

**ONLINE SECURE BANKING TRANSACTION IN CONCERN OF USER
INFORMATION**

BY

**SADIA AHMED KEYA
ID: 171-15-1442
AND**

**MIR NOSHIN TASNIM
ID: 171-15-1374**

This Report Presented in Partial Fulfillment of the Requirements for the
Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Ohidujjaman
Sr. Lecturer
Department of CSE
Daffodil International University

Co-Supervised By

Tajim Md. Niamat Ullah Akhund
Lecturer
Department of CSE
Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 15, 2021

APPROVAL

This Project titled “**Online Secure Banking Transaction in Concern of User Information**”, submitted by **Sadia Ahmed Keya** and **Mir Noshin Tasnim** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **Dec 8, 2020**

BOARD OF EXAMINERS

、
(Dr. Syed Touhid Bhuiyan)

Professor and Head

Department of CSE

Faculty of Science & Information Technology

Daffodil International University

Chairman

、
(Dr. S M Aminul Haque)

Associate Professor & Associate Head

Department of CSE

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

、
(Ohidujjaman)

Sr. Lecturer

Department of CSE

Faculty of Science & Information Technology

Daffodil International University

Internal Examiner

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Ohidujaman, Sr. Lecturer, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Mr. Ohidujaman
Sr. Lecturer
Department of CSE
Daffodil International University

Co-Supervised by:

Tajim Md. Niamat Ullah Akhund
Lecturer
Department of CSE
Daffodil International University

Submitted by:

(Sadia Ahmed Keya)
ID: -171-15-1442
Department of CSE
Daffodil International University

(Mir Noshin Tasnim)
ID: -171-15-1374
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound indebtedness to **Mr. Ohidujjaman , Sr. Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Network Security*” to carry out this project. His endless patience ,scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. S.M. Aminul Haque, Associate Professor & Head**, Department of CSE, for his kind help to finish our project and also to other faculty members and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

In today's modern world, security is the main essential part of an online transaction. We want to transact money as well as want to have full protection of that transaction. Particularly the individuals of this nation are generally working class or under neediness so they are worried about their money getting hacked on the online. In this project a Steganographic based encryption is shown for hiding data and proposed a system which can be used in an online banking system. The leading motive is to veil the undercover secret message inside the image utilizing the LSB(Least Significant Bit) technique and the Digital Steganography. Providing an extra level of security that ensures that no data can be accessed by any unwanted third party. This proposed method provides the Hybrid Steganography technique with the combination of LSB Steganography and Digital Steganography. Steganographic LSB technique is a least significant bit based encryption. All the media files like image, audio, video and also messages can be concealed inward the cover image. This two methods are used in this proposed project to conceal valuable information hidden under an image. Digital Steganography is the leading art of hiding the secret information inside of a cover image or media files without invading unintended users. Combination of both techniques conserves and provides security by enveloping the undercover hidden message. Our method will provide a commencing level of security to all the valuable transactions.

TABLE OF CONTENTS

CONTENTS	PAGE
Board of examiners	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
CHAPTER	
CHAPTER 1: INTRODUCTION	1-2
Introduction	1
Motivation	1
Objectives	1
Expected Outcome	2
CHAPTER 2: BACKGROUND	2-4
Introduction	2-3
Related Work	3
Comparative Study	4

CHAPTER 3: REQUIREMENT SPECIFICATION	4-5
Technical and Legal Requirement	4
Hardware Requirement	5
Programming Prerequisite	5
CHAPTER 4: DESIGN SPECIFICATION	6-12
Network Design prototype development	6
Digital Steganography	6
LSB Steganography	6-8
Algorithm of LSB	8-9
Design Software prototype development	9
Java	9
Ardor	9
Compilation and Interpretation	10
Position-autonomous and Portable	10
Object-Oriented	11
Robust and Consolidated	11
Distributed	11
Naive, Small and Conventional	11
Elevated Performance	12

CHAPTER 5: PROJECT DIAGRAM	12-20
System Design	12
Proposed System Design Architecture	12-13
Software Model Diagram	14
Sequence Diagram	14-15
Use Case Model	16-17
Class Diagram	18-19
Activity Diagram	20-21
CHAPTER 6: IMPLEMENTATION AND TESTING	22-30
Implementation of the System	22
Result	23
Home Page View	23
Input(Sender)	24
Generated Secret Code	25
Encrypted Message	26
Input(Receiver)	27
Output Result	28
Invalidation(Wrong Code)	29-30

CHAPTER 7: CONCLUSION AND FUTURE SCOPE	31
Discussion and Conclusion	31
Scope for Future Development	31
APPENDIX	32
REFERENCES	33

LIST OF TABLES

Tables	PAGE NO
3.1 Hardware Requirement	5
3.2 Software Requirement	5

LIST OF FIGURES

FIGURES	PAGE NO
Figure 4.1: LSB Technique	8
Figure 5.1: Proposed System Design Architecture	13
Figure 5.2 : Sequence Diagram(Sender's End)	14
Figure 5.3 Sequence Diagram(Receiver's End)	15
Figure 5.4 Usecase Diagram Model(Sender's End)	16
Figure 5.5 Usecase Diagram Model(Receiver's End)	17
Figure 5.6 Class Diagram Model	19
Figure 5.7 Activity Diagram Model	21
Figure 6.1 Home Page View	23
Figure 6.2 Input(Sender)	24
Figure 6.3 Generated Secret Code	25
Figure 6.4 Encrypted Message	26
Figure 6.5 Input(Receiver)	27
Figure 6.6 Output Result	28
Figure 6.7 Wrong Input(Receiver)	29
Figure 6.8 Invalidation	30

CHAPTER 1

INTRODUCTION

Introduction

The system proposes a method that will ensure the security of user information while transactions occur online. The given method gives an eminently effective and secure transmission of data over online which makes the data invulnerable and its unaffected towards unintended users. So users can put their trust and share their confidential data.

Motivation

1. As most of the people of Bangladesh or in any low income country have trust issues on having a transaction through online because of the fear of getting hacked of their money or personal information on the online platform. The people with low income majorly, can't gather the courage to do so. To solve this problem we have made this system design for a trustworthy transaction process.
2. Inspiring an unaccompanied to have faith for utilizing the online transaction system in an inefficient pay nation. Making the transaction process easier with proper safety.

Objectives

1. Exposition of efficiency of the algorithms used to create eminently encrypted data to avoid suspicion of hackers and not affect unwitting users.
2. Making a system design for enormously secure online transactions targeting people with insufficient wages.

Expected Outcome

1. Immensely secured user's information
2. Safely transfer data abandoning hackers
3. Only a particular authorized person can access the data
4. Provides an interface which is favorable for the users.
5. Reduces dependency on others.
6. Trustworthy for low income people.

CHAPTER 2

BACKGROUND

Introduction

Online data transaction is a secure process of transferring funds or money through the internet while ensuring the data doesn't leak to third parties. As the economy is being cashless that has replaced physically going to our banks. So, it is important to protect the information holding in our credit or debit card or other services that enable transactions. It can not be forgotten how much security is important to us. As the popularity of e-commerce is expanding the opportunities for misusing of payment networks and data theft is also growing. There's a limitation of transferring money that one can send or receive. For all those related problems that we encountered, we want to bring a better solution to prevent the vulnerability of security. That's why using the Hybridization of

two Steganography techniques. This is an excellent method of encryption to prevent data fraud in online transactions. Nowadays, people are a lot concerned about their data security. Whatever the data is they always want to protect it from unauthorized and unsecured access. Only the owner and relevant people have permission to access their data. Not only storing the data but also sharing with the right person. People are highly dependent on mobile phones and computers for sharing purposes. While sharing the data through the internet, people fear that their data may be stolen by third parties. Because it is common to hijack the data while sharing no matter how secure the connection is. So for these concerns. got the inspiration to work on this method. There are thousands of security strategies to overcome this problem, but this Steganography technique is more reliable and harder to break. Here, using the Hybridization of Steganography techniques, LSB and Digital Steganography that provides a huge complexity over data breaching. By using this data security model below significant things can be assured:

- i. Confidentiality : Maintaining confidentiality is the main priority to prevent data theft. While transferring confidential data, it will be completely encrypted to prevent cyber-attacks.
- ii. Authentication: It ensures authenticity while transferring data.

Related Work

In this field of networking there is a lot of work already done. And there are some specialized systems designed by others. But there are many systems which do not give decent or high security. Some researchers have done data encryption and decryption of networks which is used in communication systems with. Some have done that only with secret key systems. Also there are some papers that present implementation of digital signature for mobile devices and ATM debit payment systems.

Comparative Study

1. This hybridization method is solid as compared to some other existing ones.
2. Generally ,in some methods, individual Steganography techniques are being used. But here two Steganography techniques are combined together.
3. Cryptography many times affects the users who are not related to that particular data, So that here used only Steganography techniques.
4. This method has a user friendly interface, while symmetric or asymmetric cryptography most times provides an unfavorable interface for the user.
5. In this proposed method the whole secret communication is hidden, whereas in symmetric or asymmetric cryptography only the particular secret message is hidden.

CHAPTER 3

REQUIREMENT SPECIFICATION

Technical and Legal Requirement

The framework should be planned as to guarantee that they keep on working effectively with the perception with applicable enactment and to watch that they are protected and monitored from dangers for example, hackers. The necessity are recorded beneath:

- 1.Data protection and Security data transmission.
- 2.Protection against hackers / attackers.

