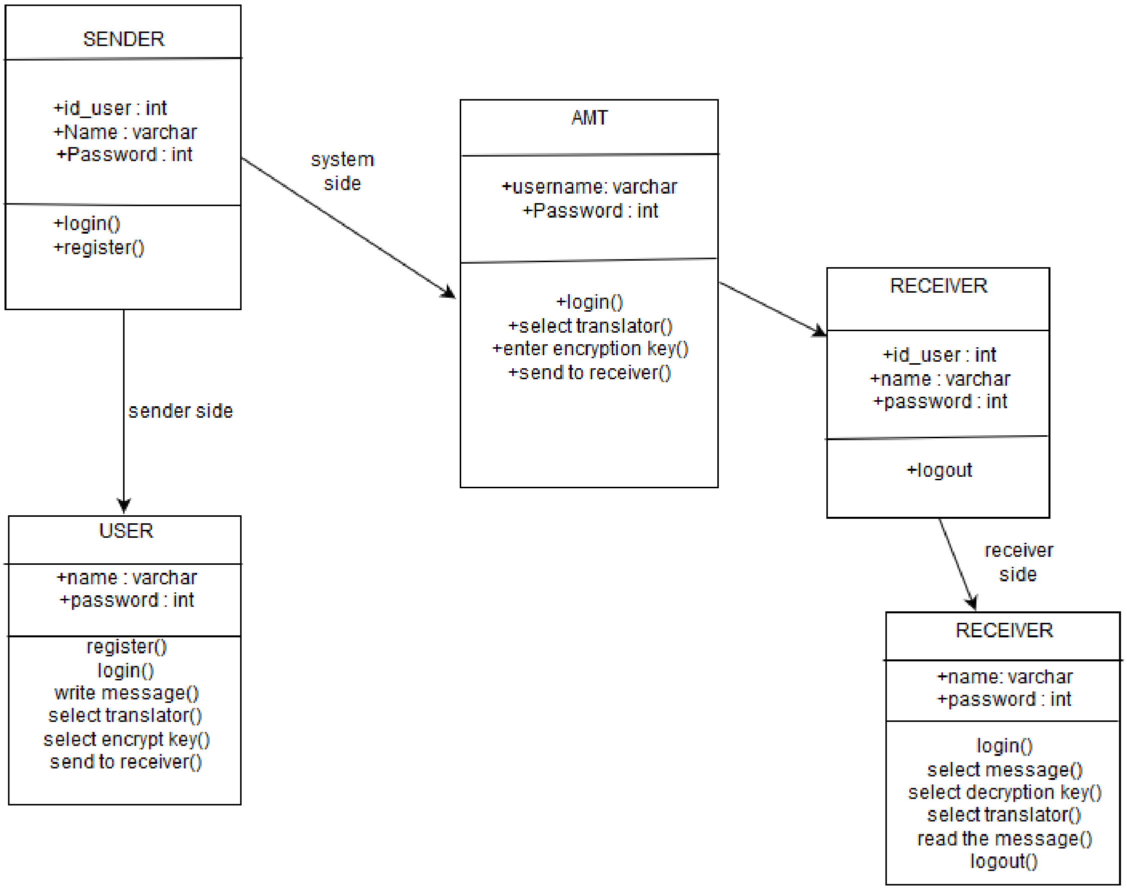


Figure 5.1: Class Diagram

5.2 Entity Relationship Diagram

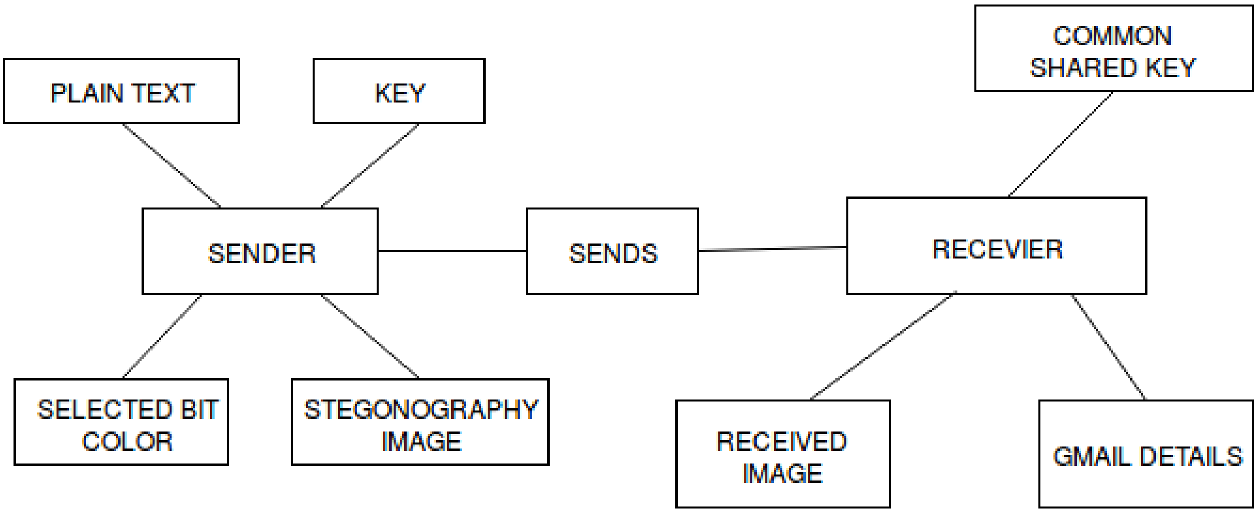


Figure 5.2: ERD

5.3 Data Flow Diagram

DFD LEVEL 0

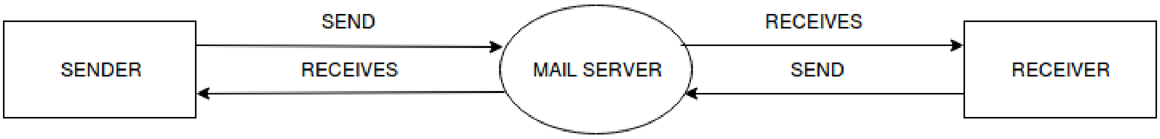


Figure 5.3: DFD Level 0

DFD LEVEL 1

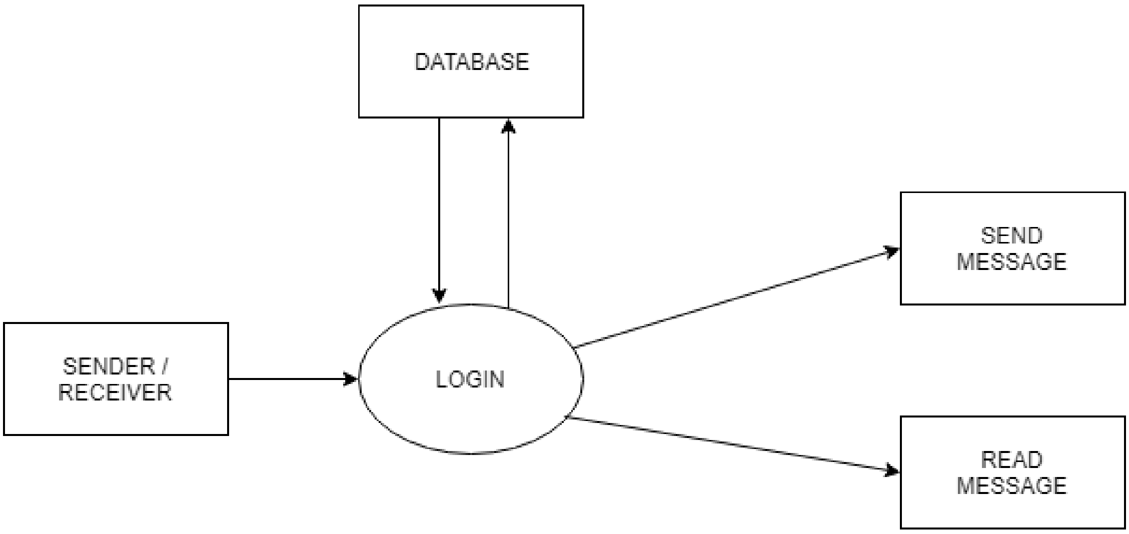


Figure 5.4: DFD Level 1

DFD LEVEL 2

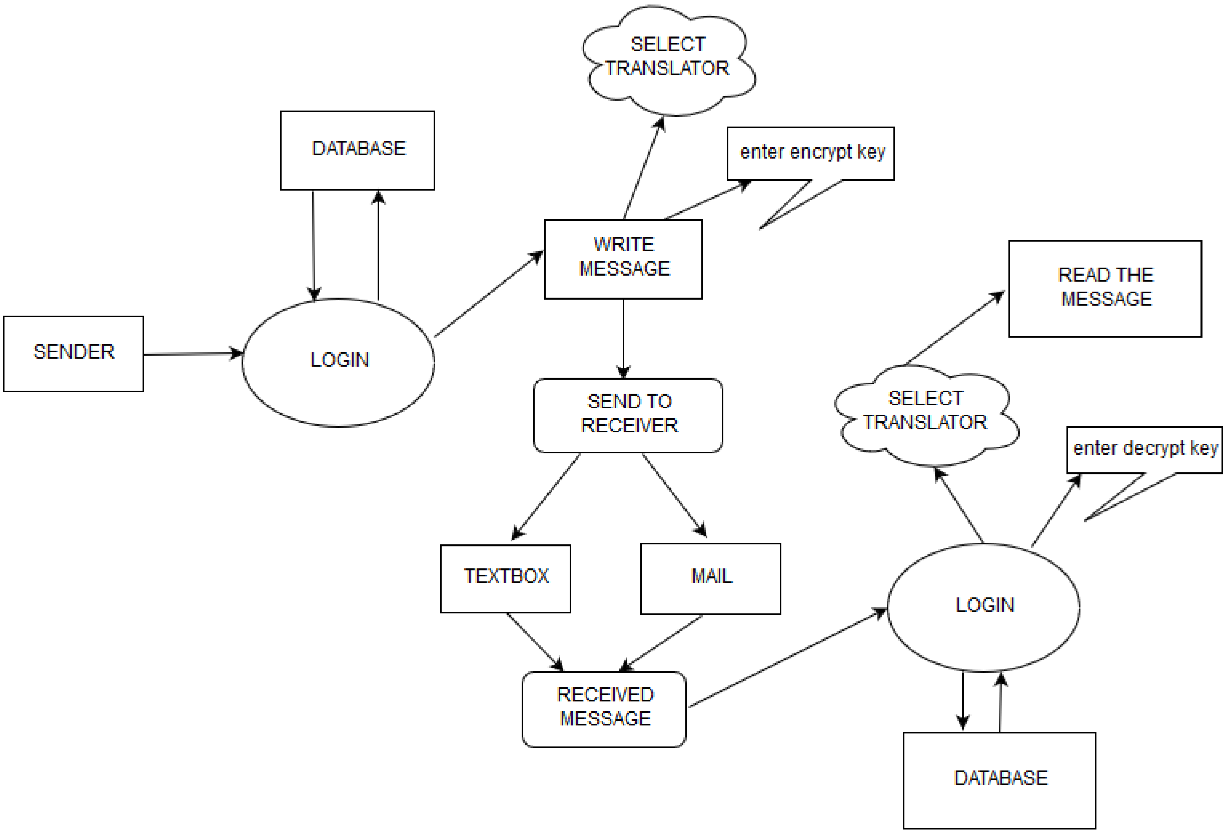


Figure 5.5: DFD Level 2

5.4 Usecase Diagram

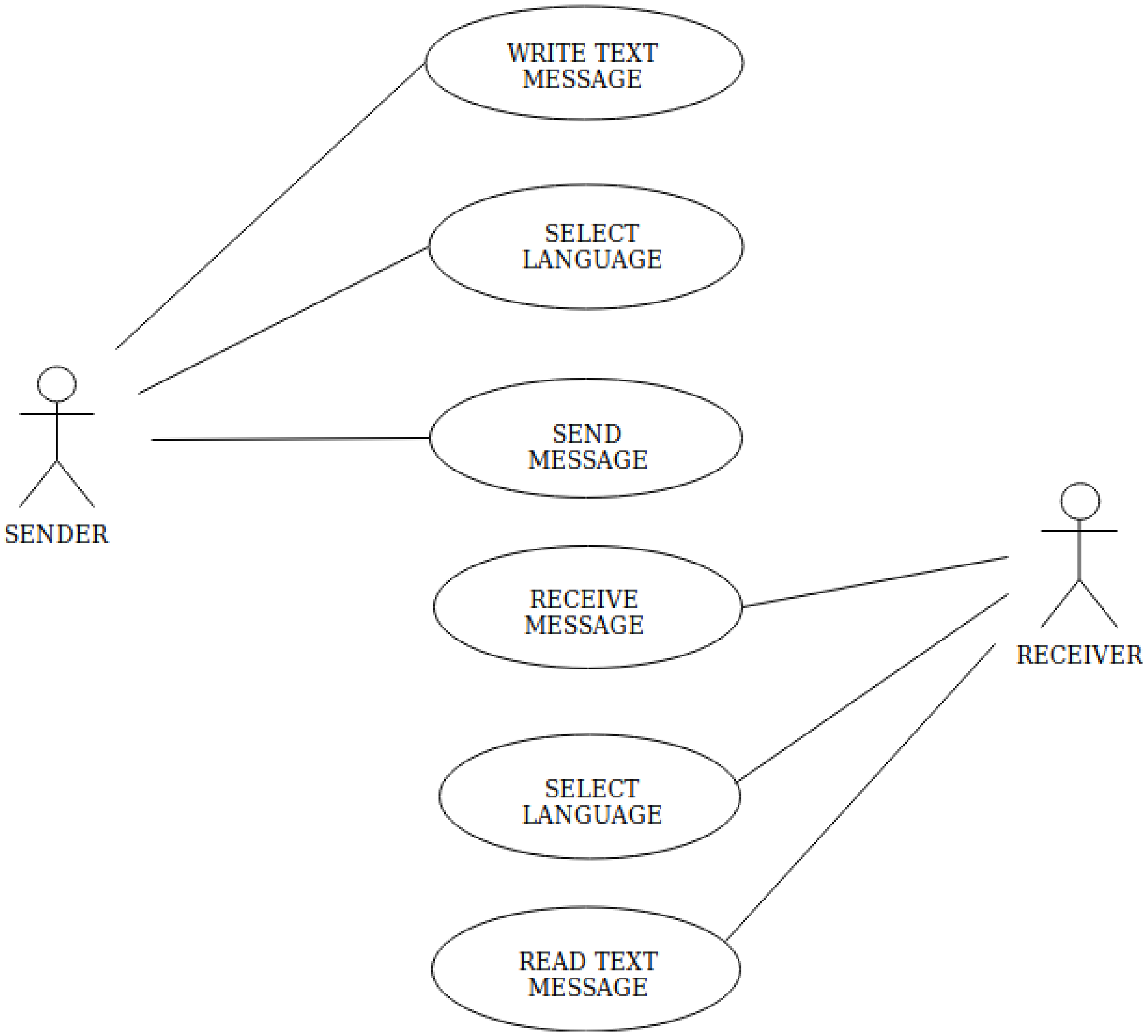


Figure 5.6: Usecase Diagram For Text

5.5 Activity Diagram

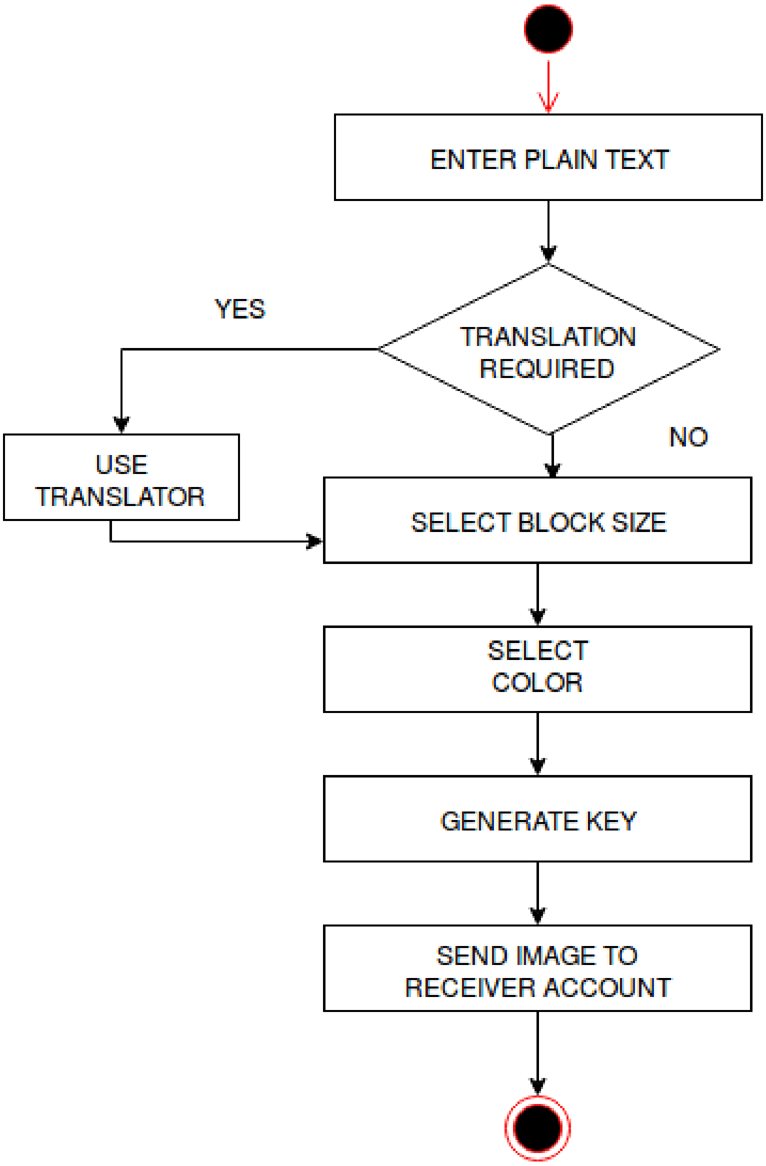


Figure 5.7: Activity Diagram for Sender

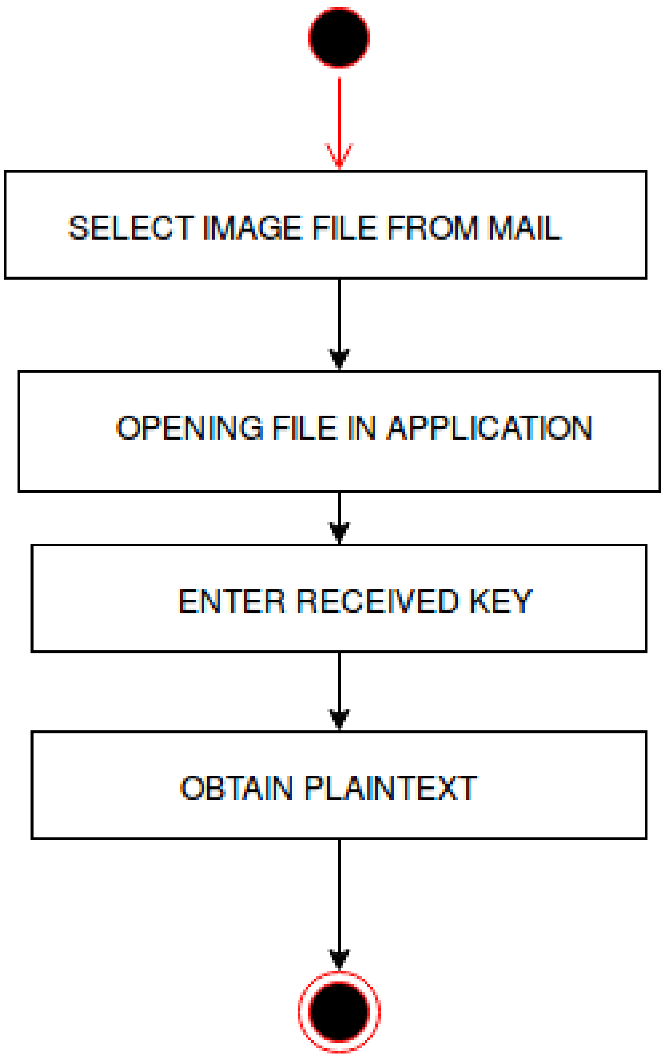


