Image Steganography

Submitted By
Motiur Rahman Rupak
ID: 182-35-354

Supervised by:
Mr. Sk. Fazlee Rabby
Senior Lecturer
Department of Software Engineering
Daffodil International University

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Declaration

This humble effort, the fruit of my thoughts and study is devoted to the people that have perpetually been there to encourage and support me. Especially to my beloved folks whose fondness, love, and prayer of day and night helped to build this project. I would also like to dedicate my teacher; those have inspired me throughout Whole life.

I hereby declare that I have done this project under the **supervision of Mr. Sk. Fazlee Rabby** Senoir Lecturer, Department of Software Engineering, and Daffodil International University**.** I also declare that this project is my original work for the degree of B.Sc. in Software Engineering and that neither the whole work nor any part has been submitted for another degree in this or any other university.

Submitted by:

Motiur Rahman Rupak
ID: 182-35-354
Department of Software Engineering
Daffodil International University.

Supervised by:

Mr. Sk. Fazlee Rabby
Senior Lecturer
Department of Software Engineering
Daffodil International University

Approval

APPROVAL (Room- 610)

This project titled on "**Image Steganography**", submitted by **Motiur Rahman Rupak (ID: 182-35-354)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Khalid Been Badruzzaman Biplob
Lecturer (Senior)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Md. Tanvir Quader
Senior Software
Engineer Technology
Team a2i Programme

Acknowledgement

My sincere gratitude to my Supervisor **Mr. Sk. Fazlee Rabby**, Senior Lecturer for guiding me throughout the planning and development phase of the system. Without her strategic guideline and counseling I would not have reached the final stage of the development. I would like to thank my close peers and my classmates for being supportive and encouraging throughout my four-year journey here in Daffodil International University. My sincere gratitude goes to **Daffodil International University** for providing the platform where I was able to cherish and nurture my compassion and improve my technical skills. Much appreciation to Daffodil International University for great support and all necessary academic materials that has taught me great helpful academic as well as life lessons. Finally, yet importantly, I am happy to acknowledge the help of all the individuals to fulfill our attempt

Abstract

The art of image steganography involves concealing data—text, images, or even videos—within a cover image. The secret information is concealed such that it cannot be seen by human sight. Recently, there has been more focus on deep learning technology, which has proven to be an effective tool in many fields, including image steganography. The primary objective of this study is to investigate and discuss the various deep learning techniques that are used in the field of image steganography. Traditional approaches, Convolutional Neural Network-based methods, and General Adversarial Network-based methods are the three basic categories into which deep learning techniques used for image steganography can be separated. This paper includes a detailed overview of the approach as well as a list of the datasets used, experimental setups taken into account, and regularly employed evaluation criteria.

ABBREVIATION

Table 1 Abbreviation

Short name	Abbreviations
DFD Data	Flow Diagram
UFP	Unadjusted Function Point
ERD	Entity Relationship Diagram
RE	Requirement Engineering
FP	Function Point
FTR	File Type

TABLE OF CONTENTS

Page no

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The science and art of concealing the existence of a message between the sender and the intended recipient is known as steganography. It is a type of security technique through obscurity. Secret messages have been concealed via steganography in a variety of formats, including digital Image

1.2 MOTIVATION

Now a days information encryption is very necessary. Steganography is less known process. By using image steganography, we can hide our message securely.

1.3 OBJECTIVES

The aim of image steganography is to conceal a concealed message within an image in a way that no one can tell that it is there. Steganography, to put it simply, "means concealing one piece of data within another," in technical terms.

1.4 EXPECTED OUTCOME

In contrast, the aim of image steganography is to subtly modify a message by concealing it within another original message. It is anticipated that the changed message will appear fairly similar to the original message.

1.5 Goals

Image steganography serves as a means of concealment and deception. It is a type of covert communication that uses any media to encrypt messages. Since it doesn't include data encryption or the usage of a key, it isn't a type of cryptography. Instead, it is a method of data concealing that can be used in cunning ways

1.6 Project Scope

A helpful technology for secret information transfer via a communications channel is steganography. The concealed picture is produced by fusing the carrier image and secret image. It is challenging to find the hidden image without retrieval.

1.7 Stakeholders

Basically, those who are using our Desktop system and involve with this system users.

- User (Sender, Receiver)

Brief descriptions about stakeholder are given below

User: who are capable of accessing or using all application modules and who have significant control over the entire systems process

1.8 Project Schedule

TABLE: 1.8 Project Schedule

Activities	**Duration (in week)**	**Total week**
Preparation	Week-1	**1**
Find Problem & Analysis	Week-2	**1**
Planning	Week-3	**1**
Detail Design	Week-4,5	**2**
Coding	Week-6,7,8	**3**
Development	Week-9	**1**
Testing	Week-10,11	**2**
Documentation	Week-12	**1**
Delivery	Week-13	**1** **Total =13**

1.9 Release Plan

Release plan is given below:

TABLE: 1.9 Release Plan

Version	Feature	Date
V-1.0	All activities of assistant, Sender and Receiver	21-10-2022

Chapter 02:
Software Requirement Specification

2.1 Functional Requirement List

1. Take image and message input
2. Give output

Non Functional Requirement List

1. A high-quality system requires that every function be fully functional.
2. User friendly interface
3. The application must appropriately extract the picture from the image after hiding it within the image.
4. The software must process data quickly.
5. The program will be presented in English.

2.2Features

1. Encrypt Message in Image
2. Decrypt Message from Image
3. Secret Capacity
4. Transparency of Perception
5. Tamper–resistance
6. Robustness

2.3Requirment Specification

The construction of requirements specifications for stenographic systems is the main topic of the study. The fundamental ideas and application areas of steganography are briefly discussed. The many non-functional needs that can be evaluated using these criteria are grouped, and their potential metrics are provided along with examples and sample requirements. The authors offer a unique methodical approach to developing stenographic system requirements based on the field of usage and the significance of each criterion in the chosen field. The strategy is similar to the idea of the Universal Steg constructor, which ensures that clients obtain the necessary stenographic system from the developers, and it also permits automated selection of stenographic algorithms based on the needs.

2.3.1 Functional Requirement

Table 2.3.1.1: user input

FR-1	Select Image
Description	User can input image
Stockholders	User

Table 2.3.1.2: Upload image

FR-2	**Upload image**
Description	The user have to upload the image that has been selected
Stakeholders	User

Table 2.3.1.3: Encryption

FR-3	**Encryption**
Description	User have to input the massage want to embed and hit encryption button
Stakeholders	User

TABLE 2.3.1.4: Load setgo image

FR-4	Load stego image
Description	User who wants the secret text have to upload the stego image to the system
Stakeholders	User

Table 2.3.1.5: Image Description

FR-5	Decryption
Description	Being uploaded the image then the user have to hit the decryption button
Stakeholders	User

2.3.2Data Requirement:

1. Image
2. Text which wants to embed

2.3.3 Performance Requirement:

Three factors can be used to evaluate the effectiveness of a steganography process.

1. hiding capacity
2. distortion control
3. security

   The quantity of data that may be completely concealed in an image is referred to as the concealing capacity. It can also be expressed as the quantity of bits in a single pixel.

2.3.4 Security Requirement:

Image steganography's security is reliant on the secret key set that is employed to insert the hidden image. The hidden image can be obtained by using the secret key, which has been revealed. We suggest a new kind of steganography technique employing visual cryptography to address this security issue.

Chapter 03: System Design

3.1 Use Case Diagram

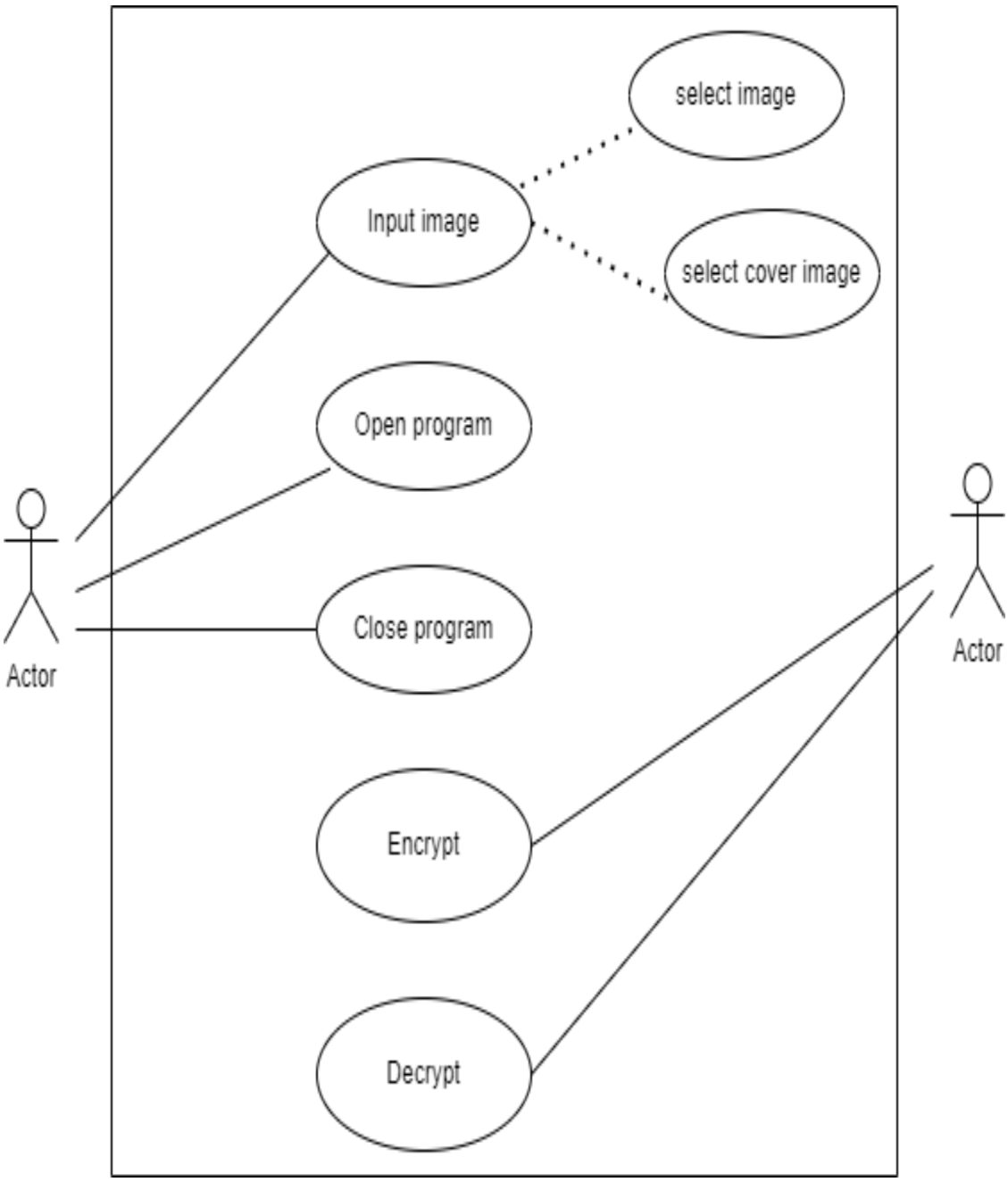


Figure: 3.1 Use Case Diagram

3.2 Use Case Description

Table 3.2.1 Sender Side

Use Case No	01
Use Case Name	Image Steganography
Actor	Sender
Description	Allow to Encrypt
Precondition	Way Image Steganography
Trigger	Click Encrypt Button
Flow of Event	1.Select Image 2.Press Encrypt Button 3.Hidden Encrypted Message in Image