Hardware Requirement

To run this project minimum one PC is required, the requirements are given beneath in the table :

Table 3.1 Hardware Requirement

Processor	Intel Pentium/ADM processor(500 MHZ)
Motherboard	Any
Ram	300 GB or More
Hard Disk	100GB
Floppy Disk Drive	1.44 floppy disk drive
Monitor	Any Color Monitor
Keyboard	Any
Mouse	Mouse with minimum two buttons
CD Rom	52X

Programming Prerequisite

Different kinds of programming need to make and keep up to foresee the process. Subtleties given underneath:

3.2 Software Requirement

Software	Use
Any form of windows working system / Linux.	To fire up the PC and organize all equipment segments, application and altered the product

CHAPTER 4

DESIGN SPECIFICATION

4.1. Network Design prototype development

Digital Steganography

In this modern digital domain, steganography plays a significant role in securing data. It means in a real sense signifies covered composition. Steganography is used to shroud the way that a message is being transferred. While cryptography only encrypts the particular message, Steganography hides the whole conversation that is transferred. It includes concealing information in digital documents, and other digital structures. Digital Steganography works by supplanting pieces of pointless information. All the media files work as a hidden medium for the secret message such as audio, video, image etc.

LSB Steganography

LSB-Steganography is a steganography procedure where we shroud messages inside a picture by supplanting Least critical piece of picture with the pieces of message to be covered up.

This encryption method uses the LSB (Least Significant Bit) image steganography algorithm. All the pixels of an image are deflected. The deflection process occurs to a bit of a message that is to be concealed underneath the particular image. The cipher text is concealed underneath the image. After completion of the process the stego image stil

looks like before but in reality a message is hidden inside. which normally humanbeing can not see.

Let's contemplate grayscale bitmap. The bitmap is a 8-digit grayscale bitmap. So, in this picture every pixel is put away as a byte speaking to a grayscale shading estimation of the picture. Assume the initial eight pixels having the accompanying dark shading esteems as:

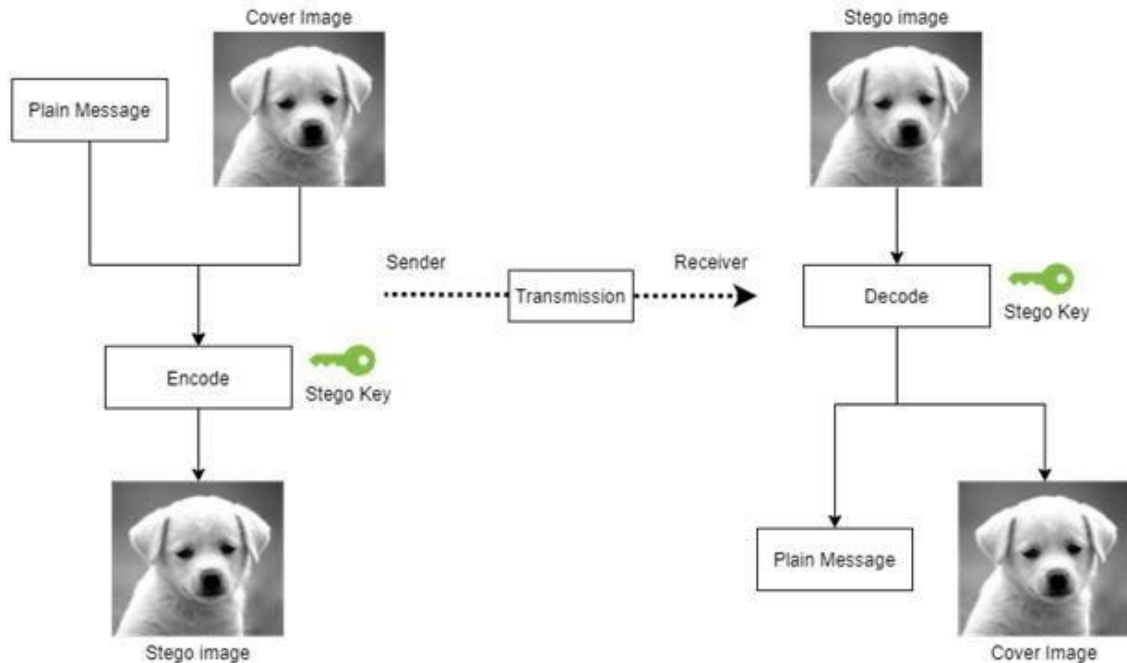
```
01010010  01001010  10010111  11001100  
11010101  01010111  00100110  01000011
```

The objective is to conceal the letter "S". The ASCII code of the letter s is 83. 1010011 is the binary value of s. LSB replacement is the aim of these pixels. Beneath is the following new values as:

```
01010011  01001010  10010111  11001100  
11010100  01010111  00100111  01000011
```

As it is seen in the example that only three bits of the gray color have been changed out of eight bits. It depends on the secret message that is to be embedded. Digital images can be either 8 bit or 24 bit. Maximum 1 bit is permitted at a time for embedding in 8 bits images. 3 bits are permitted in a 24 bits image. Usually in 24-bits LSB techniques are implemented.

This process is given in the figure 4.1 below.



4.1. Figure of LSB Technique

Algorithm of LSB

The means of the calculation to insert instant message utilizing grayscale Image is:

Stage 1: First, peruse the picture where the message will be hidden and instant message which is to be covered up in the picture.

Stage 2: Alter the instant message into the double/binary.

Stage 3: For every pixel count the LSB of the picture.

Stage 4: Change the location of the LSB of the particular picture, each piece of the mystery message individually.

Stage 5: Compose the Stego picture.

The means of the calculation with the means to recover instant message utilizing grayscale Image:

Stage 1: First, peruse the Stego picture.

Stage 2: For every pixel count the LSB of the picture.

Stage 3: Finally recover the pieces and complete the conversion of each and every 8 bit into the relating character.

What's more, the means of the calculation to implant instant message utilizing the shading Image is:

Stage 1: Read the pixels and store it in a cluster.

Stage 2: Alter the message(s) that will be inserted into the paired message.

Stage 3: Read this parallel binary message into an exhibit..

Stage 4: Select the pixel and pick the characters from the and spot it in the LSB of the pixel.

Stage 5: Ultimately, the gained picture will be the Stego picture that comprises the concealed information.

Design Software prototype development

Java

Ardor

Java is a universally useful, elevated level programming language previously delivered by Sun Microsystems in 1995. It executes conditions as expected under the circumstances, is allowed to utilize, and can run on all stages. It is simultaneous, class-based, and object-situated. The stacking of classes of Java are dynamic. The stack of classes holds interest as it narrates the classes. It is a language that is oriented towards objects. It has complementary capacities as C and similar languages. Java upholds dynamic accumulation and programmed memory of executives (trash assortment).

Compilation and Interpretation

Java system is a double way system including both compilation and interpretation. The way java works is , firstly the compiler does it's job of narrating the origin code into another code. That another code is called bytecode and its not instruction by machine At the second platform java does its job of interpretation. It originates the apparatus code that can be straight away attained. This process is attained by the machine that is extending the program of java. So it can surely be said that java is a double path language which includes compilation and interpretation.

Position-autonomous and Portable

Java ensures its portability because the main commitment of java over different dialects is its convenience. The projects can be effortlessly driven starting with one PC framework then onto the next. It is a locomotive that can be transferred to a place and whenever. Java programs. has the ability to manage when comes to variation and redesigns in working frameworks, processors and frameworks. These assets won't drive any adjustments of the program. This is the motivation behind the popularity of Java programs. It has become a mainstream dialect for programming on the Internet. This language program interconnects various types of frameworks around the world. An applet of Java programs can be downloaded. The time when it is being downloaded, can be out of a distant PC onto a neighborhood framework by means of the Internet and execute it locally. The whole process generates the portability where the Internet works as an expansion of the client's fundamental framework giving for all intents. Java guarantees versatility twoly, one is compilation another one is interpretation.

Object-Oriented

The veritable truth is that this language is an object-oriented language. In the java program nearly all things are objects. There are classes in which the datas inhabit. The program inherits in the immense swarm of classes. The object norm placed in java is facile and malleable.

Robust and Consolidated

The Java program takes measure for ensuring the codes are dependable which makes this language robust. Ensures the precise compilation and run time, also designed greatly that it manages all its problems related to memory management by its own-self. This program abstracts the notion of exception handling. Series errors are seized by this and diverges any risk of corrupting the system.

Distributed

Applications on networks are sketched by Java which makes it a distributed language. Both information and projects are imparted by Java. Far off articles on the Internet can be undeterred and accessed by Java as effectively as they can do in a nearby framework.

Naive, Small and Conventional

Numerous highlights of C and similar language that are either repetitive or wellsprings. Those temperamental codes are not pieces of the language Java. Java doesn't utilize pointers, preprocessor header documents for instance. Java additionally kills administrators over-burdening and various legacy.

Elevated Performance

Regarding the use of intermediate bytecode its performance is indeed captivating. The sketch of java is specially developed to decrease run time. Multithreading improves the general execution speed of java programs majorly.