Figure 5.8: Activity Diagram for Receiver

5.6 Sequence Diagram

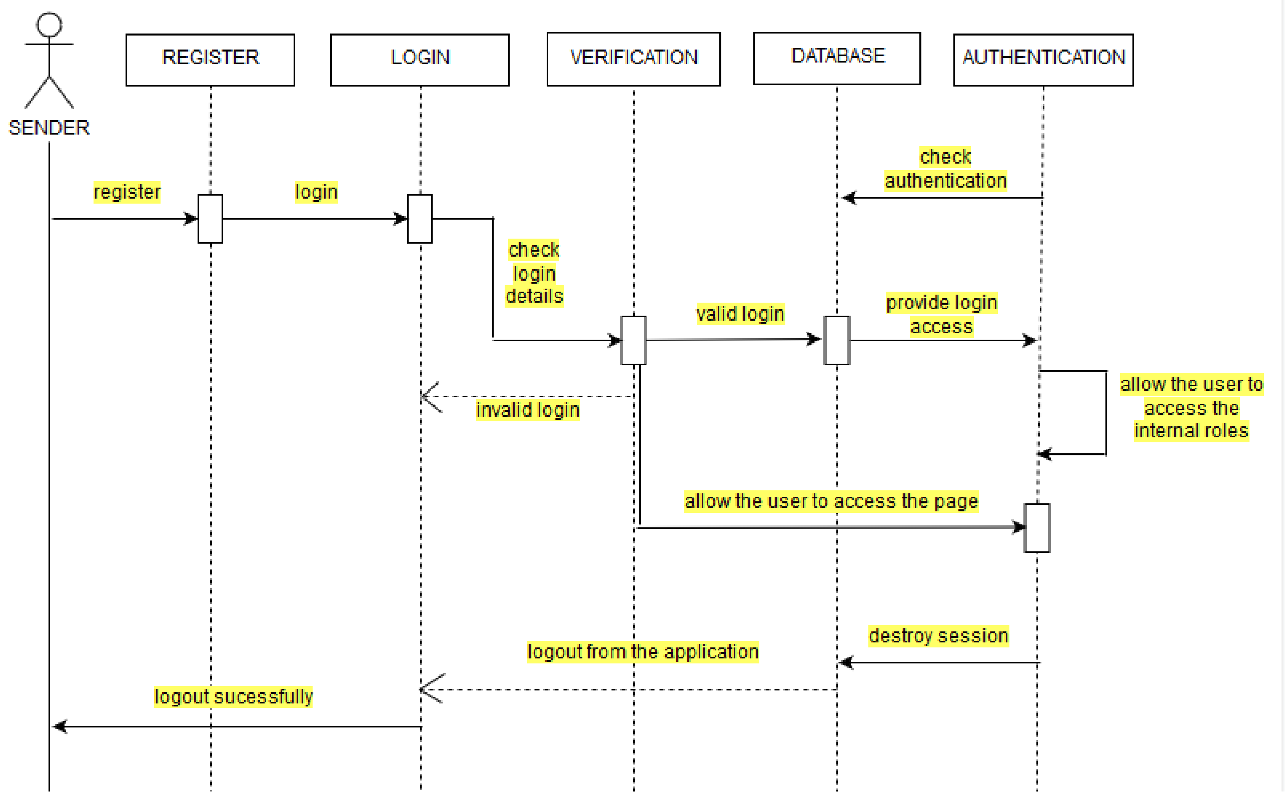


Figure 5.9: Sequence Diagram

Chapter 6

System Work Flow

Design At sender side:

- Accept the input text/image from the user.
- If the input is in the hindi, english, use the google translator.
- Apply RSA algorithm which generates Asymmetric key on the input data.
- Cipher text obtained from asymmetric algorithm.
- Separate the intermediate cipher text into individual characters.
- Input the color-channel (R/G/B) and a color (RGB value).
- The picture box is divided into a grid of blocks, each of size n, where n is the variable block size.