Table 3.2.2 Receiver Side

Use Case No	02
Use Case Name	Image Steganography
Actor	Receiver
Description	Allow to Decrypt
Precondition	Way Image Steganography
Trigger	Click Decrypt Button
Flow of Event	1.Select Stegano Image 2.Press Decrypt Button 3.Show Hidden Encrypted Message

3.3 Activity Diagram

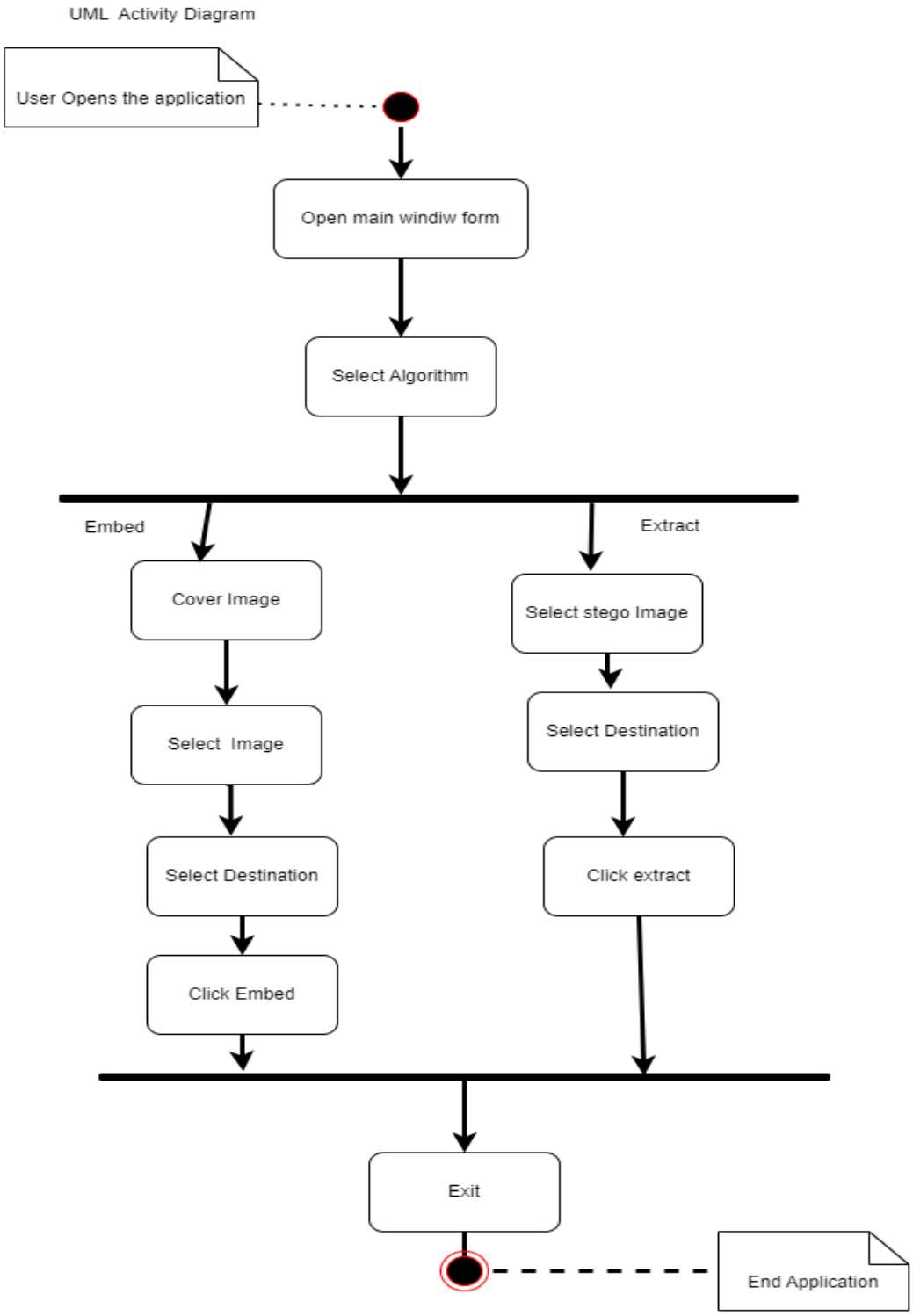


Figure: 3.3 Activity Diagram

3.4 Data Flow Diagram

Figure: 3.4 Data Flow Diagram

3.5 Class Diagram

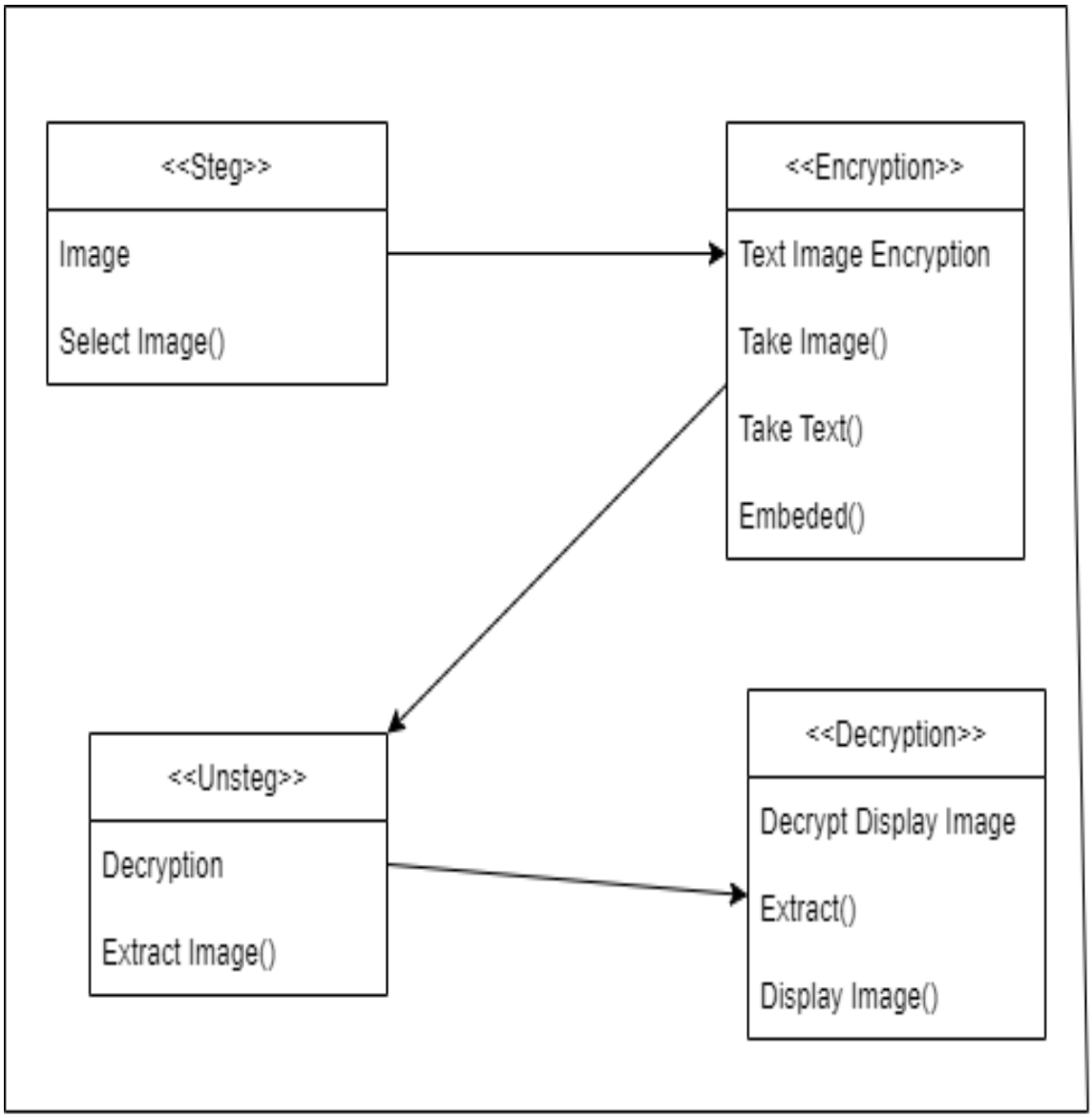


Figure: 3.5 Class Diagram

Chapter 04: System Test and Development

4.1 Testing Introduction

Software testing is a crucial part of software quality assurance, and many software companies devote up to 40% of their budgets to it. Testing life-critical software can be quite expensive. This has led to a large number of studies on risk analysis. In software projects, this term refers to the likelihood of unfavorable occurrences like schedule delays, cost overruns,

Software testing

There are various methods for testing an application built with the .NET framework.

The many test kinds are:

1. Unit testing
2. Validation testing
3. Integration testing
4. User acceptance testing
5. Output testing
6. Black box and white box testing

.

4.2 Maintenance and Environment

It's one of the most popular approaches since it allows for the hiding of sensitive information within an image so that no one can discover it. This approach involves adding the message on the image's edge. Message can be read if image is viewed in text editor rather than image viewer application, which ignores concealed message.