CHAPTER 5

PROJECT DIAGRAM

System Design

Proposed System Design Architecture

Two scruple in this proposed method :

- I. First scruple is to generate the Stegano Medium
- II. Second is to receive concealed data from stegano medium.

Both of the scruples are discussed beneath :

- ★ The process of generating the stegano medium part, these obligatory things should be done. Firstly inside an image the undercover concealed data is veiled. For the major security purpose the user has to encroach an input of a decent code and add the secret data or message. By utilizing the given user code with mystic data a concealed code will be generated. That particular concealed code will be utilized by the receiver. Using the concealed code the receiver will be able to extract the secret concealed information. Afterwards the completion of generating concealed code, the particular medium which is stegano medium will be originated. Finally the ultimate output from the sender side will be gained.

- ★ Extracting data from the receiver side needs a major component which is definitely the concealed code. In reality anybody may apprehend the medium that means stegano medium because that is an image including secret data. But that is only about just seeing the picture, they can not gain the original concealed data. Whereas the particular person having knowledge about the concealed code can only extract and read the secret information hidden within the picture. The breaking rule of stegano medium is to give the inputs which includes Concealed Code and Stegano medium.

The whole process is given in the figure 5.1 below.

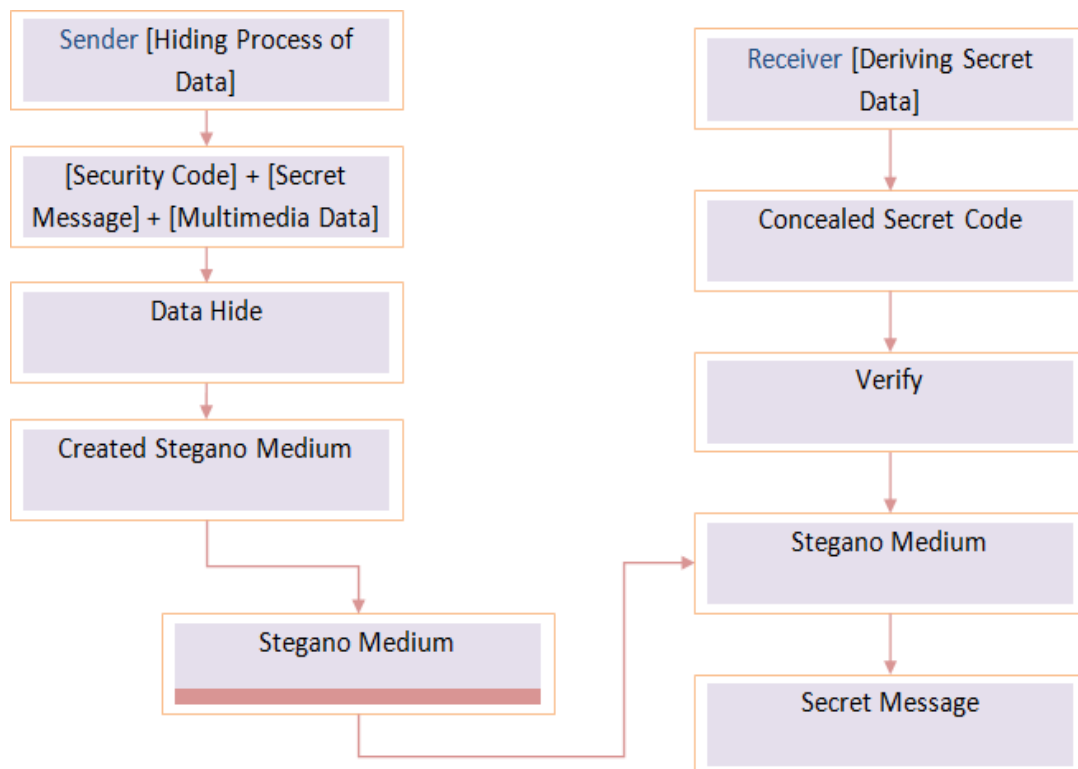


Figure of Proposed System Design Architecture

Software Model Diagram

Sequence Diagram

The hiding process of data starts with loading the picture where the given secret information will be hidden. Give the user code and secret data information. Then after fulfilling the stegano medium the concealed or secret code is generated. After gaining the secret code the completion of the sender's side is done.

This process is given in the figure 5.2 below.

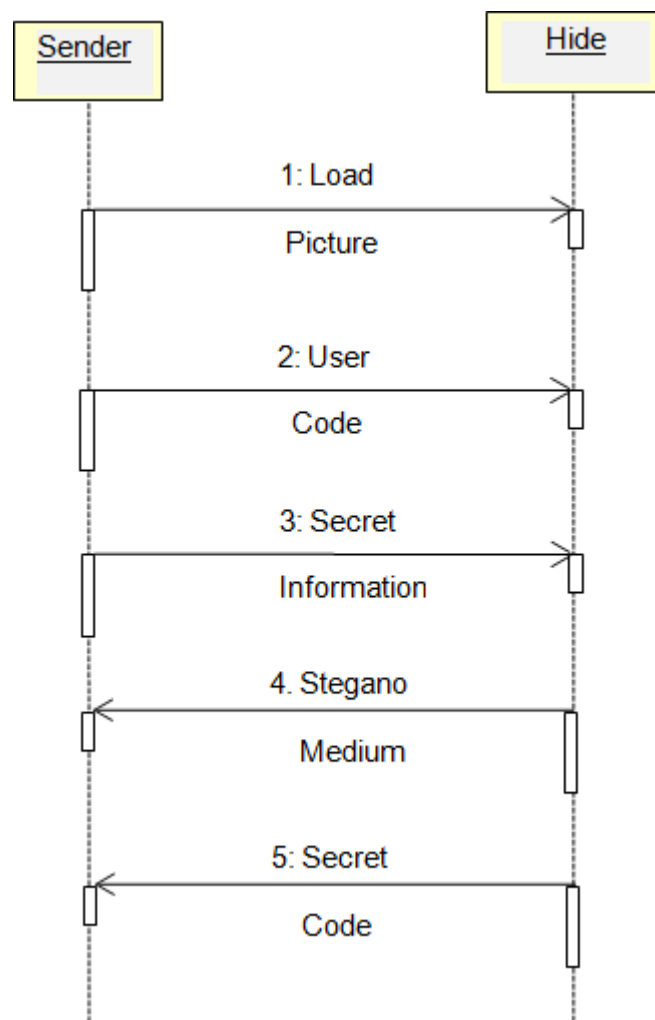
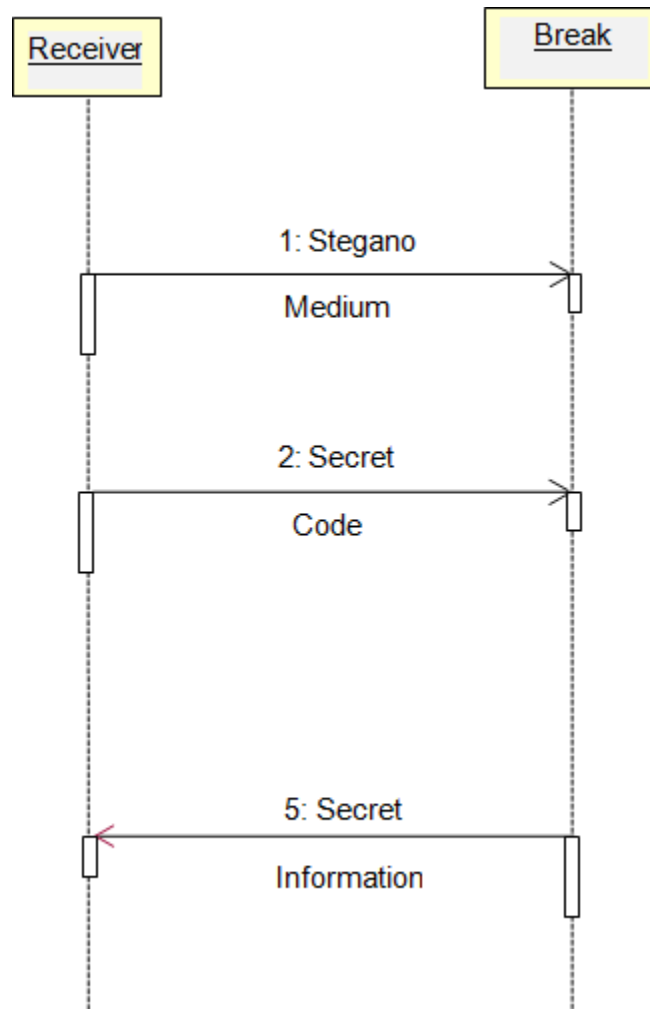


Figure of Sequence Diagram(Sender's End)

After transmitting the secret information the receiver will receive the image including the secret message. Then the receiver will start the process of breaking the encrypted message in order to get the original message. The process must go through the stegano medium . The receiver has to enter the concealed secret code which was generated in the sender's end. Only if the receiver is the authorized person then he/she can decode it using the concealed secret code in order to get the original secret information, otherwise the system will show that the code he has entered is not valid.

This process is given in the figure 5.3 below.



Use Case Model

A use case model is the way that most easily depicts a user's fellowship along with the framework. Here it depicts the links between the user as well as the diverse use cases in which the user is ancillary. The Sender will start the process. The concealing cycle of information begins with stacking the image where the given mystery data will be covered up. Give the client code and mystery information data. At that point subsequent to satisfying the stegano medium the disguised or mystery code is produced. In the wake of picking up the mystery code the fulfillment of the sender's side is finished.

