**DIGITAL STEGANOGRAPHY**

**MCA36 MINI PROJECT USING**

**JAVA AND DBMS CONCEPTS**

A Project Report submitted in partial fulfillment of the requirements for the award of degree of

**MASTER OF COMPUTER APPLICATIONS**

An Autonomous Institution Affiliated to VTU

Submitted by

**SANDIP LAHA**

(**USN:** 1NH17MCA28)

3rd Semester MCA

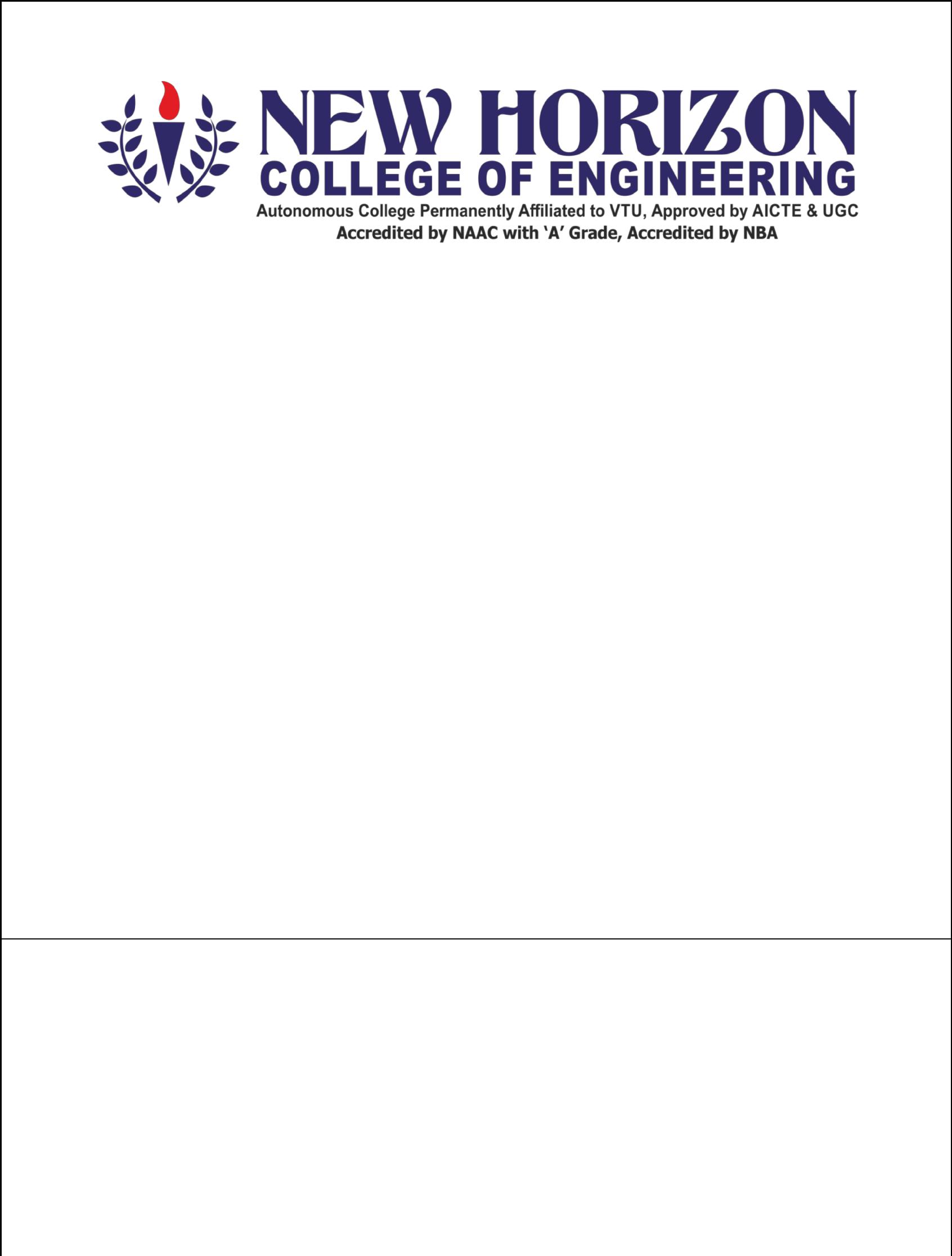
Under the Guidance of

**Dr. A.P. NIRMALA**

**ASSOCIATE PROFESSOR**



**DEC 2018**



**DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS**

**CERTIFICATE**

This is to certify that **SANDIP LAHA (USN:1NH17MCA28)** has successfully completed his Third Semester **Mini Project using** **Java and DBMS Concepts (MCA36)** entitled“**Digital Steganography**” as a partial fulfillment for the award of Master ofComputer Applications degree, during the academic year 2018-2019.

**PROJECT GUIDE** **HEAD OF THE DEPARTMENT**

**VIVA-VOCE**

**EXTERNAL EXAMINER** **INTERNAL EXAMINER**

**DECLARATION**

I, **SANDIP LAHA**, student of 3rd Semester MCA, New Horizon College of Engineering, bearing **USN** -**1NH17MCA28** hereby declare that **Mini Project using JAVA and DBMS Concepts** entitled“**DIGITAL STEGANOGRAPHY“** has been carried out by me under the guidance of **Dr. A.P. NIRMALA, Associate Professor**, Department of MCA which issubmitted for partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications during the academic year **2018-2019**. This report has not been submitted to any other Institutionor University for any award of degree.

**Name:**

**Signature:**

**Date :**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** |  | **TABLE OF CONTENTS** | **PAGE NO** |
| **1.** | **INTRODUCTION** | | **1** |
|  | 1.1 | Project Description | **1** |
| **2.** | **LITERATURE SURVEY** | | **2** |
|  | 2.1 | Existing System | **2** |
|  | 2.2 | Proposed System | **2** |
|  | 2.3 | Tools and Technologies used | **3** |
| **3. HARDWARE & SOFTWARE REQUIREMENTS** | | | **3** |
|  | 3.1 | Software Configuration | **3** |
|  | 3.2 | Hardware Configuration | **4** |
| **4.** | **SYSTEM DESIGN ARCHITECTURE** | | **4** |
|  | 4.1 | Module Description | **4-6** |
|  | 4.2 | Data Flow Diagram | **7-8** |
| **5.** | **IMPLEMENTATION** | | **9** |
|  | 5.1 | Screen Shots | **9-18** |
|  | 5.2 | Sample Coding | **19-27** |
| **6.** | **SOFTWARE TESTING** | | **28-29** |
| **7.** | **CONCLUSION** | | **30** |
| **8. FUTURE ENHANCEMENTS** | | | **30** |
| **9.** | **BIBLIOGRAPHY** | | **31** |
| **10. APPENDICES** | | | **32** |
|  | 10.1 | Plagiarism Certificate | **32-33** |

DIGITAL STEGANOGRAPHY 1NH17MCA28

1. **INTRODUCTION**

Steganography, the word came from Greek word steganos, which means covered or secret, and the word graphy, it means writing or drawing. Steganography is the process or art of hiding (writing or drawing) secret information in some other information. It is to be written in such a way that only the intended recipients will be known about the existence of the message or information. Secrecy is very important to maintain in a large organization because as we know nowadays hackers become more intelligent and it becomes tedious.

1.1 PROJECT DESCRIPTION

In order to hide the information, many different carrier files format can be used, but images are the best because of their frequency on the internet. Although we have cryptography to transmit the secret messages, sometime it will give suspicion to the hackers and also it affects unintended users.

So to overcome the problem of cryptography, our project ‘Digital Steganography’ has built. In our project, we use multimedia data as an image as a covering medium. We can add or extract our secret information into or from the media. Also, we can send the message easily to other systems without any suspicion to others. The receiver only is known about the information’s existence in the image and about the decryption idea.

The secret information can be hidden in an image file.