4.3 Development tool and Technology.

4.3.1 Tools and Technology

4.3.2 Platform

- Windows 10

Programing Language

- C#
- .Net Framework

Tools

- Visual studio

Chapter 5: Risk Management

5.1Software Risk Identification

Iterative processes are used to identify risks. More knowledge about the program will be obtained as it goes along, and the risk statement will be modified to reflect this knowledge. As the project moves forward through its life cycle, more risks will be found. Making a risk list is a step in the risk identification process. Identification of risks that have consistently occurred in past software projects is necessary for the creation of a risk list.

5.2Risk Analysis and Prioritization

Analysis is the evaluation of the working conditions within an organization.

Determining the issues posing risk to the project. Determining how the issue is affecting people.

Create a table with all the values in it, and rank the risks according to the risk exposure factor.

TABLE: 5.2Risk Analysis and Prioritization

Risk No	**Problems**	**Probability of Problem Occurrence**	**Impact of Problem**	**Risk Exposition**	**Priority**
R-1	Delay of Load Image	3	4	7	10
R-2	Text Capacity	2	3	1	7
R-3	Design is no robust	1	9	8	5

5.3 Risk Matrix

1. Decide which event outcomes should be given top priority.
2. Provide an effective graphical representation of project-wide risks.
3. Facilitates the process of risk management.
4. Aids in identifying potential risk reduction areas
5. Offer a timely and reasonably priced risk analysis.
6. Make it possible to concentrate more in-depth investigation on high-risk regions.

Chapter 06:

User Manual

6.1 Home Page.

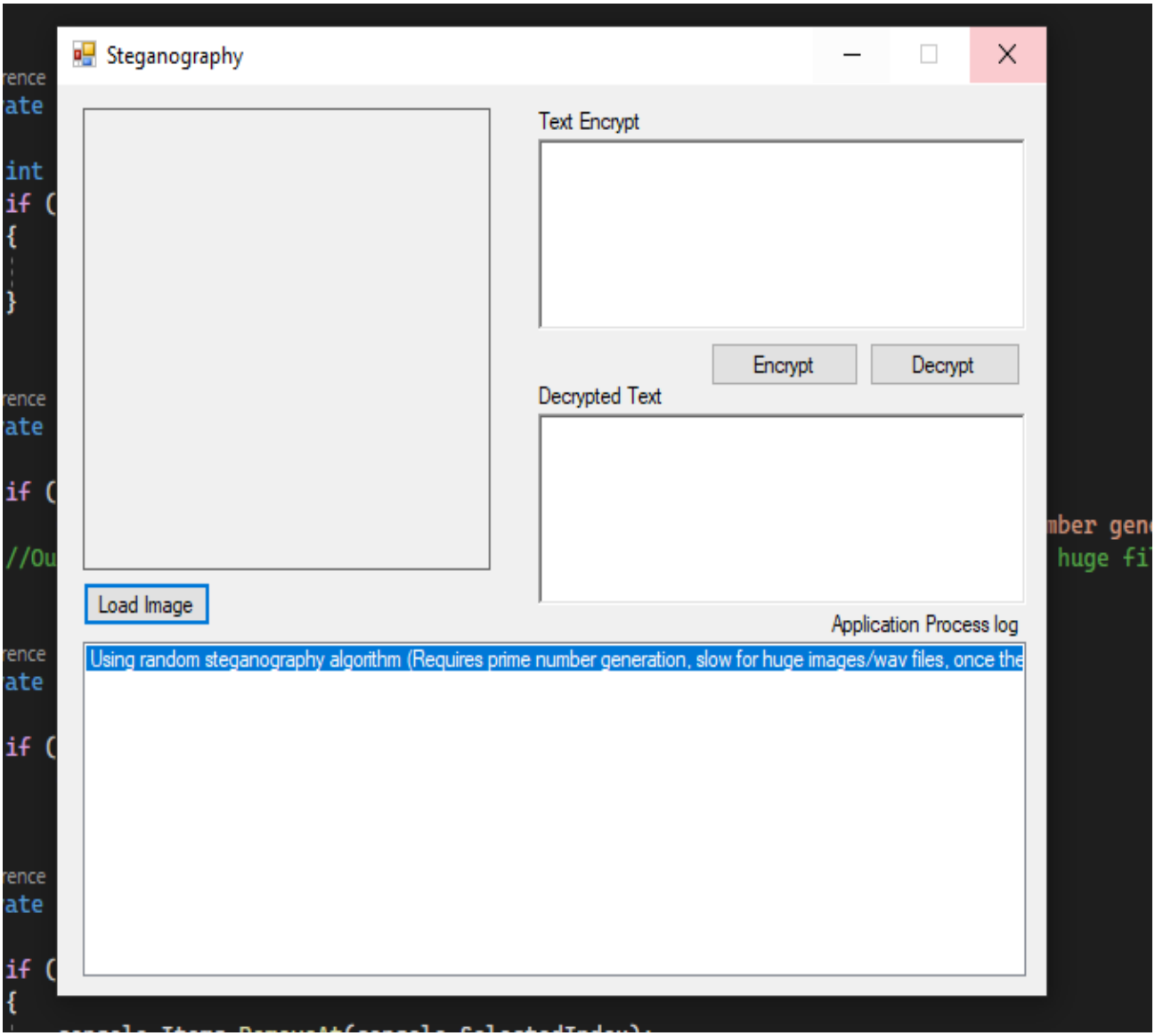


Figure: 6.1 Home Page.