This cycle is given in the figure 5.4 underneath.

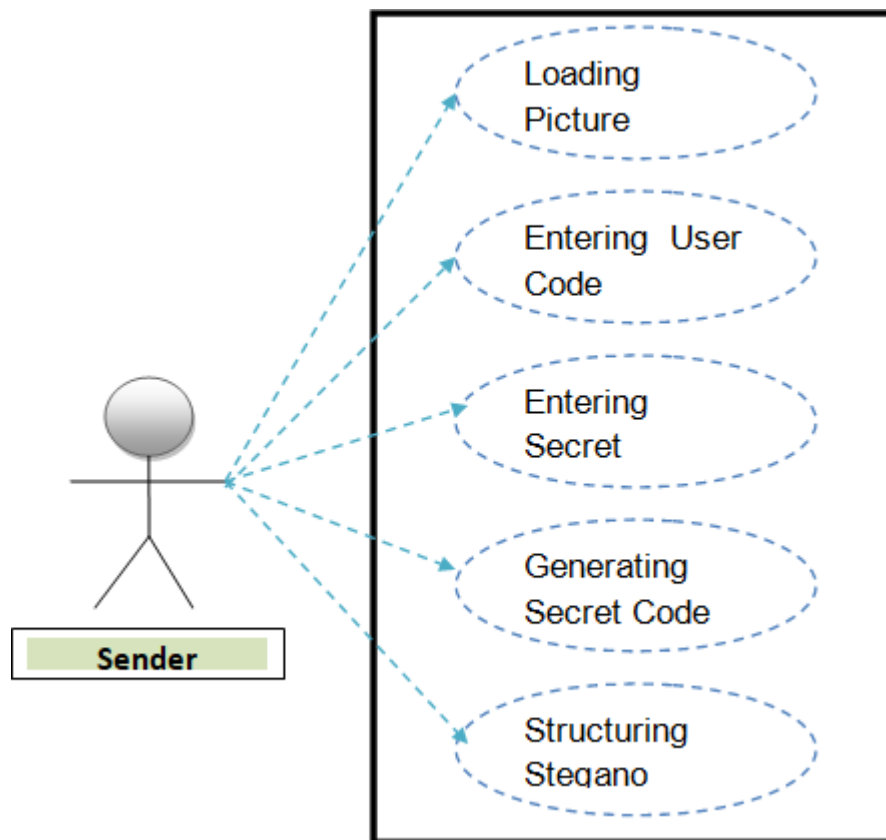


Figure of Usecase Diagram Model(Sender's End)

The receiver will start the process of decoding. In the wake of communicating the mystery data the recipient will get the picture including the mystery message. At that point the collector will begin the way toward breaking the scrambled message to get the first message. The cycle must experience the stegano medium first. The collector needs to enter the hid mystery code which was produced at the sender's end. Just on the off chance that the beneficiary is the approved individual, at that point he/she can unravel it utilizing the disguised mystery code to get the first mystery data, in any case the framework will show that the code he has entered isn't substantial.

This cycle is given in the figure 5.5 underneath.

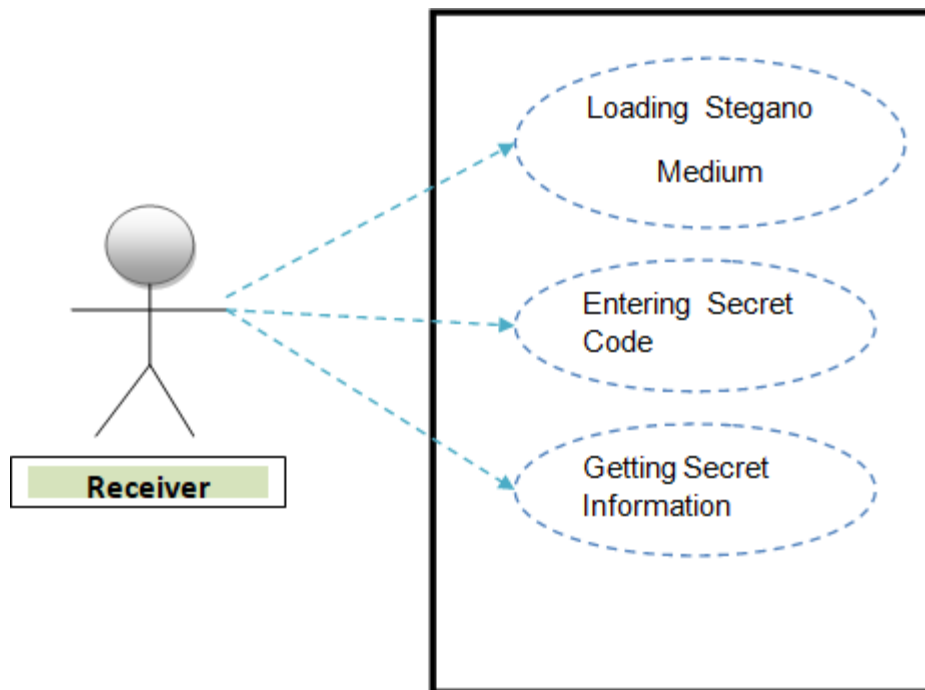


Figure of Usecase Diagram Model(Receiver's End)

Class Diagram

The user chooses to hide or break. if hide then its sender. If break then its receiver.

✓ Sender : Hides message

(User Code + Secret message + Cover image) → Stegano medium originated
Concealed secret code → The message is transmitted to the receiver.

The concealing process of the information begins with stacking the image where the given mystery data will be covered up. Give the client code and mystery information data. At that point subsequent to satisfying the stegano medium the hide or mystery code is created. In the wake of picking up the mystery code the finishing of the sender's side is finished.

✓ Receiver : Break message

Concealed secret code → Stegano medium decrypted the original message → The original secret data is gained.

Subsequent to communicating the mystery data the recipient will get the picture including the mystery message. At that point the recipient will begin the way toward breaking the scrambled message to get the first message. The cycle must experience the stegano medium . The beneficiary needs to enter the hid mystery code which was produced in the sender's end. Just on the off chance that the beneficiary is the approved individual, at that point he/she can unravel it utilizing the hid mystery code to get the first mystery data, in any case the framework will show that the code he has entered isn't substantial.

This process is given in the figure 5.6 below.

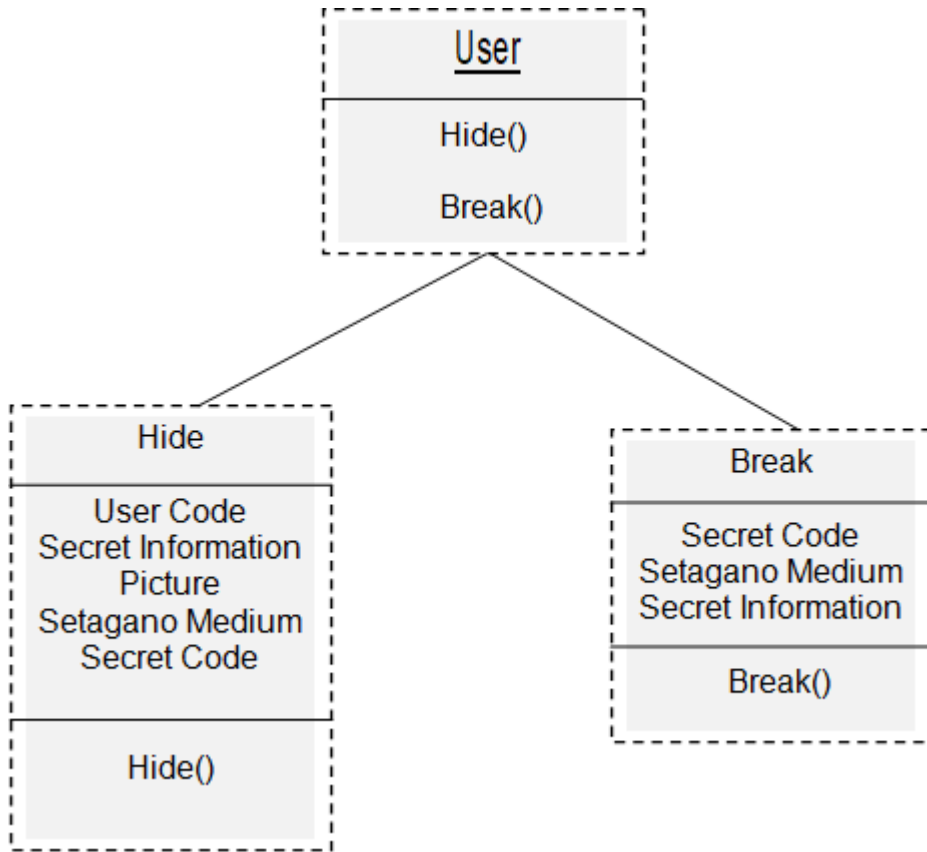


Figure of Class Diagram Model

Activity Diagram

Start → Start stegano application → Select operation

Hide :

- Load an image where the secret information or message will be hidden.
- Then give input of the user code
- A concealed secret code will be originated
- Stegano medium will be generated

So the process is, Load a picture where the mystery data or message will be covered up. At that point give contribution of the client code. A hid mystery code will be begun Stegano medium will be created

Break :

- The receiver will load the image
- The receiver has to enter the concealed secret code which was generated in the sender's end.
- The extraction of the secret information is completed.

