A Project Report

on

A Methodology Based on
Steganography and
Cryptography to Protect
Highly Secure Messages

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

Bachelor of Technology in Computer Science and
Engineering

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Under The Supervision of
Ms. Kiran Singh
Assistant Professor
Department of Computer Science and Engineering

Submitted By

18SCSE1010286 - DEEPAK SAHU
18SCSE1010374 -DIVYANKAR SHARMA

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND

ENGINEERING GALGOTIAS UNIVERSITY, GREATER

NOIDA, INDIA DECEMBER - 2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the project, entitled **"A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages "** in partial fulfillment of the requirements for the award of the **BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING**

submitted in the **School of Computing Science and Engineering** of Galgotias University, Greater Noida, is an original work carried out during the period of **JULY-2021 to DECEMBER-2021**, under the supervision of **Ms. Kiran Singh, Assistant Professor**, **Department of Computer Science and Engineering** of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the project has not been submitted by me/us for the award of any other degree of this or any other places.

18SCSE1010286 - DEEPAK SAHU
18SCSE1010374 - DIVYANKAR SHARMA

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor

(Ms. Kiran Singh, Assistant Professor)

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of **18SCSE1010286 - DEEPAK SAHU, 18SCSE1010374 - DIVYANKAR SHARMA** has been held on _____ and his/her work is recommended for the award of **BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING**.

Signature of Examiner(s)   **Signature of Supervisor(s)**

Signature of Project Coordinator   **Signature of Dean**

Date:

Place:

ABSTRACT

Maintaining secrecy is very important in a large corporation and because of the intelligent of the hackers it becomes tedious. Already we have cryptography for transmitting secret information. Even though cryptography successfully transmitting secret information, it will give a suspicion to the hackers and it affects unintended users.

Our project, ''A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages'' overcomes this factor and it gives a solution for transmitting secret formation with out affecting unintended users. Stegano graphy uses multimedia data as a covering medium (Covering secret information). By using steganography data (secret information) can hided with in data (multimedia data, here multimedia data is an image) and it can be sent anywhere to transfer the message easily without giving any suspicion to others.

Table of Contents

List of Figures

CHAPTER-1

Introduction

This project combines the art of steganography with cryptology. It encodes a message and then,hides it in a file. This makes the message unreadable even after it is disclosed. By this way we can conceal our information. This project hides text files inside jpg files and creates a jpg file with secret message. A key should be given by the user to encode the message. The message is first encoded with this key and then embedded inside the specified file. It is then stored as per the name specified.

To reveal the message that is inside a file, one should give the right key and then this key will decrypt the message and then the embedded message is extracted out for viewing. If an attempt is made with a wrong key, a warning is made to tell that that key is invalid. By this method we hide our secret message from invalid users.

Several options are provided for the users so that they work in a modish environment. Users are provided with a facility to locate the files on the system through browsing. The image files can be viewed on the display panel and we could select one. Information about jpg as well as bmp files could be retrieved.

The working of the system is very simple but powerful. It uses bit shift method to encrypt. The encrypted message is then embedded inside the specified jpg file bit by bit after hard manipulations. The key is used to do this crypting works. The characters in the key are converted into binary strings and they are manipulated against the binary streams that are obtained from the individual characters of the secret message.

Since the key is used to encrypt and embed it would be hard to reveal a secret message that is embedded inside the picture.

Chapter 2

Literature Survey/Project Design

In this section we are discussing about the research paper that has been done on steganography in last previous years.Steganography is the most encouraging field in which people want to research on it.A literature goes beyond the tracking for information or knowledge
Steganography is a technique used for hiding data in an ordinary file and to decrease the suspicion and send the necessary information to the right person. We are using this technique from so many decades[1][8]

.In 2013 Akhtar, N.; Johri, P.; Khan, S., [21] performed an different approach on LSB (Least Significant Bit) algorithm. With the help of bit inversion technique the stego image quality has been improved. With LSB method improving the PSNR of stegoimage. By stroing the bit pattern in which LBSs are reversed the image can get correctly.

Ki-Hyun Jung et al. [22] in 2014, proposed steganography method for hiding secret data in order to provide high level data such as video or an image.Therefore,the reversible data hiding method can extract information to cover image inplace from a stego image without any intorsion after getting the hidden data.

In 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. [23] examined on Medical records that are extremely responsive patient information as multi secured medical image based on steganography scheme is proposed. This technique gives an adequate and storage security process for the security of digital medical images. Researcher gives a feasible steganography method with the help of Integer Wavelet Transform to secure the MRI medical image and convert into a single container image. The diagnosis image of that patient takes as a secret image and Arnold transform had executed and clambered secret image had obtained. In this case, the confused secret image was placed into the dope container image and Inverse IWT had applied to get a dope secret image. In this research we have observed that the quality parameters are increased with acceptable PSNR and compare with the existing algorithms.

After reading all the papers I m trying steganography technique for color RGB images to improve the security level of data transfer .24 bit RGB image is utilized as cover image to embed secret data in red ,green and blue pixels using the Least Significant Technique .

Chapter 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In the existing system, secret messages can be transferred but it gives irritation to the unintended people. And also maintaining secrecy is very tough because of the intelligent of the hackers. Already we have crypto graphy for transmitting secret information. Even though crypto graphy successfully transmitting secret information, it will give a suspicion to the hackers and it affects unintended users.

3.2 PROPOSED SYSTEM

Our project, **DIGITAL STEGANO GRAPHY** overcomes this factor and it gives a solution for transmitting secret formation with out affecting unintended users. Stegano graphy uses multimedia data as a covering medium (Covering secret information). By using stegano graphy data (secret information) can hided with in data (multimedia data, here multimedia data is an image) and it can be sent anywhere to transfer the message easily without giving any suspicion to others.

Features of proposed system:
1　Provides a user friendlier interface.
2　Developed in java. So platform independent.
3　Highly flexible.