6.2 Input image

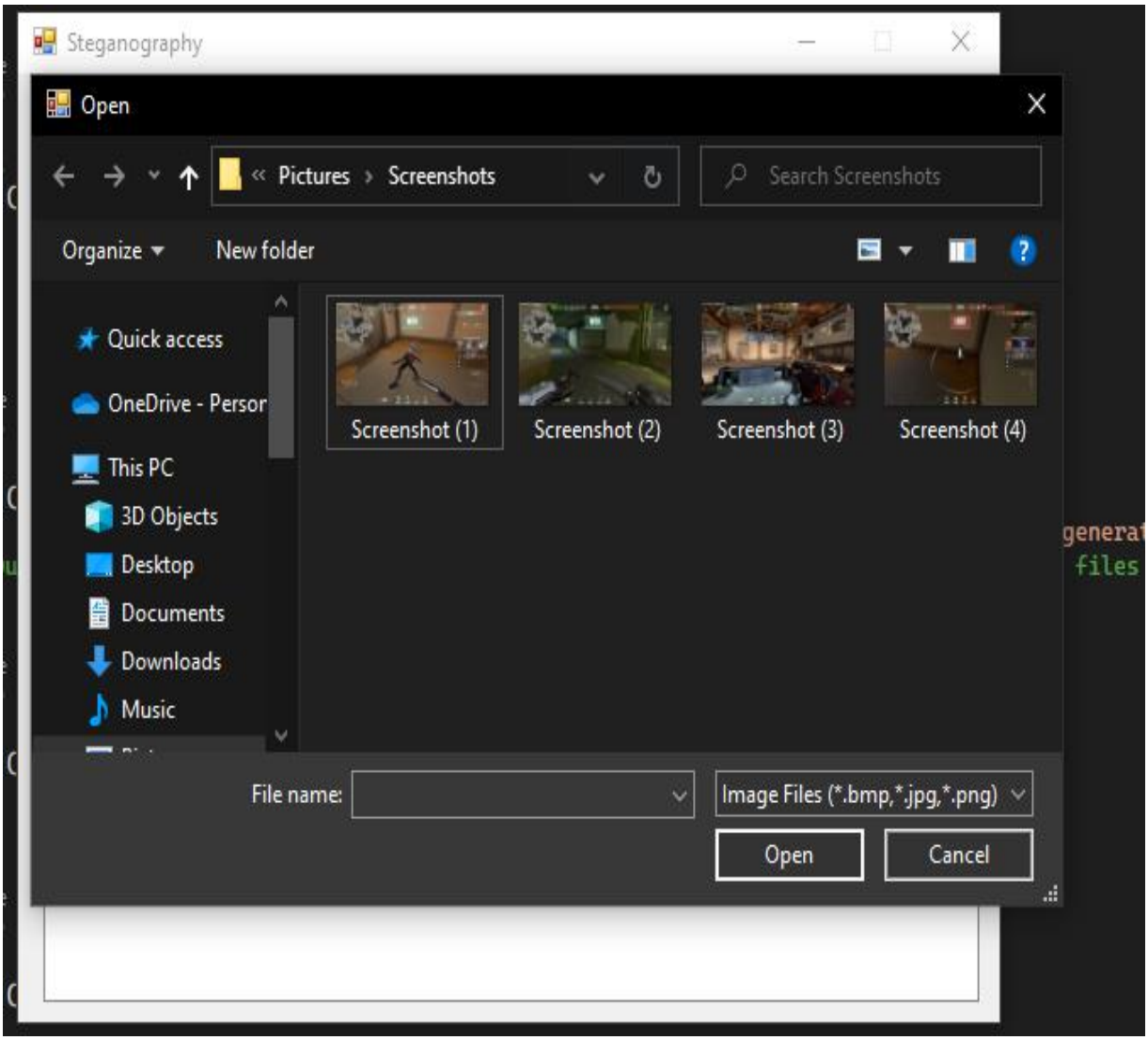


Figure: 6.2 Input image

6.3 Load Image

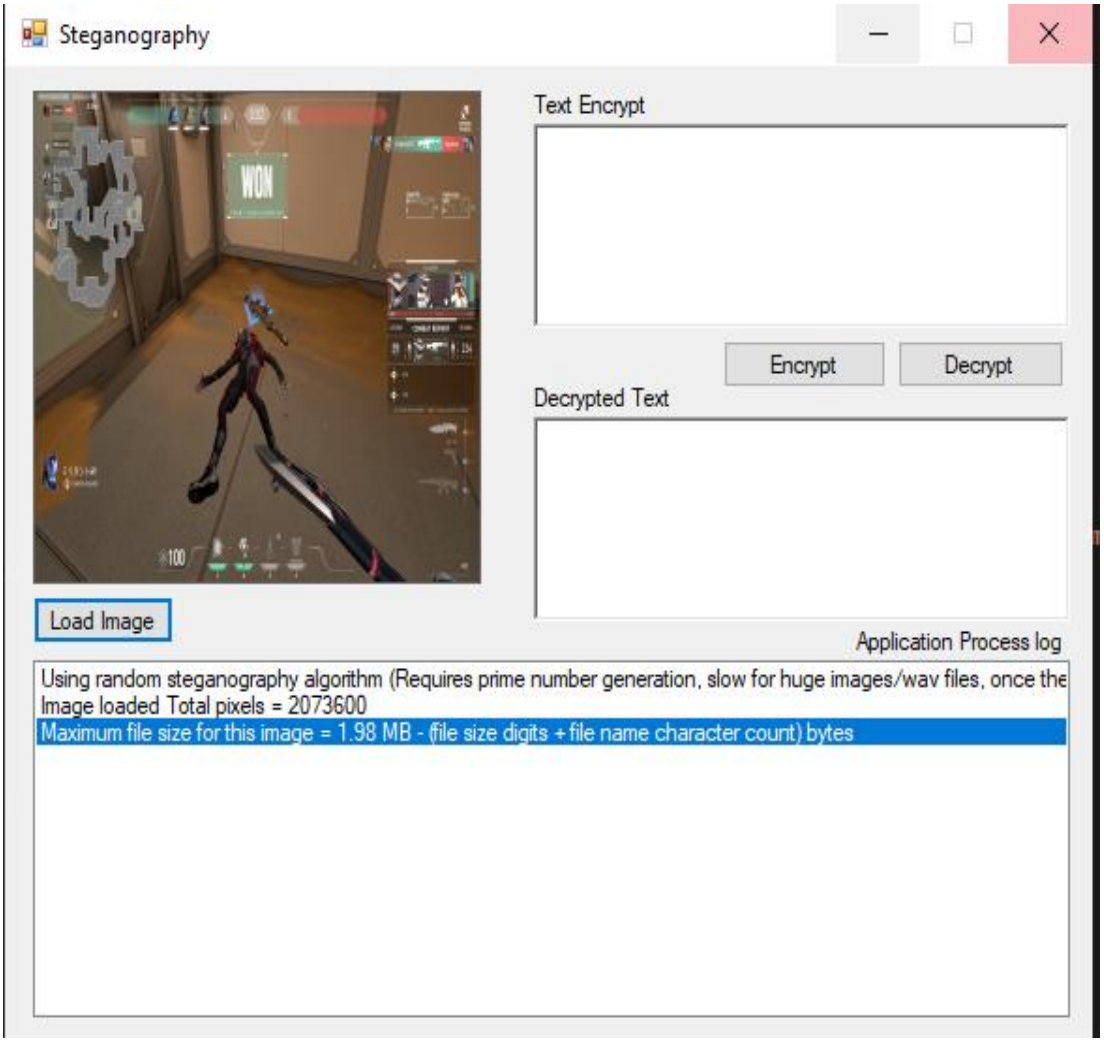


Figure: 6.3 Load Image

6.4 Input Message

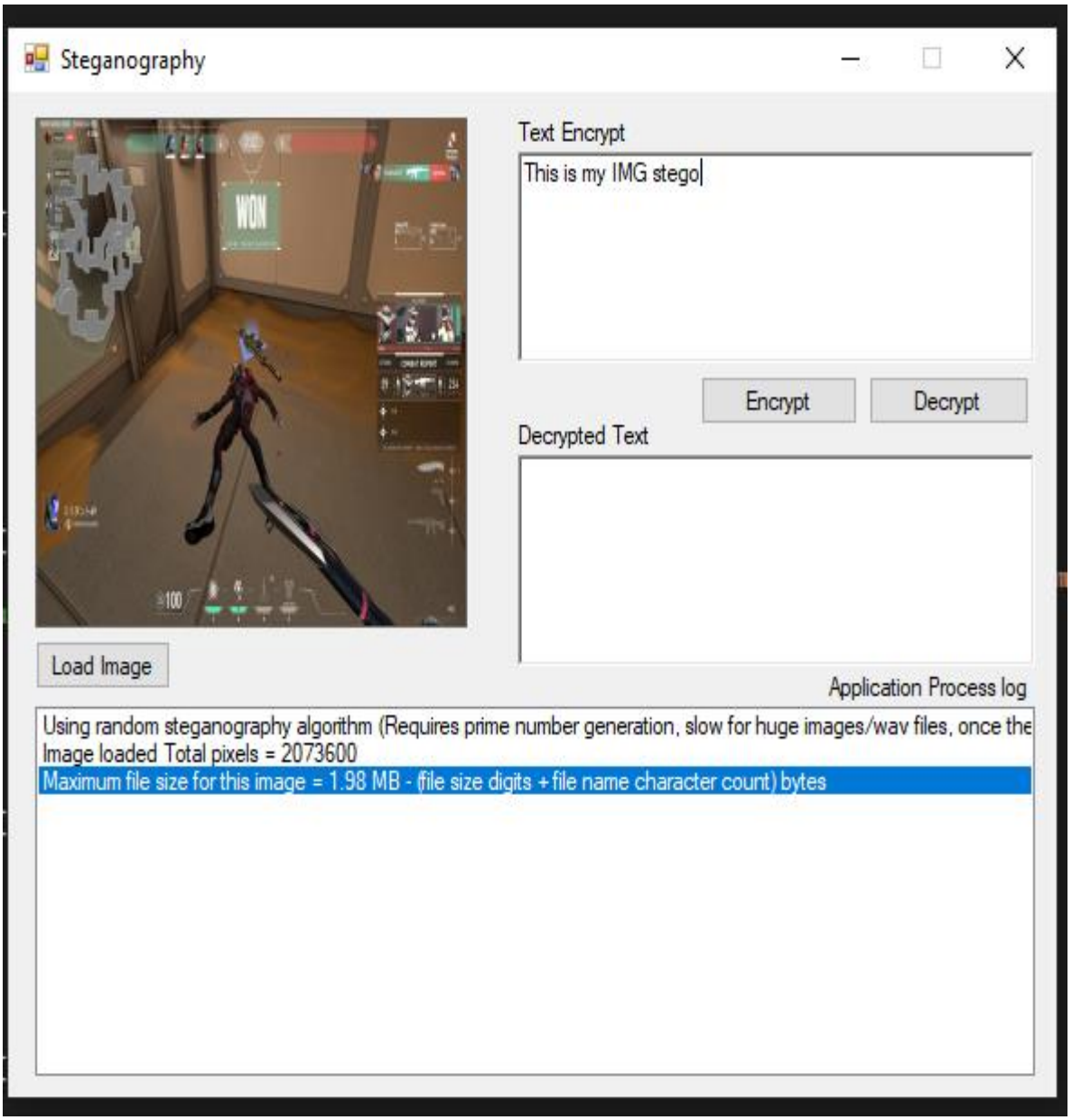


Figure: 6.4 Input Messages

6.5Stego Image

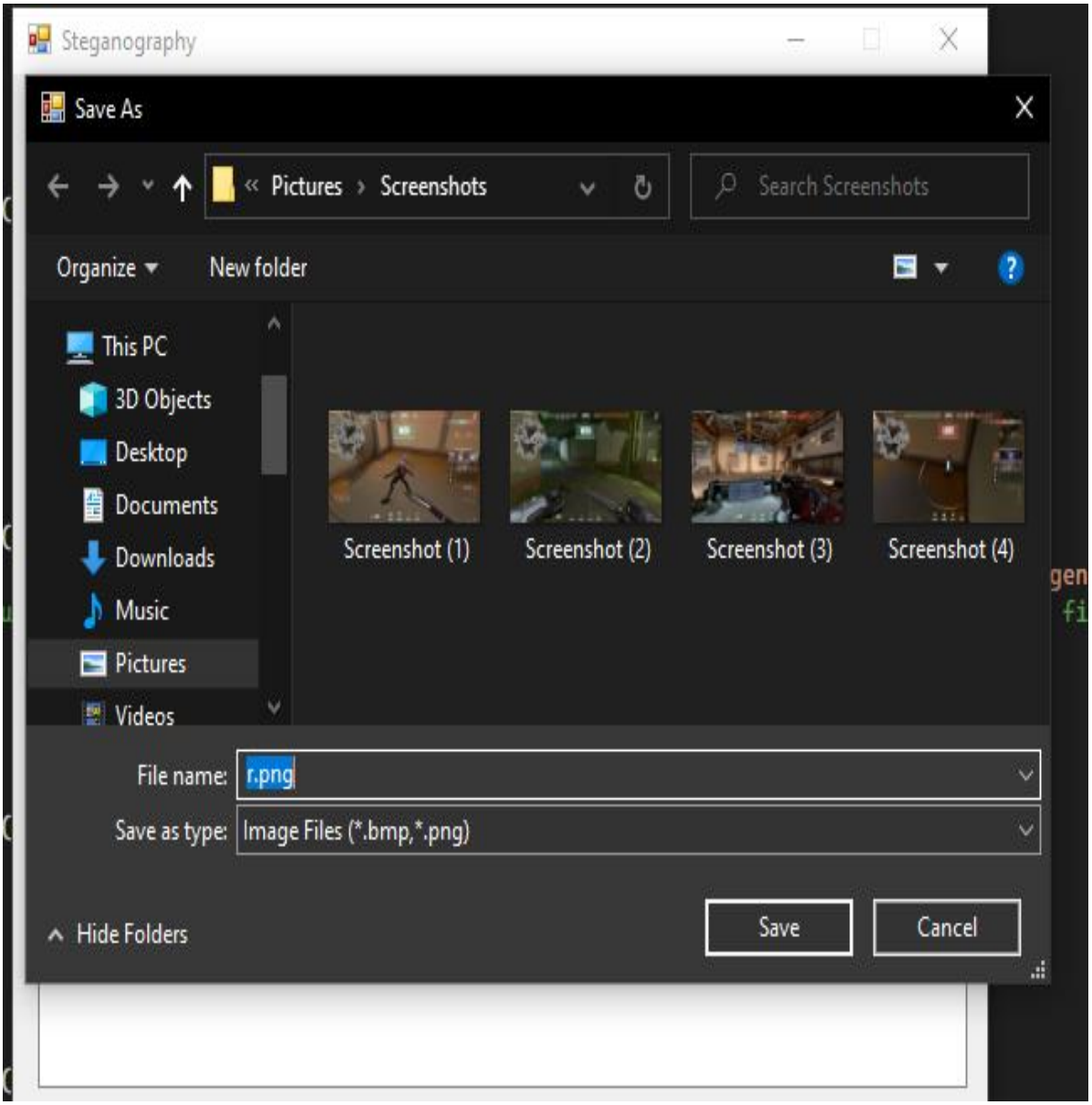


Figure: 6.5Stego Image

6.6 Text Encrypted

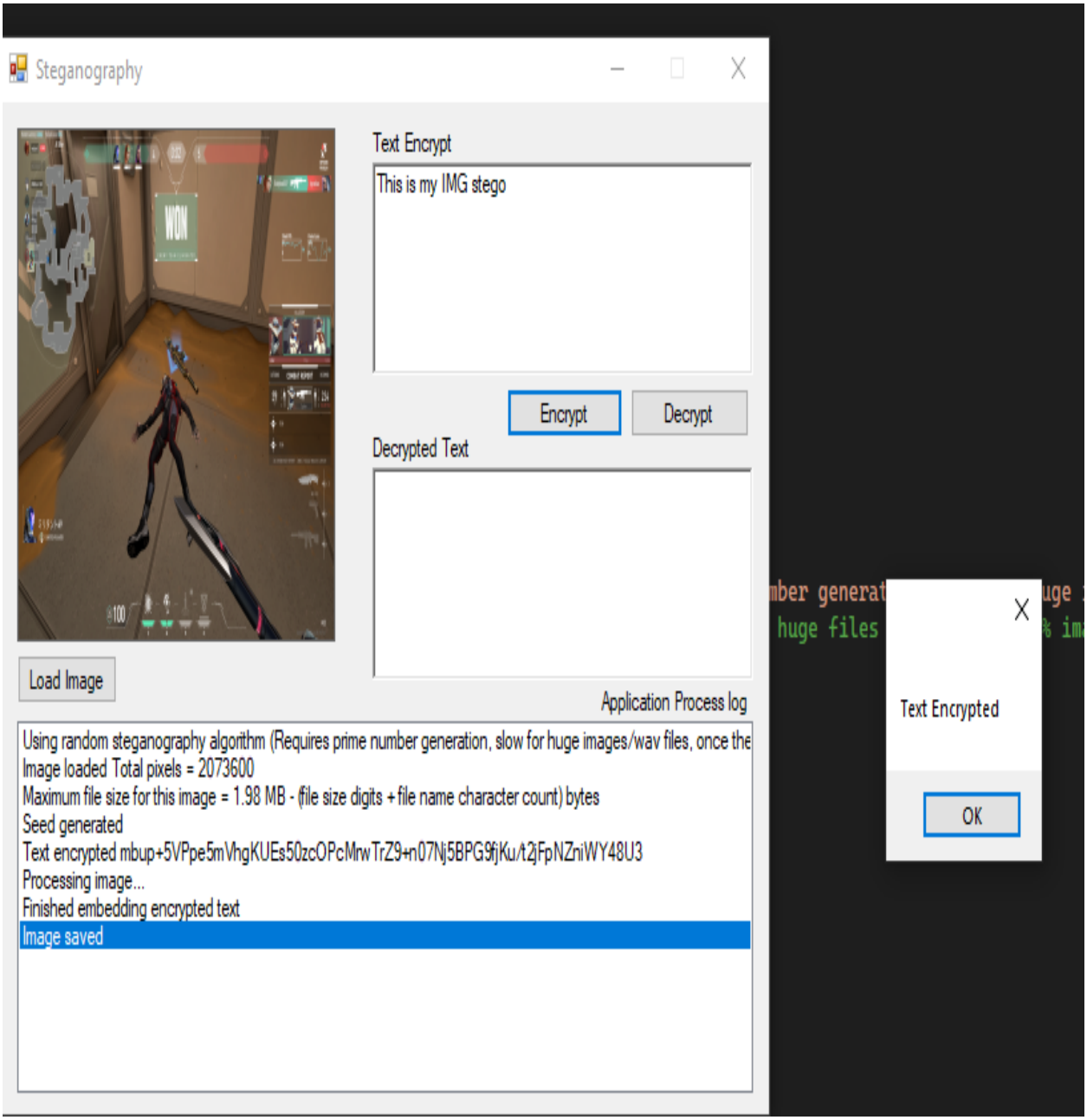


Figure: 6.6 Texts Encrypted

6.7 Load Stego Image

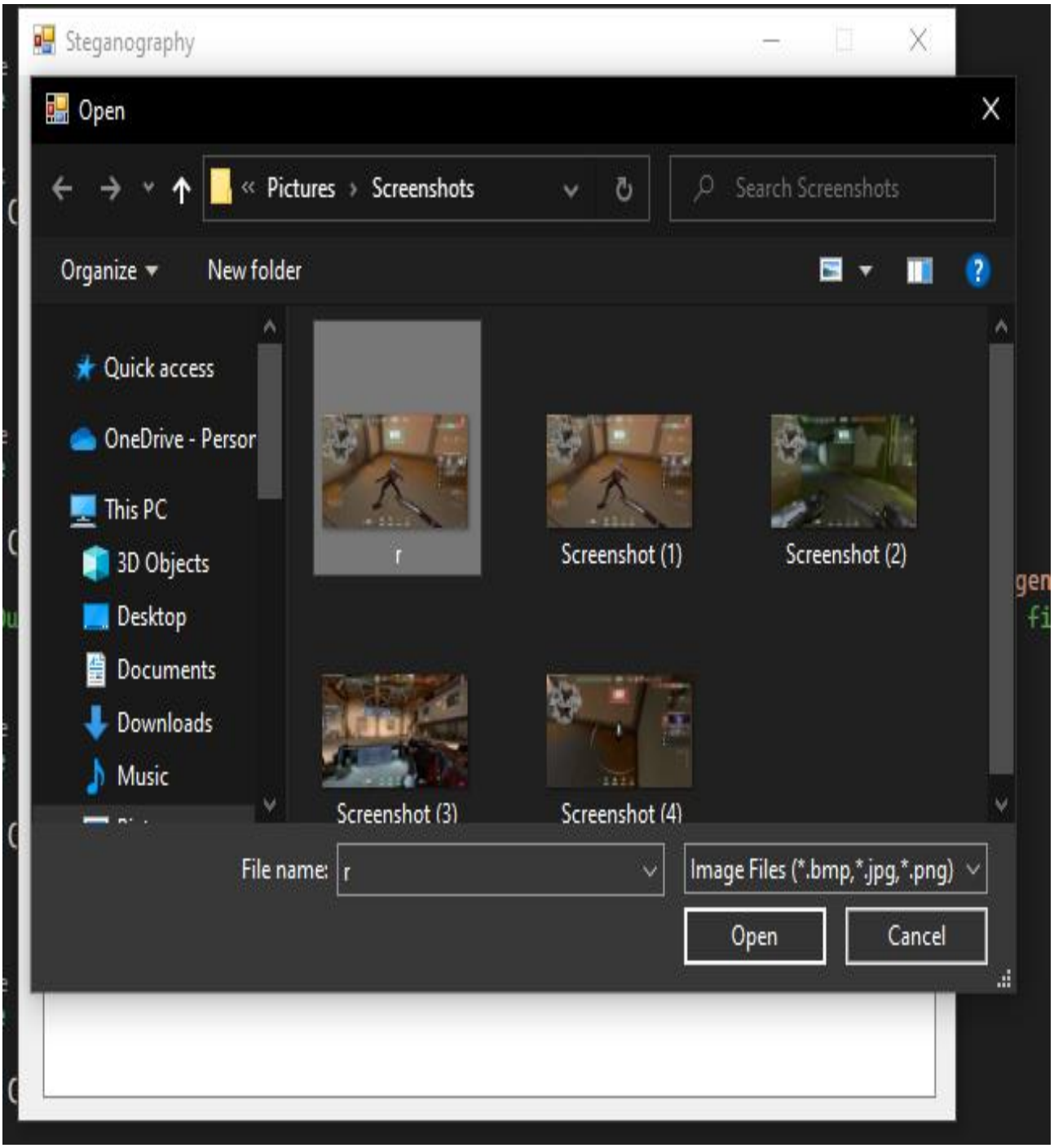


Figure: 6.7 Load Stego Image

6.8 Enter Decrypt

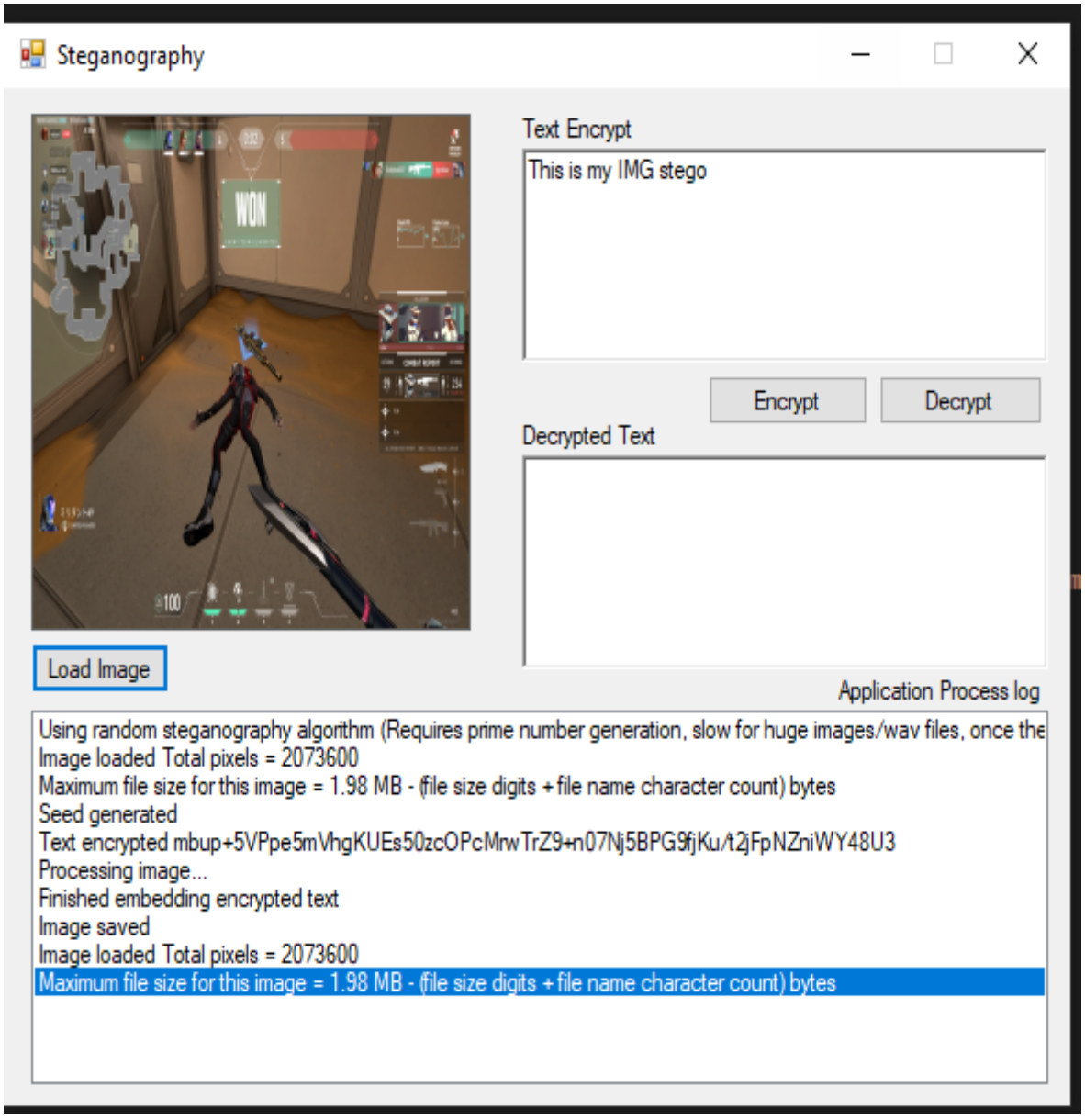


Figure: 6.8 Enter Decrypt

6.9 Text Decrypted

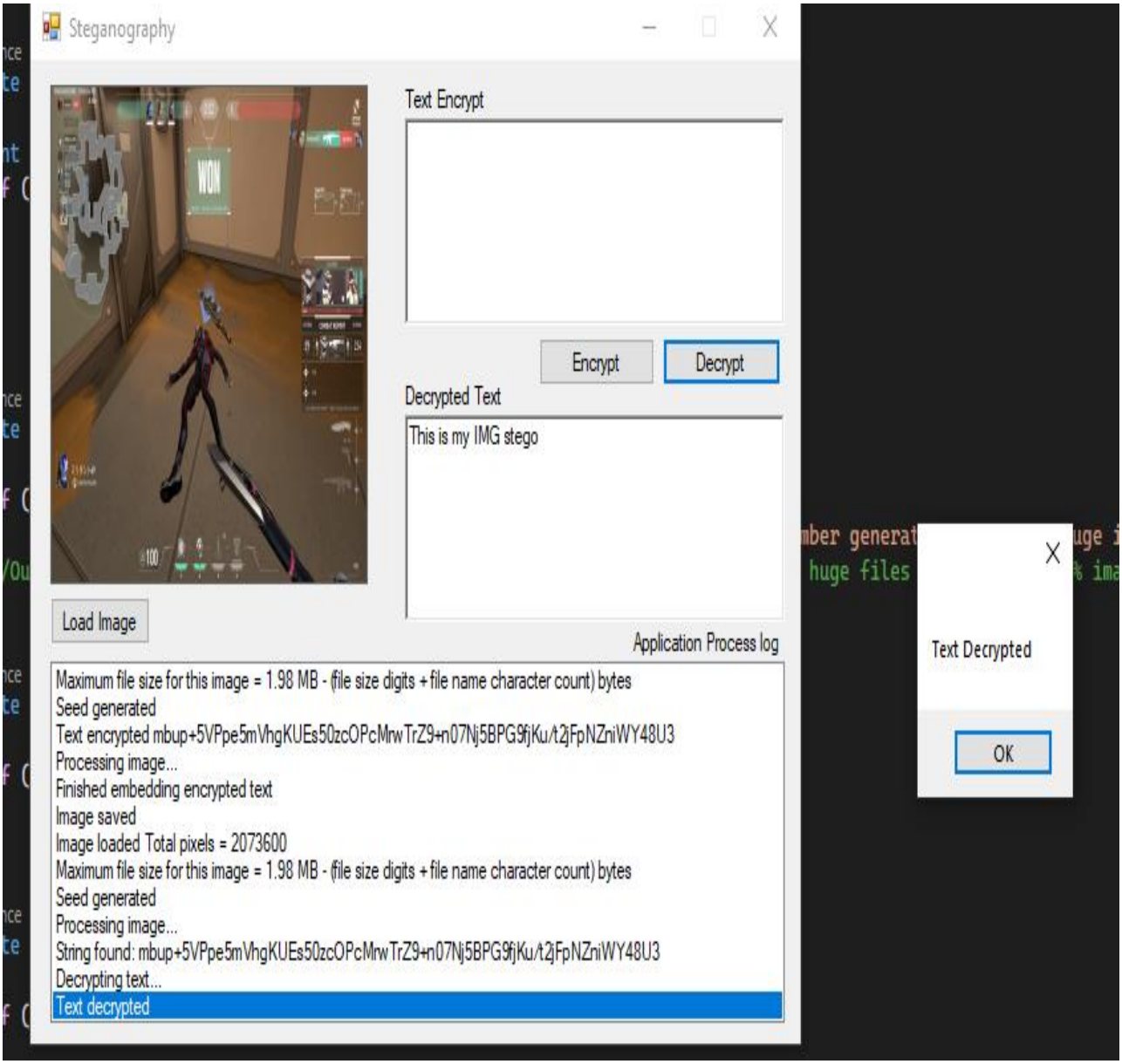


Figure: 6.9 Texts Decrypted

Chapter 7

Project Summery

6.1 SUMMARY

Although only a few of the most common image steganography techniques were covered in this document, it is clear that there are many different methods for concealing information in photographs. Each of the main image file formats has a unique way of hiding messages, each with different strengths and weaknesses. The other strategy lacks robustness where the first technique lacks payload capacity. For instance, the patchwork technique is quite resistant against the majority of attacks but can only conceal a very tiny quantity of data.

The strategy advocated in this research makes use of image steganography, a fresh method of steganography. The personal information is contained inside the cover file image that the application creates as a stego image.

6.2 SUGGESTIONS FOR THE FUTURE