So the breaking or decoding process will start. The receiver or collector will stack the picture. The collector needs to enter the hid mystery code which was produced at the sender's end. The extraction of the mystery data is finished.

This process is given in the figure 5.7 below.

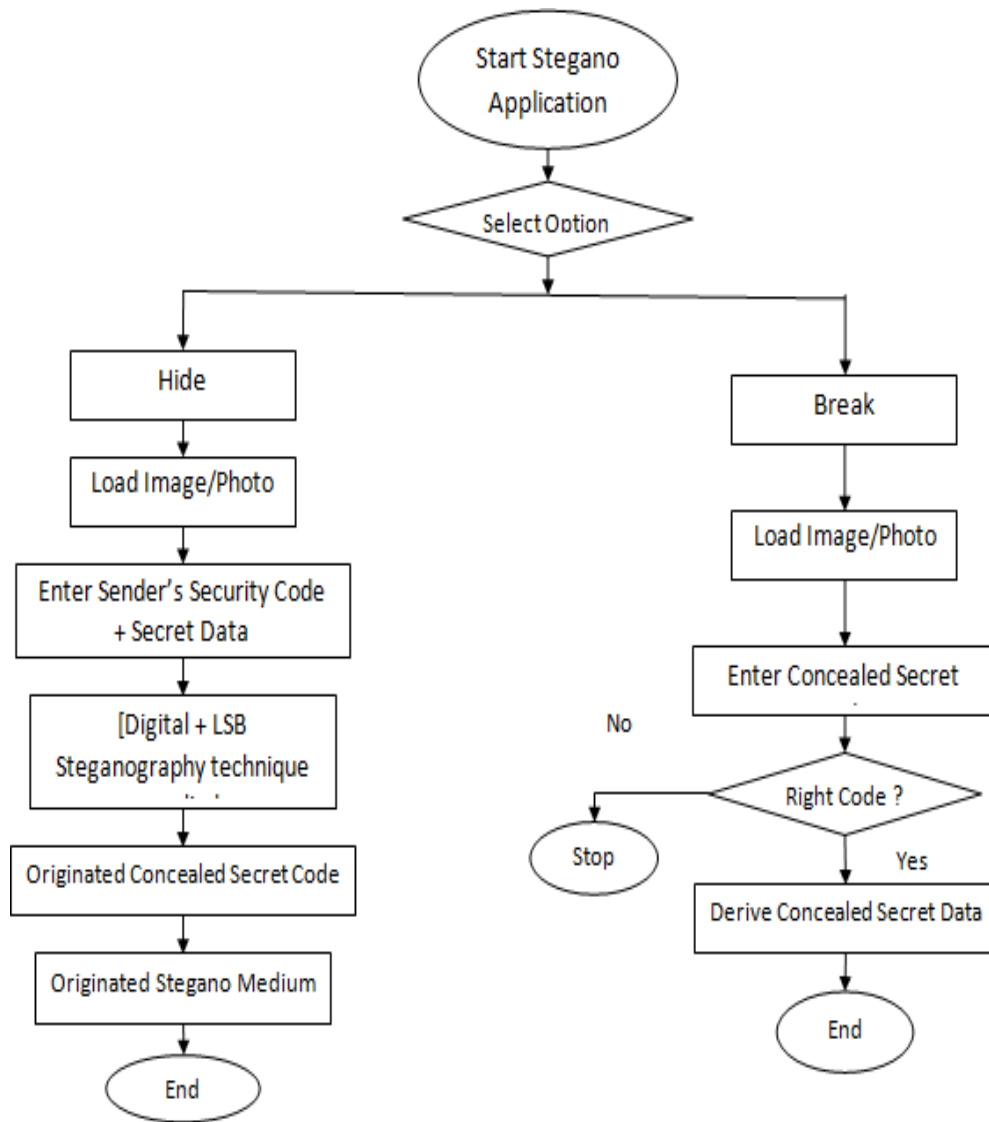


Figure of Activity Diagram Model

CHAPTER 6

IMPLEMENTATION AND TESTING

Implementation of the System

A java development kit (better if latest version) is needed for this project. This proposed project is accomplished utilizing Java. This project can be conducted in any operating system. In order to veil the original data one needs to perform the functionality of the sender's end program. In order to unveil the original data to get the concealed secret message one needs to perform the functionality of the receiver's end program.

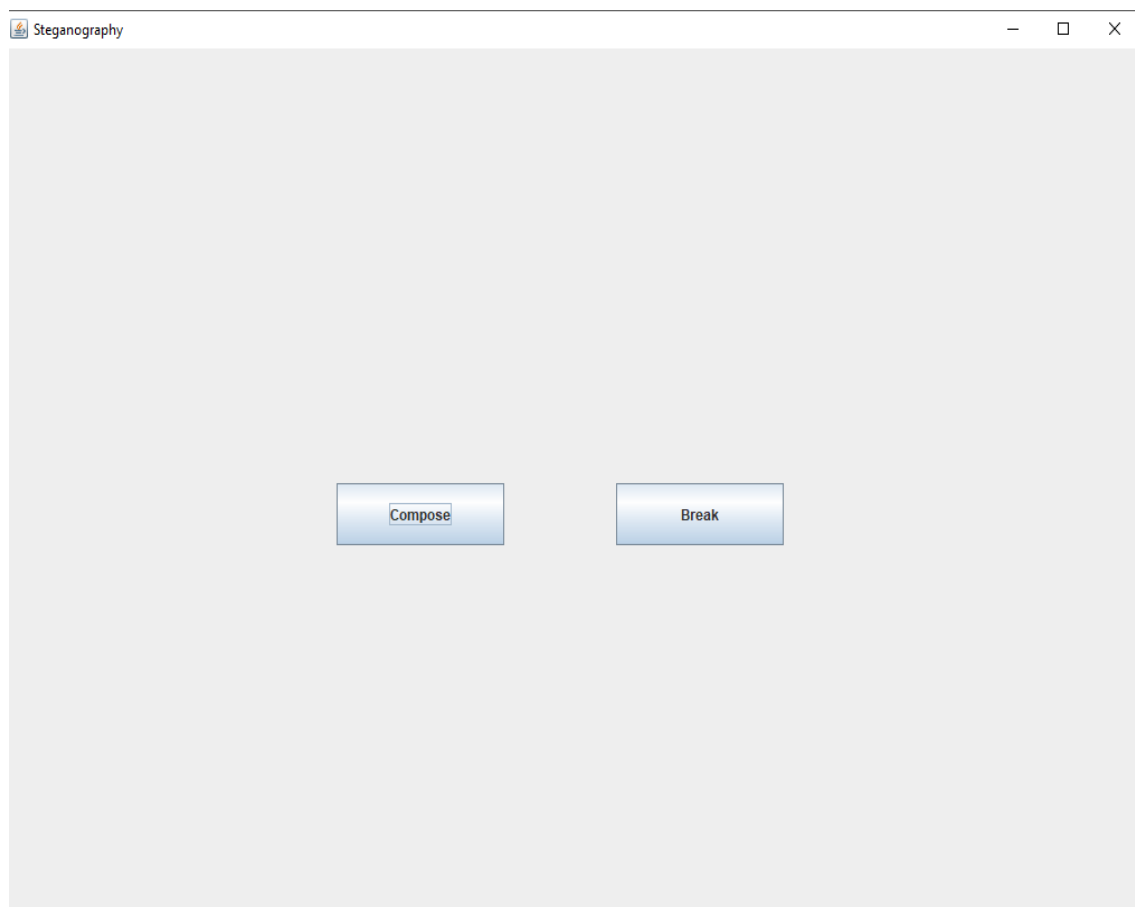
This proposed method of LSB and Digital Steganography inhibits the sender as well as the receiver end program. For the purpose of hiding data, users can utilize the sender's end program and for decoding the original message user can utilize the receiver's end program. To shroud information, clients can use the sender's end program and for translating the first message client can use the recipient's end program.

Result

Home Page View

The user will at first see the home page. The home page contains two buttons Compose and Break. If the user is a sender then he or she has to choose the button which is called “Compose”. After clicking Compose he or she will be able to do the information encoding. As the home page contains two buttons Compose and Break, so if the user is a receiver then he or she has to choose the button which is called “Break”. After clicking Break he or she will be able to do the information decoding which is sent from the sender.