- Add the ASCII value of every character with its position and put the value in the color channel selected.
- For the remaining 2 channels, put the value of the Color input by the user.
- Draw the bitmap image.
- Send the image to the receiver.

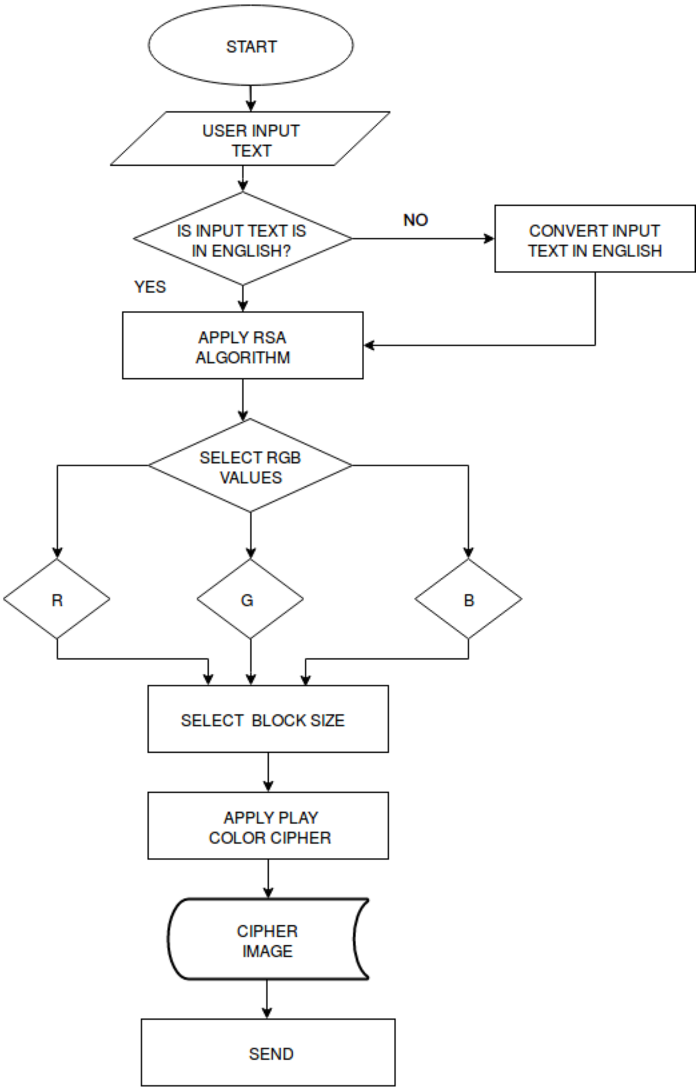


Figure 6.1: Sender side

Working of Sender side

Above Figure describes the working of the proposed concept. The input given by the user is first determined whether its in English or not. If the language is used for encryption is determined to be in English, RSA algorithm is applied. One color channel from RGB is chosen. The next step is that the block size for encryption in PCC is chosen. The play color cipher algorithm is applied on this to obtain the cipher image. This cipher image is then sent to the receiver side thus completing encryption.

Design At Receiver side:

- From each block, the pixel value of the central pixel is extracted and then converted to a character. This is done for all blocks and the corresponding characters are extracted.
- The block size and the color channel are extracted from the key.
- Convert the resulting value into character and get the text.
- Decrypt the text using the decryption process of the standard encryption algorithm used.
- Thus the message is retrieved after applying Key on the encrypted data.
- Get the original text back, using translator.