Encryption of the same message is done in the image file.

Retrieval of the message can also possible by decrypting the message.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 1 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**2. LITERATURE SURVEY**

2.1 EXISTING SYSTEM

Here As we stated cryptography can be used only in the situation where the message clearly was written and it also can be shown to others, but only the meaning of the message is obscured. Therefore the effective hackers might identify the meaning of the message which we don’t want to happen. So in the existing system maintaining secrecy will be very risky. Cryptography and Steganography can be used together or separately.

2.2 PROPOSED SYSTEM

In Digital Steganography, we overcome the problem of Cryptography that gives a solution to transfer secret information without any knowledge of the unintended user.

By using steganography we can easily hide the message in an image which can’t be distinguishable from the original one, so we can easily exploit the human perception.

Here we use an image as a multimedia medium to encrypt the secret information. As we know the primary goal of steganography is to hide a secret information in

some other data. So when we encrypt or decrypt the secret information we will always use a password.

**Features of proposed system:**

It is very user-friendly for the intended user.

As we develop this project in Java, so it is platform independent. The Flexibility of this project is very high.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 2 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

2.2 TOOLS AND TECHNOLOGIES USED

Language

Front End

Back End

: JAVA

: Eclipse IDE Photon

: Least Significant bit (LSB) and Triple data

Encryption Standard (3DES)

**3. HARDWARE & SOFTWARE REQUIREMENTS**

3.1 SOFTWARE CONFIGURATION

Operating system

: Windows / Linux / Solaris

Front end

: Java (jdk1.4.1 and above)

IDE

: Eclipse Photon

Language used

: Java Programming

Documentations

: MS Word, Notepad

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 3 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

3.2 HARDWARE CONFIGURATION

Processor

Hard disk capacity

Display card

Screen

Input Device

: Intel® Core™ i3-5200 1.4 GHz

: 80GB or more

: Intel® 512MB

: 15.2” color

: Keyboard and mouse etc.

Output Device

: Monitor and printer

**4. SYSTEM DESIGN ARCHITECTURE**

4.1 MODULE DESCRIPTION

The project consists of mainly five modules.

4.1.1 Login: -

The user has to give a proper username and password, in order to get in the system. By giving only the correct username and password one can start the process of hiding information and encrypt the information. If the username and password are incorrect then it will show an error message.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 4 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

4.1.2 Encryption: -

Encryption requires a medium or a file encrypting. It means it will cover the secret information in the covering medium. It will be done only by giving a secret password, which provides the security while converting the message. Therefore it will be difficult for hackers to decrypt. So as it is password protected while retrieving the message, the retriever has to give the correct password to get the secret information.

4.1.3 Decryption: -

Decryption requires a medium or a file decrypting. It means it requires the image that has already been encrypted. While decrypting the user has to enter the secret password. After providing the password and browsed the image user can decrypt the secret message that was encrypted. So without any knowledge of the unintended user, we can decrypt the information in this module.

4.1.4 Send Image: -

If you want to send the image to any other system, so you can do this by establishing a proper connection with both the sender and receiver. The receiver system’s IP address can be used to send the secret media. That we will use for future enhancements.

4.1.5 Exit: -

After completion of all the upper modules or at any time you can exit from the system by using the exit module.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 5 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**Algorithm Explanation**

**Making Encryption Medium:-**

Step 1: Start Digital Steganography System.

Step 2: Choose the Encryption Medium.

Step 3: Browse the source medium (Image file) from the system.

Step 4: Create user defined password for secure the message.

Step 5: Hide secret information by saving the file in your system.

Step 6: Stop the Encryption process.

**Decryption of the secret information from stegano medium:-**

Step 1: Start the Decryption Medium.

Step 2: Browse the source medium (Encrypted Image file) from the system.

Step 3: Enter the Secret Code to get the secret information that had used during Encryption.

Step 4: Extract the given message from Stegano Medium.

Step 5: Stop the Decryption Process.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 6 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

4.2 DATA FLOW DIAGRAM

Data flow diagrams originated with Chris Gane and Trish Sarson in 1979, who popularized the technique for structured analysis and design. Edward Yourdon and Tom DeMarco introduced another method in the 1980s which used circles instead of rounded rectangles to denote processes and which became popular.

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. A DFD is often used as a preliminary step to create an overview of the system without going into great detail, which can later be elaborated.

In our project, we have two part under the DFD

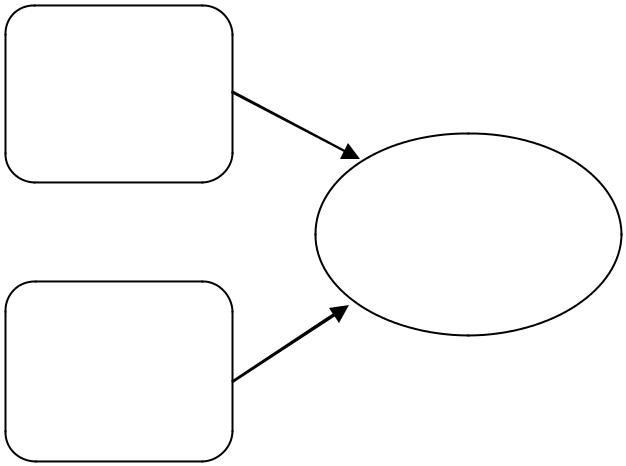
4.2.1 Information Storage: - In information storage, we need to encrypt the secret information in the image file. By giving a particular password, which will be known only by the intended user.

4.2.2 Information Retrieval: - In information retrieval, we need to decrypt the secret information from the existing encrypted message. Here we have to give that particular password that has been given at the time of encryption.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 7 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

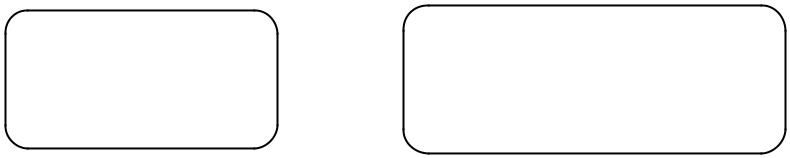
Information Storage



Multimedia

data(Image

file)



Stego

Medium

Secret

Password

Encoded Information

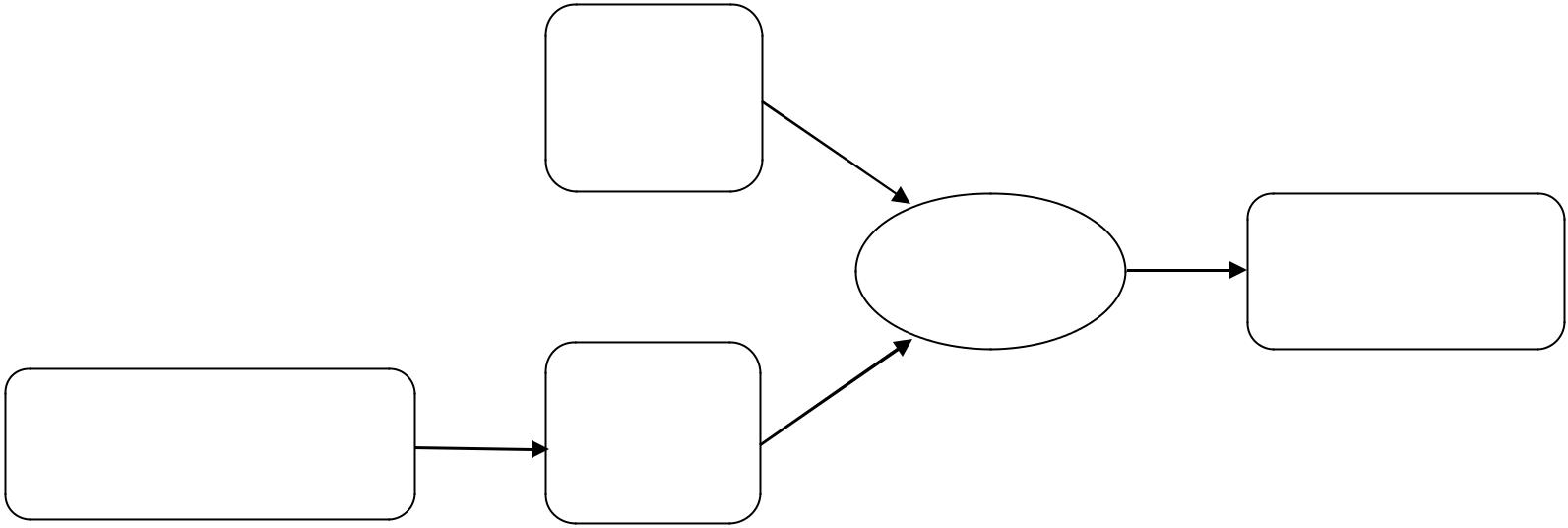
for Storage

Secret

Information

Fig no.4.2.1 Information Storage

Information Retrieval



Multimedia

Data

|  |  |  |
| --- | --- | --- |
| Stego | Information |  |
|  |  |
| Medium | Retrieved |  |
|  |  |