The application's main restriction is that it was made to open image files. All carrier files must be pictures. Enhancing the image to text compression ratio will be the focus of future work on this project. The scope of this project can be increased to the point where it can be applied to many sorts of multimedia files.

GitLink: https://github.com/rupak8108/ImageSteganography.git

Reference :

1. Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji , B. N. (2022). Digital image steganography: A literature survey. Information Sciences.

2. Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.

3. Kharrazi, M., Sencar, H. T., & Memon, N. (2004). Image steganography: Concepts and practice. Lecture Note Series, Institute for Mathematical Sciences, National University of Singapore.

4. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (Vol. 1, No. 2, pp. 1-11).

5.https://www.researchgate.net/publication/314116270_Image_Steganography

Turnitin Originality Report

11/8/22, 2:17 PM Turnitin - Originality Report - 182-35-354

Turnitin Originality Report

Processed on: 06-Nov-2022 15:16 +06
ID: 194574425[illegible]
Word Count: 2202
Submitted: 1

182-35-354 By Md. Matiur Rahman Rupak

Similarity Index	Similarity by Source	
30%	Internet Sources:	19%
	Publications:	1%
	Student Papers:	21%

6% match (student papers from 27-Aug-2022)
Submitted to Nectar Technical Training Foundation on 2022-08-27

5% match (Internet from 04-Jun-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8052/162-35-152%20%2822%25%29.pdf?isAllowed=y&sequence=1

3% match (Internet from 12-Jun-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8132/171-35-172%20%2818%25%29.pdf?isAllowed=y&sequence=1

2% match (Internet from 04-Jun-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8083/161-35-1523%2817_%29.pdf?isAllowed=y&sequence=1