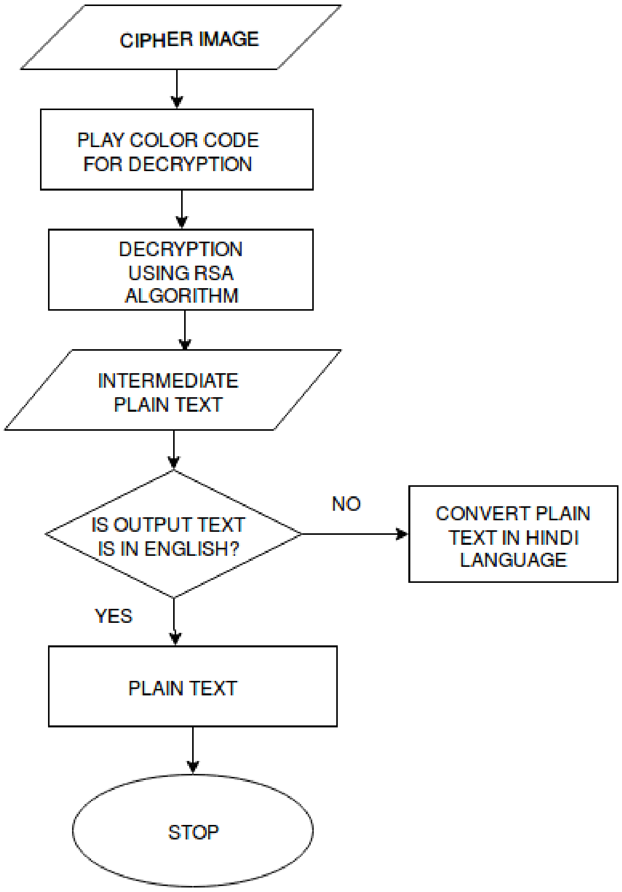

CIPHER IMAGE
PLAY COLOR CODE FOR DECRYPTION
DECRYPTION USING RSA ALGORITHM
INTERMEDIATE PLAIN TEXT
IS OUTPUT TEXT IS IN ENGLISH?
NO
CONVERT PLAIN TEXT IN HINDI LANGUAGE
YES
PLAIN TEXT
STOP

Figure 6.2: Receiver side

Working of Receiver side

In above Figure the play color cipher algorithm for decryption is applied on the cipher image obtained after encryption. The next step is to apply the RSA algorithm. The intermediate plain text is thus obtained. If this is needed in the English language then it is sent forth, otherwise translated and then sent as the plain text needed.

Chapter 7

Testing

Software testing is the process of executing a program or application with the intention to find out the software bugs or errors to eradicate or remove them before releasing the software. It can also be stated as validating and verifying the system for proper functioning which meets the business ans technical requirements, works as expected.

Why testing is necessary ?

The system or software development is manual work. Hence during the software development specifications, source code and test documents are written by human beings. Any human can make an errors regardless of how they have experienced or skilled. So a number of faults in system are expected. It is not possible for any particular person to understand every aspect of program or software because of complexity to develop many of the computer systems. The developed system can be validated and verified to check whether it is working according to specified requirements or not testing and test cases. As the number of defects increases; the quality of developed software decreases. While developing the software system it is important to minimize the number of defects.

White Box Testing:

White Box Testing is a software testing method in which the internal structure or design or implementation of the item being tested is known to the tester. The tester chooses inputs to exercise paths through the code and determines the appropriate outputs. Programming know-how and the implementation knowledge is essential. The White Box Testing usually done by developers. All the developer checks program or code, whether their code contain an error or not before releasing the application to markets.

Security Testing:

Security Testing is defined as a type of Software Testing that ensures software systems and applications are free from any vulnerabilities, threats, risks that may cause a big loss. Security testing of any system is about finding all possible loopholes and weaknesses of the system which might result into a loss of information.

The goal of security testing is to identify the threats in the system, so the system does not stop functioning or is exploited. It also helps in detecting all possible security risks in the system and help developers in fixing these problems through coding.

Security Testing Roles:

- Hackers - Access computer system or network without authorization.
- Crackers - Break into the systems to steal or destroy data.
- Ethical Hacker - Performs most of the breaking activities but with permission from the owner.

Chapter 8

System Maintenance

Web Application requires maintenance because there are some residual errors remaining in the system that must be removed as they are discovered. In Maintenance we will be doing the following:

- Fixing bugs if at all anything found during actual working.
- Any minor changes that is required when the client working with it will be done.
- Periodic checking of application at regular intervals.
- Make better use of existing tools and techniques.

Chapter 9

Result

- The main page of the system is seen where all the options provided by the system is displayed. The user can choose any option based on his choice.

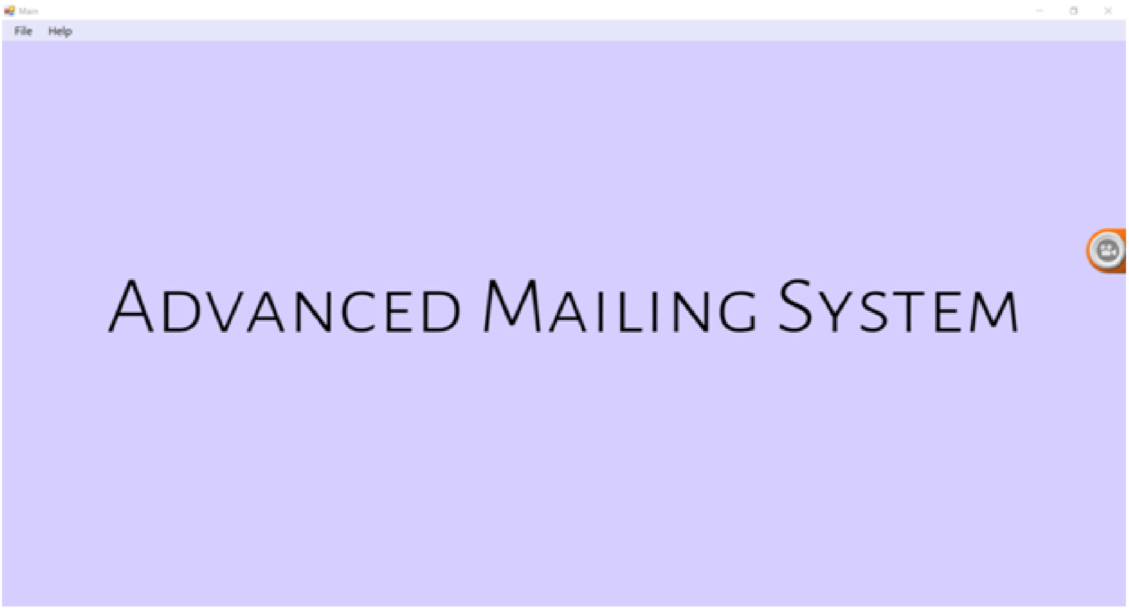
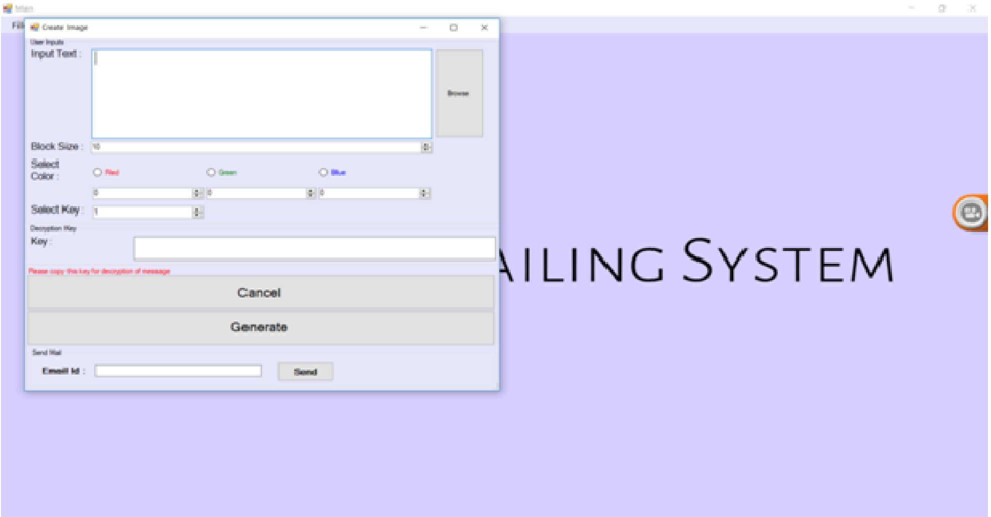


