KOLEJ UNIVERSITI POLY-TECH MARA

FILE HIDING WEB APPLICATION

AMIRUL NAIM BIN MOHD SHAFIEE

KOLEJ UNIVERSITY POLY-TECH MARA KUALA LUMPUR
Faculty of Computing & Multimedia

FILE HIDING WEB APPLICATION

AMIRUL NAIM BIN MOHD SHAFIEE
AM1901005018

NET401
NOVEMBER 2020

Declaration of Originality

This project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet, etc.) has been acknowledged within the main report to an item in the References or Bibliography lists.

I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Copyright Acknowledgement

I acknowledge that the copyright of this project and report belongs to Kolej University Poly-Tech MARA.

Signed: Date:

Office Stamp

Abstract

This project describes the development of web applications. The name of this web application is File Hiding Web Application. This web application will help any users that want to hide their confidential files securely. Thus, this system provides a security element such as steganography and cryptography techniques. This system should hide the user's confidential data by using image steganography and cryptography methods. Besides, this web application is a very useful medium to make sure the user's confidential data can be hidden from unauthorized users. In this web application, we have two entities, which is the administrator and user. Administrator act as the person in charge to manage user's data who has been registered in the system. Thus, the admin should be the owner or developer of the website. For users, they can perform the main features of this web application, which is to hide their confidential files inside the image and reveal their hidden files contained in the image file. Thus, this web application allows users to easily hide their confidential files and those files will not be easily known by unauthorized users since there is some security element implemented in this system.

This project was develop based on Agile methodology. Thus, the process of this project consists of five phases such as planning and analysis, design, implementation, testing and feedback. If there is an adjustment on the system, new iteration will be proceeded. During the development of this project, all the information related to this project has been gathered. This including the literature review, questionnaire and testing of the system given to the target user. The result helps this project produce a better output. Based on the result, this web application able to provide its main feature which is hiding a file inside the image and revealing the hidden files contained in the image file. This web application also able to provide encryption method to secure user’s confidential files. This web application produces an output same as been expected.

During the time given to complete this project, finally this project achieves its objectives. The File Hiding Web Application has successfully developed, and the main objective of the application such as hide a file inside the image, revealing the hidden files, and able encrypt the hidden file are all achieved. With this achievement, this web application helps to solve the problem when someone wants to hide their files from being viewed by unauthorized users. As a result, this project was successfully completed before the deadline.

Table of Contents

Additional Materials on the Accompanying CD **14**
1 Introduction **16**
1.1 Introduction **16**
1.2 Background to the Project **16**
1.3 Problem Statement **19**
1.3.1 Limited file type to hide the data 19
1.3.2 Unauthorized user easily finds and view hidden file 19
1.3.3 Revealing process is not provided and only certain file types can be revealed 19
1.4 Project Objectives **20**
1.4.1 To enable a user to hide any type of file inside an image 20
1.4.2 To ensure that hidden files are not read or viewed by unauthorized users 20
1.4.3 To allow a user to reveal any type of files contained inside the image file 20
1.5 Project Scope **21**
1.6 Target User **21**
1.7 Overview of This Report **22**
1.8 Conclusion **24**
2 Investigation **25**
2.1 Introduction **25**
2.2 Steganography **26**
2.2.1 Concept and Theory of Steganography 26
2.2.3 Type of Steganography 27
2.2.2 Method Used 28
2.2.2.1 Image Steganography 28
2.2.4 Benefits of Steganography 29
2.3 Cryptography **30**
2.3.1 Concept and Theory of Cryptography 30
2.3.2 Type of Cryptography 31
2.3.3 Algorithm Implementation 34
2.3.4 Benefits of Combining Cryptography and Steganography 37
2.4 Existing Project **38**
2.4.1 Steganography Online Codec by PELock 38
2.4.2 Steganofile 40
2.4.3 SteganPEG 42
2.5 Discussion **44**
2.5.1 Comparison About 3 Existing Project 44
2.5.2 Discussion of Existing Project 45
2.6 Conclusion **46**
3 Methodology **47**
3.1 Introduction **47**
3.2 Agile Methodology **47**

3.2.1 Concept and Theory 47
3.3 Phases in Agile Methodology 49
3.3.1 Planning & Analysis 50
3.3.2 Design 50
3.3.3 Implementation 51
3.3.4 Testing 51
3.3.5 Review and Feedback 51
3.4 Conclusion 52
4 Requirements 53
4.1 Introduction 53
4.2 Data Gathering Techniques 53
4.2.1 Questionnaire 53
4.2.2 Inspecting on the existing systems 54
4.3 System Requirement 55
4.3.1 Functional Requirements 55
4.3.2 Non-Functional Requirements 57
4.3.2.1 Availability 57
4.3.2.2 Reliability 57
4.3.2.3 Portability 57
4.3.2.4 Security 58
4.3.3 Software Requirements 58
4.3.3.1 Visual Studio Code 58
4.3.3.2 Windows 59
4.3.3.3 MongoDB Compass Community 59
4.3.3.4 Microsoft Office Professional Plus 2019 60
4.3.4 Hardware Requirements 60
4.3.4.1 Laptop 60
4.3.4.2 Laser Printer 61
4.4 Conclusion 61
5 Analysis 62
5.1 Introduction 62
5.2 Data and System Modeling 63
5.3 Use Case Diagram 64
5.4 Flowchart Diagram 65
5.5 Data Finding and Analysis 67
5.5.1 Questionnaire Feedback 67
5.5.1.1 Section A: Respondent Information 67
5.5.1.2 Section B: Image Steganography Techniques 70
5.5.1.3 Section C: Use of File Hiding Application 72
5.6 Conclusion 77
6 Design 78
6.1 Introduction 78
6.2 Interface Design 79
6.2.1 Homepage Design 79
6.2.2 Login Design 79

6.3.3 Sign-Up Design....80
6.3.4 User Account Design....81
6.3.5 Steganography Hiding Files Design....82
6.3.6 Steganography Reveal Files Design....83
6.3.7 Admin Account Design....84
6.3.8 Manage User Design....85
6.3.9 Add New User Design....85
6.3.10 Edit User Information Design....86

6.3 Database Design....87
6.3.1 Data Dictionary....87
6.3.2 Data Flow Diagram....88
6.3.3 Entity-Relationship Diagram (ERD)....89

6.4 Security System Framework....90
6.4.1 Security Element Framework....90

6.5 Flow of the System....92

6.6 Conclusion....94

7 Implementation....95

7.1 Introduction....95

7.2 Execution Platform....95
7.2.1 Windows 10....95
7.2.2 Google Chrome....96

7.3 Implementation Tools....96
7.3.1 Software....96
7.3.1.1 Visual Studio Code....96
7.3.1.2 MongoDB Compass Community....97
7.3.1.3 JavaScript Programming Language....97
7.3.1.4 Node.js....98
7.3.2 Hardware....98

7.4 System Interface....99
7.4.1 Homepage Interface....99
7.4.2 About Interface....100
7.4.3 Sign-up Interface....100
7.4.4 Login Interface....101
7.4.5 Login Validation Error Interface....102
7.4.6 User Account Interface....102
7.4.7 Steganography Hiding Files Interface....103
7.4.8 Steganography Revealing Files Interface....104
7.4.9 Guide Interface....105
7.4.10 Admin Account Interface....106
7.4.11 Manage User Interface....106
7.4.12 Add New User Interface....107
7.4.13 Edit User Information Interface....108

7.5 Significant Function....109
7.5.1 Encrypting Algorithm....109
7.5.2 Hiding the Files Algorithm....110
7.5.3 Decrypting Algorithm....111
7.5.4 Revealing the Files Algorithm....112
7.5.5 Hashed the User Password....113

7.6 Conclusion 113

8 Testing 114

8.1 Introduction 114

8.2 Unit Testing 114

8.3 Integration Testing 121

8.4 System Testing 128

8.4.1 Functional Testing 128

8.4.2 Non-Functional Testing 130

8.5 Acceptance Testing 131

8.5.1 Alpha Testing 131

8.5.2 Beta Testing 131

8.5.3 Analysis of Acceptance Testing 132

8.5.3.1 Part A: System Design 132

8.5.3.2 Part B: System Functionalities 133

8.5.3.3 Part C: System Security 135

8.5.3.4 Part D: Opinion 137

8.6 Conclusion 137

9 Project Management 138

9.1 Introduction 138

9.2 Project Schedule 138

9.2.1 Work Breakdown Structure (WBS) 139

9.2.2 Gantt Chart 140

9.3 Risk Management 141

9.4 Conclusion 142

10 Conclusion 143

10.1 Introduction 143

10.3 Achievements 143

10.3 Future Work 144

10.3.1 Build the system for mobile application 144

10.3.2 Add cloud storage feature 144

10.3.3 Add digital watermarking feature 144

10.3.4 Improve the interface design 145

10.4 Project Evaluation 145

10.5 Conclusion 146

References 147

Appendix A – Requirements Specification Document 151

Appendix B – User Manual 160

Appendix C – Turnitin Result 166

Appendix D – Log Book 177

List of Figures

Figure 1.0.1 Combining Steganography and Cryptography Structure 17
Figure 2.1 Main Diagram of Steganography 26
Figure 2.2 Cryptography System 30
Figure 2.3 Symmetric-key Encryption 31
Figure 2.4 Asymmetric-key Encryption 32
Figure 2.5 Hash Function Structure 33
Figure 2.6 Steganography Online Codec Page 38
Figure 2.7 PELock Encode and Decode Interface 39
Figure 2.8 Steganofile Dashboard 40
Figure 2.9 Encoding File Interface 41
Figure 2.10 Decoding File Interface 41
Figure 2.11 SteganPEG Dashboard 42
Figure 2.12 Adding Secret Files Interface 43
Figure 3.1 Agile Model 48
Figure 4.1 Visual Studio Code Logo 58
Figure 4.2 Windows Operating System Logo 59
Figure 4.3 MongoDB Compass Community Logo 59
Figure 4.4 Microsoft Office 2019 Logo 60
Figure 4.5 Acer Nitro 5 Laptop 60
Figure 5.1 Use Case Diagram for File Hiding Web Application 64
Figure 5.2 Flowchart Diagram of File Hiding Web Application 65
Figure 5.3 Questionnaire Result for Gender in percentage 67
Figure 5.4 Questionnaire Result for Age in percentage 68
Figure 5.5 Questionnaire Result for Race in percentage 69
Figure 5.6 Questionnaire Result for Occupation Status in percentage 69
Figure 5.7 Result of Question 1 for Section B 70
Figure 5.8 Result of Question 2 for Section B 71
Figure 5.9 Result of Question 3 for Section B 71
Figure 5.10 Result of Question 1 for Section C 72
Figure 5.11 Result of Question 2 for Section C 73
Figure 5.12 Result of Question 3 for Section C 73
Figure 5.13 Result of Question 4 for Section C 74
Figure 5.14 Result of Question 5 for Section C 75
Figure 5.15 Result of Question 6 for Section C 75

Figure 5.16 Result of Question 7 for Section C 76
Figure 6.1 Homepage Design 79
Figure 6.2 Login Design 79
Figure 6.3 Sign-Up Design 80
Figure 6.4 User Account Design 81
Figure 6.5 Steganography Hiding Files Design 82
Figure 6.6 Steganography Reveal Files Design 83
Figure 6.7 Admin Account Design 84
Figure 6.8 Manage User Design 85
Figure 6.9 Add New User Design 85
Figure 6.10 Edit User Information Design 86
Figure 6.11 Data Flow Diagram 88
Figure 6.12 Entity-Relationship Diagram 89
Figure 6.13 Security Element Framework 90
Figure 6.14 Application Flowchart 92
Figure 7.1 Windows 10 Logo 95
Figure 7.2 Google Chrome Logo 96
Figure 7.3 Visual Code Studio Logo 96
Figure 7.4 MongoDB Compass Community Logo 97
Figure 7.5 JavaScript Logo 97
Figure 7.6 Node.js Logo 98
Figure 7.7 Homepage Interface 99
Figure 7.8 About Interface 100
Figure 7.9 Sign-up Interface 100
Figure 7.10 Login Interface 101
Figure 7.11 Login Validation Error 102
Figure 7.12 User Account Interface 102
Figure 7.13 Hiding Files Interface 103
Figure 7.14 Revealing Files Interface 104
Figure 7.15 Guide Interface 105
Figure 7.16 Admin Account Interface 106
Figure 7.17 Manage User Interface 106
Figure 7.18 Add New User Interface 107
Figure 7.19 Edit User Information Interface 108
Figure 7.20 Encrypting Algorithm 109
Figure 7.21 Hiding the Files Algorithm 110
Figure 7.22 Decrypting Algorithm 111

Figure 7.23 Revealing the Files Algorithm 112
Figure 7.24 Hashed User Password 113
Figure 8.1 Result of Question 1 for Section A 132
Figure 8.2 Result of Question 2 for Section A 133
Figure 8.3 Result of Question 1 for Section B 133
Figure 8.4 Result of Question 2 for Section B 134
Figure 8.5 Result of Question 3 for Section B 134
Figure 8.6 Result of Question 1 for Section C 135
Figure 8.7 Result of Question 2 for Section C 135
Figure 8.8 Result of Question 3 for Section C 136
Figure 8.9 Result of Question 4 for Section C 136
Figure 8.10 Result of Question 1 for Section D 137
Figure 9.1 Work Breakdown Structure (WBS) 139

List of Tables

Table 2.1 Comparison of 3 Existing Project 44
Table 4.1 Administrator Functional Requirements 55
Table 4.2 Users Functional Requirements 56
Table 4.3 Hardware Specification 61
Table 6.1 Data Dictionary for File Hiding Web App 87
Table 7.1 Laptop Specification 98
Table 8.1 Unit Testing 114
Table 8.2 Integration Testing 121
Table 8.3 Functional Testing 128
Table 8.4 Non-Functional Testing 130
Table 9.1 Gant Chart for Week 1 – 14 140
Table 9.2 Gant Chart for Week 15 – 28 140
Table 9.3 Risk Management 141

Additional Materials on the Accompanying CD

Acknowledgements

Bismilliahirrahmanirrahim, Alhamdulillah thanks to Allah SWT, the Most Gracious, Most Merciful Praise, Lord of the Worlds, Master of the Day of Judgement, God of the first and the last, Sustainer of heaven and earth, and peace and blessings be upon His Prophet, the Teacher of Mankind, sent as a Mercy to the worlds. Thanks to Allah SWT for giving me strength and with His permission I can complete this thesis paper project. I would like to express my gratitude and appreciation to all those who had given me the possibility to complete this thesis for Final Year Project of Semester 8 CC202.

Without hesitation, I may say that the final year project I had for eight months could not be done successfully without the valuable support of a number of people. For instance, my family, friends, lecturers who never give up motivate me. I have a responsibility to thank all the people who have given valuable cooperation, assistance and guidance to succeed in my final year project.

First of all, my sincere thanks to Allah S.W.T. for grace and compassion and ease me in all matters during the development of this project. Secondly, special thanks to our beloved supervisor, Madam Noraliza Binti Azizan, who help me by giving me suggestions and encouragement. She also helps and guides us in writing this report chapter by chapter throughout the process development of the project File Hiding Web Application. Then, deepest thanks and gratitude to my parents, relatives, friends and others for their cooperation, guidance, suggestion and full support from the beginning to the end.

Last but not least, many thanks go to all those who have helped me through this project and who have made every effort to guide me towards the goal, as well as to encourage me to keep my progress on track. I would like to thank the feedback provided by the supervisor and other lecturers that has developed my presenting skills through suggestions and tips since the semester 1. And I would like to thanks Kolej Universiti Poly-Tech MARA Kuala Lumpur for providing this opportunity to complete a final year report as a part of the requirement in the Bachelor (Hons) in Information Security.

In short, thank you to every person who has impacted my life, and particularly those who have been involved in writing this thesis misery. Thank you, from the point of view of my heart policy, because I cannot do this without you.

1 Introduction

1.1 Introduction

This chapter will discuss about the project that needs to be developed by the developer. This including the background of the project, problem statement and objective of the project. Project background should explain according to what type of project will be developed such as the current issues and problems on the existing projects. Other than that, the security concept on this project should be simply described in this section. Then, the problem statement which is the reason why developers need to build this project should be explained in detail. The project objective must be mentioned to achieve the goals of this project. It also will be discussed in this chapter. Finally, the overview of the report is where the simple explanation is written for each chapter available in this project.

1.2 Background to the Project

The project is to develop a web-based application which allows user to hide their file into another file, which is an image file. This project aims to develop a file hiding web application using image steganography method. The system should be used by any users that would like to hide their confidential information or send secret information to other people. Intended users should use this application because this application will ease the user to perform the process of hiding and revealing the files inside the image file which is easy to perform rather than using the existing system which is quite difficult to perform both hiding and revealing the files. In this project, the objective is to add some new features from the current system.

The reason users need to use this system is that the existing system has an issue where only certain files can be hidden. Some of the systems can hide text messages only and some others only can hide image files. Thus, it is difficult for users to hide any file that they want to keep secret because they need to use many tools or applications that support the file type to be hidden. Therefore, the significance of this project to the users is they can hide any file type that they want, including text message, image, audio, video, and document.

Other than that, the current issue gets worse when some of the current systems did not provide encryption for the hidden file. This will become a problem to the user since their confidential information or file should be secured from unintended users. Thus, this system will implement additional features which are encryption techniques to secure the hidden file. Users can set a password to lock the hidden file and only authorized users can decrypt the hidden file.

Then, some current similar system is lack of features such as able to perform a revealing the file inside the image file process. Although some current systems provide the revealing process, they can only reveal certain types of files only. Thus, to overcome this problem, this project will give significance to the users because the new features in this project will allow users to perform a revealing process no matter what type of file inside the image is, either it is audio, video, image or document. This project also allows the user to save the image files contain a secret file or the secret file itself by downloading it and save it on user devices.

Therefore, this project will secure user confidential information by hiding their information using the image steganography method. This project also provides encryption for the hidden file and improve the feature of the current system by providing revealing process to view the hidden file inside the image. With the web-based application that will be developed, this will guarantee the security of the hidden file.

Hiding a file with steganography techniques is not enough because it only can hide the secret data but not to encrypt it. Thus, this project focuses more on combining steganography and cryptography techniques. With cryptography techniques, users can secure the hidden file using the encryption method.

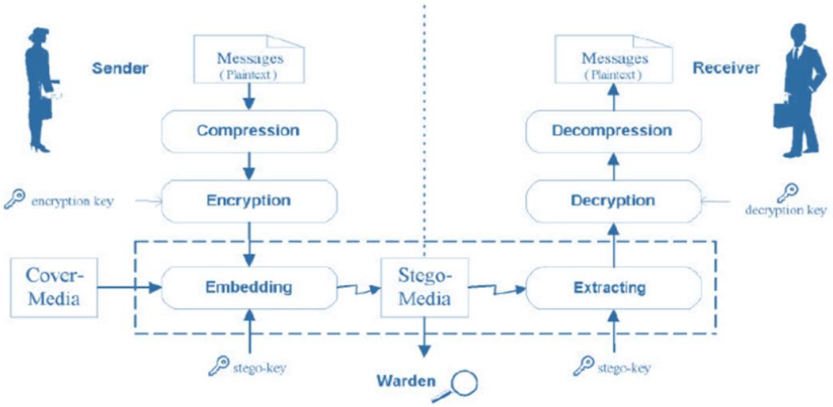


Figure 1.0.1 Combining Steganography and Cryptography Structure (Altigani & Barry, 2013)

Figure 1.1 shows an example structure of combining steganography and cryptography. The cryptography method is the process of encrypting the secret message write by the sender. Then in this structure, the secret message is compressed then the sender sets a password to encrypt the secret message. After being encrypted, the steganography method continues the process by covering the secret message using any media such as images. Thus, the secret message is concealed in the image file.

To reveal or extract the secret message, the reverse process of concealing the message should be executed. Thus, the receiver needs to get the decrypted key or password that has been set by the sender.

Then, the password will be used by the receiver can reveal the secret message after extracting and decompression processes are done.

In summary, the structure above is the process that will be implemented in this project. File Hiding Web Applications enables users to hide any file using this combination technique. With this technique, this project can ensure the effectiveness and reliability of the application to hide user confidential data.

1.3 Problem Statement

1.3.1 Limited file type to hide the data

Most of the current system provides only one type of file to be hidden. For example, some systems can only hide text messages and other systems can only hide the image files. This can be difficult for users because they need to find different hiding tools or software to hide any file type that they want. User may give up to hide their confidential information since it cost time to search for a tool that can hide any specific file type. Thus, the confidential information is in danger since it is stored in a raw format and can be easily leaked to unauthorized users.