The view is given below in figure 6.1

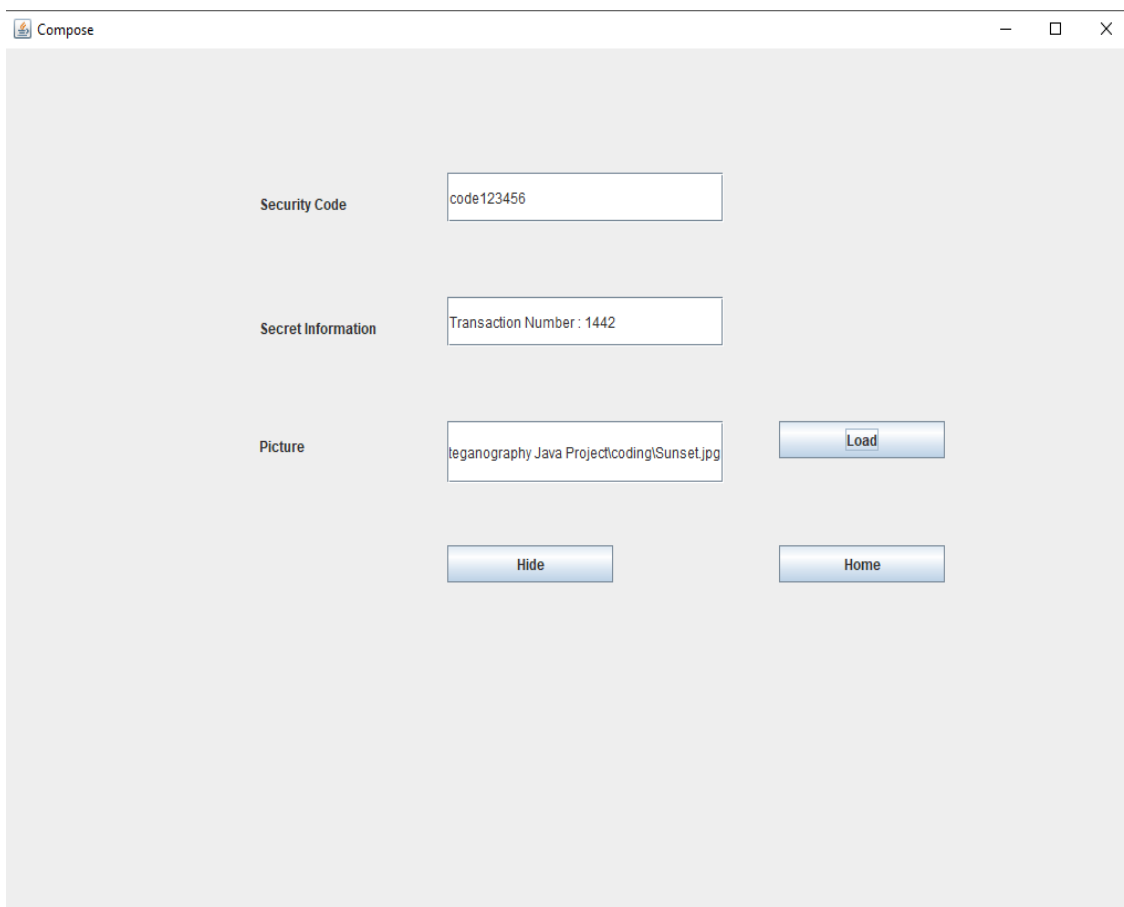


6.1 Figure of Home Page View

Input(Sender)

After clicking the button called “Compose” the will enter to the composing section. The sender will enter the inputs needed in this section in order to encrypt the information. Firstly he/she has to load the picture or image where the secret information will be hidden inside. The sender will enter a user code which is called a security code. Then the sender will give input of the secret information or message he/she wants to transmit to the receiver. Then he/she will click the button “Hide”. These are all the inputs a sender must have to fulfill in this section.

The view is given below in figure 6.2



The screenshot shows a window titled "Compose" with a light gray background. It contains three input fields and three buttons. The first input field is labeled "Security Code" and contains the text "code123456". The second input field is labeled "Secret Information" and contains the text "Transaction Number : 1442". The third input field is labeled "Picture" and contains the text "teganography Java Projectcoding\Sunset.jpg". To the right of the "Picture" input field is a blue button labeled "Load". Below the "Picture" input field are two blue buttons: "Hide" on the left and "Home" on the right. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

Figure of Input(Sender)

Generated Secret Code

After inputting all the required information when the sender will click “Hide”, a concealed secret code will be generated in that section. The secret code will be generated relating with the security code given as an input by the sender. The secret code will be needed while the decryption process of the original message will be performed by the receiver. Without knowing the generated secret code the receiver will not be able to decrypt the original information.

The view is given below in figure 6.3

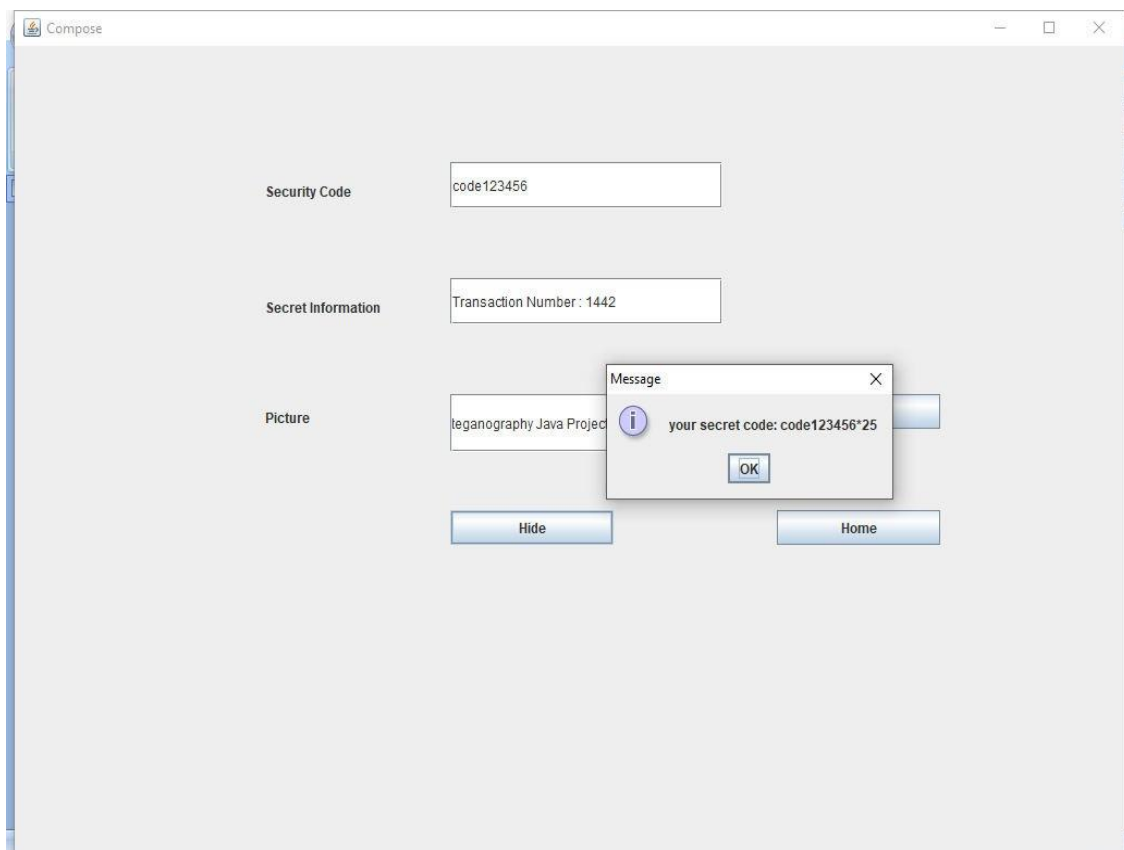


Figure of Generated Secret Code

Encrypted Message

After the process of fulfilling all the required information in that section and clicking hide, the secret information will be hidden in the image that was loaded by the sender. As the message is hidden inside the image no one can detect that there is a hidden information inside. The receiver will get the image but normally can not see the original information concealed inside that image. So, the secret message is hidden inside the image. So the message is encrypted finally.