Figure 9.1: Main Page

- The encryption window is displayed; where the input text can be entered by the user in order to encrypt it.



Input Text :

Block Size : 10

Select Color : ○ Red ○ Green ○ Blue

0 0 0

Select Key : 1

Key :

Please copy this key for decryption of message

Email Id :

Figure 9.2: Encryption window

- The cipher image is obtained which is majorly in the shade of red. This is due to the color channel selected is red.

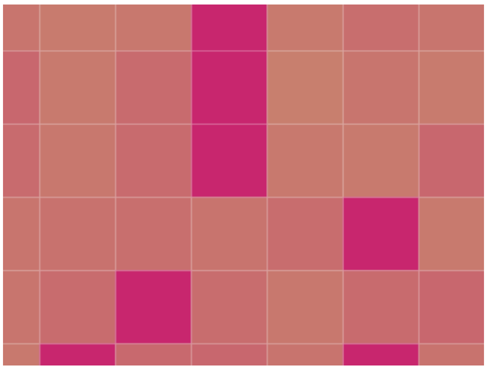


Figure 9.3: Cipher Image

- The decryption window can be seen where the receiver can obtain the original data sent to him by using the cipher image and the key sent by the sender.

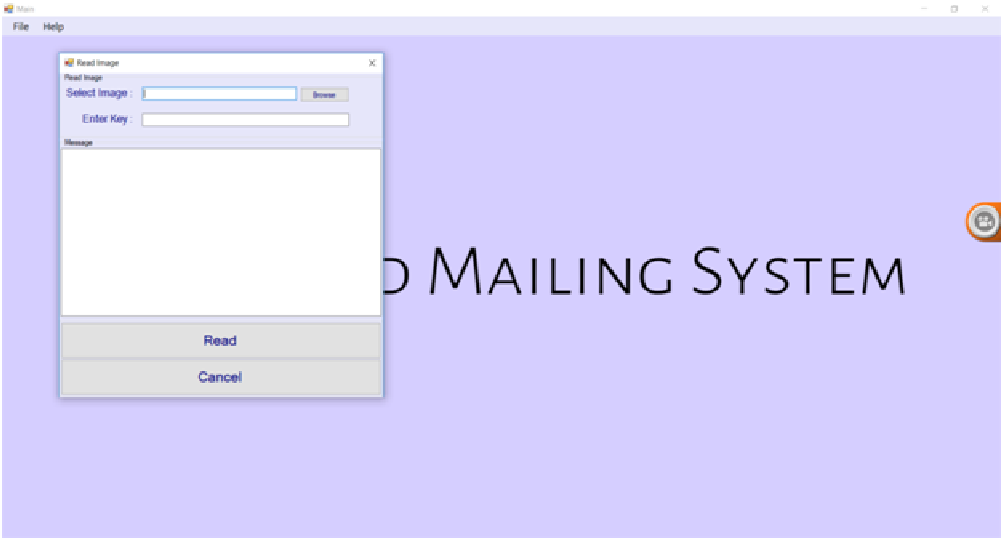
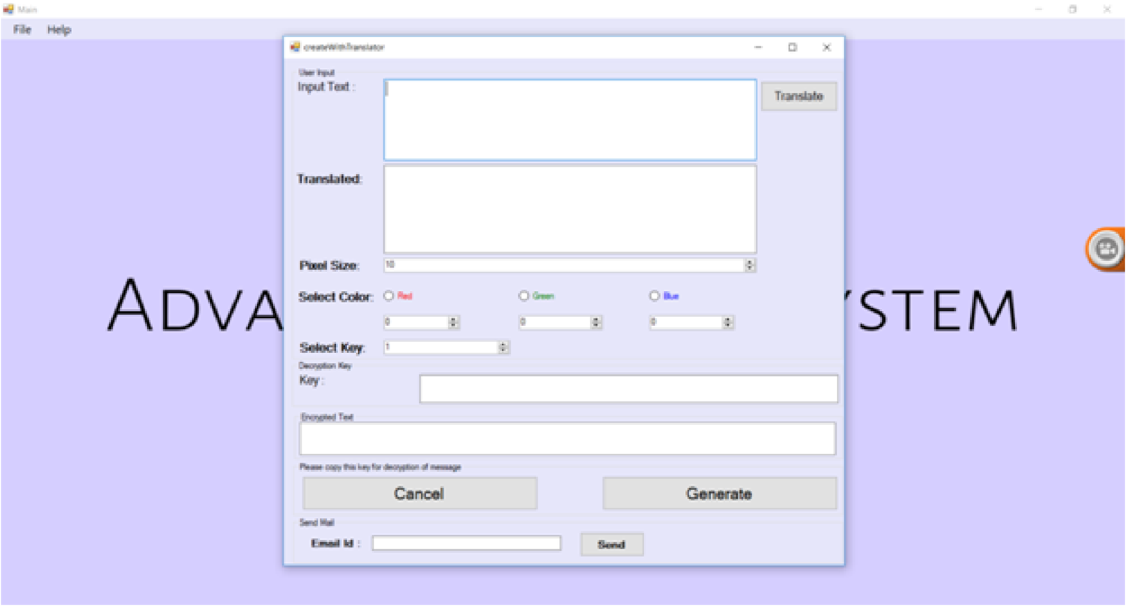


Figure 9.4: Decryption window

- Encryption using a translator is displayed. Here the sender can send data which is originally in Hindi by using a translator. The translated data is then encrypted.