1.3.2 Unauthorized user easily finds and view hidden file

Some of the current systems did not provide encryption or password to lock the hidden file. When the hidden file does not have any password or encryption to open it, the process of hiding data is simply pointless. It is still not secure even the user already hides the data because an intruder may detect the secret information easily and find a solution to conceal or reveal it since the hidden file is not encrypted. Without encrypting this hidden file, it will make it easier for intruders to obtain secret data.

1.3.3 Revealing process is not provided and only certain file types can be revealed

Most of the current systems may not provide the revealing of the files inside the image file process. Although some current systems provide the revealing process, the system can only reveal certain types of files only. This can be difficult for users because they cannot reveal the hidden file easily since some current systems did not provide the revealing process. Other than that, since some of the current systems only can hide certain file types, then the system also only could reveal certain types of hidden files. Thus, they need to find different revealing tools or software to reveal the hidden files inside the image file.

1.4 Project Objectives

1.4.1 To enable a user to hide any type of file inside an image

This project is to allow a user to hide any type of secret files or information into another file which is an image file. To make this happen, image steganography techniques need to be implemented in this system. With this technique, the user will be able to hide and unhide the secret file. Other than that, users can hide any type of file including text message, image, audio, video, and any document file type together with the image data. Thus, the secret data can keep in secure since the data are being concealed.

1.4.2 To ensure that hidden files are not read or viewed by unauthorized users

The hidden file being secure with the implementation of cryptography in this system. This project enables the user to set a password and encrypt their hidden file. Only the user who has the encryption key or password can decrypt the hidden file. This will ensure that unauthorized users are unable to decrypt and viewed the hidden file. With this web application, users should not worry about their secret data to be leak since the hidden file is being encrypted.

1.4.3 To allow a user to reveal any type of files contained inside the image file

With this web application, users not only can hide their confidential file inside the image, but they also can reveal the hidden files inside the image file. To develop this process, the reverse image steganography technique or it can be called steganalysis will be implemented in this system. Users can reveal any type of files such as text message, image, audio, video, and any document file type that is hidden inside the image file. Thus, the secret data or file that has been hidden in the image file could be revealed easily and also, they need to enter the password that has been set to reveal the files.

1.5 Project Scope

This project should produce a web application system. The scope of this project is, it must implement image steganography techniques. This web application enables the users to hide their files into another file which is an image. The file to be hide could be any type of files such as words, PDF, PowerPoint, Excel, images, audio, and video. The application must be able to process the steganography method to hide the user's confidential files. Other than that, this application also includes the cryptographic method which able the users to set a secret password for encrypting and decrypting the confidential file. Then, this application allows users to reveal any type of hidden files inside the image file by performing the steganalysis or revealing process. Users also can download and store the image that contains the hidden file and the hidden files that have been revealed inside their local storage or devices. Besides, this application could be used everywhere since it is a web-based application. Lastly, this web application must be user-friendly where it is easy to use and easy to understand how the applications work.

1.6 Target User

This file hiding web application is open to the public. This means any users that would like to hide their confidential information from the unauthorized user can use this application. This web application provides the usage of administrators and users.

1. **Administrator**

   Administrator roles should be the owner of this web application or the developer. Administrator roles able to add, update and delete any users that have been registered in this application. Admin can view some user information such as name and email. However, they cannot view the user’s password since it has been encrypted. They also can perform the main feature of the system which is hiding the file and revealing the file.

2. **Users**

   Users should be anyone who wants to hide their confidential information. User's roles in this application can hide any type of confidential file into another file which is an image. They can add any file that they want to hide. Other than that, they can add an image that is used as a cover image to hide the user’s secret file. Users can set a password to encrypt the hidden file. Those passwords also will be used to decrypt the hidden file. Users can also decrypt or reveal the hidden file by adding the image file which contains a secret file. Then, they need to enter the same password that has been set to encrypt the hidden file. Lastly, users also able to download the encrypted file and decrypted file and stored it in their devices or local storage.

1.7 Overview of This Report

The project will concentrate on the security of personal or confidential files and how to conceal them from unauthorized people. The overview of this study will be discussed based on the chapter below.

a) Chapter 1: Introduction

Chapter 1 will focus more on introducing the project that will be developed. This including the background of the project. This chapter also provides the objectives of the project and the problem statement that the current system faced by the user.

b) Chapter 2: Investigation

Chapter 2 will focus more on the literature review, which is one of the approaches used to meet the project requirements that can be applied in the project. Usually, the current or existing projects available will be used as a literature review. A discussion about the existing project is included in this chapter. This chapter also provides the concept and theory about the system that will be implemented in the project.

c) Chapter 3: Methodology

Chapter 3 should explain the methodology that has been used in this project. The methodology indicates how the project will be executed to achieve the objectives. This chapter also describes the justification for the use of methods or approaches. It will demonstrate the flow of the project from stage one to the last. The methodology enables developers to achieve their objectives and help the developer complete the project.

d) Chapter 4: Requirement

Chapter 4 will explain more about the requirement needed during the project. This including user and system requirements. This chapter also explains the method used to gather data to meet user requirements. The software and hardware used in this project are also discussed under system requirements.

e) Chapter 5: Analysis

Chapter 5 will analyze all the input gathered from user and system requirements. Developers use questionnaire methods to meet the user requirement and identify what the system needs. The data

may be present and explain in a chart. Moreover, this chapter may contain the illustration of the use case diagram, flow chart, and business process model and notation (BPMN).

f) Chapter 6: Design

Chapter 6 should focus more on designing the system. Analysis from Chapter 5 is important to ensure that the system design meets the user requirement. Moreover, in this chapter developer will design the system based on the user requirement.

g) Chapter 7: Implementation

Chapter 7 is where the development of the system is started. The system will be built and fully operational. Development skills will be implemented in this chapter to code and design the system before it can be tested by the users. The system will be developed in good order until the system becomes the final product.

h) Chapter 8: Testing

Chapter 8 will focus more on testing the product by the users. The final product should be tested to get feedback either it is good and meet the requirement or not. The user can now use it and it includes data changing, testing as well as user training. To test the product, the alpha and beta testing process will be used. Other than that, final changes are possible to made and the developer and user will continue looking for bugs in the system.

i) Chapter 9: Project Management

Chapter 9 describes the process of system development in terms of understanding, tools, and skills. The project schedules are provided in this chapter. This chapter also explains risk management for the project and how to overcome it.9 describes the process of system development in terms of understanding, tools and skills. Project schedule are provided in this chapter. This chapter also explain about risk management for the project and how to overcome it.

j) Chapter 10: Conclusion

Chapter 10 is the last chapter to summarise all the work that has been conducted. The achievement of this project will be discussed either the project meets its objective or not. Moreover, future work is explained to improve the system.

1.8 Conclusion

The web application must be built successfully to achieve the objective of this project. This web application could improve the current security of the file hiding system. The user who wants to hide their confidential information could depend on this application once this application is applied. Users are no longer worried about the reliability of this application to hide their data since the system that will be developed in this project will use both steganography and cryptography techniques to strengthens the system security. The secret data has been in a safe condition since it will be encrypted first before the output image is produced. Also, the security element is a bit tighter than the current application since some algorithms will be implemented in this project.

The problem statement, project objective, and overview of the report that have been discussed above could guide the developer to complete this project before the deadline. The problem statements will help the developers to enhance the feature of the system. Without the objective of the project, the developer could not achieve the aims of this project since there are no goals to be realized. Thus, with the explanation of the project objective, it will help the developer to finish develop this application. An overview of the report can help the developer to organize what to do to complete this project. Therefore, we hope that this chapter could help the developer organize this project in an orderly manner and be able to complete it before the deadline.

2 Investigation

2.1 Introduction

In this modern era, there has been a wide variety of other steganographic inventions and methods over the years (Lake, 2019). Steganography and cryptography are two different techniques that preserve data confidentiality and integrity. According to Telsy (2020), steganography actually comes from ancient Greece, where Herodotus told two cases in his Stories, but the first documented use of the word was in 1499 by Johannes Trithemius in his Steganographia book. However, steganography continues to be used to this day, with technologically advanced versions frequently used by the users to conceal data in images, audio, and other media. File hiding web application is a web-based application that enables a user to hide any file especially confidential files into another file which is an image.

In this chapter, the goal is to make research about the security element concept that will be used in this project and make it as a reference for developing this project. Besides, we have to identify and research some of the image steganography applications that relate to our project.

For the literature review, we will explain more about the concept and theory of the security element that will be used in this system. This includes the algorithm which will be used in this project. Other than that, we studied on the three existing projects that have a similar function as the system that will be developed in this project such as steganography tools on the PELock website, Steganofile, and SteganPEG. From our research, we have found that these applications are related to our web application system.

With these studies, we may draw a comparison with our system. We can identify and analyze the feature of the system to improve the quality of the application in our project. There are also strengths and weaknesses in these three existing applications that we would examine besides those systems that can be used as guides to enhance our application to create an effective system ahead.

2.2 Steganography

2.2.1 Concept and Theory of Steganography

Steganography refers to a method intended to hide interactions between the two communicators. The words steganography is composed specifically of Greek terms στεγανός, covered and γραφία, writing (Telsy, 2020). According to Taha et al. (2019), steganography defines as how a secret message is kept hidden in a cover message in such a manner that its existence is completely hidden. It is also can be referred to as the art or activity of hiding a file, image, audio, or message within another file which is image, audio, or video. The secret message could be in the form of a text file, an image, a ciphertext, or something that can be interpreted as a bit. Thus, the main objective of steganography is to communicate privately with secret information through the cover file. Steganography can also be used in command and control protocols for malware, including reading content from image files accessible by sharing and social media platforms (Yoon, 2019). Therefore, the use of steganography is actually to hide confidential or secret data from unauthorized users. For example, information that is not supposed to be revealed with others can be protected using steganography. Sensitive information, such as financial records, can also be concealed in a cover object and stored on a private computer.

On the other side, steganalysis is the process of identifying or discovering secret messages. It is the reverse process of steganography. Since this project may include this process to reveal the hidden message, steganalysis is one of the important processes in this project. This process aims to evaluate if the file or any other medium contains a secret message and if the result is positive, we can reveal the hidden message contained in the medium (Telsy, 2020).

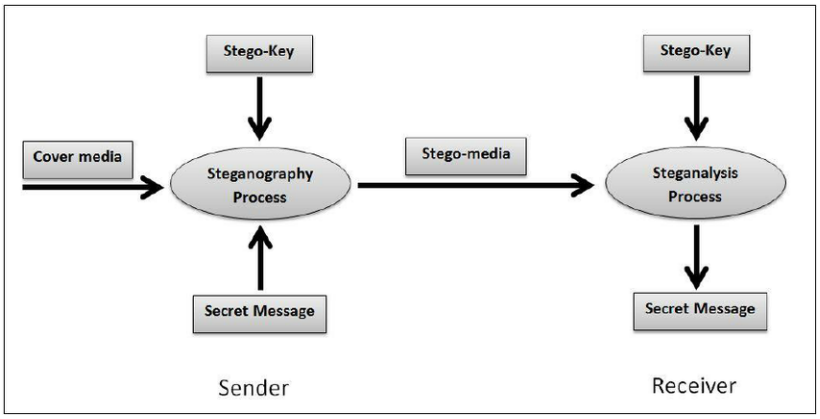


Figure 2.1 Main Diagram of Steganography
(Al Sadi, 2015)

Figure 2.1 shows the process of steganography and steganalysis. The process involves interaction between two people which is sender and receiver. The steganography process executes when the sender hides the secret message in cover media such as an image. Then, the sender includes a stego-key or

password that also be used in this project. The steganalysis process will be executed if the receiver has the stego-key and the secret message sent by the sender should be revealed.

2.2.3 Type of Steganography

According to Pal and Dubey (2016), steganography has five types. The type is listed below:

1) Text Steganography

Text steganography consists of hiding data within text files. In this approach, the secret message is covered behind each ordinal letter of each text message word. A number of ways in which information can be concealed in the text. The ways are format based mostly methodology, random and statistical method, and linguistics method.

2) Image Steganography

This type of steganography uses an image to hide the secret data. Intensities of the image steganography element are used to hide the data. In digital steganography, images are popularly used as a cover source since there are a number of bits present in the digital illustration of an image.

3) Audio Steganography

Audio steganography involves hiding data in audio files. For example, this method hides the secret data in WAV, AU, and MP3 audio formats. There are entirely different ways to do audio steganography. These approaches are low bit encryption, phase, and spread spectrum.

4) Video Steganography

This technique is a way to hide some sort of files or data in a digital video format. In this case, video is used as a cover for the secrecy of information. transform (DCT) adjusts the values such as 8.774 to 9 used to cover the data in each of the images in the video, which is not visible to the human eye. Mp4, MPEG, and AVI are the formats that can be used for video steganography.

5) Network Steganography

Network steganography requires covering information by using a network protocol such as TCP, UDP, ICMP, and IP as a cover entity. There are secret channels in the OSI layer network model anywhere steganography is regularly used.

2.2.2 Method Used

2.2.2.1 Image Steganography

This project uses image steganography which can hide the confidential information within the image file. Means, this project will use an image as a cover to hide the secret data. According to Ives (2017), there are several steganography techniques for hiding the data, however, with the intention of hiding files within images, only two methods were feasible:

1) Hiding the file data within the image data (Least Significant Bit Method)

This type of method actually replacing irrelevant image data with information to be concealed. Normally this approach works by hiding the data in the Least Significant Bits (LSB) of the color component of the images. Therefore, the size of the file shall remain the same as the data or secret message is just replaced, not added. This will ensure that the steganography is tough to locate. However, only a very small amount of secret information can be covered in each image.

2) Adding the file data together with image data

This method can increase the overall file size of secret data and retains full image quality. By adding secret data to an unnoticed part of the file, such as after the logical end of the image, any amount of data can be concealed. Therefore, the user may add secret data in the cover image without regarding the file size of the secret data which is different from hiding the data in the Least Significant Bits (LSB) where it can hide an only a small amount of secret information. However, this approach is easier to detect as the file size increases and the file can be analyzed to reveal secret information.

Thus, the second approach was selected as the objective of the project is to enable the users to hide any number of files in the image, regardless of the resolution of the image. Besides that, file hiding web application uses end of file (EOF) markers to incorporate data that will not normally be found in an image format. The EOF markers for images file types include PNG: AE426082, JPEG: FFD9, and GIF: 3B. Hence, there should be no information after the EOF marker, so any data that is stored after the marker will be ignored by software scanning the file. Other than that, we also implement the cryptography element in this project to secure the confidentiality of the hidden data. The cryptography element will be discussed more in the next section.

2.2.4 Benefits of Steganography

Information security is important to most organizations and even personal computer users. Customer data, financial records, personal data, bank account details, all of this data can be difficult to replace and possibly dangerous if it falls into the unauthorized person. According to Rout and Mishra (2014), it is frustrating if these data lose due to disasters and calamities but losing it to hackers or malware attacks can have much greater implications. It needs appropriate conditions to make steganography techniques effective (Lake, 2019). Steganography may be difficult and time-consuming and also need a secured channel that you can interact with where steganographic technique being used and where the data is concealed. However, this project also combines steganography and cryptography techniques to secure the confidentiality and integrity of data. Using methods such as public-key encryption, you can still communicate without a secure channel. Thus, the use of steganography techniques is one of the solution users can use to secure all these data.

The reason why the steganography method is feasible to hide confidential information is that it is:

1) One-Way Hashing

It is used to ensure that an unauthorized user does not interfere with the secret message. This is implemented by providing a message hash using a specified character length for each input image in the file, while the actual images are actually variable character length (Rout & Mishra, 2014). Whenever the receiver receives the data, it will be decoded. If the hash in the decoded message does not match the hash with the encrypted message, both the sender and receiver of the message will know that it has been compromised. In this project, we also implement one of the hash functions available to keep the data secure.

2) Able to attach text to an image

With steganography, explanatory notes can be added to the image. In a real application, this could be used in the medical profession where when one medical office sends a snapshot to another medical office (Rout & Mishra, 2014). If the issuing medical office wants to include explanatory notes on what the receiving medical office should be focused on, then the steganography method should be used. In this project, this method can be used by the user since the objective of this project is to enable the users to hide any file or data in the image file.

3) Can be used as watermarking

Watermarking can also be implemented using steganography. Watermarking can be used to secure copyright by attaching any additional details to the cover image (Chugh, 2013). Therefore, with

steganography users can maintain the secrecy of confidential information to prevent data from potential intrusion and fraud.

Consequently, the use of steganography is accurate for anyone who wants to hide their secret information. This is because, normally the basic model of steganography consists of a carrier, message, and password. Carrier works as a cover-object which we will use to hide the hidden files in our project. The message is the information that the sender wants to keep secret. For this project, a message can be any text, other images, document, video, audio, or anything that may be concealed in a bitstream, such as a copyright mark, secret communication, or a serial number. While the password is used to ensure that only authorized users who know the secret password able to reveal the data or information from the cover-object (cover image). Therefore, the steganography method gives users an advantage in terms of integrity and confidentiality for hiding secret information.

2.3 Cryptography

2.3.1 Concept and Theory of Cryptography

Cryptography is one of the traditional principles to ensure the secrecy of information sharing between both parties. According to Saleh, Aly and Omara (2016), the accurate meaning of cryptography is "hidden writing" where the word cryptography is originated from the Greek word "kryptós" which stands for "hidden" and "gràphin" which stands for "writing". Cryptography also can be defined as the art of secret sharing that is used to encrypt plain text with a code to the ciphertext to be transmitted between the parties on an unsafe platform (Almuhammadi & Al-Shaaby, 2017). In simple terms, this process is to secure data and prevent unauthorized users to access it. Cryptography can be used in many services such as confidential information, key exchange, authentication, and non-repudiation. This service is to ensure that the communication is secure across the insecure channels.

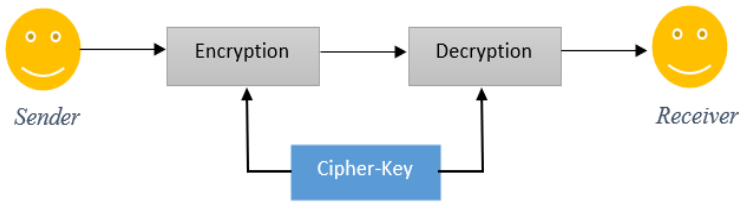


Figure 2.2 Cryptography System

In a cryptography system, as shown in Figure 2.2, the sender should encrypt their secret message first before sending it to the receiver. Then, the receiver needs to decrypt the cipher-key to reveal the secret message delivered by the sender.

According to Saleh, Aly and Omara (2016), plain text, ciphertext, encryption algorithm, decryption algorithm, and key are needed in the cryptography system. The plaintext is a message or information that can be read normally, which means it is not in an encrypted form. Encryption is a conversion process of plain text to ciphertext using a key. While ciphertext is an output from the encryption process where the encryption key is applied on the plaintext. Decryption is the process of extracting the plain text from the ciphertext. The key is used to control the cryptography system and can only be known by the sender and receiver.

However, cryptanalysis could succeed in breaking the ciphers by analyzing the details of the ciphertext to get back the plain text even though this cryptography system is effective for securing data (Saleh, Aly & Omara, 2016). The research of methods and techniques for revealing information from encrypted text is called cryptanalysis (Sharief, 2020). The purpose of cryptanalysis is to counter the cryptography system by using mathematical analysis and algorithms to decipher the ciphers.

2.3.2 Type of Cryptography

There are three types of cryptographic schemes available for securing the data which are public-key (asymmetric-key) cryptography, secret key (symmetric-key) cryptography, and hash functions (Almuhammadi & Al-Shaaby, 2017).