2% match (Internet from 06-Aug-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8182/171-35-226%20%2823%25%29.pdf?isAllowed=y&sequence=1

2% match (Internet from 10-Apr-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/6140/161-35-130%2021_.pdf?isAllowed=y&sequence=1

2% match (student papers from 28-Mar-2018)
Class: Article 2018
Assignment: Journal Article
Paper ID: 937400554

1% match (Internet from 19-May-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/7813/153-35-1356%20%2823_%29.pdf?isAllowed=y&sequence=1

1% match (Internet from 05-Jan-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5693/171-35-1870%20%2824_%29.pdf?isAllowed=y&sequence=1

1% match (Internet from 26-Oct-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8221/181-35-2423%20%2830%25%29.pdf?isAllowed=y&sequence=1

1% match (student papers from 27-Aug-2022)
Submitted to Nectar Technical Training Foundation on 2022-08-27

1% match (Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane. "Image Steganography: A Review of the Recent Advances", IEEE Access, 2021)
Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane. "Image Steganography: A Review of the Recent Advances", IEEE Access, 2021

1% match (student papers from 08-Aug-2022)
Submitted to Coventry University on 2022-08-08

1% match (Internet from 18-Feb-2022)

https://www.turnitin.com/newreport_printview.asp?eq=1&eb=1&esm=10&oid=1945744254&sid=0&n=0&m=2&svr=9[illegible] 1/5

https://www.coursehero.com/file/119820534/Software-Design-Document-Group-3pdf/

1% match (student papers from 23-Sep-2022)
Submitted to Midlands State University on 2022-09-23