Input Text :

Translated:

Pixel Size: 10

Select Color: ○ Red ○ Green ○ Blue

0 0 0

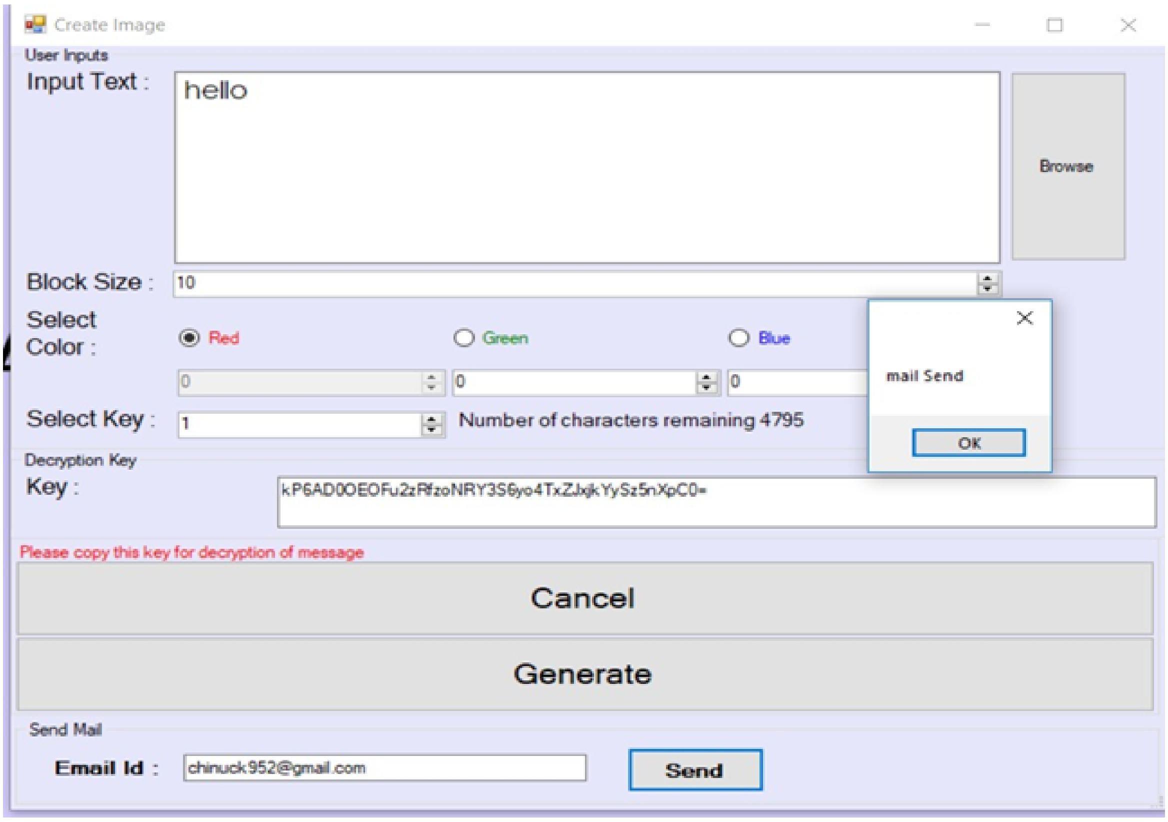
Select Key: 1

Key :

Email Id :

Figure 9.5: Encryption Using Translator

- The automated mail generation shows that once the cipher image is generated, it can be sent to receiver via email.



Create Image

User Inputs

Input Text : hello

Block Size : 10

Select Color : ● Red ○ Green ○ Blue

0 0 0

Select Key : 1 Number of characters remaining 4795

mail Send

Decryption Key

Key : kP6AD0OEOFu2zRfzoNRY3S6yo4TxZJxjkYySz5nXpC0=

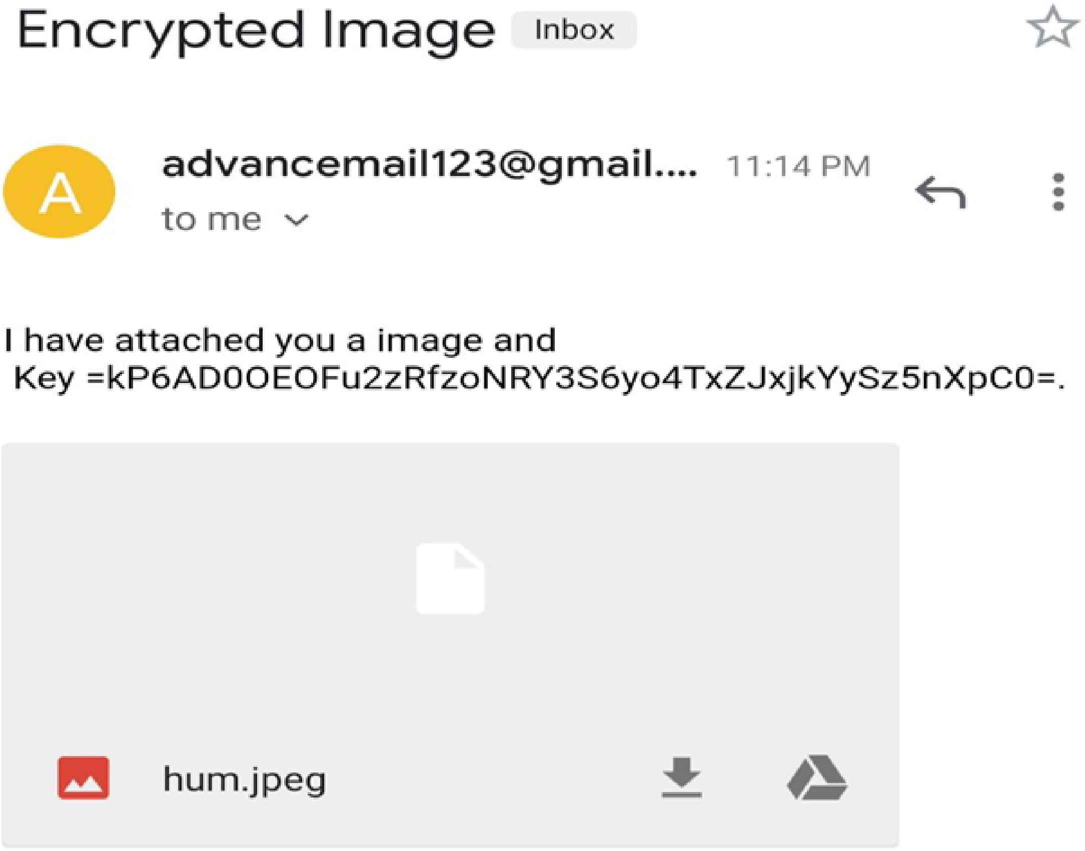
Please copy this key for decryption of message

Send Mail

Email Id : chinuck952@gmail.com

Figure 9.6: Automated Email Generation

- The mail of the receiver is seen. The receiver obtains the cipher image and the key used for decryption.



Encrypted Image

advancemail123@gmail.... 11:14 PM

to me

I have attached you a image and
Key =kP6AD0OE0Fu2zRfzoNRY3S6yo4TxZJxjkYySz5nXpC0=.

hum.jpeg

Figure 9.7: Receiver Side Email

- The receiver side decryption is seen where the data is obtained using the cipher image and the encrypted text and the key used for decryption.