The view is given below in figure 6.4

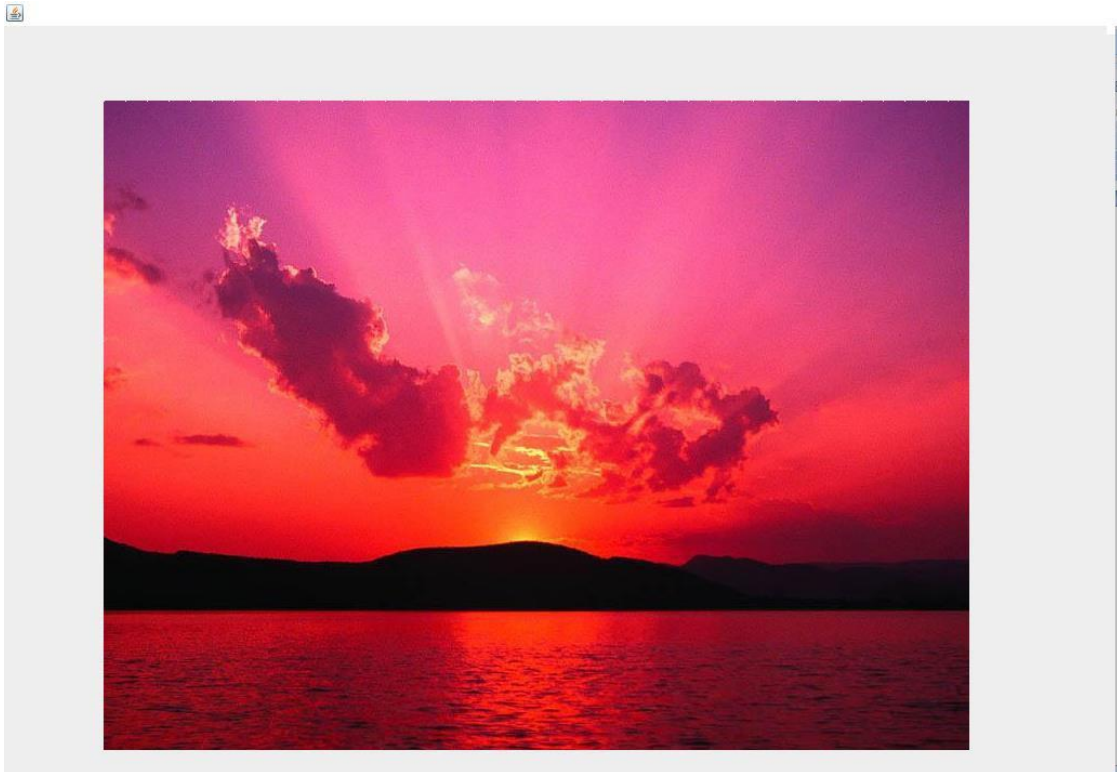
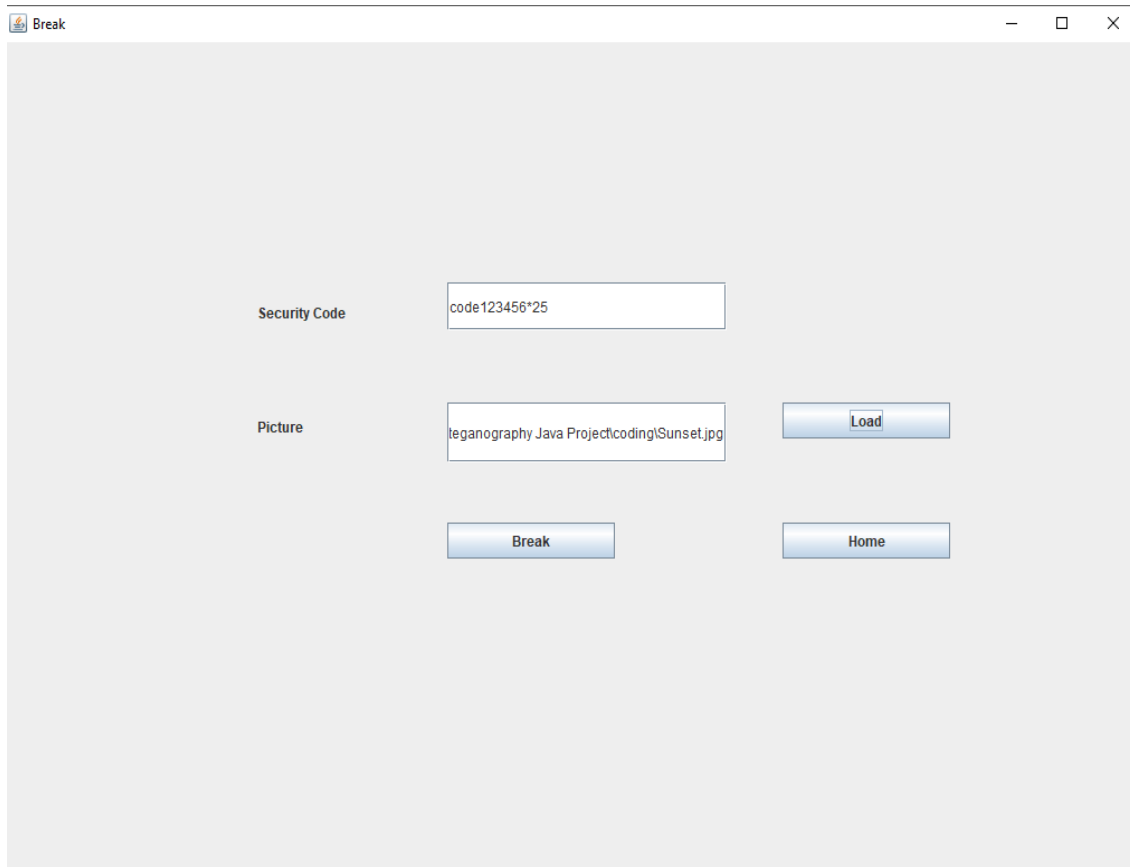


Figure of Encrypted Message

Input(Receiver)

The image will be transmitted to the receiver. Then the receiver will get to see the image but he will not be able to see the real message hidden underneath the cover image. Then the user/receiver will click “Break”. For getting the original information he/she needs to fulfil all required information in that section. The receiver will enter the inputs needed in this section in order to decrypt the information. The receiver will load the image, then, the receiver has to enter the concealed secret code which was generated in the sender’s end. After completing all the processes the receiver will click “Break”. Finally the extraction of the secret information will be complete.

The view is given below in figure 6.5



The screenshot shows a web application window titled "Break" with a standard Windows-style title bar (minimize, maximize, close buttons). The main content area is light gray and contains the following elements:

- A label "Security Code" followed by a text input field containing the text "code123456*25".
- A label "Picture" followed by a text input field containing the file path "teganography Java ProjectcodingISunset.jpg".
- A blue button labeled "Load" positioned to the right of the "Picture" input field.
- A blue button labeled "Break" positioned below the "Security Code" input field.
- A blue button labeled "Home" positioned below the "Picture" input field.

Figure of Input(Receiver)

Output Result

Completing the process of giving input of all the required information and clicking to break the decoded message will be shown. If the input of concealed secret code entered by the receiver is perfectly correct only then the system will showcase the original secret message hidden inside the particular picture. The message is the final output result of the whole process.

The view is given below in figure 6.6

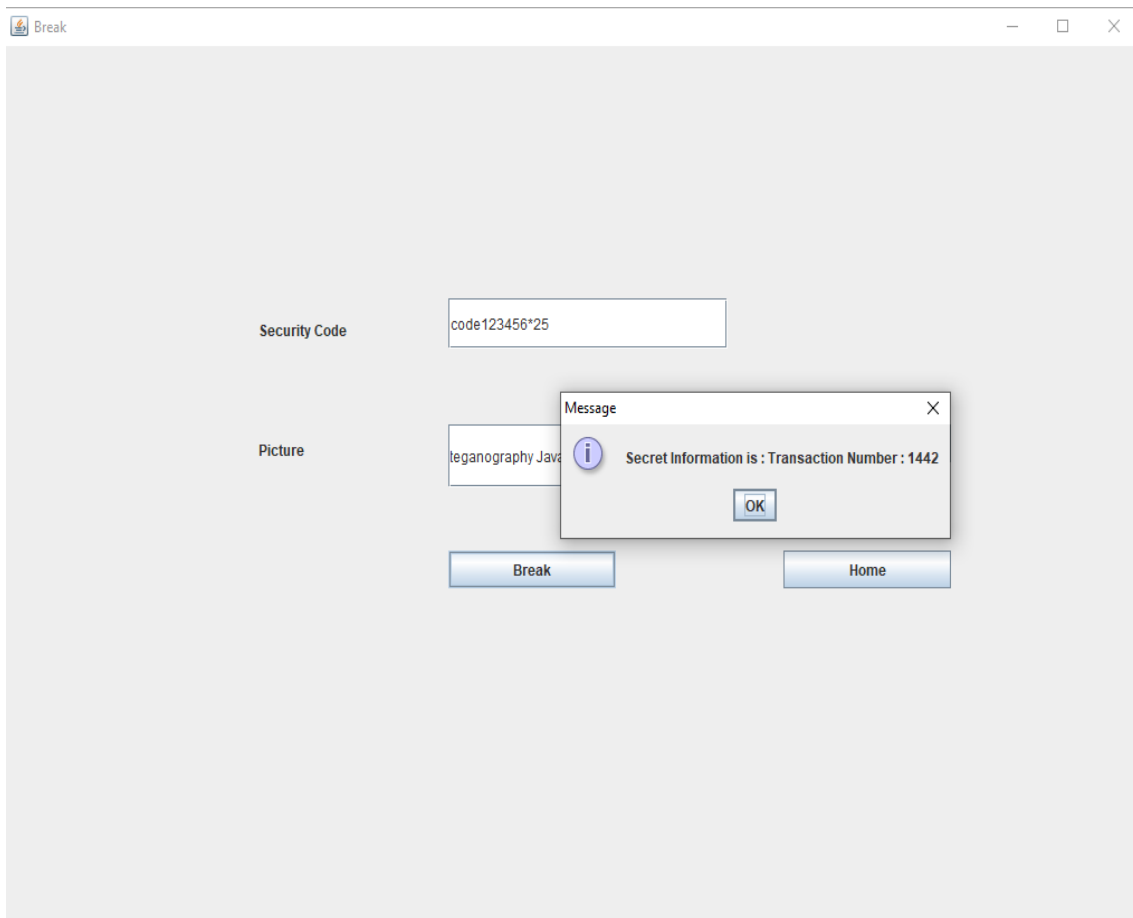


Figure of Output Result

Invalidation(Wrong Code)

After getting the cover image and fulfilling the required sections which enter the secret code generated in the sender's side the system will showcase invalidation in one case. If the input of concealed secret code entered by the receiver is wrong then the system will declare that "code you entered is not valid". So, for getting the original secret information the receiver must need to enter the real secret code otherwise the system will display invalidation.