Chapter 4

SYSTEM IMPLEMENTATION

4.1 HARDWARE REQUIREMENT

- ➢ Processor: Pentium IV
- ➢ 40 GB hard disk space.
- ➢ 256 MB RAM or more.
- ➢ 1.44 Floppy Disk Drive.
- ➢ 104 keys keyboard.
- ➢ Display capable of showing 65,000 colors or more.
- ➢ CD-ROM Drive for installing the package.
- ➢ Mouse with minimum two buttons.

4.2 SOFTWARE REQUIREMENT

- ➢ Front End: Java (jdk1.4.1 and above)
- ➢ OS   :   Windows / Linux / Solaris

4.3 SOFTWARE DESCRIPTION

4.3.1 JAVA

Java Features Of Java

The inventors of Java wanted to design a language which could offer solutions to some of the problems encountered in modern programming. They wanted the language to be not only reliable, portable and distributed but also simple, compact and interactive. Sun Microsystems officially describes java with the following attributes.

Compiled and Interpreted

Usually a computer language is either compiled or interpreted. Java combines both these approaches thus making java a two-stage system. First, java compiler translates source code into what is known as byte code instructions. Byte codes are not machine instructions and therefore, in the second stage, java interpreter generates machine code that can be directly executed by the machine that is running the java program. We can thus say that java is both a compiled and interpreted languages.

Platform-Independent and Portable

The most significant contribution of java over other languages is its portability. Java programs can be easily moved from one computer system to another, anywhere and anytime. Changes and upgrades in operating systems, processors and system resources will not force any changes in Java programs. This is the reason why Java has become a popular language for programming on Internet which interconnects different kinds of systems worldwide. We can download a Java applet from a remote computer onto out local system via Internet and execute it locally. This makes the Internet an extension of the user's basic system providing practically unlimited number of accessible applets and applications.

Java ensures portability in two ways. First, Java compiler generates byte code instructions that can be implemented on any machine. Secondly, the sizes of the primitive's data types are machine-independent.

Object-Oriented

Java is a true object-oriented language. Almost everything in Java is an object. All program code and data reside within objects and classes. Java comes with an extensive set of classes, arranged in packages that we can use in our programs by inheritance. The object model in Java is simple and easy to extend.

Robust and Secure

Java is a robust language. It provides many safeguards to ensure reliable code. It has strict compile time and run time checking for data types. It is designed as a garbage-collected language relieving the programmers virtually all memory management problems. Java also incorporates the concept of exception handling which captures series errors and eliminates any risk of crashing the system.

Security becomes an important issue for a language that is used for programming on Internet. Threat of viruses and abuse of resources is everywhere. Java systems not only verify all memory access but also ensure that no viruses are communicated with an applet. The absence of pointer in Java ensures that programs cannot gain access to memory locations without proper authorization.

Distributed

Java is designed as a distributed language for creating applications on networks. It has the ability to share both data and programs. Java applications can open and access remote objects on Internet as easily as they can do in a local system. This enables multiple programmers at multiple remote locations to collaborate and work together on a single project.

Simple, Small and Familiar

Java is a small and simple language. Many features of C and C++ that are either redundant or sources of unreliable code are not part of Java. For example, java does not use pointers, preprocessor header files, go to statement and many others. It also eliminates operators overloading and multiple inheritance.

Familiarity is another striking feature of Java. To make the language look familiar to

the existing programmers, it was modeled on C and C++ languages. Java uses many constructs of C and C++ and therefore, Java code "looks like a C++" code.

Multithreaded and Interactive

Multithreaded means handling multiple tasks simultaneously. Java supports multithreaded programs. This means that we need not wait for the application to finish one task before beginning another. For example, we can listen to an audio clip while scrolling a page and at the same time download an applet from a distant computer. This feature greatly improves the interactive performance of graphical applications.

The Java runtimes comes with tools that support multiprocess synchronization and construct smoothly running interactive systems.

High Performance

Java performance is impressive for an interpreted language, mainly due to the use of intermediate byte code. According to Sun, Java speed is comparable to the native C/C++. Java architecture is also designed to reduce overheads during runtime. Further, the incorporation of multithreading enhances the overall execution speed of java programs.

Dynamic and Extensible

Java is a dynamic language. Java is capable of dynamically linking in new class libraries, methods and objects. Java can also determine the type of class through a query, making it possible to either dynamically link or abort the program, depending on the response.

Java programs support functions written in other languages such as C and C++.

These functions are known as native methods. This facility enables the programmers to use the efficient functions available in these languages. Native methods are linked dynamically at runtime.

4.3.2 SWING - OVERVIEW

The original GUI components from the Abstract Windowing Toolkit package Java.awt (also called the AWT) are tied directly to the local platform's graphical user interface capabilities. So, a java program executing on different platforms has a different appearance and sometimes even different user interacts with the program are known as that program's look and feel. The Swing components allow the programmer to specify a different look and feel across all platforms, or even to change the look-and-feel while the program is running.

Swing components are often referred to as lightweight components they are written completely in java so they are not "weighed down" by the complex GUI capabilities of the platform on which they are used. AWT

Components (many of which parallel the Swing components) that are tied to the local platform are correspondingly called heavyweight components they are rely on the local platform's windowing system to determine their functionality and their look feel. Each heavyweight component has a peer (from package java.awt.peer) that is responsible for the interactions between the component and the local platform to display and manipulate the component.

FEATURES OF SWING OVER AWT:

Even the simplest Swing components have capabilities far beyond what the AWT components offer.