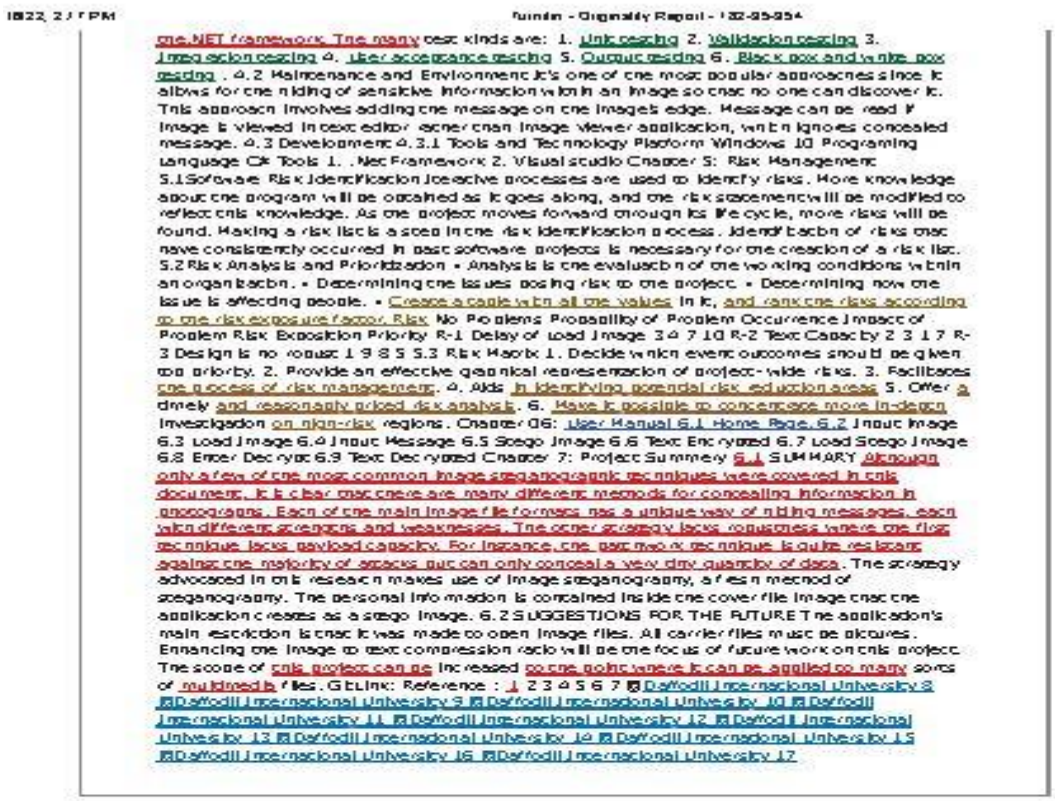
1% match (student papers from 16-Jan-2015)
Submitted to MCAST on 2015-01-16

< 1% match (Internet from 15-Mar-2020)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/3553/P13659%20%28%29%25%29.pdf?isAllowed=y&sequence=1

Daffodil International University Department of Software Engineering SWE-431 Project/Thesis Project Documentation Image Steganography Supervised By: Mr. Sk. Fazlee Rabby Senior Lecturer Department of SWE Daffodil International University Submitted By: Modur Rahman Rubak ID: 182-35-354 Department of SWE Daffodil International University This Report Presented In Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Software Engineering. APPROVAL This Project titled "Image Steganography – A Desktop application developed with (C#,.net Framework)", submitted by , Modur Rahman Rubak ID: 182-35-354 to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the wants for the degree of B.Sc. in Software Engineering and approved on its style and contents. DECLARATION It hereby declares that this project has been done by me under the supervision of Mr. Sk.Fazle Rabby Senior lecturer, Department of Software Engineering, Daffodil International University. It also declare that neither this project nor any part of this has been submitted anywhere else for award of any degree. Supervised by: Mr. Sk. Fazlee Rabby Senior Lecturer Department of SWE Daffodil International University Submitted by: Md. Modur Rahman Rubak ID: 182-35 -354 Department of SWE Daffodil International University ACKNOWLEDGEMENT My sincere gratitude to my Supervisor Mr. Sk. Fazlee Rabby, Lecturer for guiding me throughout the planning and development phase of the system. Without her strategic guideline and counseling I would not have reached the final stage of the development. I would like to thank my close peers and my classmates for being supportive and encouraging throughout my four-year journey here in Daffodil International University. My sincere gratitude goes to Daffodil International University for providing the platform where I was able to cherish and nurture my compassion and improve my technical skills. Much appreciation to Daffodil International University for great support and all necessary academic materials that has taught me great helpful academic as well as life lessons. Finally, yet importantly, I am happy to acknowledge the help of all the individuals to fulfill our attempt. ABSTRACT The art of image steganography involves concealing data—text, images, or even videos—within a cover image. The secret information is concealed such that it cannot be seen by human sight. Recently, there has been more focus on deep learning technology, which has proven to be an effective tool in many fields, including image steganography. The primary objective of this study is to investigate and discuss the various deep learning techniques that are used in the field of image steganography. Traditional approaches, Convolutional Neural Network-based methods, and General Adversarial Network-based methods are the three basic categories into which deep learning techniques used for image steganography can be separated. This paper includes a detailed overview of the approach as well as a list of the datasets used, experimental setups taken into account, and regularly employed evaluation criteria. Approval

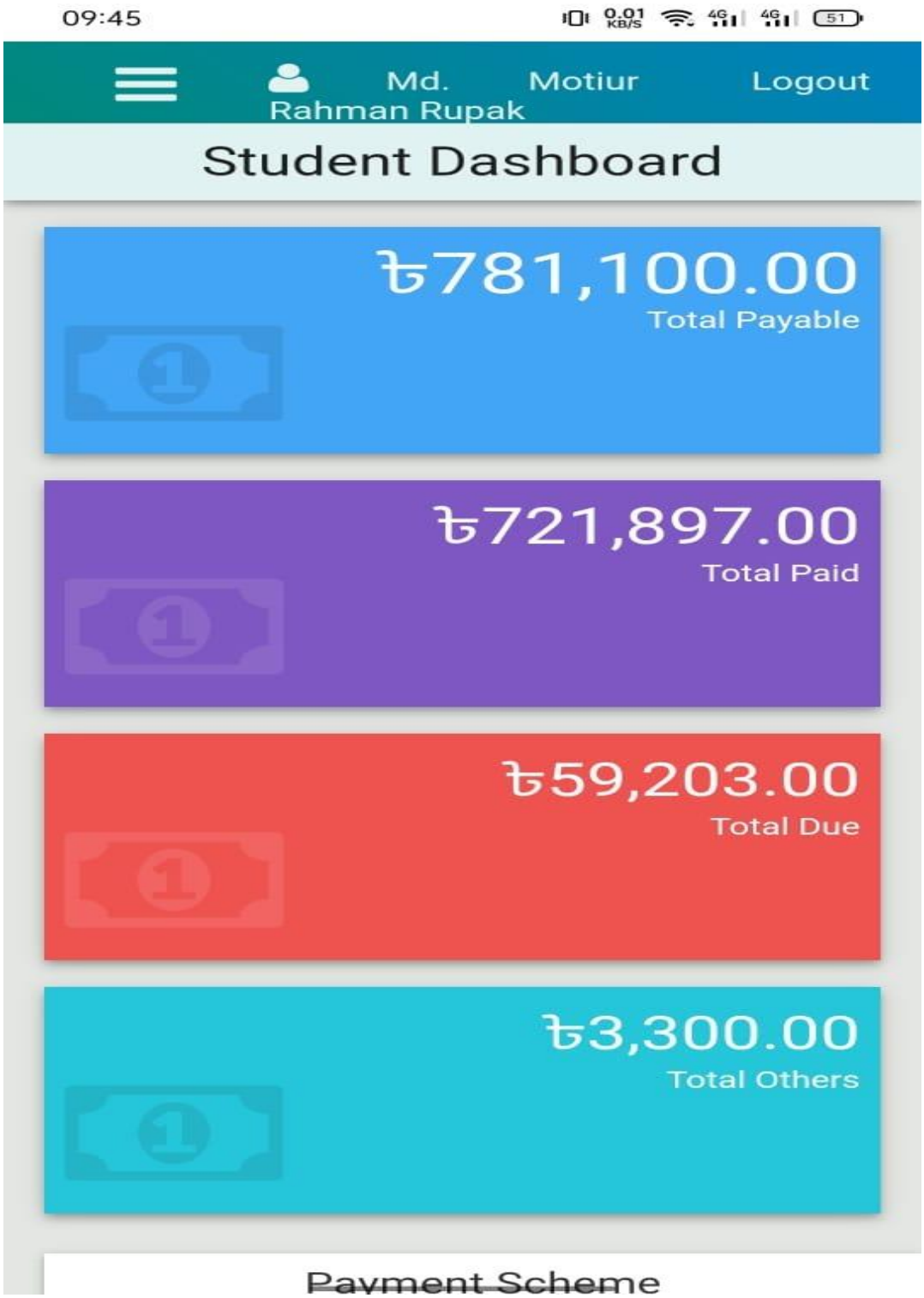
CHAPTER 1 : INTRODUCTION 1.1 INTRODUCTION The science and art of concealing the existence of a message between the sender and the intended recipient is known as