1) Symmetric-Key

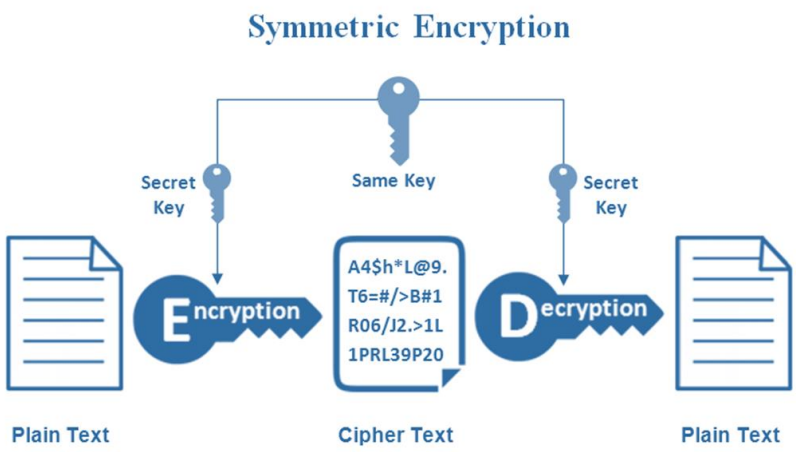


Figure 2.3 Symmetric-key Encryption
(ssl2buy, 2019)

Symmetric-key encryption is also called as shared-key, single-key, and secret-key encryption. According to Mishra (2019), a single secret key that is used by both sender and receiver to encrypt and decrypt the message is a method of cryptography called symmetric key. As shown in Figure 2.3,

to encrypt and decrypt the secret message, the sender and receiver need to use the same secret-key. The key is known only to those two parties who are required to perform encryption and decryption. The method provides better data protection for the transmission. But there is a drawback in the distribution of key (Almuhammadi & Al-Shaaby, 2017). It is because both parties must somehow collect the key or password securely, as there is only one key for both the encryption and the decryption process. Other than that, If the key or password is compromised, the security of the entire data is threatened. Examples of symmetric-key types include Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest Cipher 4 (RC4), and Blowfish algorithm. In this project, we may use this symmetric-key technique to encrypt the hidden data.

2) Asymmetric-Key

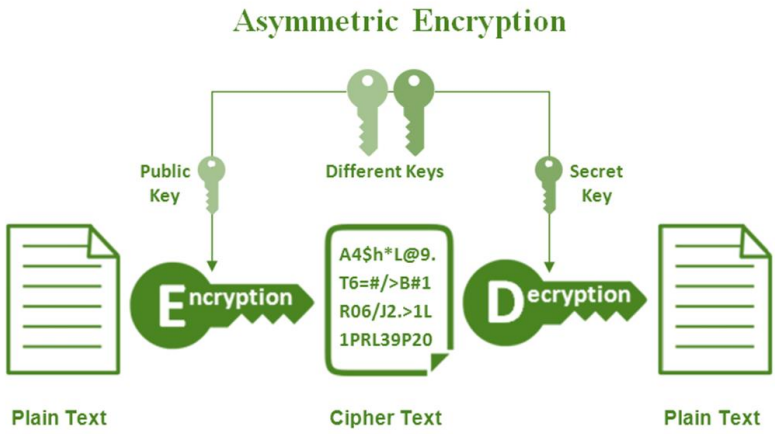


Figure 2.4 Asymmetric-key Encryption
(ssl2buy, 2019)

Asymmetric-key is also called public-key cryptography. This type of cryptography is a totally different and better approach than symmetric-key cryptography (Mishra, 2019). As shown in Figure 2.4, asymmetric encryption uses a pair of keys which is a private key and public key for the encryption and decryption process. Therefore, both keys are needed for each user to run the process. The private key must keep as a secret for the user while the public key is allocated over the network so that if someone wants to send a message to another user, they can use the public keys. Both keys can be used to encrypt a message, and the left key will be used for the decryption process. Examples of asymmetric-key types include RSA, DSA, and Elliptic Curve techniques.

3) Hash Function

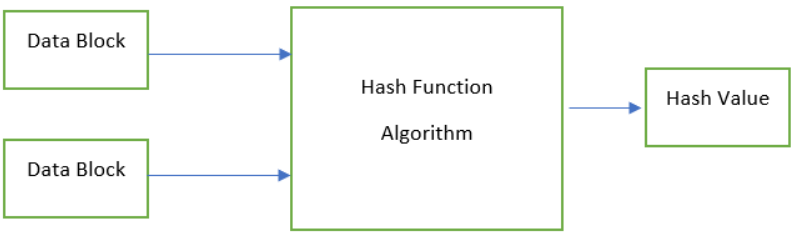


Figure 2.5 Hash Function Structure

A hash function takes a group of characters known as a key and converts it to a value of some length known as a hash value or hash. The hash value defines the original character string but is usually smaller than the original (Techopedia, 2018). One-way, non-collision function with fixed-length output is called a hash function and it is also called a message digest (Almuhammadi & Al-Shaaby, 2017). It

is an algorithm that does not use any key. But, the fixed-length hash value is evaluated based on input data in such a way that it is conceptually difficult to obtain input data from the hash value or even any input string that suits the given hash value.

As shown in Figure 2.5, the hash function works when it executes on two blocks of fixed-length binary data and then produces a hash code. There are numerous rounds of hashing functions, then each round takes the input of the most recent block combination and the output of the last round (Mishra, 2019).

Hashing is being used for encryption too. It can be used to fixed-length output and to make sure the efficiency of operation. Hash functions process faster than symmetric encryption. It is extremely useful and appears in almost all information security applications. It is commonly used to make digital fingerprints of data and to ensure the integrity of files. Examples of popular hash functions are Secure Hash Algorithm (SHA), Message Digest 5 (MD5), Whirlpool, and PBKDF2 (Password-Based Key Derivation Function 2). In this project, we may use this hash function to derive the key for the encryption method.

2.3.3 Algorithm Implementation

I. Algorithm Used

This project may use the combination of steganography and cryptography techniques to ensure the integrity and confidentiality of the hidden file. Therefore, symmetric-key and hash functions will be implemented in the system. Below are the symmetric key and the hash function used in this project:

1) AES-CTR Algorithm

This project will use the symmetric AES-CTR algorithm to encrypt the data. According to Housley (2004), Advanced Encryption Standard Counter Mode (AES-CTR) allows the encryptor to generate a random per-packet value to interact with this value with the decryptor. This specification refers to this per-packet value as an initialization vector (IV). The same IV and key combinations must not be used multiple times. To create a stream cipher, AES-CTR utilizes the AES block cipher. Data will be encrypted and decrypted by XORing with the keystream generated by AES by encrypting simultaneous counter block values. This algorithm is used because it is easy to implement and it supports the precomputation of key streams. AES-CTR is using only AES encryption operation for encryption and decryption processes. Thus, making AES-CTR implementation smaller than other AES modes. Because of highly effective security and large software/hardware implementation quality, AES-CTR is still one of the most popular and reliable encryption methods (Jyothi & Ali, 2020). Therefore,

this algorithm is suitable for this project because it provides a high level of confidentiality in securing data.

2) SHA-256 Algorithm

SHA-256 algorithm will be used to hash the derivation key in this project. SHA-256 stands for Secure Hash Algorithm – 256 Bit. It is a relative of cryptographic hashing algorithms developed by the National Institute of Standards and Technology (NIST) to prevent data loss. According to Khillar (2019), SHA-256 is a new advanced because it was developed as a new generation of SHA functions in 2000 and it was proposed as FIPS standard 2002 make it a more reliable cryptographic hash function. The SHA-256 file compression method worked with a 512-bit message block and a 256-bit intermediate hash value. This algorithm can generate a 256-bit hash value from 512-bit padded message blocks and the original message size could be up to 264-1 bits. SHA-256 always assigns a 256-bit hash internally for security purposes, however, the resulting hash can be compressed to either 196 or 128-bit printing and storage. However, the truncated SHA-256 provides a significant advantage for human reliability in

printed citations and helps improve security only at cost of a small reduction in MD5 in terms of performance. SHA-256 can be used as file compression functions and messaging schedule. Therefore, SHA-256 is more effective since it always computes a 256-bit hash value internally (Khillar, 2019).

3) PBKDF2 Algorithm

PBKDF2 (Password-Based Key Derivation Function 2) is presented by Internet Engineering Task Force as RFC 2898 and it is a public key algorithm (Ertaul, Kaur & Gudise, 2016). This key derivation method is constructed to be slow by increasing data processing and complexity. Therefore, it is also called a key stretching function that protects it from any cryptographic attacks. According to Ertaul, Kaur, and Gudise (2016), PBKDF2 key derivation function has five input parameters which are Password (P), Number of Iteration (c), Salt, dkLen, and Pseudorandom function (PRF). A password is where a user chooses the password that needs to be hashed. The number of iteration (c), is an algorithm that iterates a numerous time before returning to hash password. It helps to secure against security attacks. Salt can be any number that can append to the password to make it more secure. While dkLen refers to the length of the derived key in octets. PRF is a pseudorandom function that uses two input parameters and the output length of hLen. PBKDF2 may create produces some important situations which would make it difficult for hackers to attack the system. Other than that, if salt is used in the hashing process, the potential to use pre-compiled hashes might be lessened by the passwords itself for threats to the system. Thus, th is algorithm helps users to reduce such personal data attacks in every way and at the same time makes it difficult for the unauthorized user to guess the actual passwords. PBKDF2 can be used for protecting passwords or passcodes. Therefore, this algorithm suits our project since the system requires a password to reveal the hidden file.

4) Bcrypt Algorithm

Bcrypt is developed by Niels Provos and David Mazières based on the Blowfish cipher which is b for Blowfish and crypt define as the hashing feature used by the UNIX password scheme (Arias, 2018). Bcrypt is an adaptive function, with time, the number of iterations can be expanded to make it slower, so it remains vulnerable to brute-force search attacks, even with increasing processing power. The Blowfish cipher is a fast block cipher except for the parameters that set the practical performance of a cryptographic algorithm while changing keys. Each new key requires a pre-processing equivalent of around 4 kilobytes of text, which is known to be very slow compared to other block ciphers. This slow key change is useful for password hashing methods such as bcrypt because high computational demand helps defend against dictionary and brute force attacks by slowing down the attack. According to Arias (2018), bcrypt is able to minimize these types of attacks by integrating the costly key initialization step of Blowfish with a variable number of iterations to maximize the workload and length of the hash calculations. The key advantage of bcrypt is that over the period, iteration counts can be

improved to make it slower to allow bcrypt to scale with computing power. This work factor value determines how slow the hash function can be, which ensures that different work factors can produce different hash values in different time periods, making it highly resistant to brute force attacks (Anonymous, 2014). Thus, this bcrypt will be used to hash the user password. This means the developer will not be able to view the user's actual password since their password has been stored in hash code.

II. Implementation

This project will use all the algorithms that have been mentioned above. The algorithm should be implemented in both processes which are hiding and revealing the files. Below are the steps of how this algorithm is implemented:

a) Hiding the files

1. Firstly, the image is read and all files will be read as an array buffer using FileReaderAPI. Then, the image may convert into a Uint8Array which an array of 8-bit unsigned integers.

2. Then, the files are archive using JSZip (a javascript library) to allow the compression process. The output of the ZIP file will be hidden inside the image.

3. Next, to encrypt the ZIP files since the files inside the ZIP, the system will use SubtleCrypto API. In this process, to create a derivation key the plaintext password is imported. SHA-256 and a salt are used to hash the derivation key. To prevent a dictionary attack of passwords, the salt which is Uint8Array is taken from the start of the image. Then, a new key is derived using the PBKDF2 algorithm. Thus, the files should be encrypted using a new encryption key. Therefore, the system uses the symmetric AES-CTR algorithm to encrypt the data.

4. After finish encrypting the ZIP files, the output is converted to another Uint8Array. Then, the encrypted ZIP and the image concatenated, and place the files after the EOF marker.

5. Now, the files are being hidden inside the image and being converted to a blob then it can be download and stored to the user's devices or local storage.

b) Revealing the files

Actually, this process is similar to the hiding process but in the reverse step.

1. First, the file will be converted to a Uint8Array and read using the FileReader API.

2. Then, the files are retrieved immediately and follow the EOF marker after the EOF marker was detected by iterating through the array. The image does not contain any hidden files if no content follows the EOF marker.

3. The decryption technique to hide the ZIP file is the same as the technique used in the encryption process. But, to derive decryption, the derivation key is used and then will be used with the AES-CTR algorithm to decrypt the data.

4. After the ZIP file has been decrypted, JSZip is used to extract the files.

5. Finally, the extracted ZIP files that contain hidden messages or files can be download and stored on the user devices or local storage.

2.3.4 Benefits of Combining Cryptography and Steganography

Today, information security has become a major issue in our digital life. The invention of a sustainable communication system is guided with a specific strategy of security features, especially in the state of data exchange. According to Almuhammadi and Al-Shaaby (2017), the effectiveness of network security is increased daily as the size of the data is transmitted over the Internet. Both cryptographic and steganographic systems focus on providing secret communications but are different in terms of system failure. In cryptography, when the intruder can read a secret message, the system is a failure. But in steganography, the system fails when the attacker recognizes that the steganography has been used and is capable of reading the hidden message (Rout & Mishra, 2014).

Other than that, it is possible to combine the techniques by hiding the secret information using steganography and encrypting the hidden file using cryptography. Thus, the resulting image can be exchanged without revealing that confidential data is being exchanged. In this project, the steganography method is used first to hide the confidential file, then we use the cryptography method to encrypt the hidden file. Thus, if the unauthorized user feels suspicious with the image file, they still need the key or password to reveal the hidden file from the image. According to Rout and Mishra (2014), the intruder would still need the cryptographic decoding key to decrypt the encrypted file or message, even though he successfully defeats the steganographic technique and identifies the details from the cover image. We assumed that steganography or cryptography itself is not effective for the security of information through all types of situations. However, we can create a reliable system if we combine these two systems.

As a consequence, the combination of steganography and cryptography techniques would enhance the security of confidential data. This combination will accomplish some of the required features, such as file

sizes, privacy, and strength for confidential information exchange around an open channel. This combination could be an effective tool that allows people to interact without dragging the interest of eavesdroppers who may not even know the presence of the secret information being transmitted (Almuhammadi and Al-Shaaby, 2017).

2.4 Existing Project

2.4.1 Steganography Online Codec by PELock

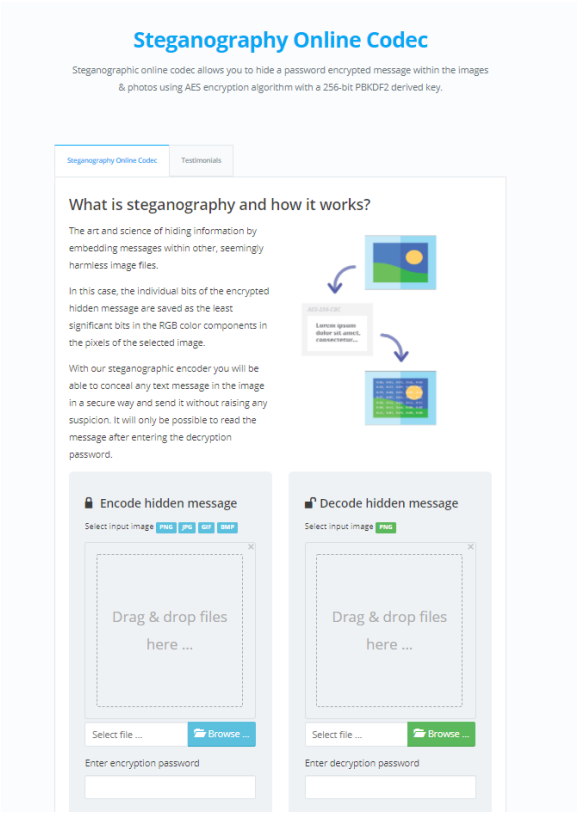


Figure 2.6 Steganography Online Codec Page (www.pelock.com, n.d.)

Steganography online codec is a web application developed by PELock. The purpose of this application is to hide a secret message inside the cover image. This web application enables users to hide a password to encrypt the data within the images or photos that using the AES encryption algorithm and 256-bit PBKDF2 derived key.

<u>Features</u>

- Allow users to hide a secret message inside the cover image.
- Image file type support to encrypt the secret message are PNG, JPG, GIF, and BMP.
- Addition encryption password is provided to encrypt and decrypt the secret message.

Navigation and Design

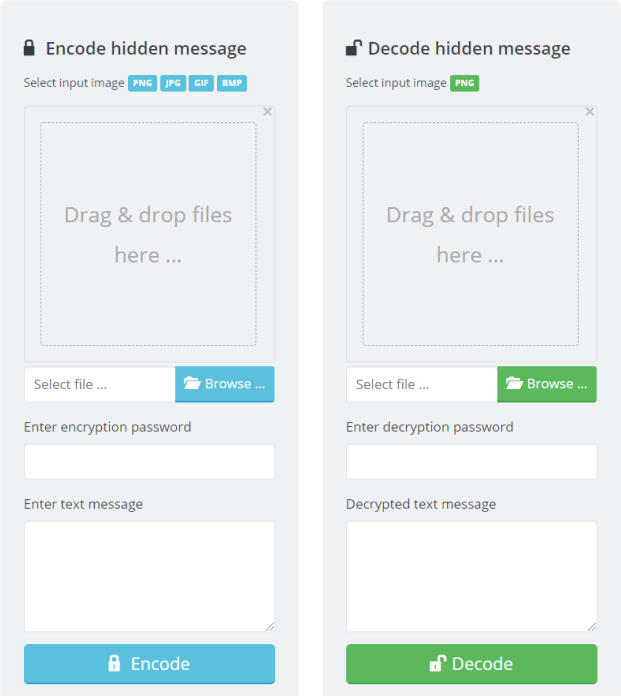


Figure 2.7 PELock Encode and Decode Interface (www.pelock.com, n.d.)

The user just needs to open the website given, https://www.pelock.com/products/steganography-online-codec, and they will directly proceed to this interface. Based on Figure 2.7, the application provides the encode and decode section. The interface is user-friendly and it is a responsive website which compatible with the users if they are using a personal computer or mobile phone.

Security Element

This web application uses steganography and cryptography for their security element. Users can store hidden and encrypted messages within images. DEFLATE algorithm is used to reduce the size of the message string that has been compressed. A strong cryptographic key is created from the password given using the 20000 repetition PBKDF2 algorithms. 256-bit AES encryption is used to encrypt the compressed data. Then, encrypted bits are implemented in the least significant bits of the RGB color components in the pixel resolution of the selected image.

Strengths

- Able to use this tool anywhere and anytime since it is a web-based application.
- Able to store hidden and encrypted messages within images and send them to anyone with email without any suspicion.
- Secure against brute-force attacks because of PBKDF2 key derivation implementation.

Weaknesses

- Users can only hide text messages
- Unable to send the image that contains a hidden message in social media because the image needs to be compressed first.

2.4.2 Steganofile

Figure 2.8 Steganofile Dashboard
(softpedia, n.d.)

Steganofile is a desktop application created by C.A.M.S Works Inc. This application aims to allow users to hide any important document into another file. This including any document, image, video, and audio file.

Features

- Able to hide any secret document into another file type including document, image, audio, and video.
- User can set a password to encrypt and decrypt the file.
- Users can pick up to 120 cover files, so the original file will be split into those sections to provide a different level of protection.
- Original file can be deleted after hiding it.
- After retrieving the original file, the cover files can be removed.

Navigation and Design

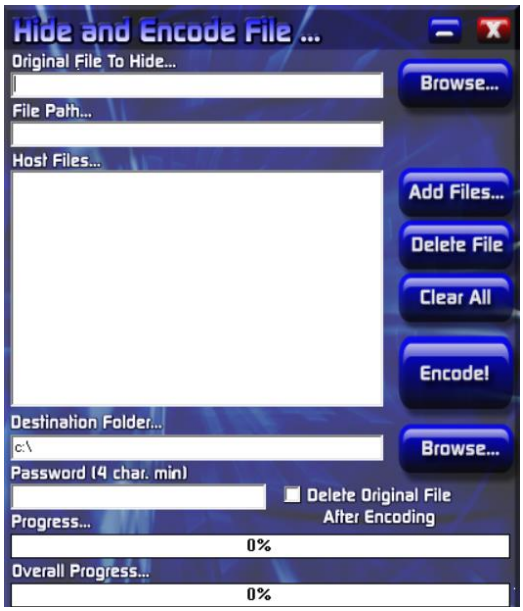


Figure 2.9 Encoding File Interface
(softpedia, n.d.)

Figure 2.9 shows the Steganofile encoding file interface. This interface provides a Browse button to select files need to hide. Add files button is to add a cover image to hide the secret file. The user also can delete and clear all the selected files. The encode button proceeds with the hiding process. Users can save the file to any destination in their PC by clicking the Browse button.

Figure 2.10 Decoding File Interface
(softpedia, n.d.)