1 Swing buttons and labels can display images instead of , or in addition to, text
2 You can easily add or change the borders drawn around most Swing components. For example, it's easy to put a box around the outside of a container or label.
3 You can easily change the behavior or appearance of a Swing component by either invoking methods on it or creating a subclass of it.
4 Swing components don't have to be rectangular. Buttons, for example, can be round.
5 Assistive technologies such as screen readers can easily get information from Swing components. For example, a tool can easily get the text that's displayed on a button or label.
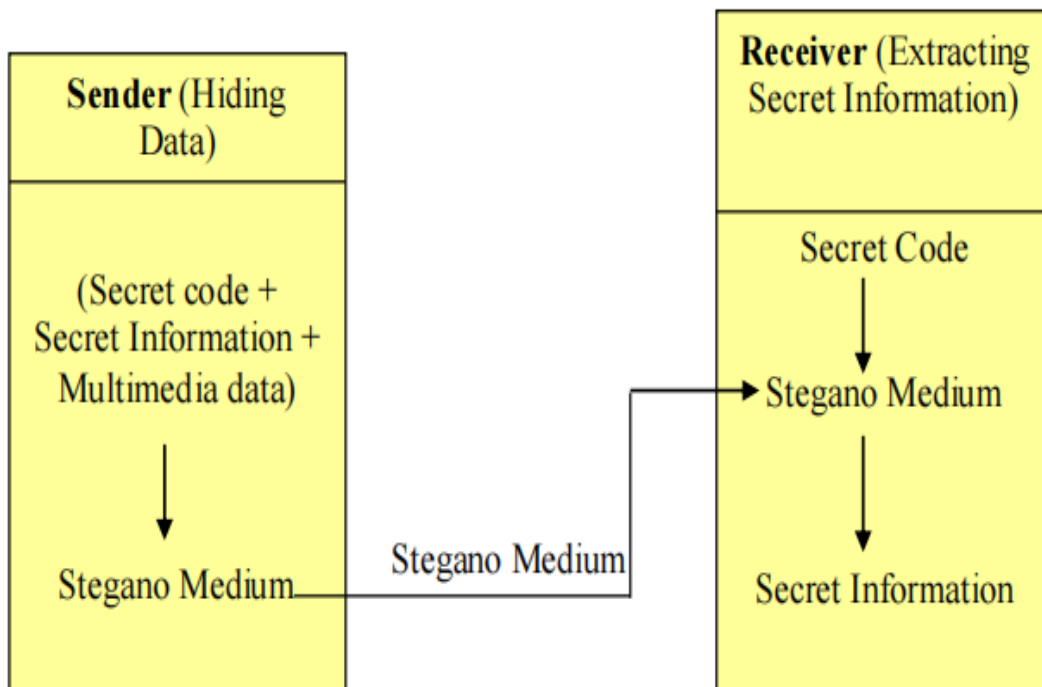
Swing lets you specify which look and feel your program's GUI uses. By contrast, AWT components always have the look and feel of the native platform.

Chapter 5

SYSTEM DESIGN

5.1 ARCHITECTURE OF THE SYSTEM

Architecture of the system

5.2 Modules Description

There are mainly two modules used in this project:

5.2.1 Creating stegano Medium :

In making stegano Medium side, the secret information is hided with in an image file. Before hiding, for security, user has to enter a user code and secret information. A secret code will be generated using user code + secret information and this secret code will be used by the receiver to extract the secret information. After generating secret code stegano medium will be generated. This stegano medium is the final output and expected output from the sender side.

5.2.2 Getting secret information from stegano medium:

In getting secret information from stegano medium Side, Actually anyone may get this stegano medium that is picture with secret information, but only the person who knows secret code can read the message. Inputs for breaking the stegano medium are stegano mediam and secret code.

1

5.3 DETAILED DESIGN

Algorithm:

Making Stegano Medium:

Step 1: Start the process
Step 2: Enter the Secret Information
Step 3: Enter the User Code
Step 4: Load a multimedia data, here it is an Image
Step 5: Creation of Secret Code by using user code + secret information
Step 6: Hiding secret information with its security into the multimedia data
Step 7: A message box showing the secret key will appear
Step 8: Stop the process

Extracting secret information from Steganography medium:

Step 1: Start the process
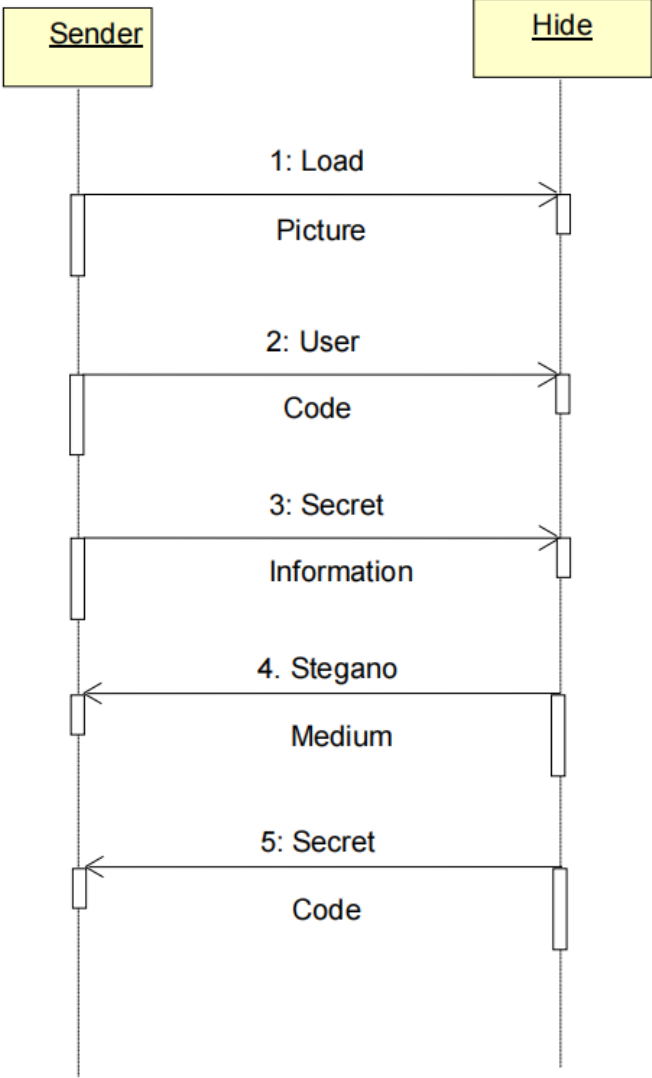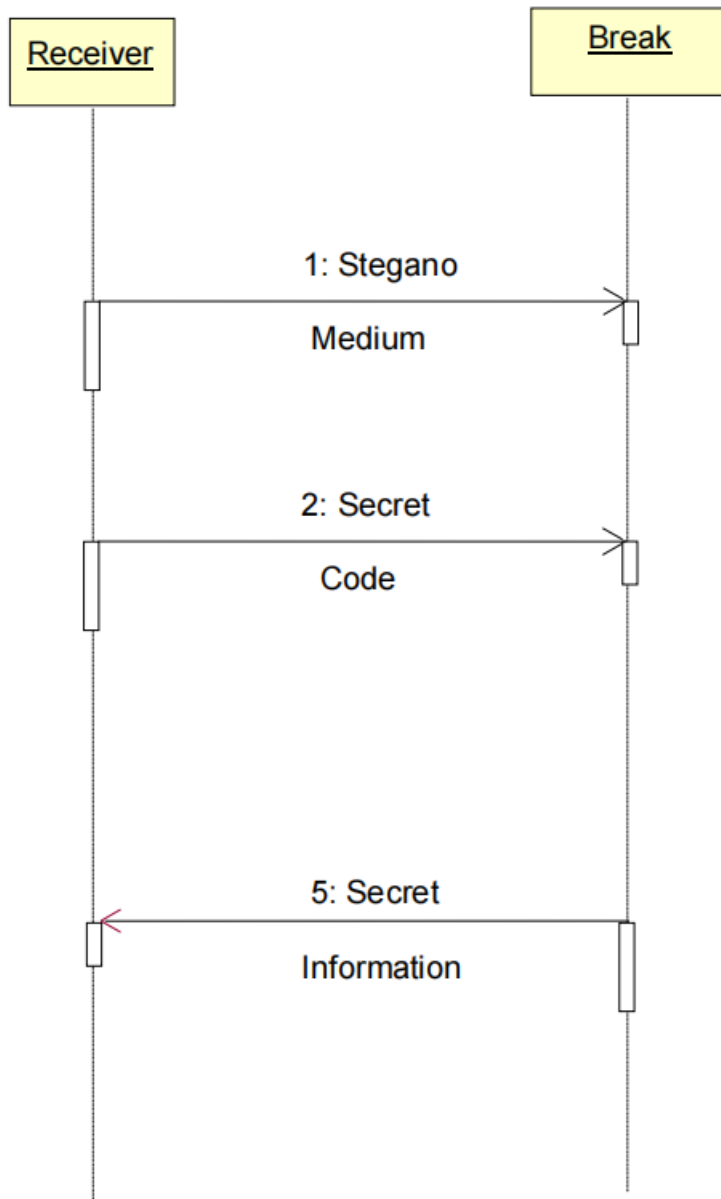Step 2: Enter the Secret Code
Step 3: Enter the Stegano Medium
Step 4: Extract secret information from stegano medium by using secret code.
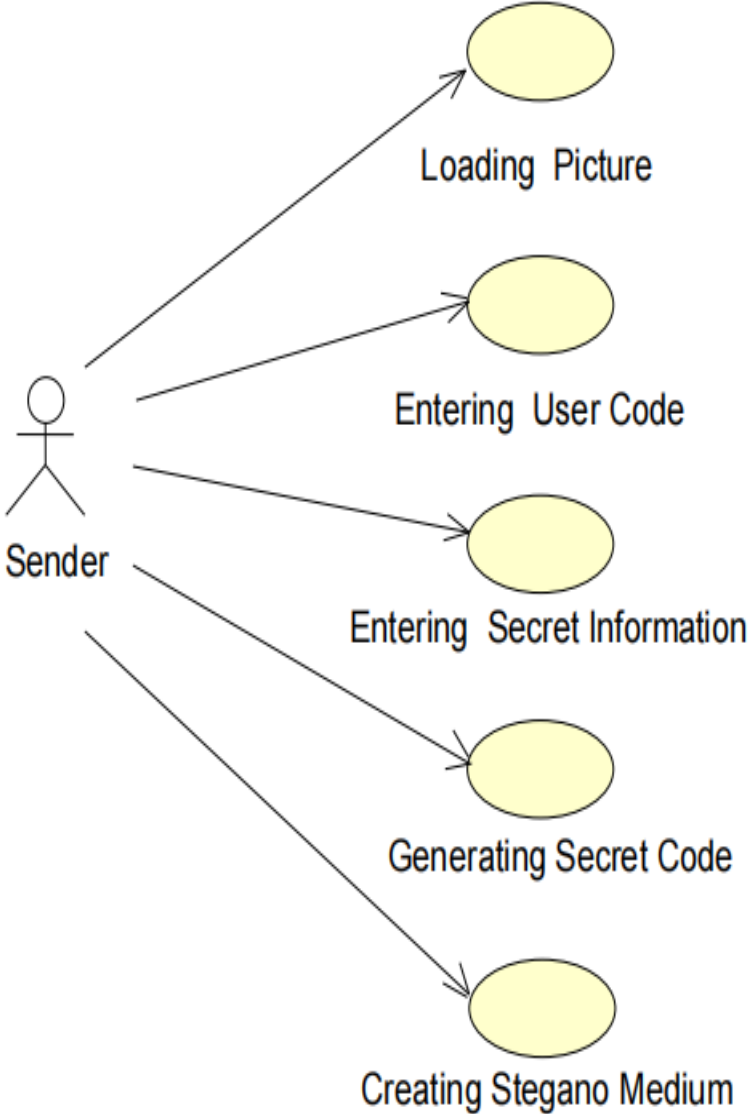Step 5: Stop the Process