Secret

|  |  |  |
| --- | --- | --- |
| Encoded Information from |  |  |
| Storage | Password |  |
|  |  |

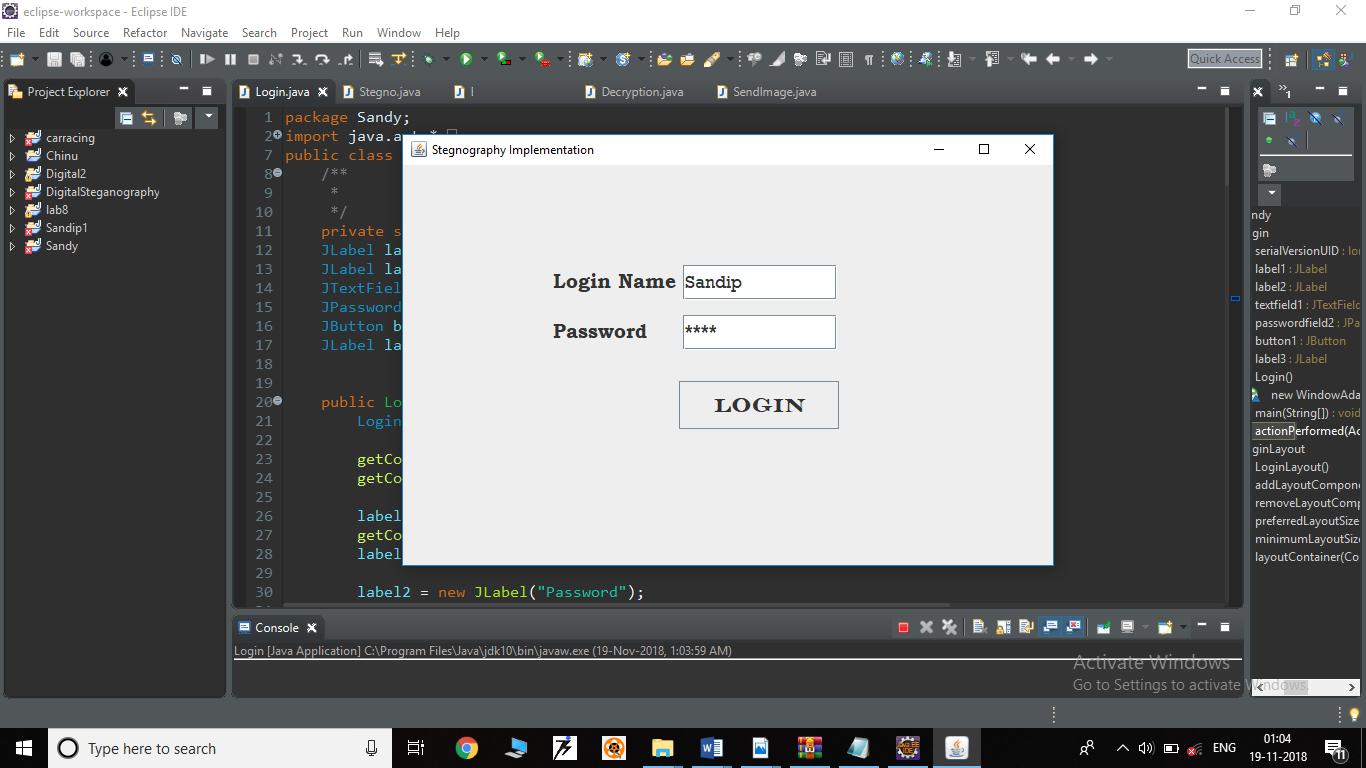
Fig no.4.2.2 Information Retrieval

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 8 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**5. IMPLEMENTATION**

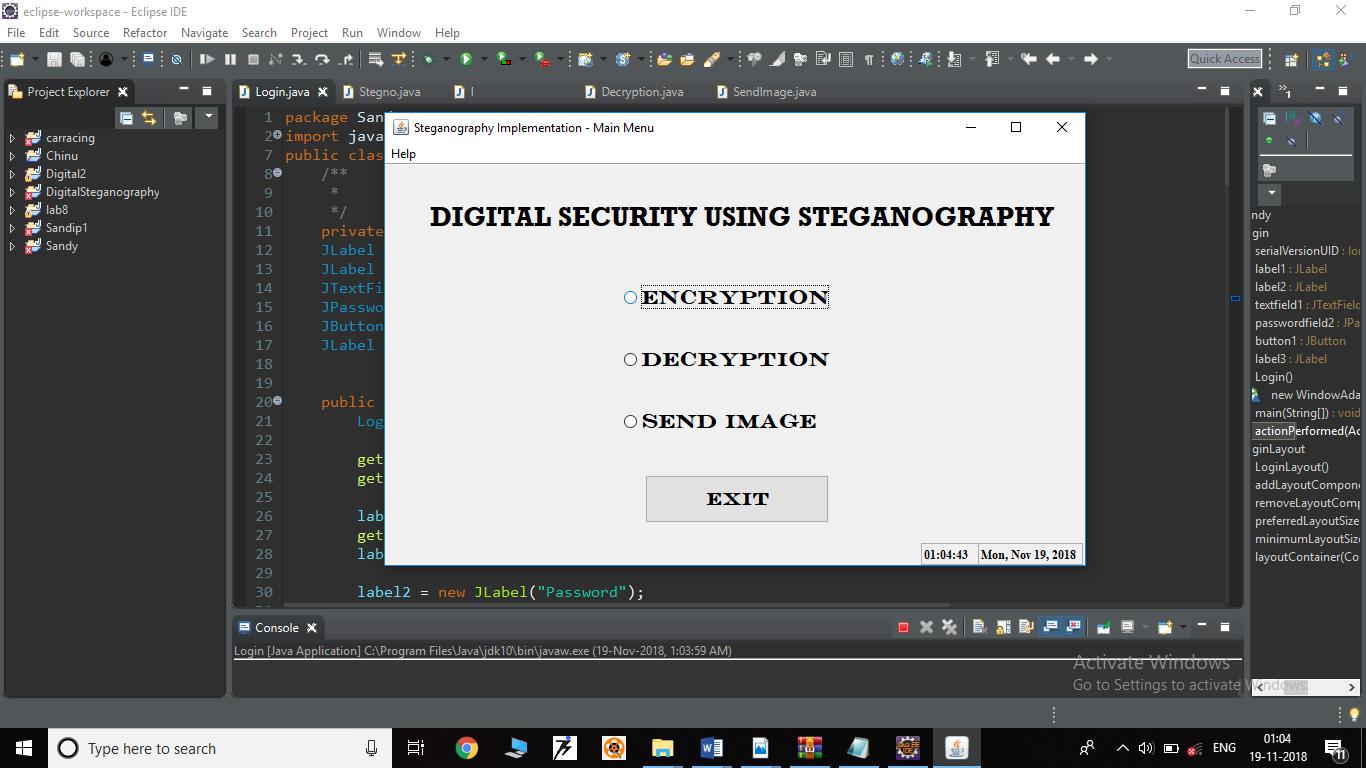
5.1 SCREEN SHOTS



The Login page allow you to enter into the system, It requires proper username and password.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 9 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