Figure 2.10 shows the Steganofile decoding file interface. This interface provides the Add Files button to select file need to be revealed. The user also can delete and clear all the selected files. The decode button proceeds with the reveal process. Users can save the file to any destination in their PC by clicking the Browse button.

Security Element

This desktop application uses steganography and cryptography for their security element. For the steganography method, the user can store a secret file or data in another file. For cryptography, a password is provided to enable the users to encrypt the secret file.

Strengths

- Can hide any type of files including image, video, audio, document into another file.
- Addition secret password is provided to encrypt and decrypt the hidden file.

Weaknesses

- Only PC that installed this application can use this feature since it is a desktop application.

2.4.3 SteganPEG

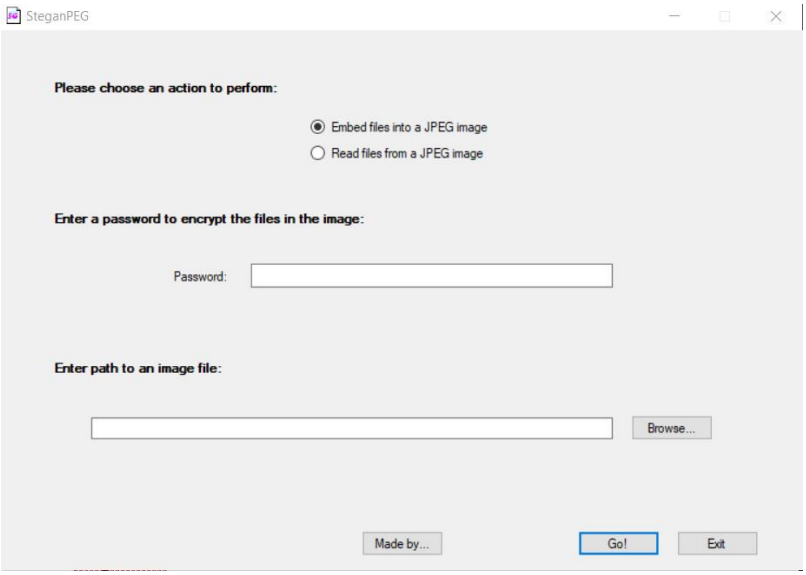


Figure 2.11 SteganPEG Dashboard
(softpedia, n.d.)

SteganPEG is a desktop application developed by Kango Abhiram. The objective of this application is to help the user to hide confidential data inside JPG images just in a few steps. It also enables users to encrypt the hidden data by setting up a password. This application doesn't take a lot of technical skills to work with it, and even beginners can understand the entire process with minimal effort.

Features

- Able to hide multiple files in the JPEG image.

- Provide the amount of space left in the image to add more secret files.
- User can set a password to protect the hidden file
- Before hiding, the system compresses the file to enable the number of files to be hidden.

Navigation and Design

Based on Figure 2.11, the user will directly proceed to this interface after opened this application. The design is simple where users can choose an action to perform which is to hide the files into a JPEG image or reveal the files from a JPEG image. A password form is provided to encrypt the files in the image. Then, the user can choose the path where to save the image file. To proceed with the action, the user needs to click the Go button.

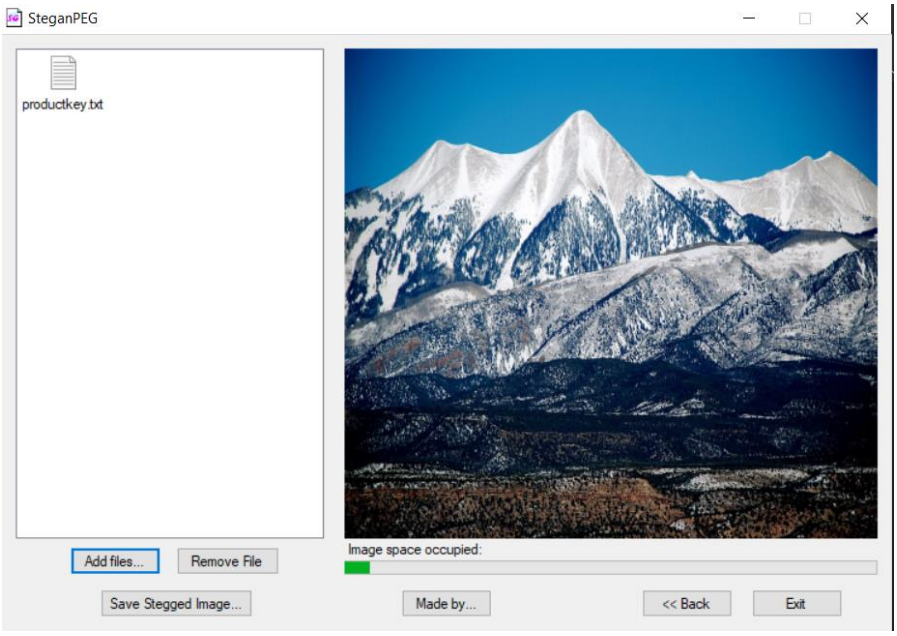


Figure 2.12 Adding Secret Files Interface
(softpedia, n.d.)

Figure 2.12 shows the interface when the user wants to add the secret files into the image files. To add the files, the user needs to click the Add files button, and the process of hiding the file automatically be executed. Then, if the user wants to remove the file just click the Remove File.

Security Element

SteganPEG also uses steganography and cryptography techniques for its security element. For steganography techniques, users can hide secret files or data in the JPEG image. For cryptography, the user can set a password to encrypt the secret file.

Strengths

- Interface is user friendly and does not need any technical skills.
- Addition secret password is provided to encrypt and decrypt the hidden file.

Weaknesses

- Data only can be hidden in JPG images.
- Not flexible to use since it is a desktop application.

2.5 Discussion

2.5.1 Comparison About 3 Existing Project

Table 2.1 Comparison of 3 Existing Project

Criteria	Steganography Online Codec by PELock	Steganofile	SteganPEG
Features	- Hide secret message inside the cover image. - Supported cover image is PNG, JPG, GIF, and BMP. - Encryption password is provided.	- Hide any file into another file. - Cover file can be an image, video, audio, and any type of document. - Encryption password is provided	- Hide multiple files in the JPEG image. - File being compress to allow several files to hide in the cover image. - Encryption password is provided
Design	- Simple. - Good color combination.	- Too many buttons in one interface. - Theme color is quite dark.	- Simple. - Design is not attractive.
Navigation	- Encode and decode section is on one page.	- Dashboard provide an encode and decode button to navigate to the next process. - Easy to understand the instruction.	- Provide simple instruction to proceed to the next process.
Security Element	- Steganography. - Cryptography. Use DEFLATE, PBKDF2, and 256-bit AES algorithm.	- Steganography. - Cryptography.	- Steganography. - Cryptography.
User Friendly	- It is user friendly. - Portable since it is a responsive site.	- It is user friendly. - Easy to use.	- It is user friendly. - Does not need technical skills to use.

2.5.2 Discussion of Existing Project

Based on Table 2.1, those three applications are mostly used to hide the secret file or file inside another file. But for Steganography Online Codec, it only can hide text messages. Then, those three applications usually use the combination of steganography and cryptography in their system. For Steganography Online Codec, they implement DEFLATE, PBKDF2, and a 256-bit algorithm to secure their encryption method. Thus, these systems provide users to set a password to encrypt the hidden file. As for the design of these three applications, it is simple however for Steganofile it is quite complex. The navigation for these applications is easy to understand by the users. Other than that, these three applications are user friendly and easy to use by the users.

Thus, these existing systems will become our references to develop the File Hiding Web Application. We may find an idea and improving the features available in these existing systems then implement them in our project. In our project, we may use the same security element as these three existing projects which are steganography and cryptography techniques. The project that will be developed will use image steganography techniques. This project enables a user to hide any confidential file into an image file. However, in steganography techniques, we may implement additional features such as End of File (EOF) markers or bits that indicate the end of the data stream of the file. The EOF is used to mark the image file types such as PNG, JPEG, and GIF. For cryptography techniques, we may follow Steganography Online Codec which is PBKDF2 and the AES-CTR algorithm will be implemented in our project. The addition of the SHA-256 hashed function also added to our system to derive the key or password for the encryption method. Besides that, we will implement our system design based on Steganography Online Codec because it is simple and user friendly to use. We will make a responsive web application to enable users to get a better experience even though they use the application either on a PC or mobile phone. To enhance the existing project, we also may add additional features which are the image file and hidden file able to be upload on using cloud storage since the current existing project did not provide this feature. Therefore, with these three existing applications as a reference, we can build a better and effective file hiding applications for the users.

2.6 Conclusion

In summary, the investigation of the related system and techniques used in this project are being researched and analyzed. With these studies, we may implement some of the concepts in our system. This includes the use of steganography and cryptography techniques. We hope that with these studies, it can ease us to develop this file hiding web application.

Besides, all of this previous study found on each application has its own strengths and weaknesses. By the study of these three applications, we could give all effort to make file hiding web application effective to the users. We may enhance and improvised the current feature available and implement it in this project. We hope that the system that will be developed by us will be a reliable and trusted application to hide any confidential data. This project should provide beneficial effects to its user as they will feel secure to use our system to hide their confidential data. Other than that, we hope that all of these studies give us an idea to improvise the current features on the application related to our project.

3 Methodology

3.1 Introduction

The developer will conclude that the File Hiding Web Application has been effectively used as a web application to help the development of the final result. The approach must be adapted to the web application that will be developed to ensure that the production of the application is well planned and properly completed. To choose a research methodology, we must begin with the final findings since the objective of our research would be the first factor. Carrying out research is always a huge step when you write your dissertation, thesis, or any report. Thus, choosing the right research methodology could decide the effectiveness and overall quality of the report (Thattamparambil, 2020).

In this chapter, the purpose is to discuss more on the methodology used in this project. This chapter further discusses the explanation for the use of approaches or methods. It will indicate the progress of the project from stage one to the last. The concept and theory of the approach will be described properly to ensure the process and development of this project follow the approach effectively. Besides that, each phase in the methodology used also be explained in this chapter. This includes the activities and tasks performed at each phase. Thus, with the explanation and methodology used, the process of developing this project would be more structured and more organized.

3.2 Agile Methodology

3.2.1 Concept and Theory

The agile methodology is a framework for developing, delivering, and evaluating high-quality applications at the least cost and in the shortest possible time. According to Azmee (2018), agile methodology is a structure of the software development life cycle that applies an iterative approach, open cooperation, and workflow adaptability over the life of the project. Agile was developed with system development in particular but has found its way to all sorts of fields, such as content marketing and IT project management. This approach prioritizes individual responsibility, short time frames for deliverables, consistent communication, feedback, and sustainable growth. This iterative agile approach is more versatile and its short-term iterations aim to develop the project on a small timeframe, with little preparation rather than a long-term strategy. It allows teams to adapt to randomness through systematic iterative work cycles, known as sprints (Azmee, 2018). Therefore, this method is very suitable and has been chosen for the project to be developed because this project requires a short time to complete.

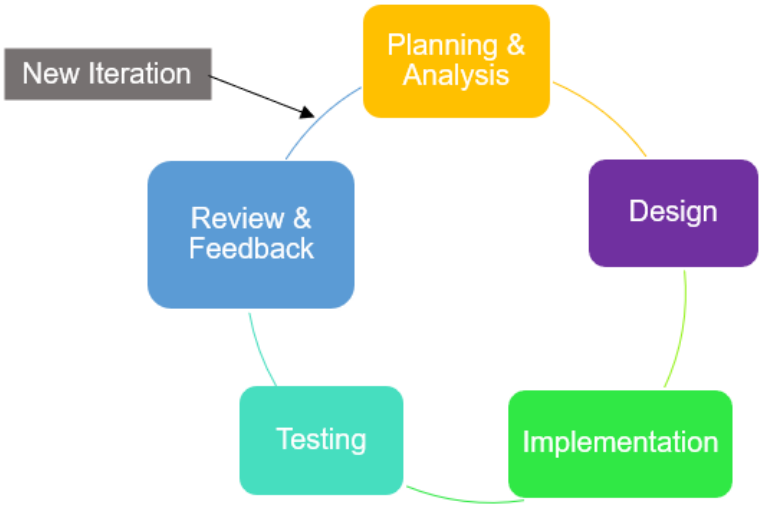


Figure 3.1 Agile Model

For this project, the agile methodology process consists of five phases. As shown in Figure 3.1, the phases include planning and analysis, design, implementation, testing and feedback. New iteration will proceed if there is a new enhancement or an adjustment in the system after being reviewed in feedback phase. With this approach, the project will be developed in systematic and organized way.

The advantages of Agile Model

1. **Faster**

   Traditional software development focused on phases such as requirements, planning, designing, installation, testing, and execution. The agile approach, on the other hand, looks to implement the first phase in a few weeks and the whole piece of software in a month.

2. **Transparency**

   A developer involved is self-organized. Instead of following a framework of management principles designed to deliver the desired outcome, they understand the targets and map out a course to accomplish them.

3. **Continuous Feedback**

   Instead of waiting for the delivery phase to determine results, teams use the Agile approach to measure the progress and pace of the production process daily. When each iteration has been delivered, the approach is driven.

The disadvantages of Agile Model

1. **Hard to maintain**

   Agile only succeed as long as you are dedicated to ensuring a certain degree of cooperation, teamwork, and iteration. As soon as these things tend to collapse, the cycle struggles from unfulfilled goals, miscommunication, and a longer period of time between deliverables. Responsibility is the key to applying agile methodologies in this project.

2. **Unpredictability**

   The agile iterative approach is perfect for the continuous development of systems but provides less predictable than other methodologies when working with projects that have a clear start and finish. The attempt to change project direction for a bit leads to more unknowns about the estimated time, cost, and motivation to finalize a project with a difficult timeline.

3. **Less in design and documentation**

   In the Agile approach, documentation develops during the process, and sometimes "just in time" to produce the results, not at the beginning. As a consequence, it gets less informative and always completed at the last minute.

In summary, every method has its owns advantages and disadvantages that the developer needs to cope with. Taking risks by using this approach means that the developer has properly considered the possibility of success and failure that could or should arise during the development of the project. However, this approach is the most efficient and adaptable for developing our project since we use minimal planning for this project. Thus, our team will be using the Agile Methodology in developing the system in this project.

3.3 Phases in Agile Methodology

Based on Figure 3.1, to run this project systematically we will follow the phase given in these Agile Model. The first phase we need to follow is Planning and Analysis, followed by Design, Implementation, Testing, and last but not least Review and Feedback. Then, after the Review and Feedback phase being executed, if there is some adjustment need to do, the developer will proceed to the new iteration. Detailed activity and description of each phase will be discussed below:

3.3.1 Planning & Analysis

Planning is a key management feature that includes determining ahead what to do when is it to be done, how to do it, and who is going to do it. It is an analytical process that sets out the objectives of the project and identifies possible courses of action from which the entity can accomplish those objectives. While analysis is an evaluation of data and facts to identify and understand the relationships between the variables, thus creating a framework for problem-solving and decision-making. It is a detailed study of real and complex-assessed continuous functions.

In this phase, the project that will be developed is planned according to the requirements. Planning will include an analysis plan, design plan, and testing plan to provide a clear path for developing this project. This includes the plan or question for the questionnaire to be asked to the user. For analysis, we will analyze and find a suitable solution regarding the system that will be developed. This phase involves breaking down the system into different pieces to analyze the situation, analyzing project goals, breaking down what needs to be created and attempting to engage users so that definite requirements can be defined. This includes analysis of user requirements, identify system requirements, and research on the algorithm used in this project which is steganography and cryptography algorithm. Other than that, in this phase, we also analyze the data gathering that have been compile, which is the questionnaire that have been distributed to the users. Thus, this planning and analysis phase is to ensure that the project runs smoothly and could achieve its objective.

3.3.2 Design

Design phases produce a design plan that explains the elements of the system, how they function, and how they operate together to meet the system requirements. This phase includes the design of the whole system and its elements. The design phase will act as a blueprint during the process of development. It guides activities for development, including detailed design, coding, implementation, and testing.

In the design phase, one or more designs are being created, from which the project outcome will apparently be achieved. For this project, we will design the process flow of the system such as use case diagrams and flowchart diagram. We also design the user interface of the system. The design must be simple and efficient and looks very informative and user friendly. Then, we will confirm the programming language used in this project. To perform the structure and design of the system, we may use a programming language such as Javascript including Node.js for backend and MongoDB to store the database. For the frontend, we used Javascript library and framework such as ReactJS and Next.js and also used Tailwind CSS and Semantic UI for designing the user interface. Other than that, the security

element and structure of this system also be designed in this phase. Therefore, this phase helps to remove any defects by defining a standard and trying to adhere to it.

3.3.3 Implementation

Implementation is a detailed, realistic plan, written in the form of a checklist. It is compiled by the developers before they start working on each requirement specification. It is a step by step guide to

execute each of the tasks that have been provided. This phase allows developers to recognize complexities and complicated moments. It also provides a more precise approximation of the tasks.

In this phase, we will develop the system according to the design and analysis that have been compiled. For this project, we use all the software and hardware requirement to develop the system or application. We also integrate the system with the security element that has been confirmed which is steganography and cryptography method. We implement higher clarity on this requirement since these builds are sent to the client or user for feedback. Thus, this phase should be able to deploy the system and can be used to train the user.

3.3.4 Testing

The test phase is an approach to manage the testing activities to ensure good quality and high-end evaluation of the software system. It mainly focuses on the actual execution of test cases on the software itself and the results of this activity describes the quality of software. This phase is to make sure that any part of the application works perfectly. However, the testing phase requires a lot of time.

For this project, alpha and beta testing will be implemented in this phase. This includes performing testing with the user. The purpose of this test is to classify any potential faults or defects. All identified defects shall be issued to the development team for adjustment. Other than that, we also test the back-end process to ensure the availability of the system. Then, we also test the functionality of the user interface, either it is meeting the requirement or not.

3.3.5 Review and Feedback

Reviews provide a depth analysis of the software or service provided by the developer. Feedback is basically generated by the user in the context of user feedback, with the intention that the developer would

use the feedback to enhance the functionality of the system. Review and feedback can be commonly defined as the experience of previous actions in the present, which can affect future actions.

For this project, after successful testing, the application is delivered or deployed to the user. The application should be fully functional because we want the customer to give feedback on the system. Once users start using a fully functional system, the potential problems will occur and it needs to be fixed. Thus, from the review and feedback, if there are any bugs and problems in the system, we will proceed to the next iteration to adjust and modified on the system. As a result, we could produce an efficient and reliable system for this project since each iteration could enhance the output of the system.

3.4 Conclusion

In conclusion, Agile Methodology is quite suitable for this web application development, which starts at the level of analysis and proceeds through different phases, and all requirements for this project are needed to ensure that the goal of this project is successfully achieved. We use this approach because it is faster and provide continuous feedback. We use this approach because this method only needs a few weeks for planning and analyzing the project because this method focuses more on software development. Since we get a short time to complete this project before the deadline, this approach is suitable for this project and developers can focus more on developing the software than focusing on planning and analysis.

Other than that, iteration in Agile Methodology provides continuous feedback that can be used to enhance our system. We can refer to the feedback given by the users to modify our system. With this approach, we can measure development and increases in productivity on a systematic basis. Besides that, getting deliverables between each iterative and having user feedback will help speed up the process of development to make a fully functional system. Therefore, this methodology is suitable for this project and the project can be run smoothly as planned in this approach.

4 Requirements

4.1 Introduction

This file hiding web application project is successful if we meet all the requirements needed. Requirements actually define what features should be offered in a system and how those features should operate. Clearly defined requirements are vital to the success of the project. These requirements help developers and people involve in this project to ensure that they are working towards the same objective.

Thus, this chapter will explain more about the requirement of this project. This includes data gathering techniques used for this project. To collect the data that relate to our project, we make a questionnaire to be answered by intended users. Then, we also observe the method used in this project. Functional and non-functional requirements also will be discussed in the system requirement section. These two requirements are important because functional requirements specify what the application should do, while non-functional requirements specify how the system operates. Other than that, software and hardware are important since these two requirements are the tools that the developer needs to use to achieve the goals of this project. Therefore, in this chapter, we will specify the software and hardware requirements in this project. With these requirements discussed, the developer will understand the goal of the project and also could make a comprehensive schedule to complete this project. Hence, this project will accomplish its objective.

4.2 Data Gathering Techniques

Data gathering is one of the most important elements to ensure the success of a project or system. To ensure that optimum requirements are fulfilled, how those requirements are obtained are equally important. The data gathering techniques have several methods such as questionnaires and surveys, observations, interviews, and inspecting of the existing system. Therefore, this section will be discussed about data gathering techniques used in this project.