steganography. It is a type of security technique through security. Secret messages have been concealed via steganography in a variety of formats, including digital image 1.2 MOTIVATION Now a days information encryption is very necessary. Steganography is less known process. By using image steganography, we can hide our message securely. 1.3 OBJECTIVES The aim of image steganography is to conceal a concealed message within an image in a way that no one can tell that it is there. Steganography, to put it simply, "means concealing one piece of data within another," In technical terms. 1.4 EXPECTED OUTCOME In contrast, the aim of image steganography is to subtly modify a message by concealing it within another original message. It is anticipated that the changed message will appear fairly similar to the original message. 1.5 Goals Image steganography serves as a means of concealment and deception. It is a type of covert communication that uses any media to encrypt messages. Since it doesn't include data encryption or the usage of a key, it isn't a type of cryptography. Instead, it is a method of data concealing that can be used in cunning ways 1.6 Project Scope A helpful technology for secret information transfer via a communications channel is steganography. The concealed picture is produced by fusing the carrier image and secret image. It is challenging to find the hidden image without retrieval. 1.7 Stakeholders Basically, those who are using our Desktop system and involve with this system users. • User |Sender,Receiver) Brief descriptions about stakeholder are given below User: who are capable of accessing or using all application modules and who have significant control over the entire systems process 1.8 Project Schedule Activities Duration (In week) Total week Preparation Week-1 1 Find Problem & Analysis Week-2 1 Planning Week-3 1 Decall Design Week-4,5 2 Coding Week-6,7,8 3 Development Week-9 1 Testing Week-10,11 2 Documentation Week-12 1 Delivery Week-13 1 Total =13 1.9 Release Plan Release plan is given below: Version Feature Date V-1.0 All activities of assistant, Sender and Receiver 21-10-2022 Chapter 02: Software Requirement Specification 2.1 Functional Requirement List 1. Take image and message input 2. Give output Non Functional Requirement List 1. A high-quality system requires that every function be fully functional. 2. User-friendly Interface 3. The application must approximately extract one picture from one image after hiding it within one image. 4. The software must process data quickly. 5. The program will be presented in English. 2.2Features 1. Encrypt Message In Image 2. Decrypt Message From Image 3. Secret Capacity 4. Transparency of Reception 5. Tamper-resistance 6. Robustness 2.3 Requirment Specification The construction of requirements specifications for steganographic systems is the main topic of the study. The fundamental ideas and application areas of steganography are briefly discussed. The many non-functional needs that can be evaluated using these criteria are grouped, and their potential metrics are provided along with examples and sample requirements. The authors offer a unique methodical approach to developing steganographant system requirements based on the field of usage and the significance of each criterion in the chosen field. The strategy is similar to the idea of the Universal Steg constructor, which ensures that clients obtain the necessary steganographic system from the developers, and it also permits automated selection of steganographic algorithms based on the needs. 2.3.1 Functional Requirment FR-1 Select Image Description User can input Image Stakeholders User FR-2 Upload Image Description The user have to upload the image that has been selected Stakeholders User FR-3 Encryption Description User have to input the message want to embed and hit encryption button Stakeholders User FR-4 Load stego Image Description User who wants the secret text have to upload the stego image to the system Stakeholders User FR-5 Decryption Description Being uploaded the image then the user have to hit the decryption button Stakeholders User 2.3.2Data Requirement 1. Image 2. Text which wants to embed 2.3.3 Performance Requirement: Three factors can be used to evaluate the effectiveness of a steganographic process. 1. hiding capacity 2. distortion control 3. security The quantity of data that may be completely concealed in an image is referred to as the concealing capacity. It can also be expressed as the quantity of bits in a single pixel. 2.3.4 Security Requirement: Image steganography's security is reliant on the secret key set that is employed to insert the hidden image. The hidden image can be obtained by using the secret key, which has been revealed. We suggest a new kind of steganography technique employing visual cryptography to address its security issue. Chapter 03: System Design 3.1 Use Case Diagram 3.2 Use Case Description Table 3.2.1 Sender Side Use Case No 01 Use Case Name Image Steganography Actor Sender Description Allow to Encrypt Precondition Way Image Steganography Trigger Click Encrypt Button Flow of Event 1.Select Image 2.Press Encrypt Button 3.Hidden Encrypted Message In Image Table 3.2.2 Receiver Side Use Case No 02 Use Case Name Image Steganography Actor Receiver Description Allow to Decrypt Precondition Way Image Steganography Trigger Click Decrypt Button Flow of Event 1.Select Stegano Image 2.Press Decrypt Button 3.Show Hidden Encrypted Message 3.3 Activity Diagram 3.4 Data Flow Diagram 3.5Class Diagram Chapter 04: System Test and Development 4.1 Testing Introduction Software testing is a crucial part of software quality assurance, and many software companies devote up to 40% of their budgets to it. Testing life-critical software can be quite expensive. This has led to a large number of studies on risk analysis. In software projects, this term refers to the likelihood of unfavorable occurrences like schedule delays, cost overruns, Software testing There are various methods for testing an application built with

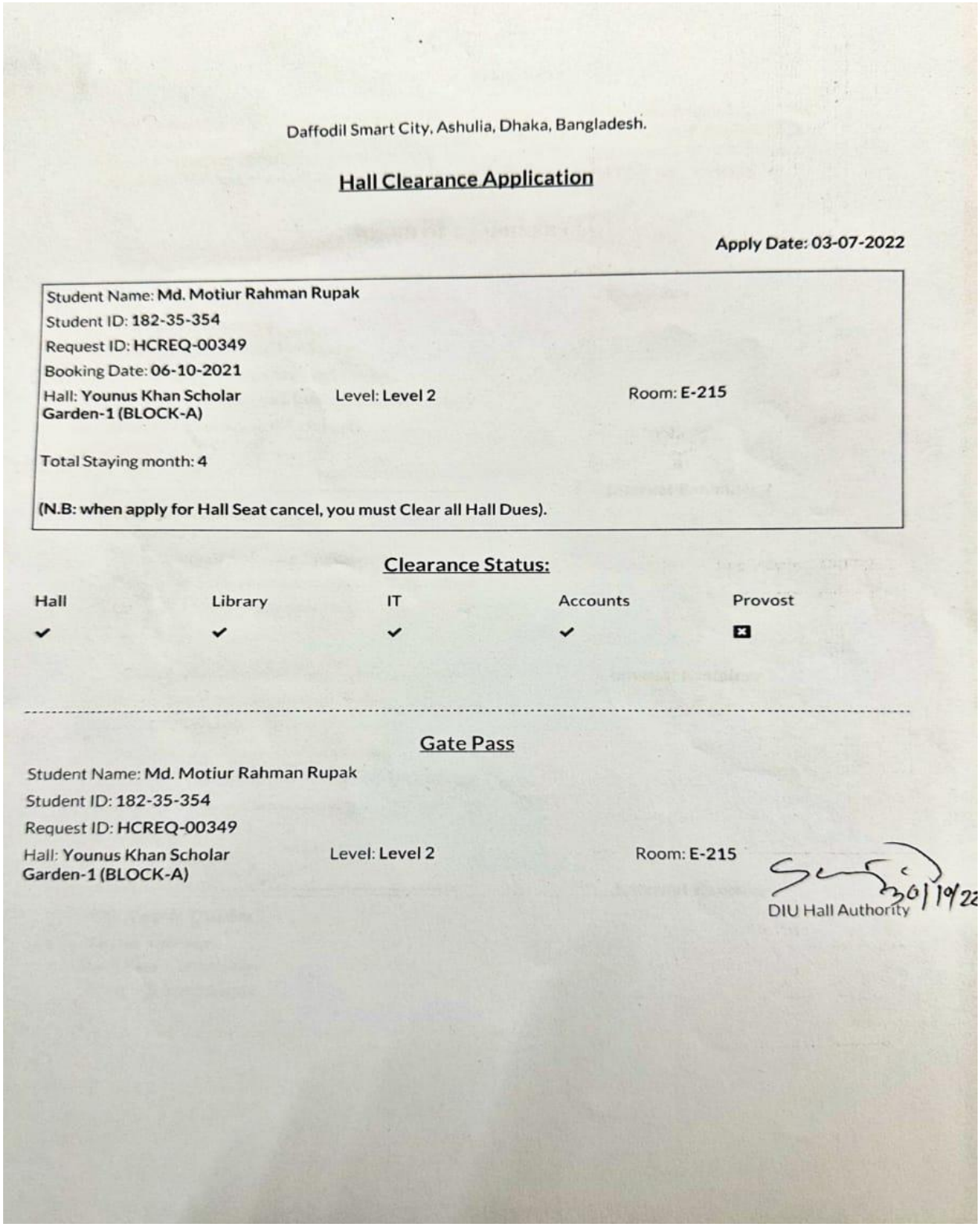


one.NET framework. The many test kinds are: 1. Unit testing 2. Validation testing 3. Integration testing 4. User acceptance testing 5. Output testing 6. Black box and white box testing . 4.2 Maintenance and Environment It's one of the most popular approaches since it allows for the hiding of sensitive information within an image so that no one can discover it. This approach involves adding the message on the image's edge. Message can be read if image is viewed in text editor other than image viewer application, which ignores concealed message. 4.3 Development 4.3.1 Tools and Technology Platform Windows 10 Programing Language C# Tools 1. .Net Framework 2. Visual studio Chapter 5: Risk Management 5.1Software Risk Identification Iterative processes are used to identify risks. More knowledge about the program will be obtained as it goes along, and the risk statements will be modified to reflect this knowledge. As the project moves forward through its life cycle, more risks will be found. Making a risk list is a step in the risk identification process. Identification of risks that have consistently occurred in past software projects is necessary for the creation of a risk list. 5.2 Risk Analysis and Prioritization • Analysis is the evaluation of the working conditions within an organization. • Determining the issues posing risk to the project. • Determining how the issue is affecting people. • Create a table with all the values in it, and rank the risks according to the risk exposure factor. Risk No Problems Probability of Problem Occurrence Impact of Problem Risk Exposition Priority R-1 Delay of load Image 3 4 7 10 R-2 Text Capacity 2 3 1 7 R-3 Design is not robust 1 9 8 5 5.3 Risk Matrix 1. Decide which event outcomes should be given top priority. 2. Provide an effective graphical representation of project-wide risks. 3. Facilitates the process of risk management. 4. Aids in identifying potential risk reduction areas 5. Offer a timely and reasonably priced risk analysis. 6. Have it possible to concentrate more in-depth investigation on high-risk regions. Chapter 06: User Manual 6.1 Home Page 6.2 Input Image 6.3 Load Image 6.4 Input Message 6.5 Stego Image 6.6 Text Encrypted 6.7 Load Stego Image 6.8 Enter Decrypt 6.9 Text Decrypted Chapter 7: Project Summery 6.1 SUMMARY Although only a few of the most common image steganographic techniques were covered in this document, it is clear that there are many different methods for concealing information in photographs. Each of the main image file formats has a unique way of hiding messages, each with different strengths and weaknesses. The other strategy lacks robustness where one first technique lacks payload capacity. For instance, the last two technique is quite resistant against the majority of attacks but can only conceal a very tiny quantity of data. The strategy advocated in this research makes use of image steganography, a fresh method of steganography. The personal information is contained inside the cover file image that the application creates as a stego image. 6.2 SUGGESTIONS FOR THE FUTURE The application's main restriction is that it was made to open image files. All carrier files must be pictures. Enhancing the image to text compression ratio will be the focus of future work on this project. The scope of this project can be increased to the point where it can be applied to many sorts of multimedia files. GitLink: Reference : 1 2 3 4 5 6 7 Daffodil International University 8 Daffodil International University 9 Daffodil International University 10 Daffodil International University 11 Daffodil International University 12 Daffodil International University 13 Daffodil International University 14 Daffodil International University 15 Daffodil International University 16 Daffodil International University 17

Accounts clearance



Hall clearance



Daffodil Smart City, Ashulia, Dhaka, Bangladesh.

Hall Clearance Application

Apply Date: 03-07-2022

Student Name: **Md. Motiur Rahman Rupak**
Student ID: **182-35-354**
Request ID: **HCREQ-00349**
Booking Date: **06-10-2021**
Hall: **Younus Khan Scholar Garden-1 (BLOCK-A)** Level: **Level 2** Room: **E-215**

Total Staying month: **4**

(N.B: when apply for Hall Seat cancel, you must Clear all Hall Dues).

Clearance Status:

Hall	Library	IT	Accounts	Provost
✔	✔	✔	✔	✖

Gate Pass

Student Name: **Md. Motiur Rahman Rupak**
Student ID: **182-35-354**
Request ID: **HCREQ-00349**
Hall: **Younus Khan Scholar Garden-1 (BLOCK-A)** Level: **Level 2** Room: **E-215**

30/10/22
DIU Hall Authority