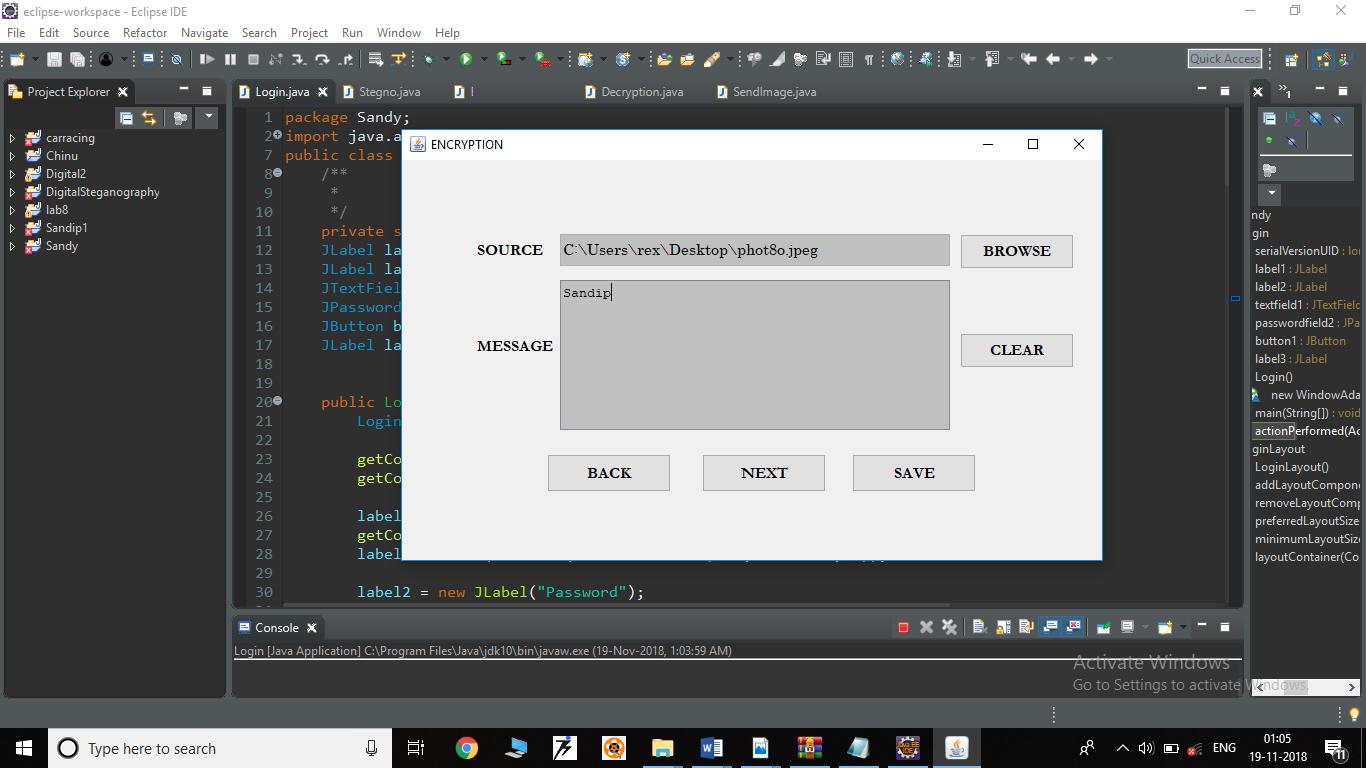


After successfully login we get the Home page of our project.

It has three option like Encryption, Decryption and Send Image button. We can select any one of this and can perform the corresponding operation.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 10 |

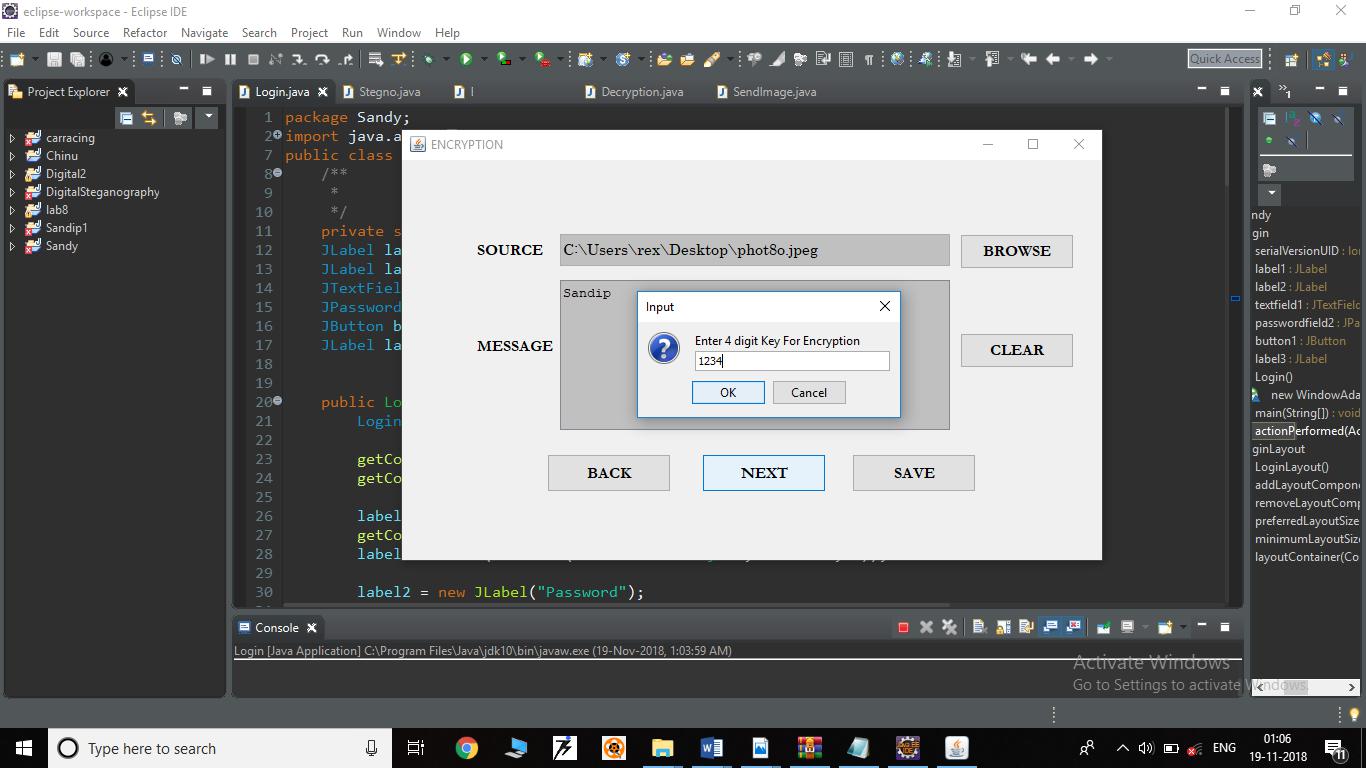
DIGITAL STEGANOGRAPHY 1NH17MCA28



In Encryption module we need to select source as an image from the system, then we have to type our secret messages for encryption.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 11 |