4.2.1 Questionnaire

Data gathering could come from several sources. Likewise, there are a variety of methods and techniques to be used to gather the data required for this project. Hence, for this project, one of the data gathering techniques used is the questionnaire method. A survey is made to gather, analyze, and evaluate the opinions of a group of people of a target user. A questionnaire is a data-gathering method that involves asking the respondent to answer a variety of oral or written questions. It has many strengths and

advantages that make it suitable for the project. It is inexpensive since it is affordable ways to collect quantitative data. Besides, the questionnaire provides scalability because it helps users to gather information from large audiences. By going online, we could simply distribute questions to everyone, everywhere around the world.

Thus, for this survey research, we make a questionnaire as an instrument to ask a set of questions to the respondent of the survey. This type of method is considered the easiest and accurate. For this project, the question is prepared in advance on a piece of paper with several questions to be answered by the respondent. Our respondent should be our target user which is any users that would like to send confidential information to other people. There are about 10 questions that will be asked to the respondents in this questionnaire. The purpose of this questionnaire is to collect and gather more information about the web application that will be developed for this project. The questions include the concept and opinion about the use of a similar system used by the users. The number of respondents should be at least 50 respondents. This is because we want to get an accurate analysis so that the system that will be developed in this project meets all the requirements needed from the users. As a result, developers will meet user requirements in developing this file hiding web application because this survey helps them to understand more what users need.

4.2.2 Inspecting on the existing systems

Inspecting on the existing systems could appear to be a useful technique for data gathering. Reviewing the previous findings and documentation will help researchers understand the current system situation. This method allows the researcher to prepare questions for questionnaires to be asked to the users to produce additional requirements. Researchers can find problems when researching the requirements that they can identify on their own.

Thus, inspecting the existing system has been chosen as our second data gathering techniques. This method is suitable for this project because the application to be developed is the enhancement based on the current existing system. In this project, we will at least inspect three existing systems that are similar to the system that will be developed. This research includes observing the interface and features of the system to understand how the system should operate. From this inspection, we could look at the previous features of the system and reuse the features that may still be significant, while at the same time removing others that are out of date. Furthermore, we also analyze existing documents that are related to our security element in this project. Reviewing these existing documents help us in understanding and observing why the system implement certain security element. Thus, we will understand more about the use of security elements, such as steganography and cryptography which will be implemented in this project. Besides, we could identify if there was a lack of information and found redundancy in which steps

are unnecessarily repeated in previous studies. As a result, inspecting the existing system will help us to enhance our system and ensure that there is a dissimilarity between our system and the existing system.

4.3 System Requirement

4.3.1 Functional Requirements

According to Tryfanava (2020), the internal operation of the system can be defined as functional requirements. It describes the features of the system that should be applied by web and application developers. It can be a computation, manipulation of data, operational processes, user interaction, or any other specific functionality that describes what kind of feature a system is likely to perform. Functional requirements help developers to recognize the required action of the system that will be developed. This activity can be represented as functions, services or actions, or as a process that is needed to perform. Below are the functional requirements contained in this project.

Table 4.1 Administrator Functional Requirements

Button	**Expected Result**
Login Credential	The administrator should be able to login to the system using their email and password.
Logout	The administrator should be able to end the session.
Add/Update	Administrator will be able to add and update user information that has been registered
Delete	The administrator will be able to delete a user that has been registered in the system
Save	The administrator should be able to save the user's information that has been updated.

Table 4.2 Users Functional Requirements

Button	**Expected Result**
Login Credential	Users should be able to login to the system using their email and password.
Logout	Users should be able to end their session.
Register	Users should be able to register to get their login credentials to log into this system.
Add Files	Users will be able to add any files that they want to keep secret.
Add Image	Users will be able to add the image that they wish to hide the files within.
Compression Level	Users should be able to choose the compression level for the file from 0 to 9.
Password/Confirm Password	Users should be able to enter a password to encrypt and decrypt the hidden files.
Encrypt	Users should enter the encrypt button to proceed with the process of hiding the files.
Add Steganography Image	Users will be able to add the image that contains a secret file to be decrypted.
Decrypt	Users should enter the decrypt button to proceed with the process of revealing the secret files.
Download	Users will be able to download the image contains a secret file or a file that has been decrypted into their devices or local storage.

4.3.2 Non-Functional Requirements

Non-functional requirements describe how the project, system, or process should operate. It is a set of requirements used to determine the specific functionality of the application. To ensure the efficiency and quality of the entire software system, a non-functional requirement is necessary. Failure to meet non-functional requirements can result in systems that fail to accomplish the research objectives. Below are the non-functional requirements contained in this project.

4.3.2.1 Availability

This system can be accessed if a user has been registered in this system. Users also can use this application whenever they want since it is a web application. This file hiding web application should be available to be accessed for 24 hours a day. However, if there are some enhancement and adjustment in this application, the application will take several hours for maintenance break. Besides, the data availability is ensured because the hidden files and image that contains secret files are stored in the user devices or local storage, not in this system. Thus, every time a user wants to view the hidden files or those image files, they did not need to log on to this system, however, they just need to open their devices or local storage.

4.3.2.2 Reliability

File hiding web application is evaluated and reviewed by the developer regularly. It is crucial to ensure that there are no issues, bugs, and technical errors that may affect user satisfaction with the application. If an error happens, the new patches will be updated.

4.3.2.3 Portability

The system that will be developed is portable since it is a web application. Users can use this system using their personal computer PC, laptop, tablet, or smartphone. The design of this web application could suite many devices since it is built with a responsive layout. This means, this system is user friendly and could be used in any platform including PC and smartphone. Thus, this file hiding web application can be used anywhere and anytime.

4.3.2.4 Security

Security was also implemented in this system. To protect the admin panel this system provides different login flow for different user roles such as admin and users. Then, we also use a combination of steganography and cryptography methods to strengthen the security of hidden files. An unauthorized user could not easily trace the hidden file since the host file which is an image is behaving and look like a normal file. Even the unauthorized user would detect the hidden file contains in the host file (image), they still need a correct password to decrypt the hidden message. Other than that, user's password who register to this system will be stored in hash code in the database server. With the implementation of the security elements, this system could prevent a dictionary attack of passwords. Thus, this file hiding web application is a reliable platform that can secure the user's confidential information.

4.3.3 Software Requirements

4.3.3.1 Visual Studio Code

Figure 4.1 Visual Studio Code Logo
(Wikimedia.org, 2020)

Visual Studio Code will be used to develop the project. It is an open-source editor created by Microsoft for Windows, Linux, and macOS. It is released under the permissive Expat License, but compiled binaries are freeware for any use It was licensed under the Expat Licence, however, the compiled binaries are freeware for any purpose. Visual Studio Code supported several programming languages such as Java, JavaScript, Go, Node.js, and C++. This software enables users to adjust the theme, keyboard shortcuts, settings, and install plugins to add extra features. For this project, we use this software to write code, debugged, and run the code. Thus, it is suitable for our project because this software support JavaScript programming language since we will use this programming language for the system.

4.3.3.2 Windows

Figure 4.2 Windows Operating System Logo
(Wikimedia.org, 2019)

Any Windows version can be used to develop this project. Microsoft Windows is a category of many popular graphical operating system communities, many of which are developed and distributed by Microsoft. Windows provides a graphical user interface (GUI), virtual memory control, multitasking, and support for a variety of input devices. It also offers a wide variety of features, tools, and services to help users get more out of Windows and their computers. Windows operating system has many versions such as Windows XP, Windows 7, and Windows 8. For this project, we use Windows 10 since it is the latest version of Windows OS. The reason why we use Windows 10 is it provided fast startup. Then, it is user-friendly because the interface is easy to understand and it eases the interaction between the users. Thus, this operating system is suitable for this project since it has fast performance and user friendly.

4.3.3.3 MongoDB Compass Community

Figure 4.3 MongoDB Compass Community Logo
(mongodb, 2021)

MongoDB is cross-platform document-based database software. It is known as a NoSQL database application because MongoDB uses JSON-like files with an alternative structure. For this project, we also will use this software because it helps us to set up a database server to store our system information and content. Thus, this software is suitable for our project since we may store certain data in the system that we will develop.

4.3.3.4 Microsoft Office Professional Plus 2019

Figure 4.4 Microsoft Office 2019 Logo
(Wikimedia.org, 2019)

Microsoft Office 2019 is the latest edition of Microsoft Office. It is a management suite, preceded by Office 2016. It has been released for general availability for Windows 10 and macOS. For this project, we will use some of the features from this software to complete the documentation of this project. For example, we use Microsoft Word to write the documentation of this project. Other than that, we use Microsoft PowerPoint to produce a slide for presenting this project. Therefore, this software is important for this project because it helps us to document all the research that has been made.

4.3.4 Hardware Requirements

4.3.4.1 Laptop

Figure 4.5 Acer Nitro 5 Laptop
(Acer, n.d.)

Table 4.3 Hardware Specification

Model	Nitro AN515-52
Processor	Intel(R) Core™ i5-8300H CPU @ 2.30GHz
RAM Memory	12GB
Hard Drive	475GB (SSD) + 931GB(HDD)
Graphic Card	NVIDIA GeForce GTX 1050
Display Resolution	1920 x 1080 pixels
Operating System	Windows 10 Home 64-bit
Battery Capacity	3220mAh

4.3.4.2 Laser Printer

A laser printer is needed to be used to print these documentations and reports.

4.4 Conclusion

Requirements are important when developing a project if you intend to achieve a desired objective on the finish line (Semusheva, 2016). Hence, this chapter must provide all the functionality and features that the system should provide. It requires time, effort, and a systematic process to determine requirements in adequate detail. Developing comprehensive requirements helps us to deliver the best software outcome.

Thus, with this requirement, developers can understand more what the system should be and how it works. Besides, this requirement could reduce the amount of time and effort used by developers to accomplish the desired system goals. This includes the effort of the researcher to collect all the data that is related to this project such as making a questionnaire and analyzing existing systems. Then, the requirement also helps us to resolve any communication problems between the user and the developer. Besides, with the functionalities and non-functionalities requirements explained in this chapter, there is less probability of possible modifications since there is less chance of a mistake on the part of the developers because they have a good understanding of the functionalities of the applications. As a consequence, we hope that all the user is involved in this project to understand the main requirements of the system that will be developed. With the understanding of the requirement, this project deliverable could achieve its goals and objectives and could complete it before the deadline.

5 Analysis

5.1 Introduction

System requirement is a problem-solving approach that includes looking at the larger system, dividing up parts, and figuring out how it works to accomplish a specific goal. To solve the problem, a system analysis must be carried out to identify the challenges by recognizing and evaluating the strengths and limitations of the system that would be developed. Thus, the analysis enables you to understand how the system works.

This chapter will explain more about system modeling and finding analyses that have been made. Means, we must analyze all the input gathered from user and system requirements. The system modeling includes the illustration of a use case diagram and flowchart diagram. For analysis of user requirements, questionnaire feedback and analysis also will be described in this chapter since we use questionnaires and survey methods for data gathering. For questionnaire feedback, each question will be present and explain in a chart for analyzing. Those details will be explained properly in this chapter.

5.2 Data and System Modeling

Data and system modeling is a technique for documenting software and the business architecture of the system. It is an explanation of how the data can be used to fulfill the requirements of the end-user. This system architecture is then usually implemented in the development of software applications. The "modeling" of these numerous structures and processes also includes the use of diagrams, symbols, and text references to describe the flow of data through a software application (Knight, 2017).

Data modeling is a method used to identify and evaluate the data specifications required to support business activities within the structure of applicable information systems in organizations. It involves practices such as business process design, which deals with larger conceptual organizational structures and decision-making processes in the whole organization. Thus, the data model is used to document, describe, manage, and present how data structures within a given database, design, application, or platform are linked, stored, retrieved, and processed within a given system and between other systems.

In this project, for data and system modeling, we will present the use case and flow chart diagram. These diagrams will show the flow of the system and who should involve in the system. These diagrams enable both developers and end-users to understand the requirements of the system because it helps end-users to identify their requirements and allow developers to develop a system that meets the required specifications. As a consequence, data and system modeling is important for both the representation and documentation of data. Thus, with a clear understanding of the requirements, terms, and other development aspects of the system, there are fewer errors across the development of the system.

5.3 Use Case Diagram

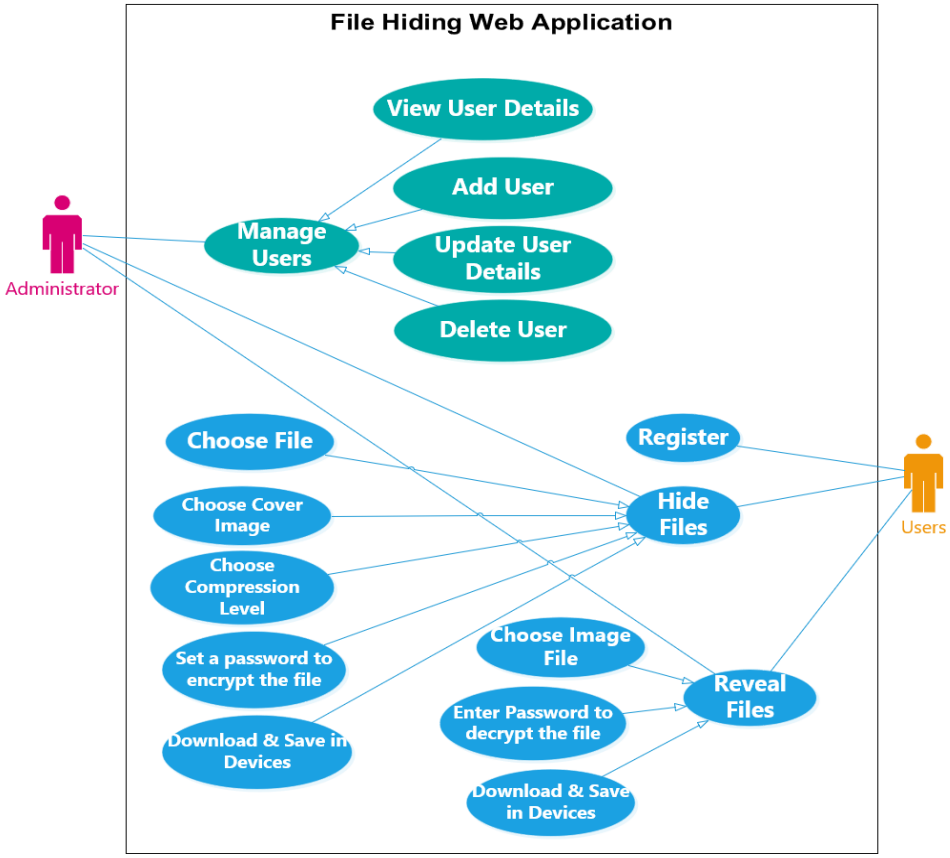


Figure 5.1 Use Case Diagram for File Hiding Web Application

Figure 5.1 shows the use case diagram for this project, which is a file hiding web application. This use case represents the actors or users involved in this system and how they interact with the system. Based on Figure 5.1, the actors in this system are Administrator and Users. In this system, the Administrator can manage users that have been registered in this system. Hence, they can view user details in this system. Besides, Administrators will be able to add new users, update user details, and delete a user who has been registered in this system. Administrator also can perform a hide file and reveal files feature.

Users can register to login to this system if they did not have a username and password. Other than that, they can hide their confidential file and reveal the files. To hide the file, they can choose any type of file and choose any image as a cover for their confidential file. Then, they must choose the compression level from 0 to 9 for the system able to archive the files into the ZIP file. After that, the system allows users to set a password to encrypt the confidential file that has been hidden. Lastly, the process of hiding the files should be done and users can download and save the result in their device. To reveal the file, users need to choose an image file that contains a secret file. Next, they must enter the same password used to encrypt the secret files. Then, the process of revealing the files should be done and they download and save the file in their device or local storage.

5.4 Flowchart Diagram

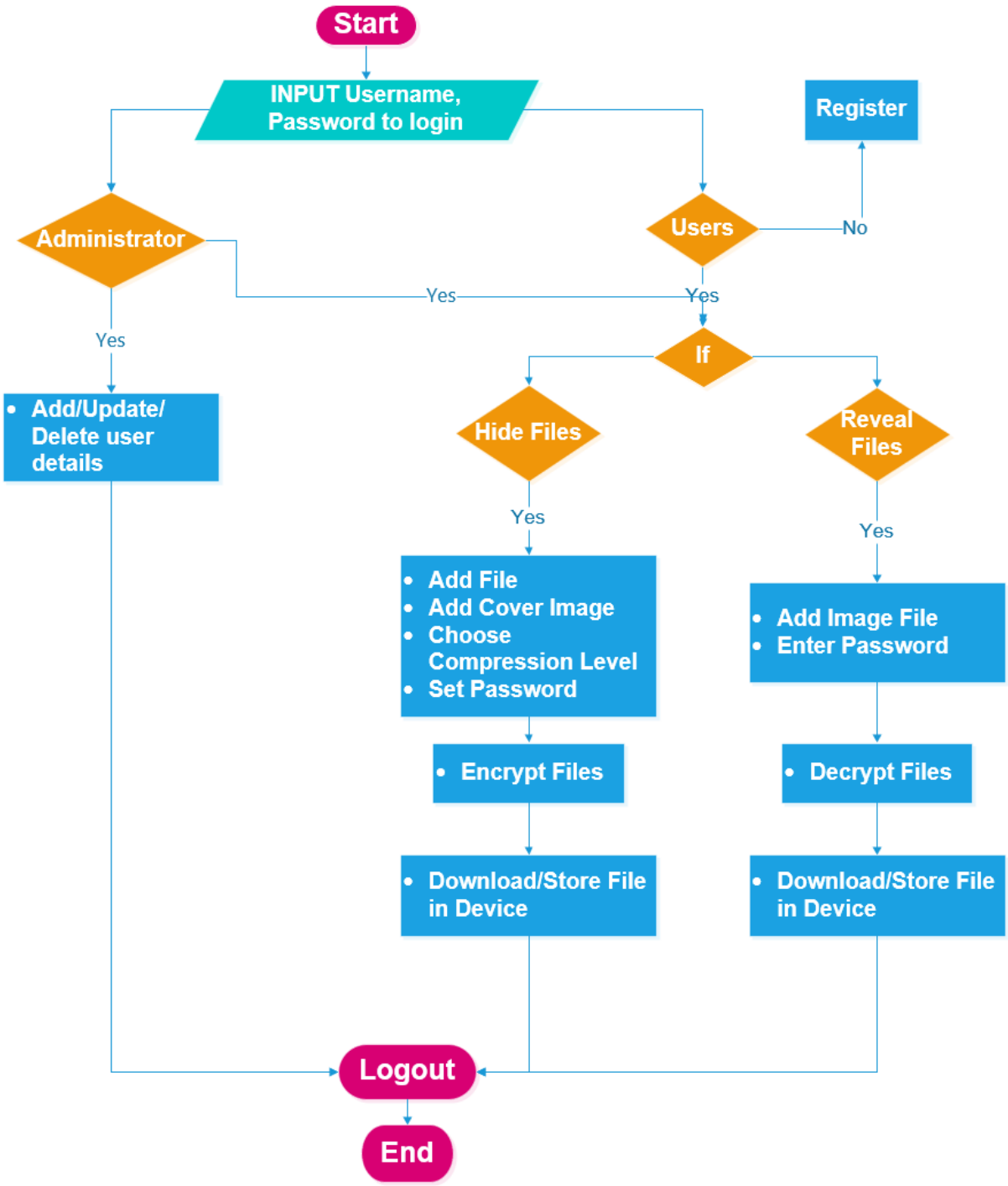


Figure 5.2 Flowchart Diagram of File Hiding Web Application

Figure 5.2 shows the flowchart diagram for this project. This flowchart diagram will demonstrate the process involved in this system such as hiding files into the image and reveal files from the image. Based on Figure 5.2, the application should start with entering the username and password to login to the system. Then this system has two roles with different functionalities which are administrators and users.

Thus, if users have administrative roles, they only can add new users, update users' detail, and delete a user who has been registered in this system. Other than that, they also can perform the main feature of this system which is to hide and reveal files inside the image.