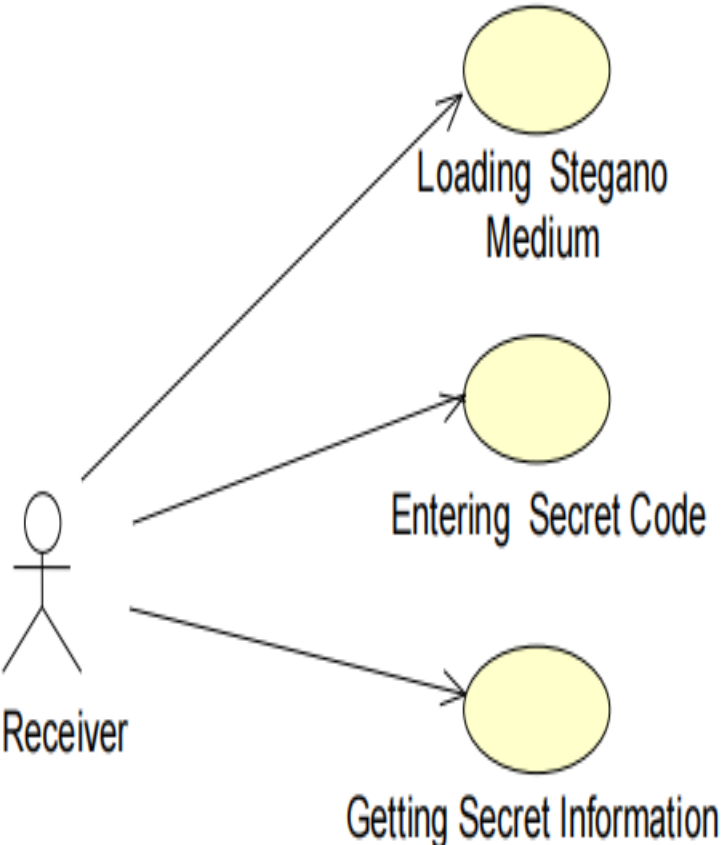## 5.4 SOFTWARE MODELING

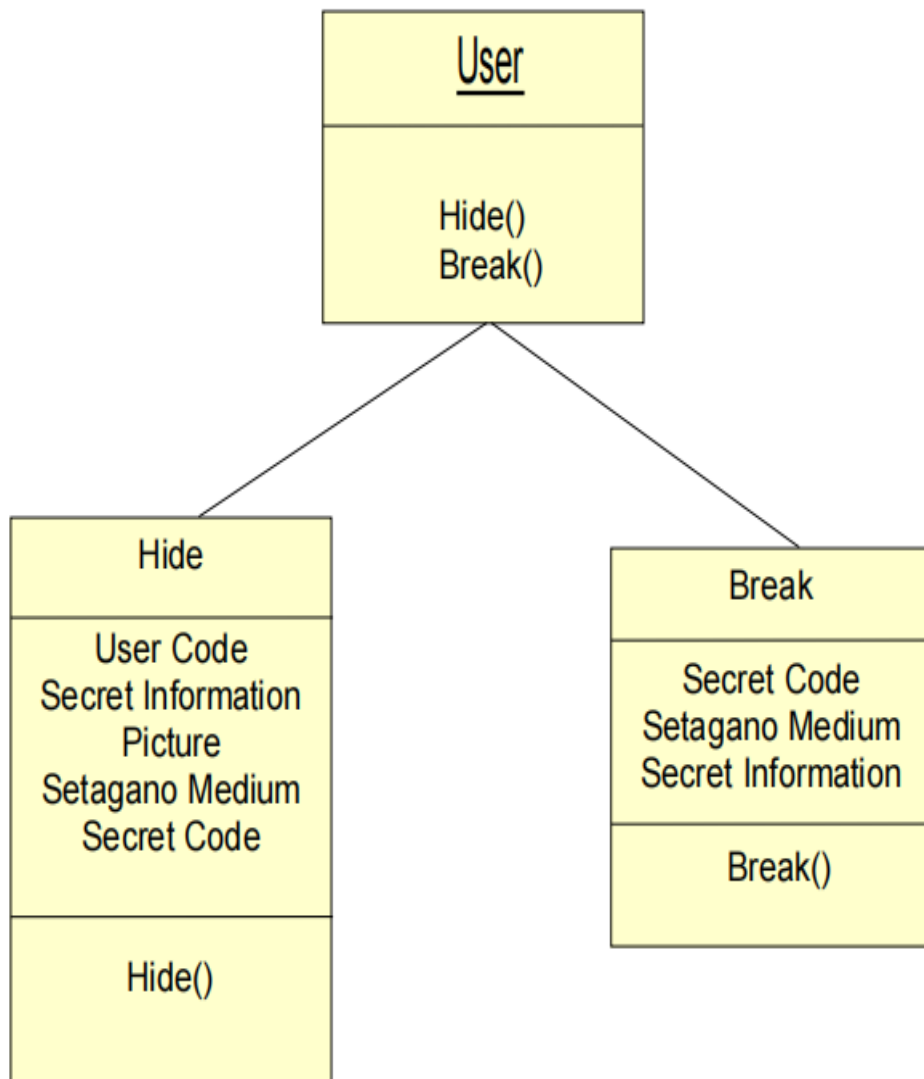## Sequence Diagram:

Use Case Diagram:

Sender:

Loading Picture

Entering User Code

Entering Secret Information

Generating Secret Code

Creating Stegano Medium

Sender

Receiver:

Class Diagram:

Client:

```
                          ┌─────────────────────┐
                          │        User         │
                          ├─────────────────────┤
                          │      Hide()         │
                          │      Break()        │
                          └─────────────────────┘
                            ╱                 ╲
                          ╱                     ╲
       ┌──────────────────────┐        ┌──────────────────────┐
       │         Hide         │        │        Break         │
       ├──────────────────────┤        ├──────────────────────┤
       │     User Code        │        │     Secret Code      │
       │  Secret Information   │        │   Setagano Medium    │
       │      Picture          │        │  Secret Information  │
       │   Setagano Medium     │        ├──────────────────────┤
       │     Secret Code       │        │      Break()         │
       ├──────────────────────┤        └──────────────────────┘
       │       Hide()         │
       │                      │
       └──────────────────────┘
```

Activity Diagram:

Start

Start Stegano
Application

Select Operation

Hide

Load Image

Enter User Code

Generate Secret Code

Generate Stegano Medium

End

Break

Load Image

Enter Secret Code

Extract Secret Information

End
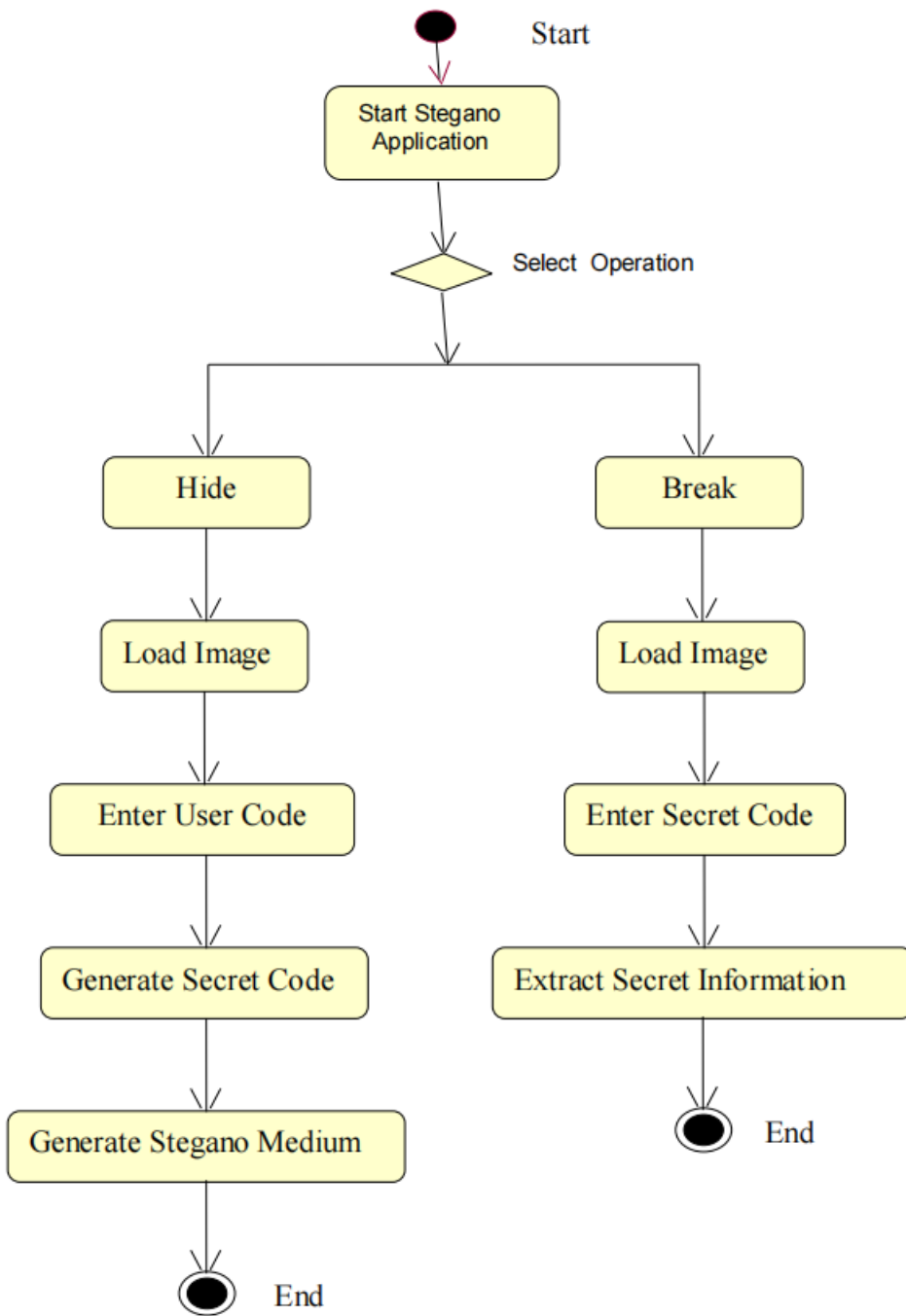
Chapter 6

SYSTEM IMPLEMENTATION

This project needs a java development kit (J2sdk1.4.1 and above). Project is implemented in java, so it can be run in any OS. For hiding data with in a picture we need to run the sender side program. For extracting the hidden secret information we need to run receiver side program.

Our stegano graphy application will contain both sender and receiver side programs. If a user wants to hide data he can use sender side program and if he wants to extract secret information he can use the receiver side program.

Chapter 7

SYSTEM TESTING

The testing of a conventional software system involves some of the following phases. They are
- ➢ Unit Testing
- ➢ Integrated Testing
- ➢ System Testing

Unit Testing:
A software module can be created by building up of many small parts into a single module. This small part is called as a unit. A unit is a piece of code that will perform a specific task. At the end of this testing all units will be tested so that we can get the correct result. By using unit testing we can easily identify the errors.

Integration Testing:

Combining all programs into a single application and testing its correct is called as Integration testing. Even all programs work correctly they may give a false result when they work together. Integration is very important to get the completed result.

System Testing:

System testing means testing the whole system at once. By giving different inputs to the system we can check its correctness. For all inputs the system should produce correct result.
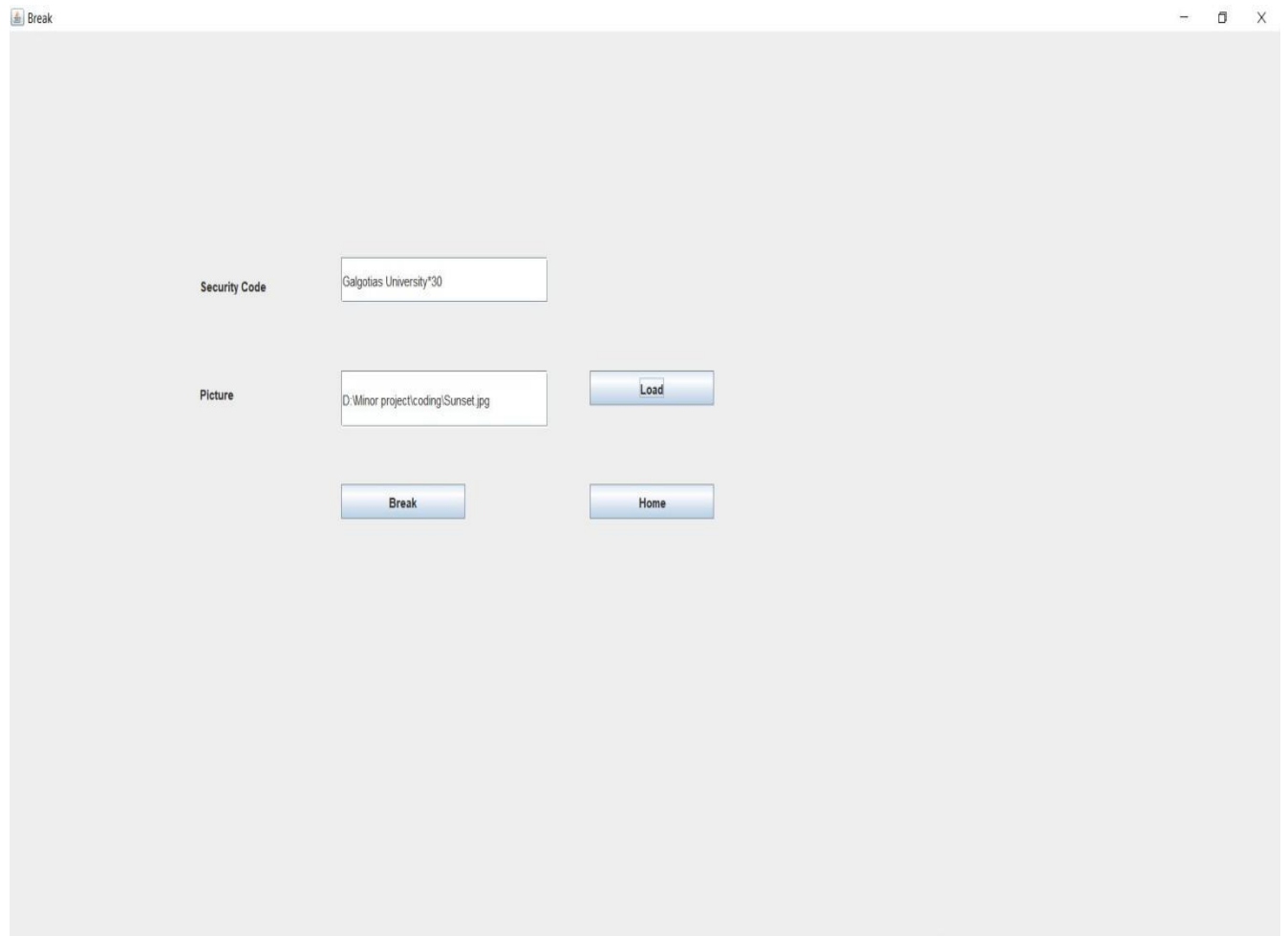
Chapter 8

RESULTS

Step 1

Step 2

Step 3

After hide we will get a secrete code
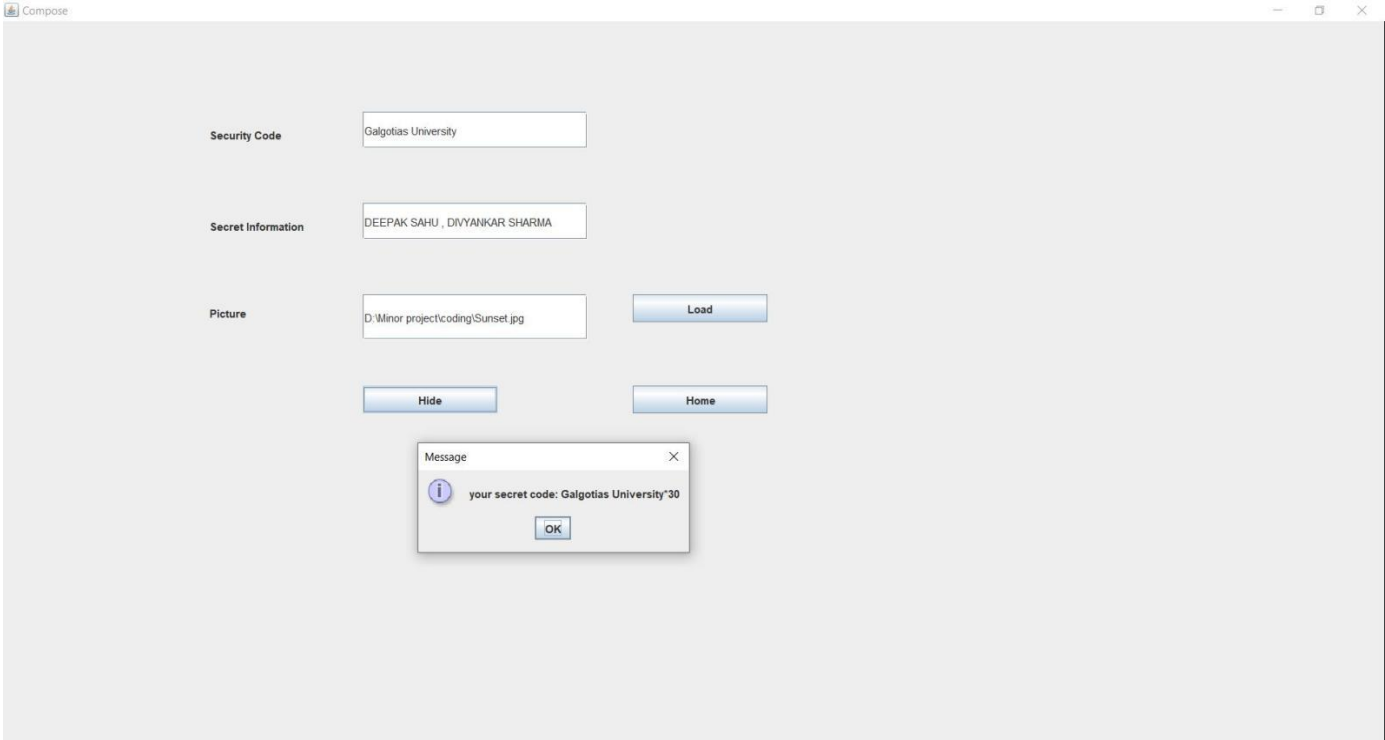
Step 4