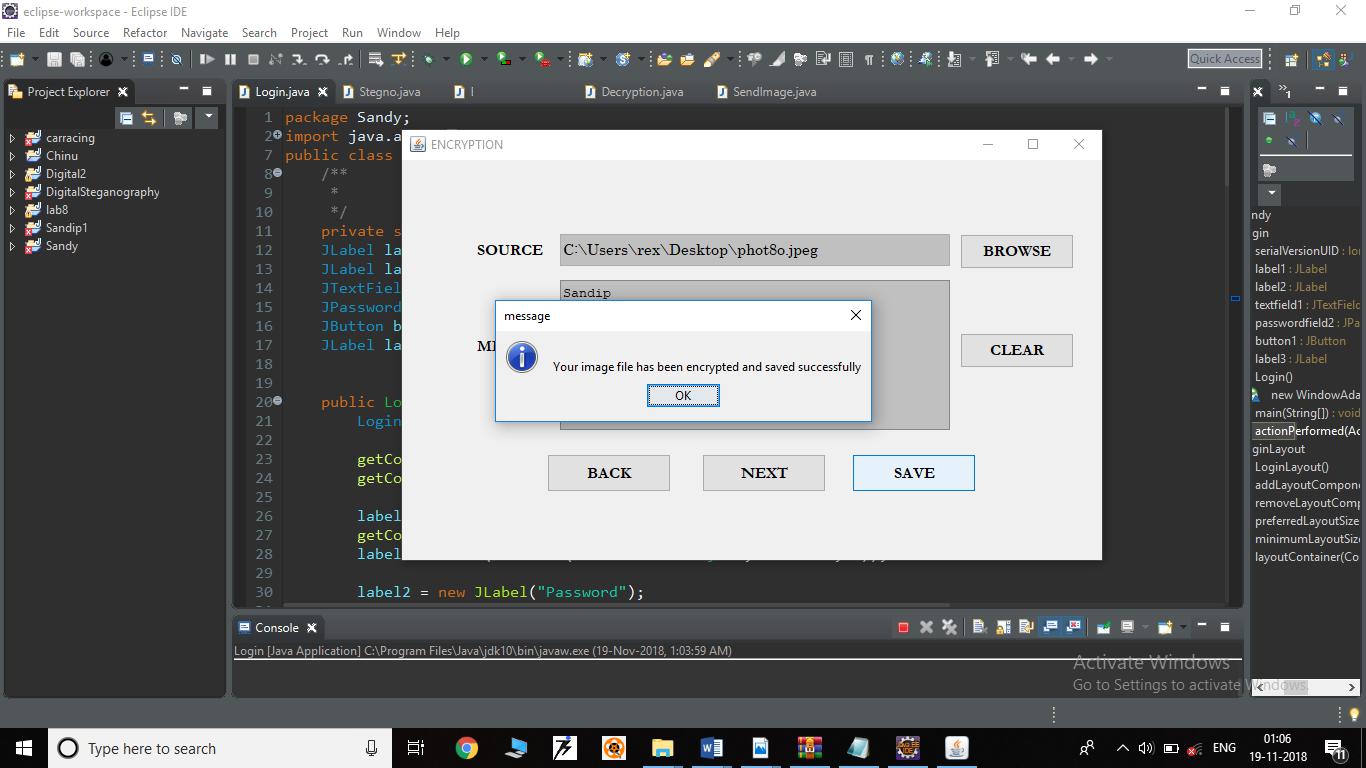
DIGITAL STEGANOGRAPHY 1NH17MCA28



Here it will ask a secret password that we have to give for more security purpose, which will only know by the intended user.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 12 |

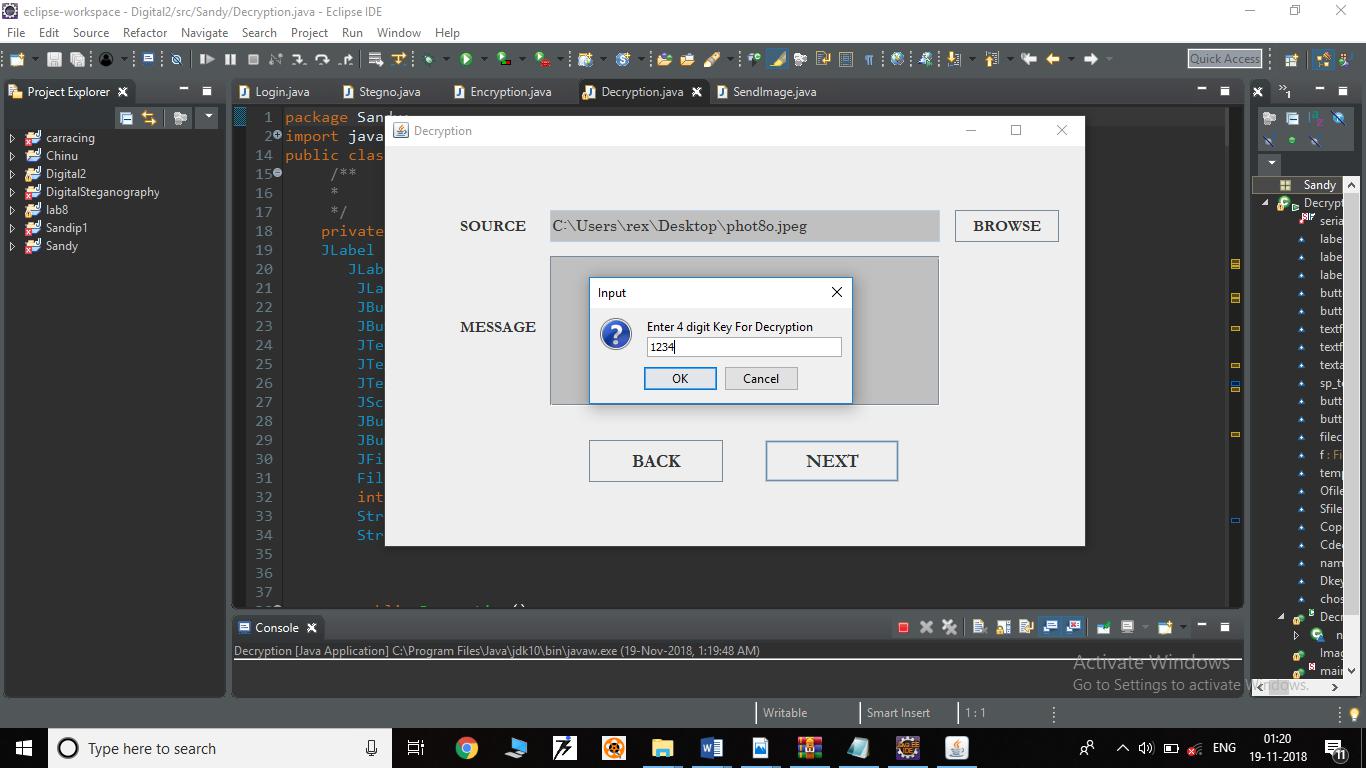
DIGITAL STEGANOGRAPHY 1NH17MCA28



After providing password your image will be encrypted and at will show a message of successfully saved image.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 13 |

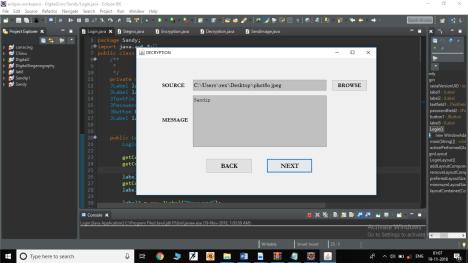
DIGITAL STEGANOGRAPHY 1NH17MCA28



At the receiver end the user need to give the same password as given at the time of encryption. Therefore it will enter into the decryption process.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 14 |

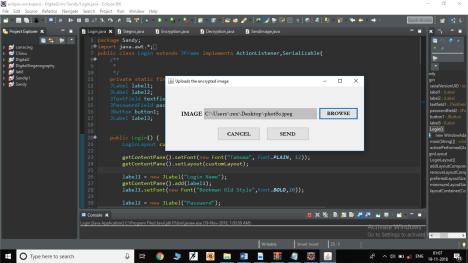
DIGITAL STEGANOGRAPHY 1NH17MCA28



Here you need to select the encrypted image to decrypt, so you will get the secret code send by the sender.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 15 |