For normal users, if they did not have a username and password to log in, they can proceed to the registration page. After successfully registering into the system, they can log in and proceed to the feature of this system which is to hide files or reveal files inside the image. If the users choose to hide the files, then they must add any file that they want to keep confidential, add a cover image, choose the compression level, and set a password to encrypt the confidential file. After that, the process of hiding and encrypting the files should be successful. Then, users can proceed to download and store the file in their device or local storage. If the users choose to reveal files, then they must add an image file that contains a secret file and enter the same password used to encrypt the secret files. After that, the process of revealing and decrypting the files should be successful. Then, users can also proceed to download and store the file in their device or local storage. Lastly, if administrators and users want to end the application sessions, they can logout from the system.

5.5 Data Finding and Analysis

5.5.1 Questionnaire Feedback

The main purpose of this questionnaire is to collect an idea and information on the development of the File Hiding Web Application so that all information can be used to improve the system that will be developed. The title of the questionnaire is “Questionnaire for File Hiding Web Application Using Image Steganography Techniques”. This questionnaire consists of three sections. Section A is all about the respondent information, Section B about the image steganography techniques, and Section C is about the use of file hiding applications.

This questionnaire was opened to the public and we spread it to many users who want to hide their confidential data. To collect the data from this questionnaire feedback, about 50 respondents are chosen to answer this questionnaire. Once the data are collected, we will analyse all the questions in the questionnaire and will present the data in the pie chart and bar chart. The result is read in percentage since it is easy to understand and could clear overall results. Below is the analysis of each of the questions.

5.5.1.1 Section A: Respondent Information

1. Gender

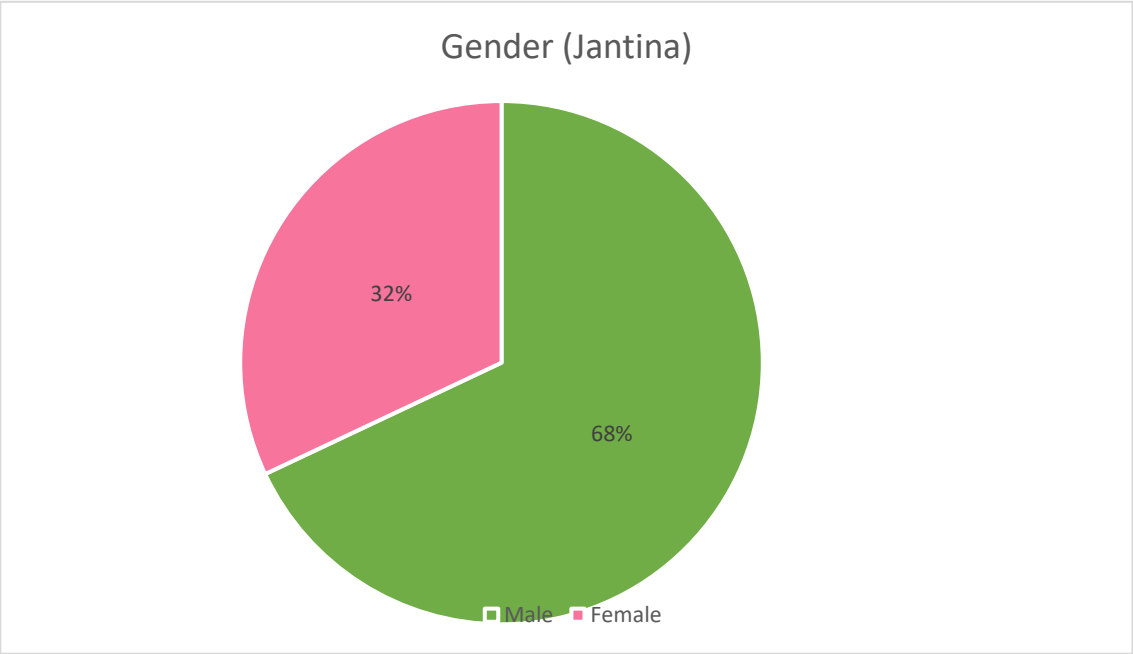


Figure 5.3 Questionnaire Result for Gender in percentage

Figure 5.3 shows that this questionnaire is being answered by both gender male and female. We found that 68% of males have answered this questionnaire, while 32% females answered this questionnaire. Thus, we will obtain a quality result because this questionnaire was answered by both genders since different gender may result from different perspectives.

2. Age

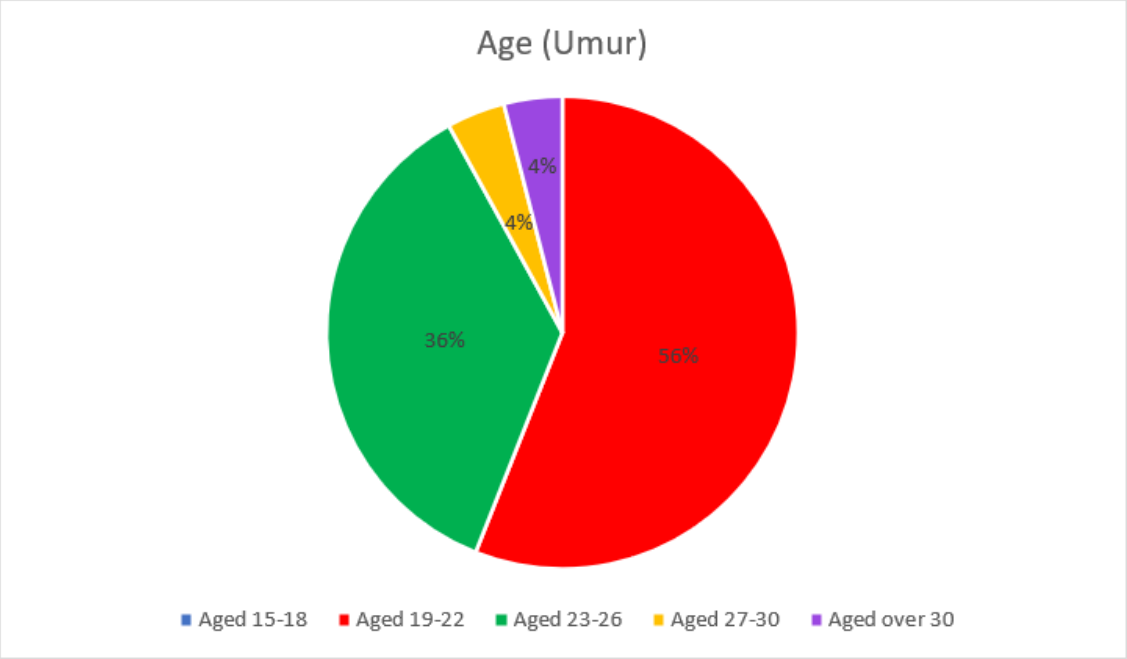


Figure 5.4 Questionnaire Result for Age in percentage

Figure 5.4 shows the age of respondents who answered this questionnaire. The age is separated into five groups which are aged 15-18, aged 19-22, aged 23-26, aged 27-30, and aged over 30. Based on Figure 5.4, we found that 56% of the respondents are age from 19 to 22 which is the highest group answered this questionnaire. The second highest group is the age from 23 to 26 where 36% of all the respondents answered this questionnaire. Then, aged 27-30 and aged over 30 above both have the same percentage which is 4% of all the respondents who answered this questionnaire and there are no respondents from ages 15 to 18. Hence, the result of this questionnaire could help us to enhance our system since there is a range of ages who answered this questionnaire as a different age may result in different ideas and experiences for this project.

3. Race

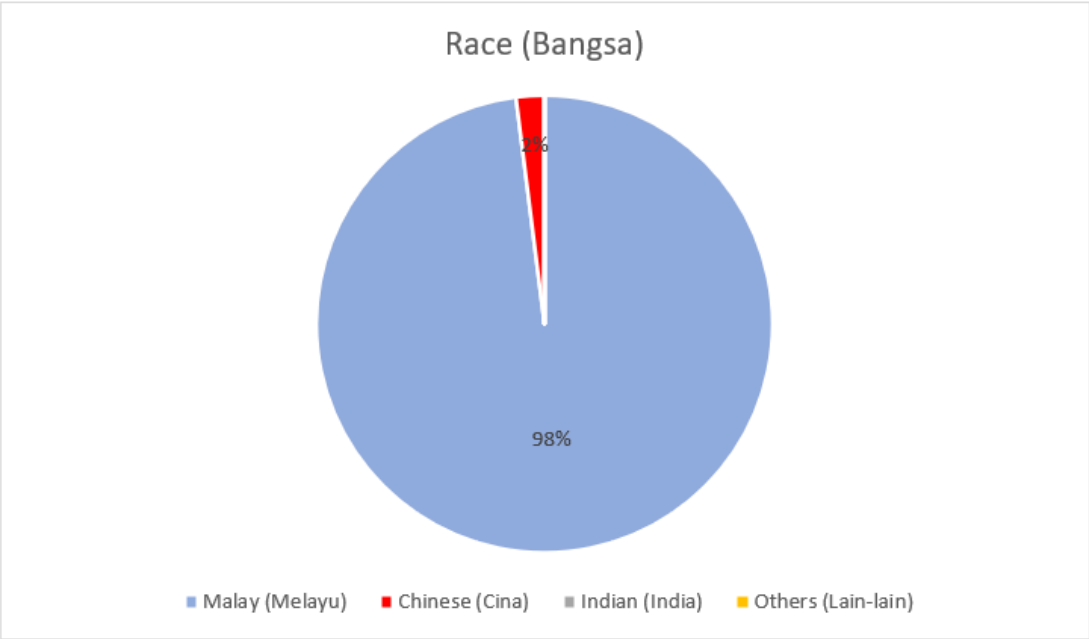


Figure 5.5 Questionnaire Result for Race in percentage

Figure 5.5 shows the race of respondents who answered this questionnaire. As we can see, most of our respondents are Malay which is 98% of respondents from them answered this questionnaire. Then, 2% of the respondents are Chinese. There are no Indian and other races answered this questionnaire. This questionnaire should answer by many races since it may produce a quality result from them. However, with these 50 respondents and only two races are involved, it also will help us to develop a better web application for this project.

4. Occupation Status

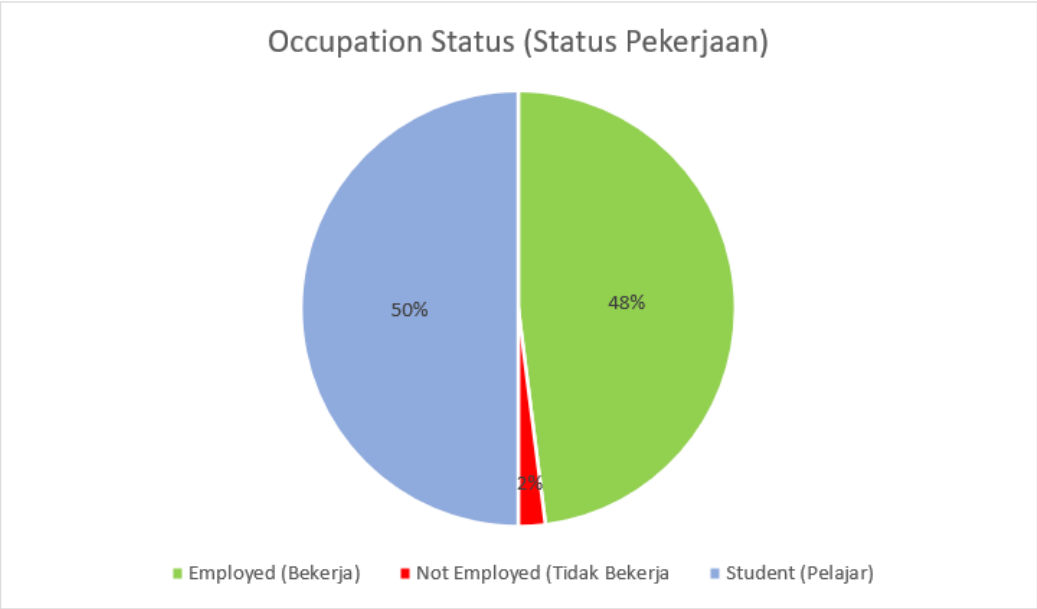


Figure 5.6 Questionnaire Result for Occupation Status in percentage

Figure 5.6 shows the occupation status of respondents who answered this questionnaire. Based on this figure, we found that 50% of the respondents are students. And 48% of the respondents are employed and only 2% of respondents are not employed. This shows that most of the users who interest in this questionnaire and want to hide their confidential files are workers and students. Thus, they might be our target users for this project.

5.5.1.2 Section B: Image Steganography Techniques

Question 1: Have you ever heard of Image Steganography Technique?

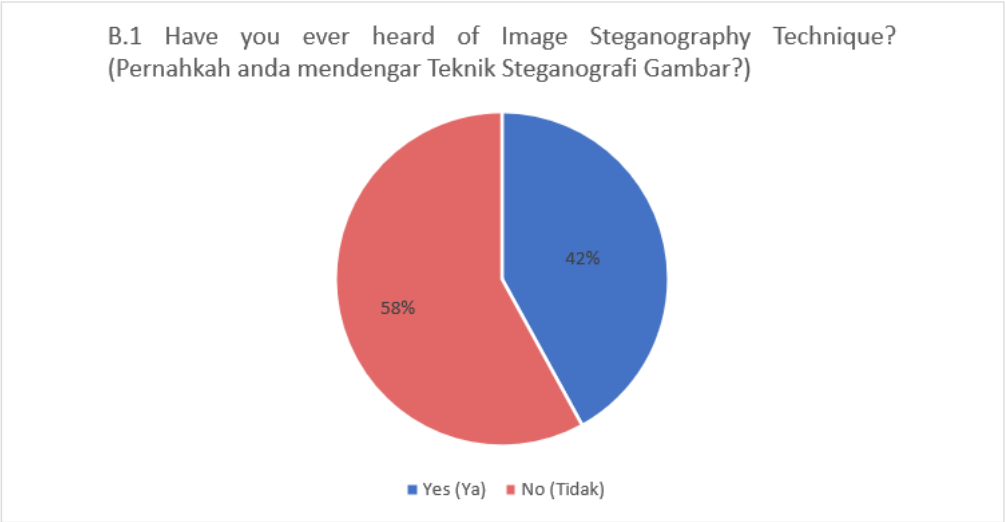


Figure 5.7 Result of Question 1 for Section B

Figure 5.7 shows the result of question 1 for section B. From the figure above, we found that 58% of the respondents have not heard about the image steganography technique. And only 42% of respondents heard about the image steganography technique. The reason why a large number of respondents do not know about image steganography techniques is that the word steganography is rarely used and heard by them. However, some respondents may have heard the word steganography and its technique.

Question 2: Have you ever heard of Image or Visual Cryptography Technique?

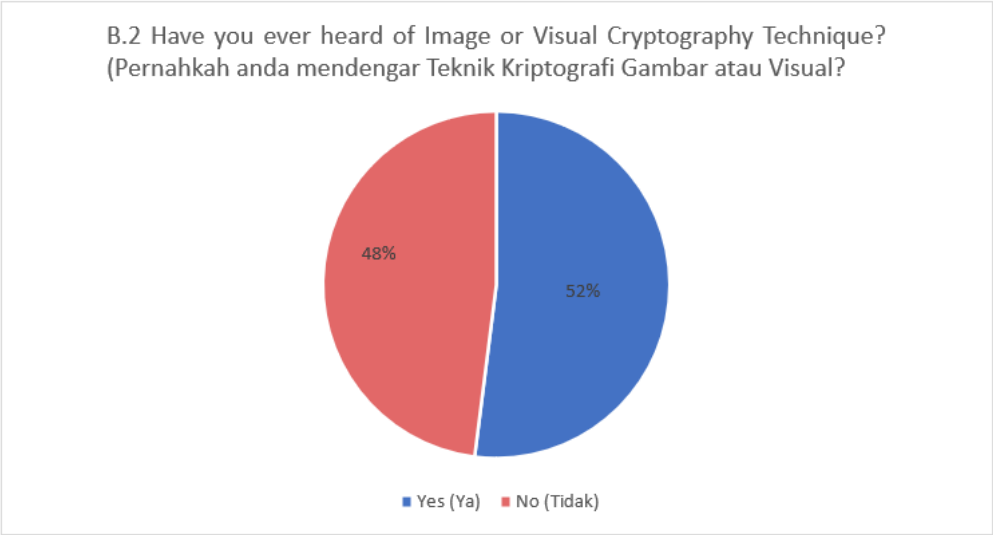


Figure 5.8 Result of Question 2 for Section B

Figure 5.8 shows the result of question 2 for section B. From the figure above, we found that 52% of the respondents have heard about the image or visual cryptography technique. And 48% of respondents have not heard about the image or visual steganography technique. The reason why respondents heard and know about image cryptography rather than image steganography is because the word cryptography is familiar to them because the word usually used in Information Technology subject. However, this question will be helpful to us since many of the respondents know the meaning of the cryptography technique and indirectly, they may understand what system we will develop.

Question 3: Do you know that Steganography and Cryptography techniques can be combined to secure your confidential file?

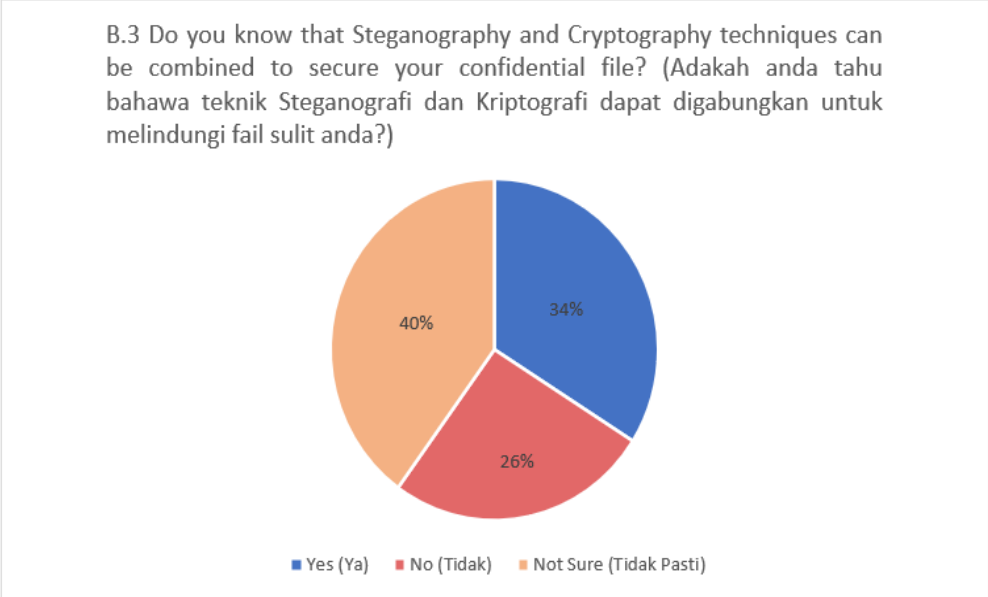


Figure 5.9 Result of Question 3 for Section B

Figure 5.9 shows the result of question 3 for section B. From the figure above, we found that 40% of the respondents not sure that steganography and cryptography techniques can be combined to secure their confidential files. And 26% did not know that those techniques can be combined to secure their confidential file. In spite of that, 34% of the respondents know that both steganography and cryptography techniques can be combined to secure their secret data or file. This means some of the respondents know how those techniques work and their feedback may help us to develop a better system for this project.

5.5.1.3 Section C: Use of File Hiding Application

Question 1: Confidential file should not be viewed by unauthorized user

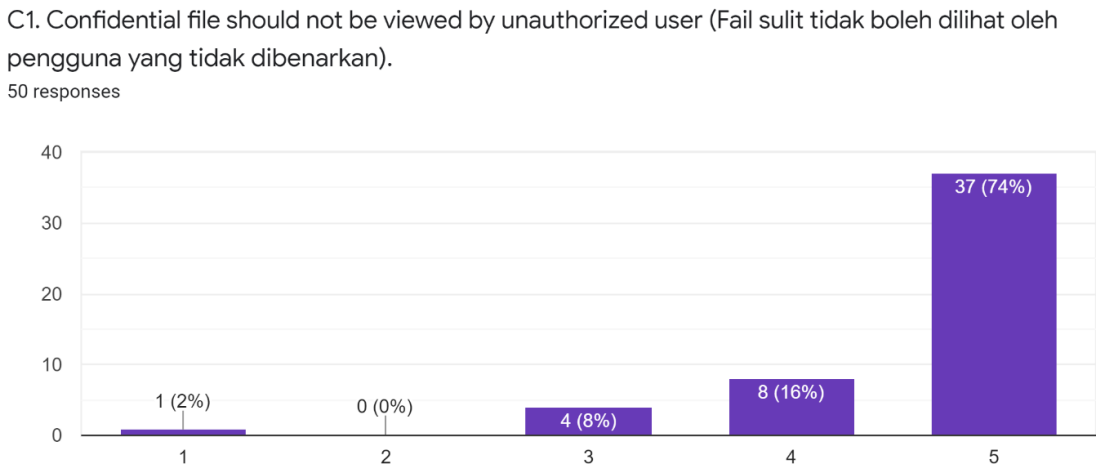


Figure 5.10 Result of Question 1 for Section C

Figure 5.10 shows the result of question 1 for section C. Based on the figure, we found that 74% of the respondents strongly agree that confidential files should not be viewed by unauthorized users. And 16% agree with the statement. However, there is 8% of respondents vote for moderate because they did not sure or not understand the meaning of this statement. And 2% of the respondents strongly disagree with this statement. As a summary, most of the respondents agree with this statement and this could strengthen the reason why this file hiding web application is needed to protect their confidential file.