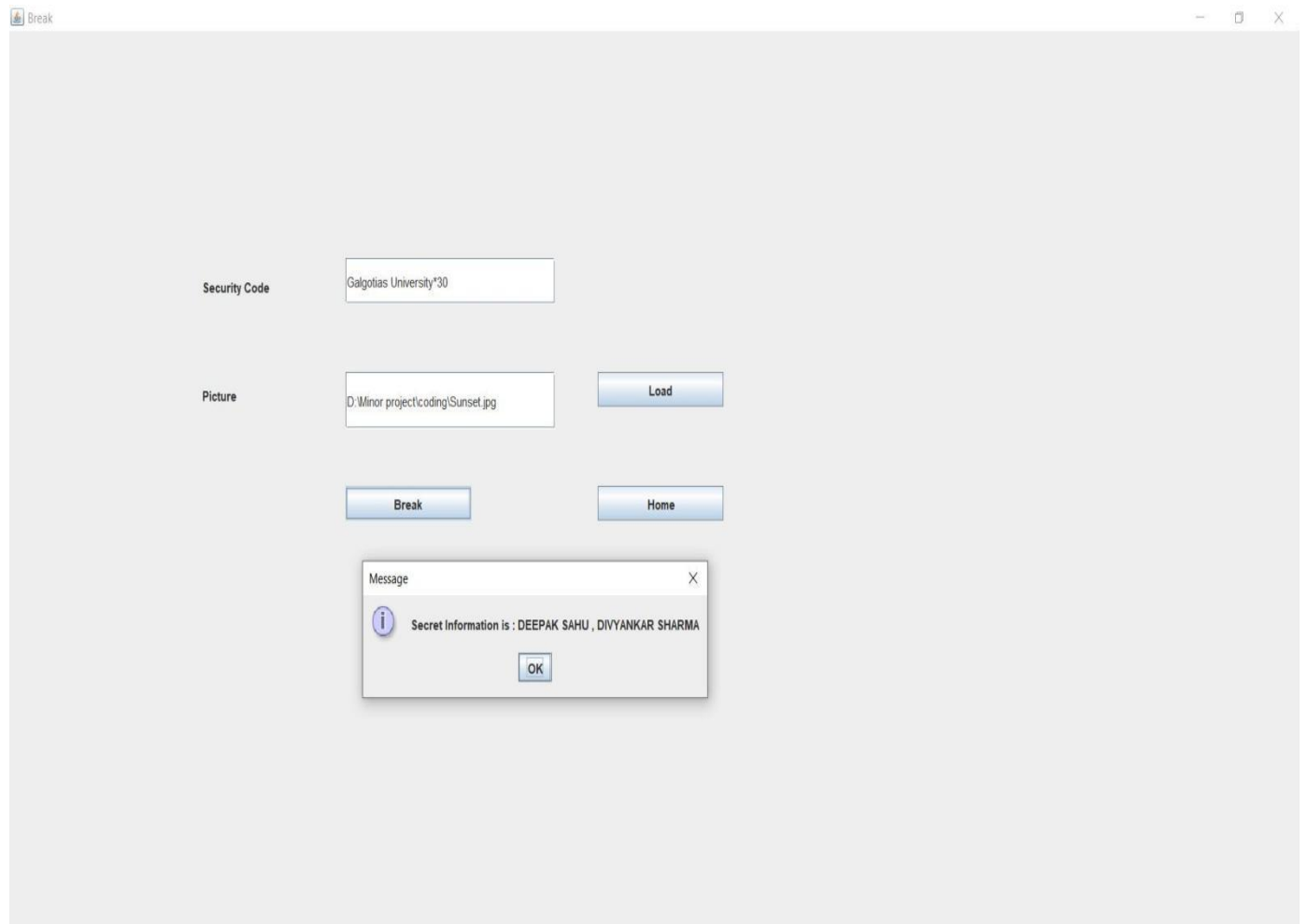For break , enter the security code and load the encrypted picture

Step 5

Finally we will get the secret information

Security Code: Galgotias University*30

Picture: D:\Minor project\coding\Sunset.jpg [Load]

[Break] [Home]

Message
Secret Information is : DEEPAK SAHU , DIVYANKAR SHARMA
[OK]

Chapter 9

<u>Conclusion</u>

This project provides a GUI, a user friendlier system, where secret information can easily be hided with in a picture file.this technique results in less modification of bits resulting in less randomness in the image.It is platform independent so that it can be used in any OS

<u>References</u>

Web Sites

- http://www.javaranch.com

- http://forum.java.sun.com

- http://java.sun.com

- http://www.javaworld.com

[1]   Tao Zhang, Wenxiang Li, Yan Zhang and Xijian Ping, "Detection of LSB matching steganography based on distribution of pixel differences in natural images," 2010 International Conference on Image Analysis and Signal Processing, 2010, pp. 548-552, doi: 10.1109/IASP.2010.5476056.

[2]   K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[3]   S. Kumar, A. K. Yadav, A. Gupta and P. Kumar, "RGB image steganography on multiple frame video using LSB technique," 2015 International Conference on Computer and Computational Sciences (ICCCS), 2015, pp. 226-231, doi: 10.1109/ICCACS.2015.7361355.

[4]   Asok and P. Mohan, "Implementation and Comparison of different Data Hiding Techniques in Image Steganography," 2019 3rd International Conference on

Trends in Electronics and Informatics (ICOEI), 2019, pp. 1180-1183, doi: 10.1109/ICOEI.2019.8862750.

[5]   J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[6]   Kavita Saini, "Recent Advances and Future Research Directions in Edge Cloud Framework", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019,   DOI: 10.35940/ijeat.B3090.129219

[7]   I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[20]   https://www.smartinsights.com/digital-marketing-strategy/online-business-revenue-models/amazon-case-study/

[21]   Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013

Ki-Hyun Jung & Kee-Young Yoo; "Steganographic method based on interpolation and LSB substitution of digital images", Multimedia Tools

Application: Springer Science Business Media New York 2014.

Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on , vol., no., pp.1188,1193, 20-21 March 2013.