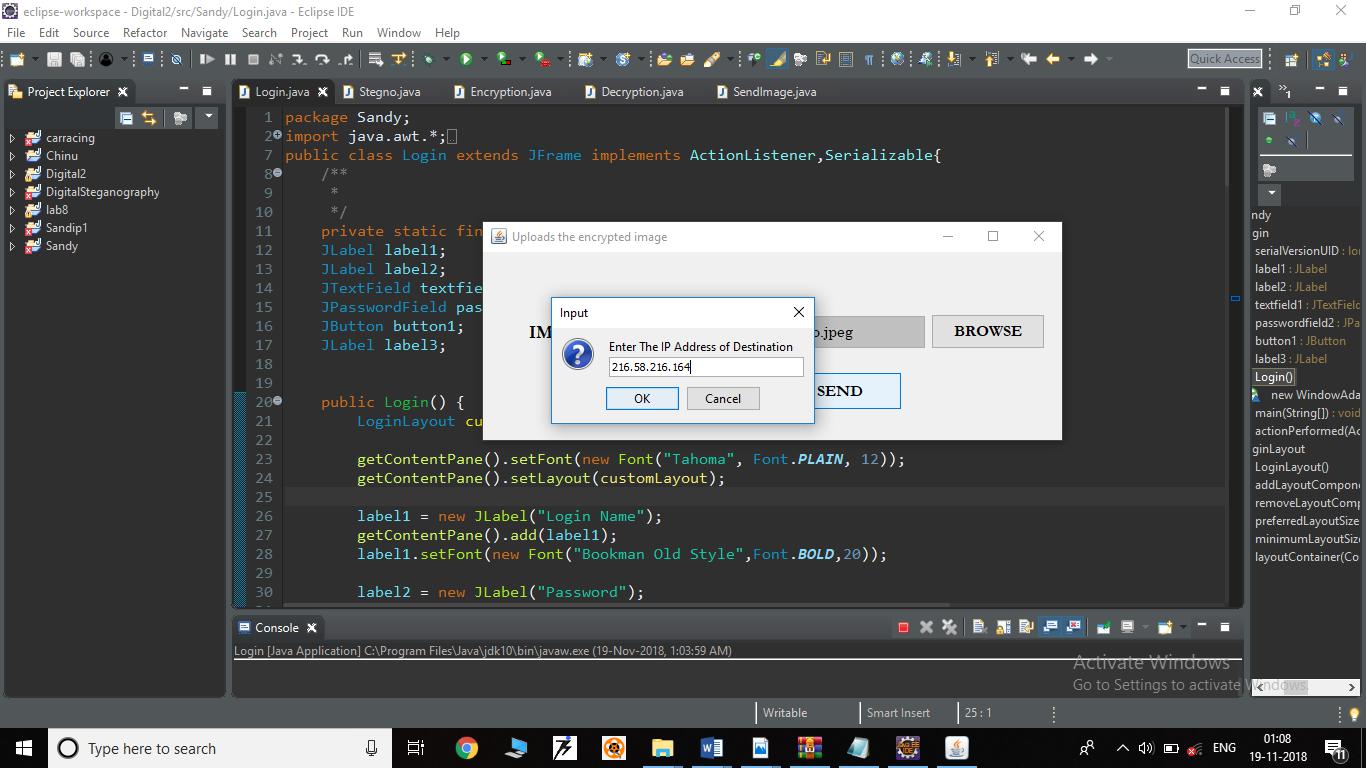
DIGITAL STEGANOGRAPHY 1NH17MCA28



In future, we can send the image to another system by establishing secure connection or using IP address of the particular system.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 16 |

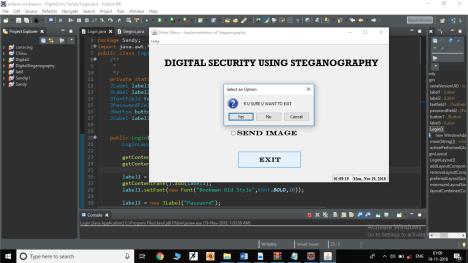
DIGITAL STEGANOGRAPHY 1NH17MCA28



By giving the address you can send the image to another system.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 17 |

DIGITAL STEGANOGRAPHY 1NH17MCA28



Final module is to exit from the system.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 18 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

5.2 SAMPLE CODING

/\* Making Stegano Medium\*/

import java.awt.\*;

import java.awt.event.\*;

import javax.swing.\*;

import java.util.\*;

import javax.swing.Icon;

import java.lang.\*;

import java.util.\*;

import java.text.\*;

import javax.swing.Icon;

import java.awt.event.ActionListener;

import java.awt.event.ActionEvent;

import java.io.Serializable;

public class Stegno extends JFrame implements ActionListener,Serializable{ JLabel label1;

ButtonGroup cbg;

JRadioButton radio1;

JRadioButton radio2;

JButton button1;

JTextField timeField;

JTextField dateLongField;

JMenuBar menuBar=new JMenuBar();

JMenuItem TopicsItem=new JMenuItem("Topics"); JRadioButton radio3;

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 19 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

public Stegno(){

StegnoLayout customLayout = new StegnoLayout();

getContentPane().setFont(new Font("Helvetica", Font.PLAIN, 12)); getContentPane().setLayout(customLayout); //getContentPane().setBackground(Color.LIGHT\_GRAY);

label1 = new JLabel("DIGITAL SECURITY USING STEGANOGRAPHY"); getContentPane().add(label1);

label1.setFont(new Font("RockWell", Font.BOLD, 27));

cbg = new ButtonGroup();

radio1 = new JRadioButton("ENCRYPTION", false);

cbg.add(radio1);

getContentPane().add(radio1);

radio1.setFocusable(true);

radio1.setRolloverEnabled(true);

radio1.setVerifyInputWhenFocusTarget(true);

radio1.addActionListener(this);

radio1.setFont(new Font("Engravers MT", Font.BOLD, 20));

radio2 = new JRadioButton("DECRYPTION", false);

cbg.add(radio2);

getContentPane().add(radio2);

radio2.addActionListener(this);

radio2.setFocusable(true);

radio2.setRolloverEnabled(true);

radio2.setVerifyInputWhenFocusTarget(true);

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 20 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

radio2.setFont(new Font("Engravers MT", Font.BOLD, 20));

button1 = new JButton("EXIT");

getContentPane().add(button1);

button1.addActionListener(this);

button1.setFocusable(true);

button1.setRolloverEnabled(true);

button1.setVerifyInputWhenFocusTarget(true);

//button1.setSelected(true);

button1.setFont(new Font("Engravers MT", Font.BOLD, 18));

timeField = new JTextField(5);

showSysTime(timeField);

timeField.setFont(new Font("TimesRoman",Font.BOLD,12));

* timeField.setForeground(Color.GRAY);

timeField.setEditable(false); getContentPane().add(timeField);

dateLongField = new JTextField(18); dateLongField.setText(showTodayDate()); getContentPane().add(dateLongField); dateLongField.setEditable(false); //dateLongField.setForeground(Color.GRAY); dateLongField.setFont(new Font("TimesRoman",Font.BOLD,12));

JMenu helpMenu=new JMenu("Help");

helpMenu.setMnemonic('h');

TopicsItem.addActionListener(this);

helpMenu.add(TopicsItem);

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 21 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

menuBar.add(helpMenu);

setJMenuBar(menuBar);

radio3 = new JRadioButton("SEND IMAGE", false);

cbg.add(radio3);

getContentPane().add(radio3);

radio3.setFocusable(true);

radio3.setRolloverEnabled(true);

radio3.setVerifyInputWhenFocusTarget(true);

radio3.addActionListener(this);

radio3.setFont(new Font("Engravers MT", Font.BOLD, 20));

setSize(getPreferredSize());

addWindowListener(new WindowAdapter() { public void windowClosing(WindowEvent e) {