Question 2: Password is normally required to protect the authorization of a system or access to a system.

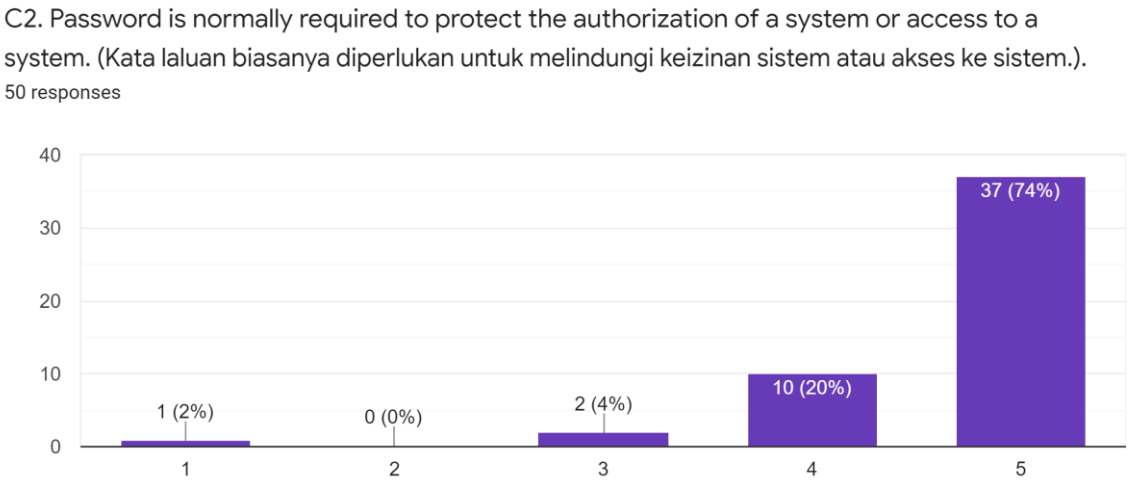


Figure 5.11 Result of Question 2 for Section C

Figure 5.11 shows the result of question 2 for section C. Based on the figure, we found that 74% of the respondents strongly agree that the password is required to protect the authorization of a system or access to a system. And 20% agree with the statement. However, there is 4% of respondents voted for moderate because they did not sure either the password is important or not to secure the authorization of the system. And 2% of the respondents strongly disagree with this statement. As a summary, most of the respondents agree with this statement and this feedback could help us to enhance our system by adding login credentials including passwords in the system that will be developed.

Question 3: Have you ever used any file hiding application or software to hide your confidential file?

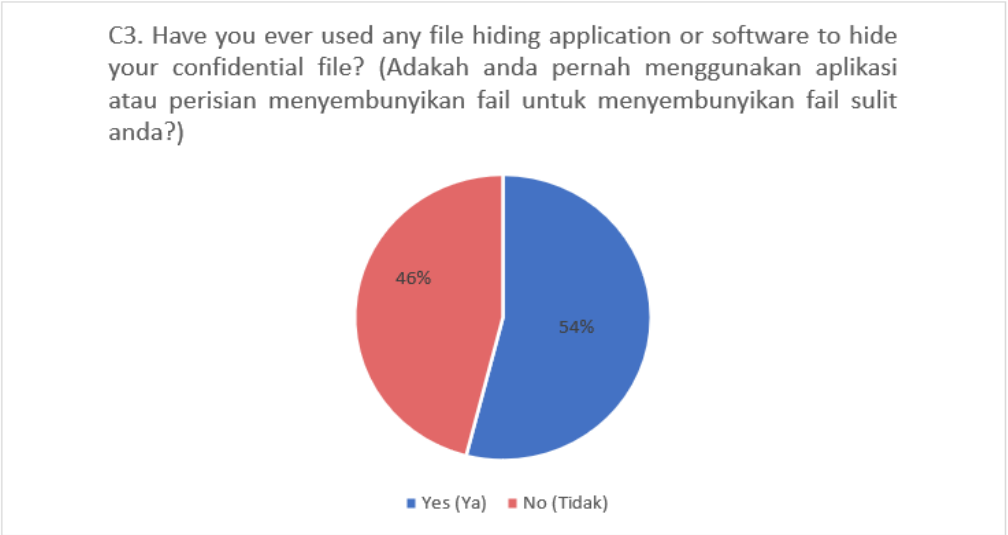


Figure 5.12 Result of Question 3 for Section C

Figure 5.12 shows the result of question 3 for section C. Based on the figure, we found that 54% of respondents once used an application or software to hide their confidential files. However, there is 46% of respondents never used any applications or software that able to hide their confidential files. Thus, this feedback could strengthen the reason why we develop this system and it will help them to secure and hide their confidential files.

Question 4: If you use a file hiding tool, what type of file you want to kept it hidden?

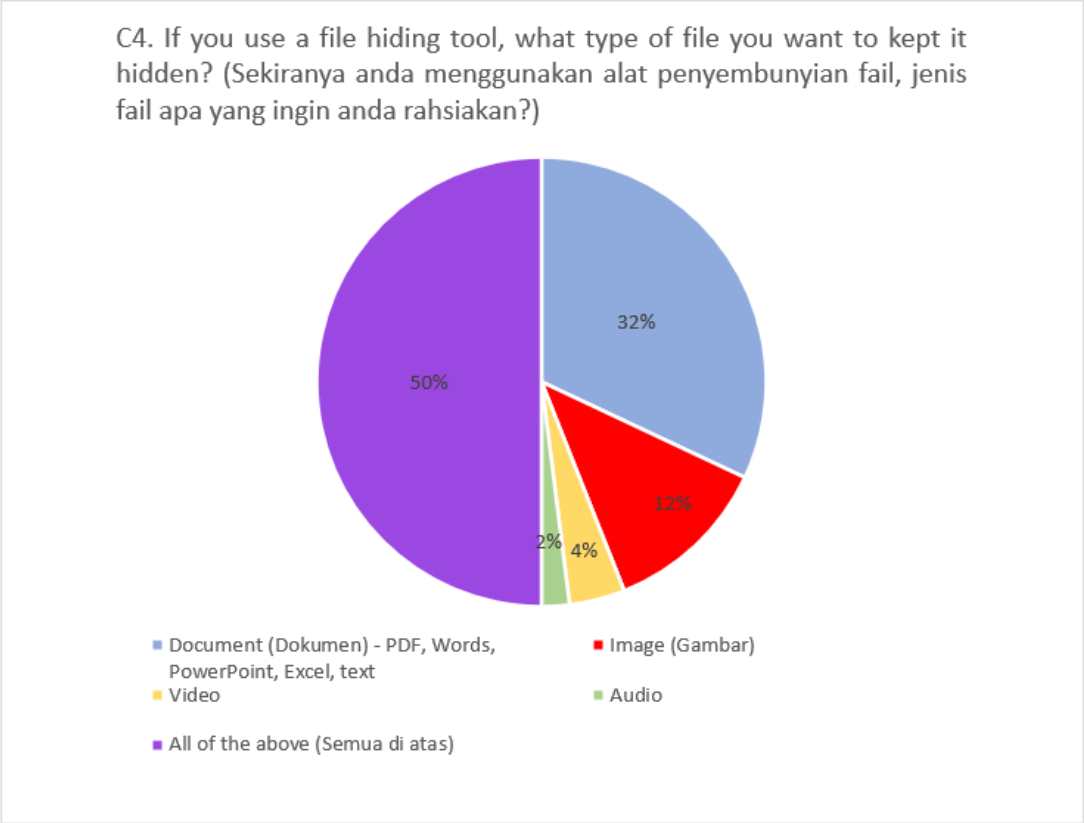


Figure 5.13 Result of Question 4 for Section C

Figure 5.13 shows the result of question 4 for section C. Based on the figure, we found that 32% of respondents want to hide a document such as PDF, Words, PowerPoint, Excel and text if they use a file hiding tools. And there is 12% of respondents want to hide their image file. Other than that, 4% of the respondents want to hide a video files and 2% want to hide the audio files. However, there is 50% of respondents want to hide all the file mentioned above. Thus, with this feedback, we can enhance our system by allowing users to hide all types of files that they want. This feature could be helpful to them to hide their confidential files easily.

Question 5: Where do you usually store your confidential files?

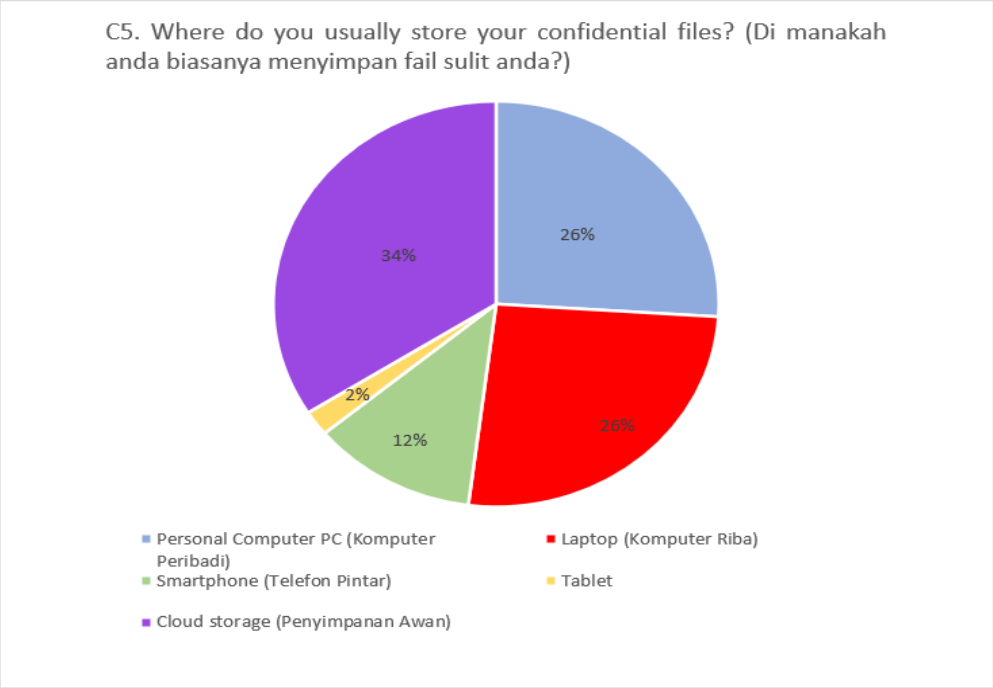


Figure 5.14 Result of Question 5 for Section C

Figure 5.14 shows the result of question 5 for section C. Based on the figure, we found that 34% of respondents usually store their confidential files in their cloud storage. Besides, PCs and laptops have the same percentage where 26% of respondents keep their confidential files in both devices. And there is 12% of respondents store their confidential files on their smartphones and 2% of them keep it on their tablets. As a summary, most of the respondents store their confidential files in their cloud storage. Thus, with this feedback, we may enhance our system by allowing users to store their confidential files in their cloud storage.

Question 6: Cloud storage makes it easy for users to store and share their confidential files.

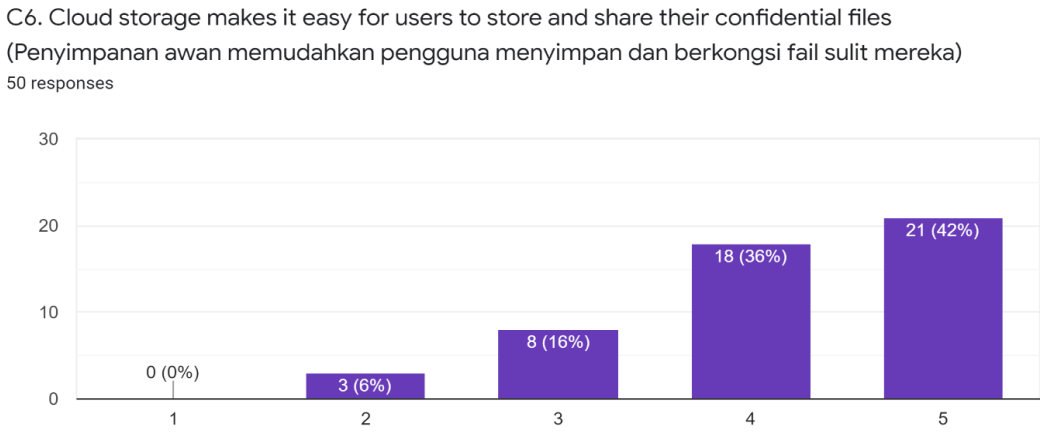


Figure 5.15 Result of Question 6 for Section C

Figure 5.15 shows the result of question 6 for section C. From the figure above, we found that 42% of respondents strongly agree that cloud storage makes it easy for users to store and share their confidential files. And there is 36% of respondents agree with this statement. However, 16% of the respondents voted for moderates and 6% disagree with these statements. This is because they do not always or never use cloud storage to store their data. As a summary, most of the respondents agree with these statements and this could strengthen the reason why we should include these cloud storage features on this project.

Question 7: In your opinion, is it necessary to develop an application that can hide confidential files?

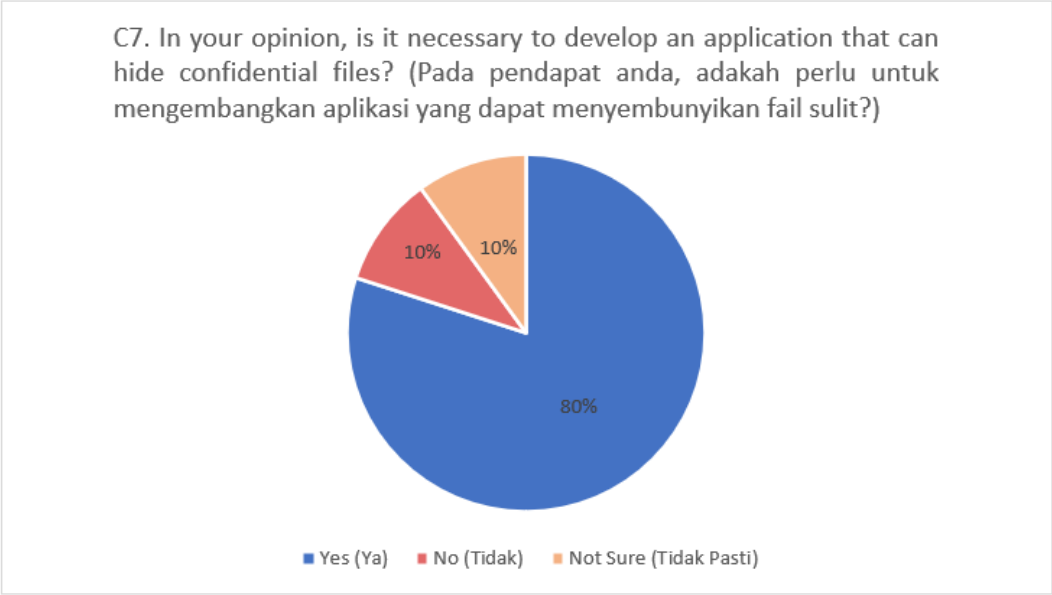


Figure 5.16 Result of Question 7 for Section C

Figure 5.16 shows the result of question 7 for section C. From the figure above, we found that 80% of respondents voted yes that it is necessary to develop an application that can hide confidential files. And there is 10% of the respondents voted no and 10% of them voted for not sure either it is necessary to develop these applications. As a summary, we can conclude that most of the respondents agree that the application that can hide the confidential files should be developed. With this feedback, this could strengthen the purpose and reasons for this project which is to develop a web application that can hide the user's confidential data.

5.6 Conclusion

This chapter helps us to understand more about the requirement needed by the users. The data and system modeling such as the use case and flowchart diagram will help the developers to understand how the system will develop works. Thus, this makes it easy for developers to build this system. Besides, questionnaire feedback by the respondents could help us the most since it may guide us to produce a system that meets the user requirement. Although this application was built to facilitate any users to hide their confidential files, the deficiencies in this application could help the developers to improve this application to be a better application by meeting all requirements needed to produce a quality and efficient system. When this project does not fulfill the requirements from the feedback, this development process needs to rebuild and produce a better result. In conclusion, this chapter is necessary to ensure the File Hiding Web Application achieves its objectives.

6 Design

6.1 Introduction

The design phase is quite simple compared to the other phase. Thus, in this chapter, the developers will present and explain the design of the system that has been created during the design process. The design of the system is based on the user requirements and the analysis of an existing system. Therefore, the design will be illustrated and presented before the software is developed.

This chapter will show and describe the design of the interface such as the sign-in and sign-up interface. Then, database design is also presented in this chapter since this system possesses data that need to be stored. Database design includes a data dictionary, data flow diagram and entity-relationship diagram (ERD). Other than that, this chapter also illustrates the security system framework that will be implemented in this system. As this project is intended to develop a file hiding web application, the security element framework may include the hash code which will be used for authentication and the process of hiding and reveal the file. To understand how the application of this project will be function, this chapter also provides and describe the flow of the system. Thus, the developer will understand what the system design and its requirement should be. Thus, they can develop a system based on the design given. This system flow also could be useful for the user to understand how to use this system.

6.2 Interface Design

6.2.1 Homepage Design

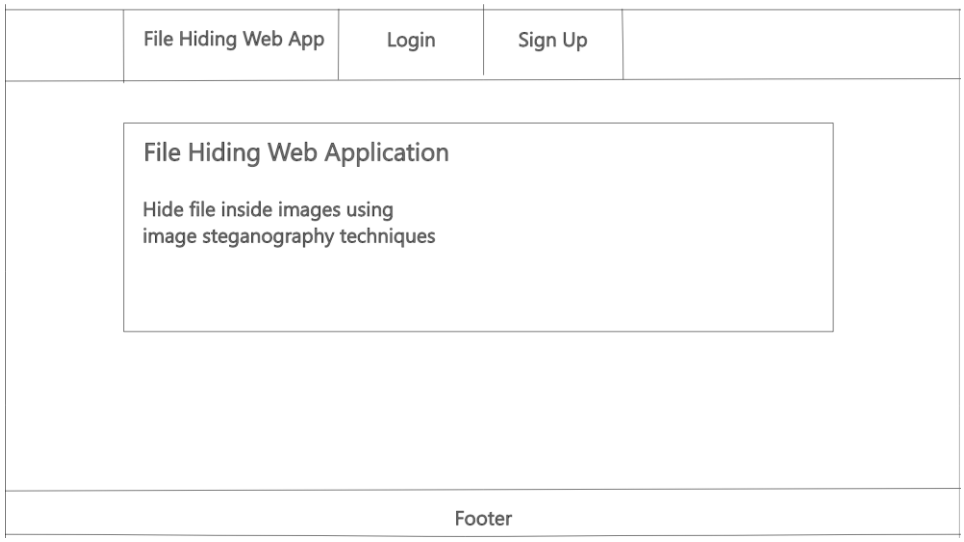


Figure 6.1 Homepage Design

Figure 6.1 above shows the homepage design and layout of this system. The user including the normal user and admin will directly go to this page first since it is the index or home page of the system. This homepage provides a menu or navigation bar for their header. This header will be presented on each page of the website. The menu consists of ‘Login’ and ‘Sign Up’. Users will go to the login page if they click the ‘Login’ menu, while for the ‘Sign Up’ menu user will go to the sign-up page. Then, on this homepage, it also provides a banner that presents the title of the website and its function. Other than that, this website also provides a footer that will be presented on each page of the website.