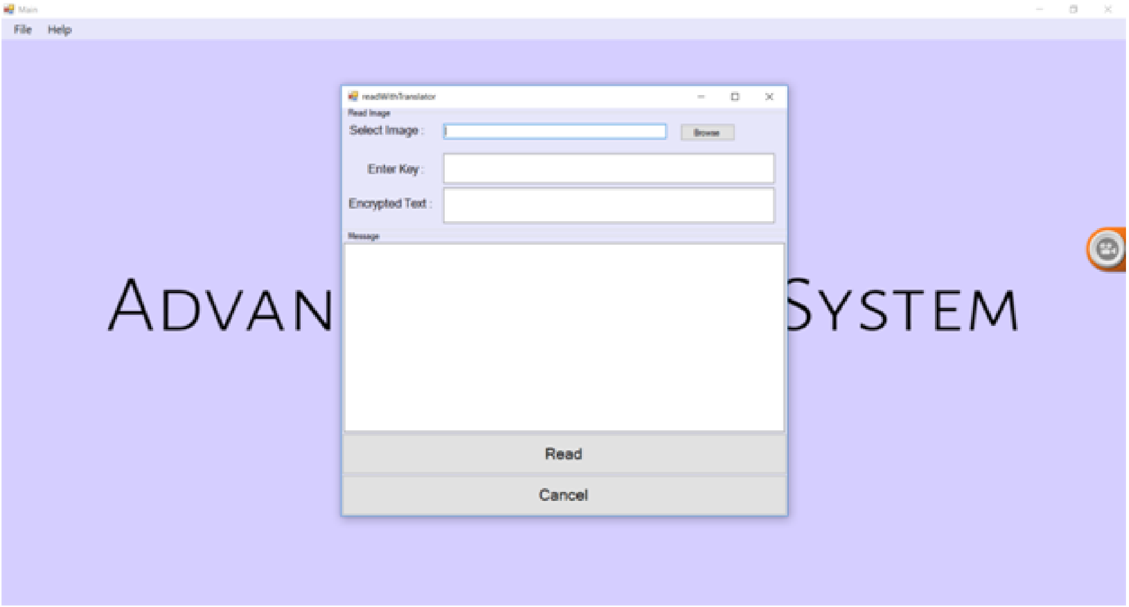
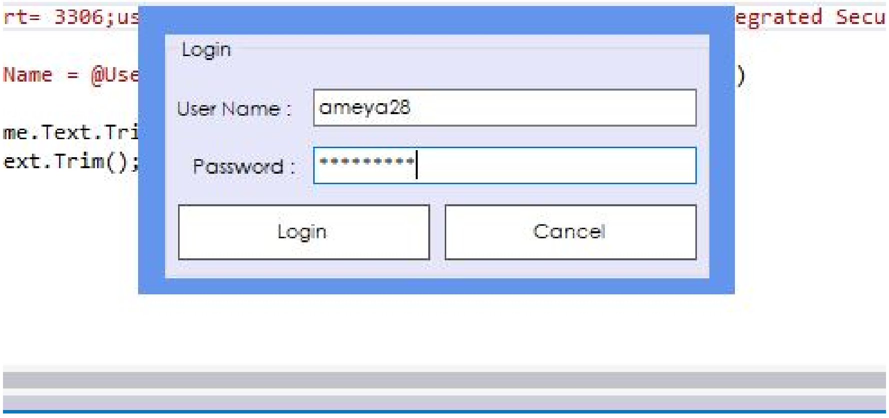


Figure 9.8: Receiver Side Decryption

- Here the user will enter their own Username and password which has been created.



```
rt= 3306;us                                        egrated Secu

Name = @Use                                        )

me.Text.Tri
ext.Trim();
```

Login

User Name : ameya28

Password : *********

Figure 9.9: Login Page

Chapter 10

Conclusion

The system carries out the cryptanalysis in such a way that it will show that 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 this system, implementation of encryption-decryption scheme is done using symmetric and asymmetric techniques for securing the transmission of data for multiple language support using variable block. The data which is encrypted uses color blocks for encryption instead of normal substitution of characters.

Steganography technique is the combination of RSA and Deflate Play Color Cipher Algorithm. The various image sizes are considered and secret information of different sizes are also considered.The framework provides an effective way to select output image to accommodate the secret information. The receiver needs to have a secret key which will be used to decode the secret message.

In future, the figures, tables, pictures, and so forth can be incorporated into the plain text for transformation and consequently the extent of the calculation can be expanded. To create a stronger cipher text the quantity of parameters (such as alpha, gamma adjustment and so on.) can be expanded for producing the color to get 18 decillions of color combinations.

Bibliography

[1] Sofyane Ladgham Chikouche, Noureddine Chikouche, An improved LSB Image Steganography using AES algorithm,October 29-31-2017 ,Boumerderdes, Algeria. University of algeria.

[2] https://pdfs.semanticscholar.org/2701/ce0d5762a8a22711b64de188ac93ef29866e.pdf

[3] AES Cryptography in Color Image Steganography By Genetic Algorithms(October,2015.)

[4] :http://crypto.com/downloads/numtheory-crypto.pdf., last accessed on 25/09/2015.

[5] Advance encryption technique using RSA algorithm (september 2017, university of mumbai).

[6] Amritpal Singh, An Improved LSB based Image Steganography Technique for RGB Images, Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on . IEEE, 2015

[7] Jharna Chopra, and Sampada K. Satav, Impact of Encryption Technique Classification Algorithm for preservation of data,published in International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 10, October 2013

Appendices

Appendix-A: Visual Studio Download and Install

1. Check the system requirements. These requirements help you know whether your computer supports Visual Studio 2017.

2. Apply the latest Windows updates. These updates ensure that your computer has both the latest security updates and the required system components for Visual Studio.

3.Reboot. The reboot ensures that any pending installs or updates don't hinder the Visual Studio install.

4. Free up space. Remove unneeded files and applications from your "SystemDrive" by, for example, running the Disk Cleanup app.

5. **Download Visual Studio:** Next, download the Visual Studio bootstrapper file. To do so, choose the following button, select the edition of Visual Studio 2017 that you want, choose Save, and then choose Open folder.

6. **Install the Visual Studio installer:**Then, run the bootstrapper file to install the Visual Studio Installer. This new lightweight installer includes everything you need to both install and customize Visual Studio 2017.

7. **Select workload:** After the installer is installed, you can use it to customize your installation by selecting the feature setsor workloadsthat you want. Here's how. * Find the workload you want in the Installing Visual Studio screen. * After you select the workload(s) you want, choose Install.Next, status screens appear that show the progress of your Visual Studio installation. * After the new workloads and components are installed, choose Launch.

8. **Select individual components:**If you don't want to use the Workloads feature to customize your Visual Studio installation, you can do so by installing individual components instead. To select individual components, choose the Individual components option from the Visual Studio Installer

9. **Install language packs:** By default, the installer program tries to match the language of the operating system when it runs for the first time. To install Visual Studio 2017 in a language of your choosing, choose the Language packs option from the Visual Studio .

Publication

Paper entitled **“Color Code Substitution Based Advance Mailing Technique”** is presented at **“International Conference on Recent Advances in Communication, Computing and Informatics”(ICRACCI)** by **“Chinmay Karangutkar”,”Ankita Gound”,”Ameya Murkute”,”Prapti Nevrekar”.**