System.exit(0);

}

});

}

public void showSysTime(final JTextField tf)

{

final SimpleDateFormat timef = new SimpleDateFormat("HH:mm:ss"); javax.swing.Timer timer = new javax.swing.Timer(1000, new

ActionListener()

{

public void actionPerformed(ActionEvent e)

{

String s = timef.format(new Date(System.currentTimeMillis()));

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 22 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

tf.setText(s);

}

});

timer.start();

}

public String showTodayDate()

{

Date dt = new Date();

System.out.println(dt.toString());

SimpleDateFormat sdf = new SimpleDateFormat("EEE, MMM d, yyyy"); return sdf.format(dt).toString();

}

public void actionPerformed(ActionEvent e)

{

String cmd;

cmd = e.getActionCommand();

if(e.getSource() == radio1)

{

dispose();

Encryption en = new Encryption();

en.setTitle("ENCRYPTION");

en.pack();

en.show();

}

if(e.getSource() == radio2)

{

dispose();

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 23 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

Decryption dn = new Decryption();

dn.setTitle("DECRYPTION");

dn.pack();

dn.show();

}

if(e.getSource()==radio3)

{

dispose();

SendImage si=new SendImage();

si.setTitle("Uploads the encrypted image");

si.show();

si.pack();

}

if(e.getSource()==TopicsItem)

{

try

{

Runtime run= Runtime.getRuntime();

run.exec("notepad help.txt");

}

catch(Exception ee)

{

System.out.println("Error: "+ ee);

}

}

if(cmd.equals("EXIT"))

{

int res;

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 24 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

res = JOptionPane.showConfirmDialog(this, "R U SURE U WANT TO EXIT");

switch(res)

{

case JOptionPane.OK\_OPTION:

System.exit(0);

break;

case JOptionPane.NO\_OPTION:

break;

}

}

}

public static void main(String args[]){

Stegno s = new Stegno();

s.setTitle("Main Menu");

s.pack();

s.show();

JFrame.setDefaultLookAndFeelDecorated(true);

JDialog.setDefaultLookAndFeelDecorated(true);

try

{

UIManager.setLookAndFeel("com.sun.java.swing.plaf.windows.WindowsLookA ndFeel");

//

javax.swing.UIManager.setLookAndFeel("com.birosoft.liquid.LiquidLookAndFeel");

}

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 25 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

catch (Exception ex)

{

System.out.println("Failed loading L&F: ");

System.out.println(ex);

}

}

}

class StegnoLayout implements LayoutManager {

public StegnoLayout() {

}

public void addLayoutComponent(String name, Component comp) { }

public void removeLayoutComponent(Component comp) { }

public Dimension preferredLayoutSize(Container parent) { Dimension dim = new Dimension(0, 0);

Insets insets = parent.getInsets();

dim.width = 700 + insets.left + insets.righ dim.height = 400 + insets.top + insets.bottom;

return dim;

}

public Dimension minimumLayoutSize(Container parent) {

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 26 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

Dimension dim = new Dimension(0, 0);

return dim;

}

public void layoutContainer(Container parent) {

Insets insets = parent.getInsets();

Component c;

c = parent.getComponent(0);

if (c.isVisible()) {c.setBounds(insets.left+45,insets.top+30,648,42);} c = parent.getComponent(1);

if (c.isVisible()) {c.setBounds(insets.left+235,insets.top+108,240,48);} c = parent.getComponent(2);

if (c.isVisible()) {c.setBounds(insets.left+235,insets.top+170,240,48);} c = parent.getComponent(3);

if (c.isVisible()) {c.setBounds(insets.left+260,insets.top+310,184,48);} c = parent.getComponent(4);

if (c.isVisible()) {c.setBounds(insets.left+536,insets.top+378,58,22);} c = parent.getComponent(5);

if (c.isVisible()) {c.setBounds(insets.left+593,insets.top+378,105,22);} c = parent.getComponent(6);

if (c.isVisible()) {c.setBounds(insets.left+235,insets.top+232,240,48);}

}

}

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 27 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**6. SOFTWARE TESTING**

Software testing is the process of finding the error from the program. To make our software error free it should be done. Until we check the software testing we can’t say where the error exactly is, for successfully run the program it must be checked.

The Principle of testing: -

1. All the requirements should be checked by the customer.
2. The Third party should check the software testing to make if perfect.
3. Software testing must be done before implementing it.

Unit testing :-

It is the first level of testing. In unit testing smallest part of the program needs to be checked by independently. In this testing, a software module may be created as a collection of several small parts. This is type of small parts are called Unit. So a Unit is a small piece of code that can be used to perform a specific or particular task.

Integration Testing :-

It is the second level of testing. In integration testing, it’s finding out the correctness of the program. Integration testing is nothing but a combination of all programs into a single program. The benefit of Integration testing is that we can get the completed outcome.

Validation testing :-

Validation testing follows integration testing. The distinction between conventional and object-oriented software disappears. Focuses on user-visible actions and user-recognizable output from the system. Demonstrates conformity with requirements.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 28 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

System testing :

Types of System Testing:

Recovery testing: -

Tests for recovery from system faults. Forces the software to fail in a variety of ways and verifies that recovery is properly performed. Tests re-initialization, check-pointing mechanisms, data recovery, and restart for correctness.

Security testing: -

Responsible for protection mechanisms built into a system will and also protect it from improper access.

Stress testing: -

Executes a system in a manner that demands resources in abnormal quantity, frequency, or volume.

Performance testing: -

Tests the run-time performance of software within the context of an integrated system.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 29 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**7. CONCLUSION**

Nowadays it’s a big problem to secure your personal information from hackers. We are seeing many Organizations such as public or private as well as government agencies also fetching the problem of secrecy. So maintaining secrecy is very important.

GUI based programs are always user-friendly. Our project is also built on Java Swing and other GUI based platform that provides maximum interaction with the user. In our project, hidden messages can easily be encrypted and also be transmitted to the intended user. That won’t create any suspicion to the unintended user. Therefore decryption of the message can be done only by the knowing recipients.

The technology used in our project Steganography is very easy to use and user-friendly, but very difficult to hacked or detect errors. So here we can conclude that it is a very secure medium in order to transfer secret information to the intended user, without giving any suspicion to other.

**8. FUTURE ENHANCEMENTS**

As we implemented our project Digital Steganography to encrypt and decrypt the messages in a multimedia as an image, therefore we can extend our project in the following way-

This project can be further extended by adding video files as a covering medium. By using more technology we can increase the capacity.

We can add other algorithms in it, as a choice of choosing algorithms as far as the user requirements.

In future, the most frequent use of Steganography will be in the context of “Digital Watermarking”.

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 30 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

**9. BIBLIOGRAPHY**

**Books**

1. Java Fundamentals, A comprehensive Introduction by Herbert Schildt and Dale Skrien, Tata McGraw Hill, Edition 2013.
2. Java Programming by Hari Mohon Pandey, Pearson Education, 2012.
3. Java The Complete Reference (Ninth Edition) By – Herbert Schieldt, Tata McGraw Hill, Edition 2014.
4. David & Deitel (1999), Java How to program Introducing Swing, Prentice Hall.

**Journals**

Natarajan Meghanathan and Lopamudra Nayak*,* Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media, Jackson State University, 1400 Lynch St., Jackson, USA.

Luis von Ahn and Nicholas, Steganography*,* Carnegie Mellon University, Pittsburgh, USA.