The view is given below in figure 6.7 and 6.8

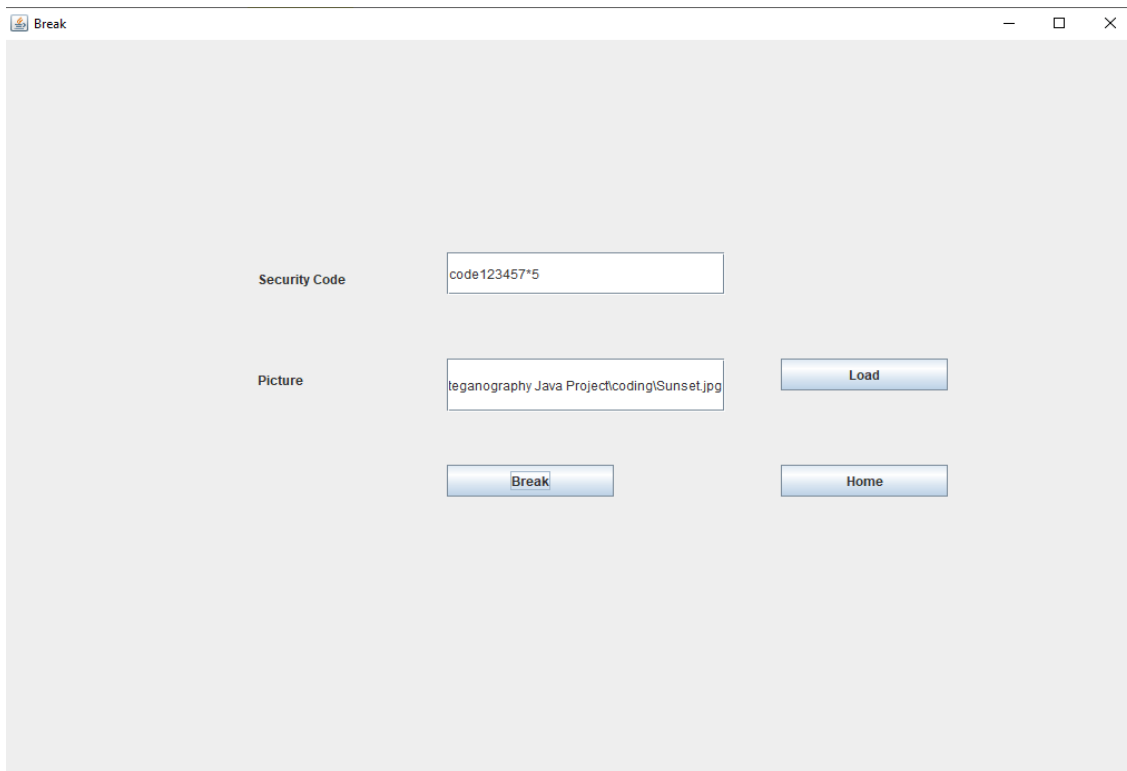


Figure of Wrong Input(Receiver)

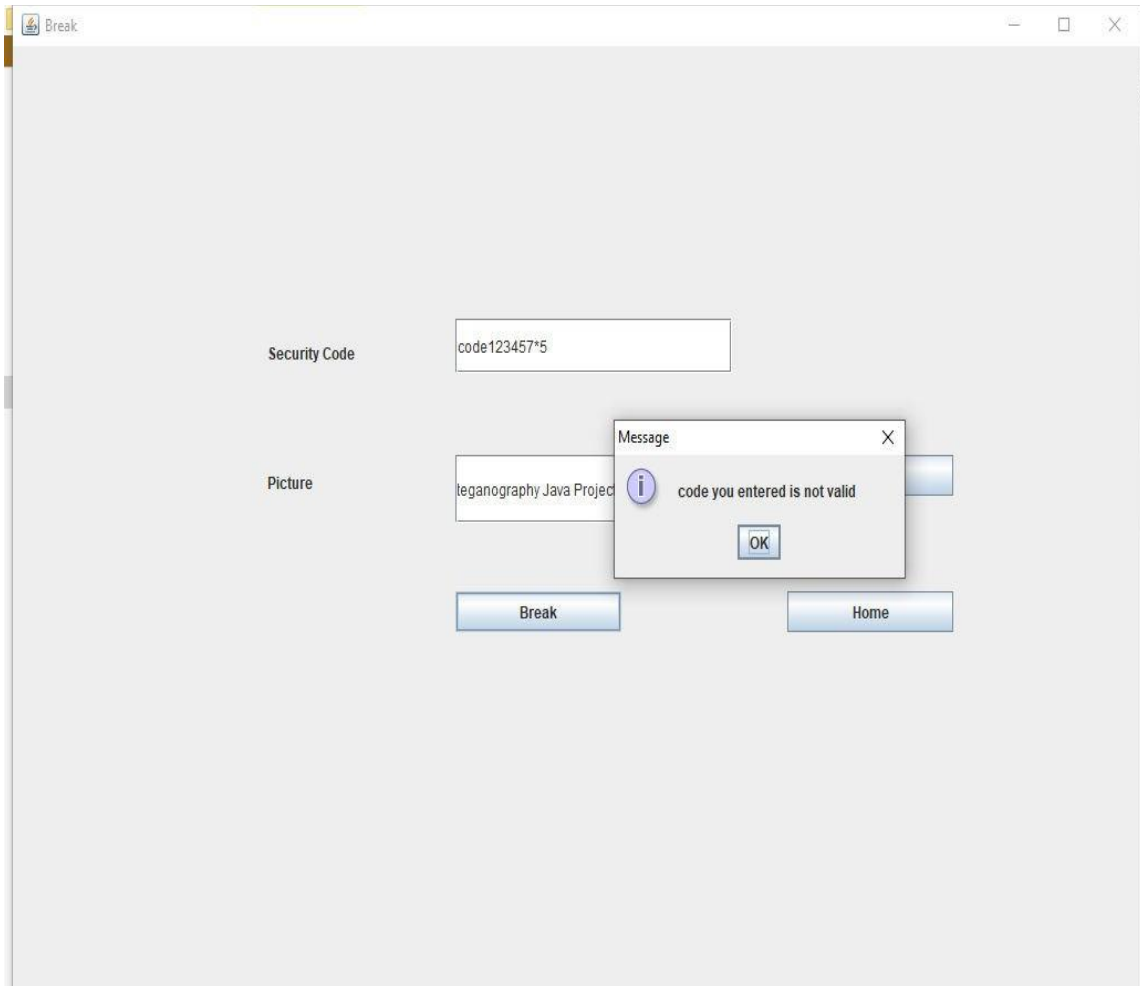


Figure of Invalidation

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

Discussion and Conclusion

In our proposed theory we have implemented LSB and Digital Steganography encryption techniques. The encryptions are used which will ascertain solitude and genuineness. This method will protect information under image based encryption to protect sensitive information and prevent fraud. This implemented method will be immensely effective for users. By using this methodology we will create a better-globalized world by exchanging money securely.

Scope for Future Development

Future endeavors our project:

- Implementation of a better version of steganography with cryptosystem.
- Our work will be more secure as here we will increase more security steps..
- The methodology can be implemented in different sectors of the security system by ensuring the data is highly intact.
- The way of further research is widespread.

APPENDIX

As the greater part of the individuals of Bangladesh or in any low pay nation have trust issues on having an exchange through online in view of the dread of getting hacked of their cash or individual data on the online stage. The individuals with low pay significantly, can't accumulate the fearlessness to do as such. To tackle this difficulty we have come up with this work plan for a reliable exchange measure. Making a framework plan for immensely secure online exchanges. Profoundly encoded information with two degree validation. Motivating a person to trust and utilize the web exchange framework in a low pay nation. Making the exchange cycle simpler with appropriate security. Execution of a superior rendition of LSB and Digital steganography. As the security framework is as yet under cycle, our work will be safer as here we have utilized the hybrid steganography. Both the techniques have been utilized so the client will discover information all the more rapidly yet will be a difficult occupation for the programmer. In future we will attempt to actualize RSA diversely to make various codes utilizing hash. The methodology can be executed in various areas of the security framework by guaranteeing the information is exceptionally unblemished. The method of additional exploration is broad.

REFERENCES

- [1] Ezeofor C. J., Ulasi A. G.” Analysis of Network Data Encryption & Decryption Techniques in Communication Systems” International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014.
- [2] Kuswaha, Shashikant, Sachin Waghmare, and P. Choudhary. "Data Transmission using AES-RSA Based Hybrid Security Algorithms." International Journal on Recent and Innovation Trends in Computing and Communication 3.4 (2015): 1964-1969.
- [3] Sankalp Jagga and Puneet Sharma on “Banking Authentication Technique” International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1305-1314 © International Research Publications House <http://www.irphouse.com>
- [4] Willeby, Tandy. "Online ATM transaction with digital certificate." U.S. Patent Application No. 10/375,290.
- [5] Gupta, Shailender, Ankur Goyal, and Bharat Bhushan. "Information hiding using least significant bit steganography and cryptography." International Journal of Modern Education and Computer Science 4.6 (2012): 27.
- [6] Akolkar, Swati, et al. "Secure Payment System using Steganography and Visual Cryptography." International Journal of Computing and Technology 3.1 (2016): 58-61.