**Web Sites**

[http://java.sun.com](http://java.sun.com/)

[http://www.javaworld.com](http://www.javaworld.com/)

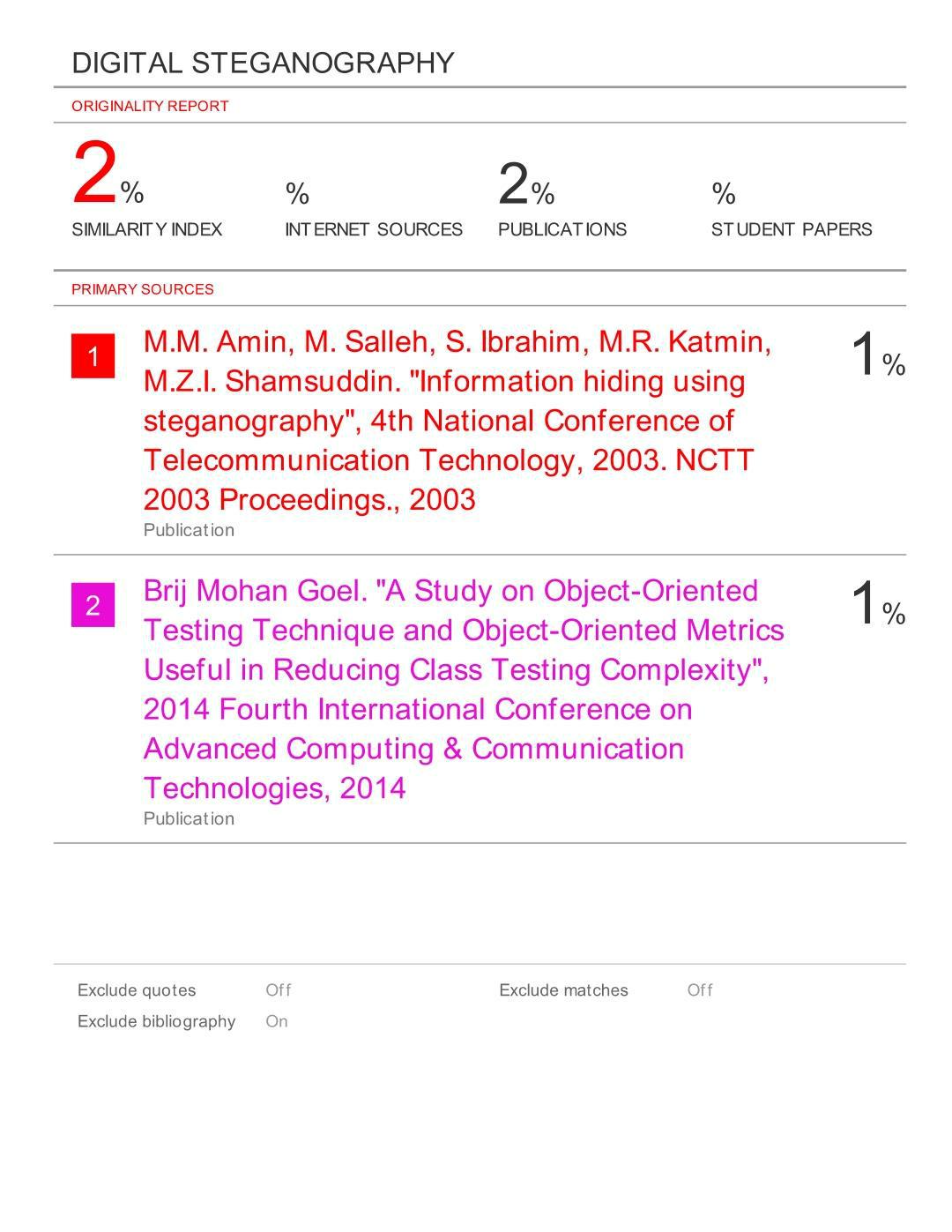
https://www.geeksforgeeks.org/java

|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 31 |

DIGITAL STEGANOGRAPHY 1NH17MCA28

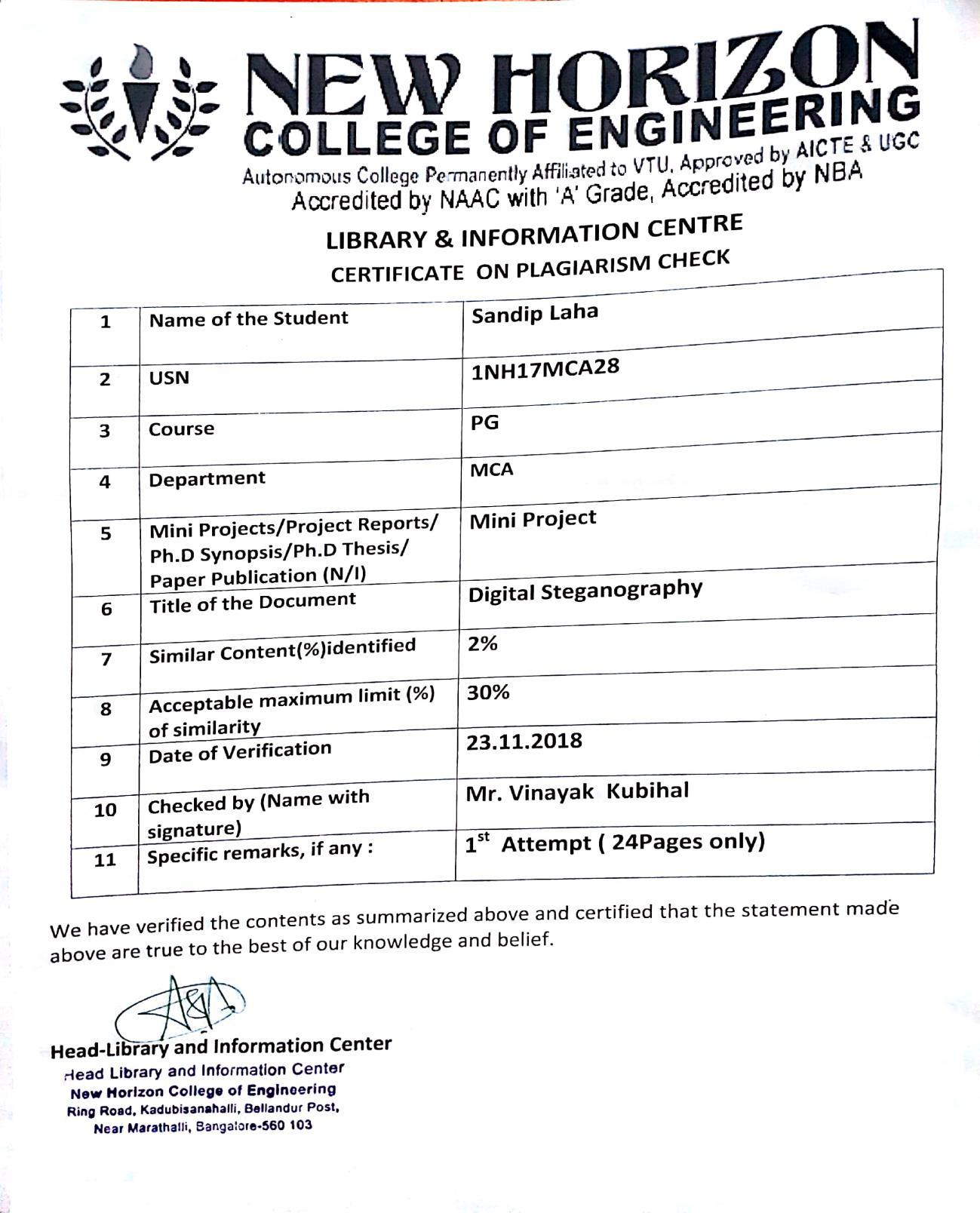
**10. APPENDICES**

**10.1 PLAGIARISM CERTIFICATE**



|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 32 |

DIGITAL STEGANOGRAPHY 1NH17MCA28



|  |  |  |
| --- | --- | --- |
| Department of MCA, NHCE | 2018-2019 | 33 |