6.2.2 Login Design

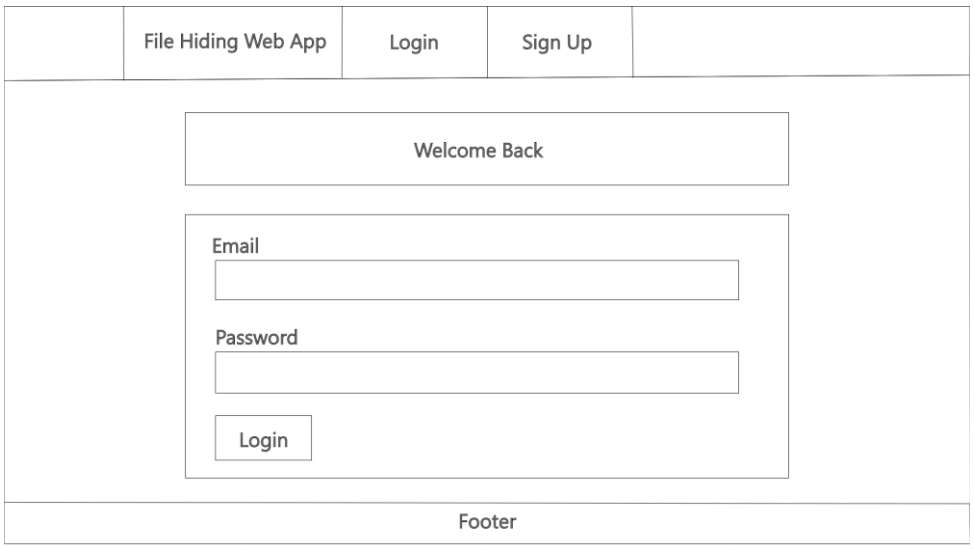


Figure 6.2 Login Design

Figure 6.2 above illustrates the login page design for this system. This page is shown when a user clicks on the ‘Login’ menu. This login page provides two information that needs to be filled in which are email and password. Users, such as normal users and administrators, need to fill in the email and password that have been registered to access the features of this system. Then, if the email and password are valid, the users will directly go to the account page after they click the ‘Login’ button. However, if users did not register to login into the system, they should go to the sign-up page by clicking the ‘Sign Up’ menu.

6.3.3 Sign-Up Design

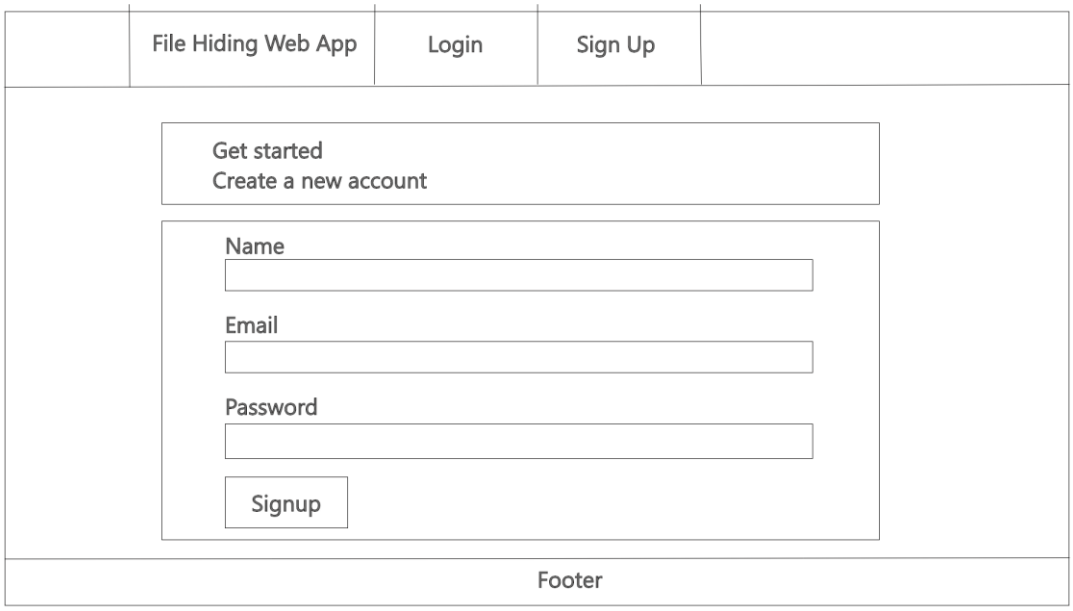


Figure 6.3 Sign-Up Design

Figure 6.3 above shows the sign-up page design and layout for this system. This page is shown when a user clicks on the ‘Sign Up’ menu. This sign-up page function is to register a user into this system and enable them to use the feature of this system. Thus, this sign-up design provides three information that needs to be filled in by the users which are name, email and password. Then, if all the information that has been filled in is valid, a user should successfully be registered into the system after they click the ‘Signup’ button and they will directly go to the account page.

6.3.4 User Account Design

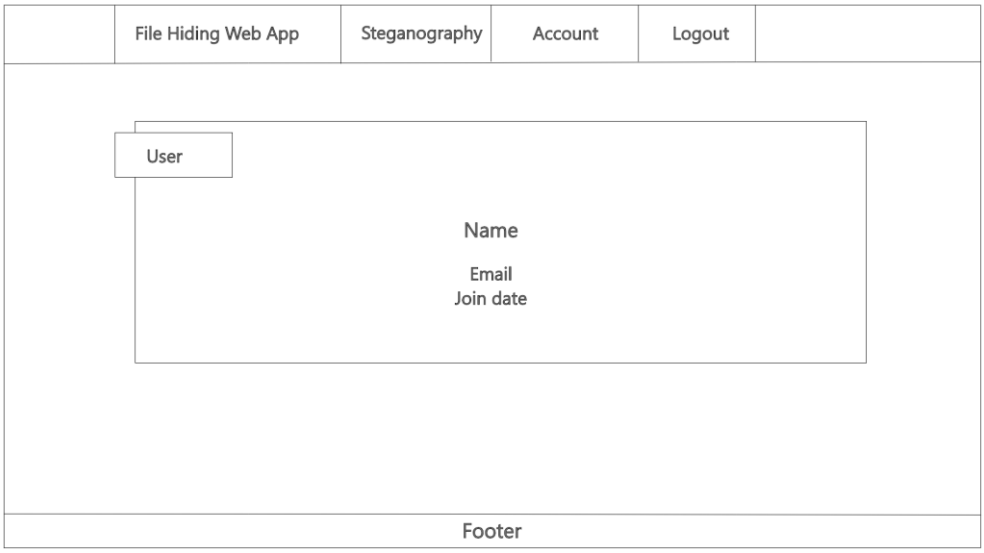


Figure 6.4 User Account Design

Figure 6.4 above shows the normal user account page design for this system. This page is shown when a normal user successfully logged in to the system. Since this page is for normal users, the menu provides in the header are ‘Steganography’, ‘Account’ and ‘Logout’. For this user account page design, the system provides a banner that displays a user name, email and joins date. At the top left of the banner, the user’s role is shown. Thus, since this account page is for a normal user, the display of the role is ‘User’. Other than that, if users click the ‘Steganography’ menu, they will proceed to the steganography page. And for the ‘Logout’ menu, if they click it, users will end their session and directly go to the login page.

6.3.5 Steganography Hiding Files Design

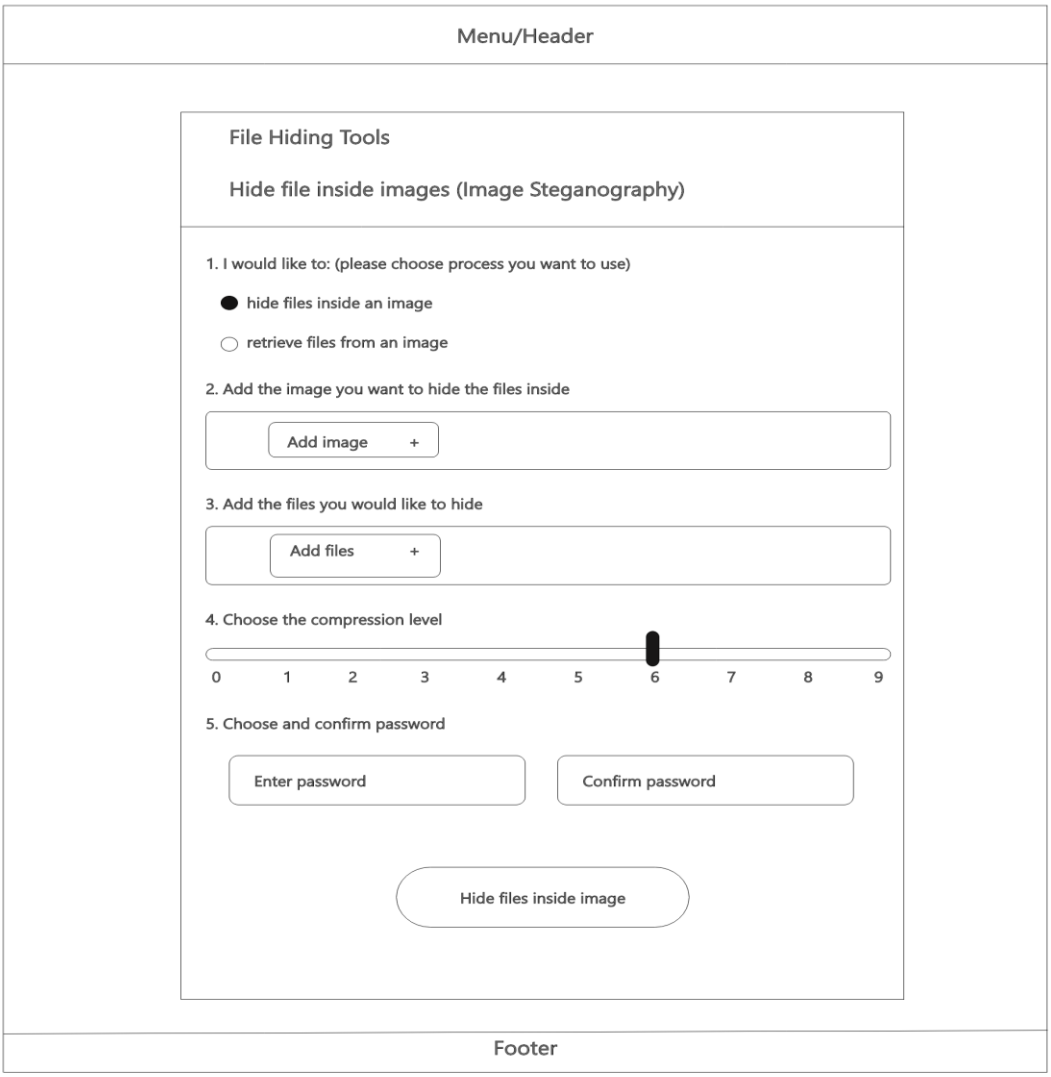


Figure 6.5 Steganography Hiding Files Design

Figure 6.5 above presented the steganography hiding files page design. This page is shown when users including normal users and administrators click the ‘Steganography’ menu. Thus, this page is available for normal users and administrators. This page provides the main function of this system which is to hide and reveal files inside the image using image steganography techniques. For hiding a file inside the image, users must click a radio button that is provided in question one which is the ‘hide files inside image’. After users click it, the system will provide a form to hide a file inside the image that needs to be filled by the users. Based on Figure 6.5, the page design provides ’Add image’ button to add the image that they want to hide the files inside. Next, users must click the ‘Add files’ button to add the files that they want to hide and choose the compression level to compress the file. The system also provides the user to set the password for the files. Then, to proceed with the hiding process, ‘Hide files inside image’ button is provided. After that, click again the button to download and store the image files that contain hidden files into the user's devices or local storage.

6.3.6 Steganography Reveal Files Design

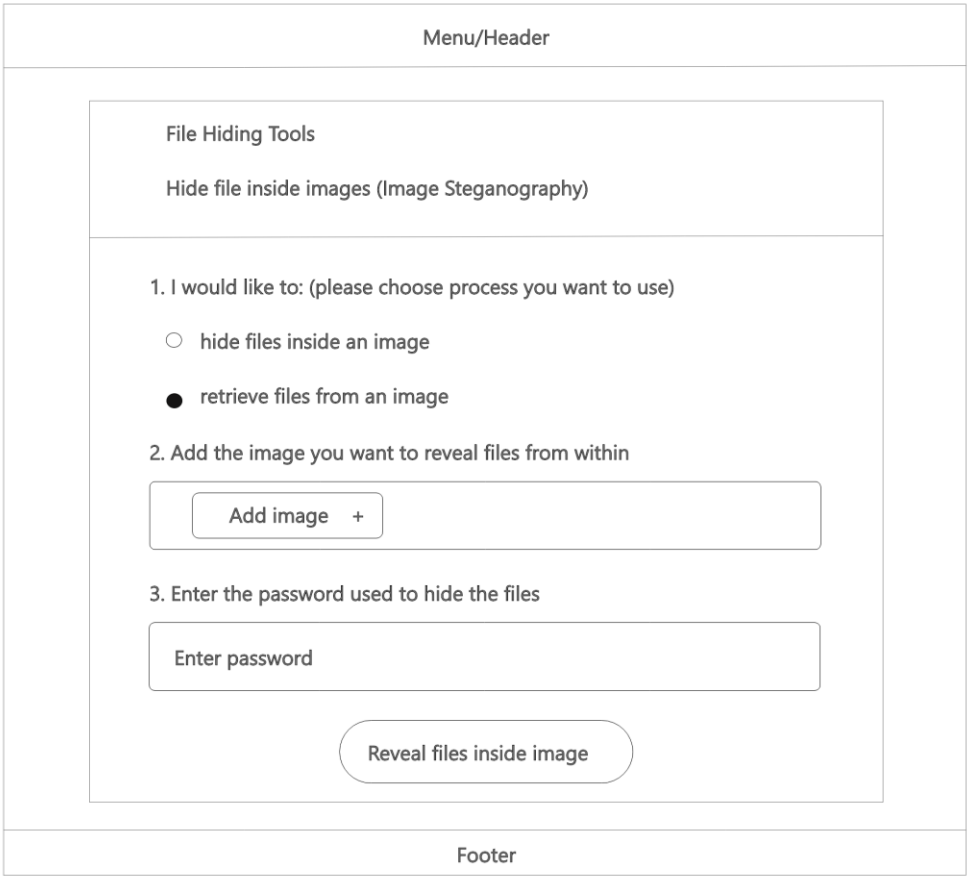


Figure 6.6 Steganography Reveal Files Design

Figure 6.6 above presented the steganography reveal files page design. This page design is also displayed on the steganography page. The difference from the steganography hide files design is their form that needs to be filled. To run the reveal files process, users must click a radio button that is provided in question one which is the ‘retrieve files from an image. After users click it, the system will provide a form that is different from hiding a file inside the image form that needs to be filled by the users. For revealing a files design, the system provided only two forms that need to be filled by the users. Based on Figure 6.6, the page design provides ‘Add image’ button to the user to add the image that they want to reveal the files from within. Then, users just need to enter the same password that has been set or used to hide the files. After that, proceed with the reveal process by clicking the ‘Reveal files inside image’ button. Then, click again the button to download and store the hidden or revealed files into the user's devices or local storage.

6.3.7 Admin Account Design

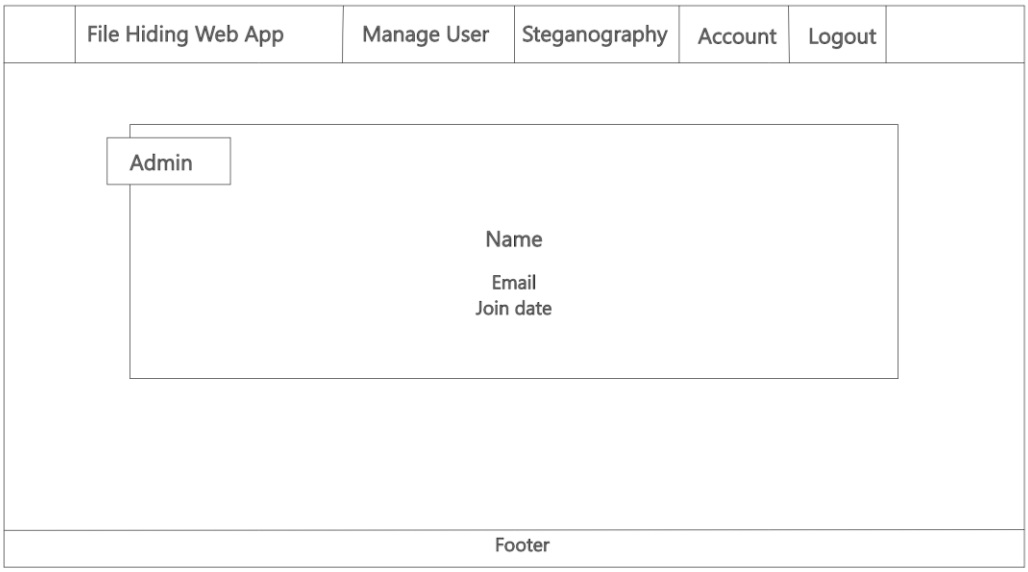


Figure 6.7 Admin Account Design

Figure 6.7 above shows the admin account page design for this system. This page is shown when an administrator successfully logged in to the system. Since this page is for administrators, an additional menu is provided in the header which is ‘Manage User’ that make it different from normal users. For this admin account page design, the system provides a banner that displays the administrator name, email and joins date. At the top left of the banner, the user’s role is shown. Thus, since this account page is for administrators, the display of the role is ‘Admin’. Other than that, if users click the ‘Manage User’ menu, they will proceed to the manage user page. Then, for the ‘Steganography’ menu, they will proceed to the steganography page. And for the ‘Logout’ menu, if they click it, the admin will end their session and directly go to the login page.

6.3.8 Manage User Design

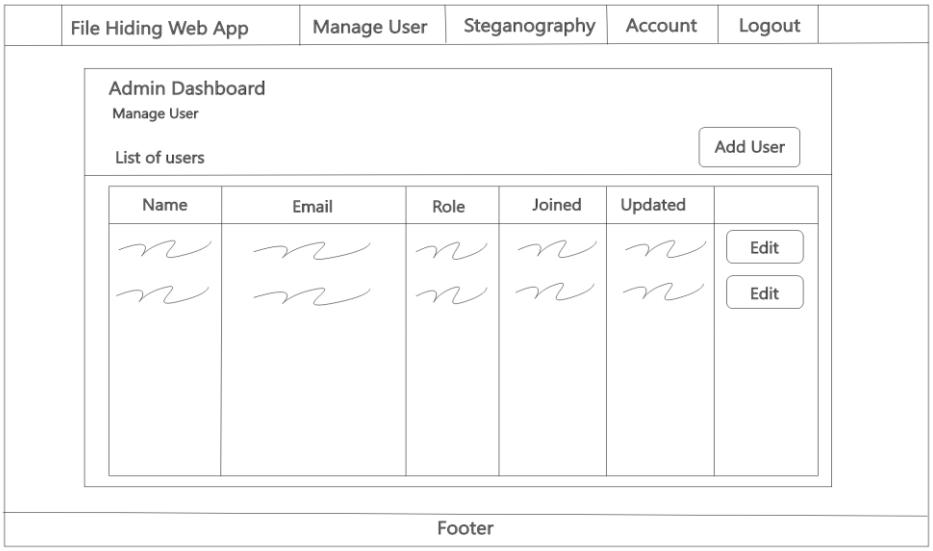


Figure 6.8 Manage User Design

Figure 6.8 above shows the manage user page design for this system. This page is shown when users with admin role click the 'Manage User' menu. This means, this feature only available for administrators. For this manage user page design, the system will display the admin dashboard that provides a list of users that has been registered in the system. Thus, the details of registered users such as name, email, role, joined date and updated date will be displayed on this page. Then, the admin can edit the user's information by clicking the 'Edit' button and they will proceed to the edit user information page. Other than that, an admin also can add a new user by clicking the 'Add User' and directly proceed to the create new user page.

6.3.9 Add New User Design

Figure 6.9 Add New User Design

Figure 6.9 above illustrated the add new user page design for this system. This page is shown when administrators click the ‘Add User’ button on the manage user page. For this add new user page design, the system will display a form that needs to be filled in by the admin to add a new user to the system. Thus, this page will provide four information that needs to be filled in by the admin which are name, email, role and password. Then, if all the information that has been filled in is valid, a new user should successfully be registered into the system after the admin clicks the ‘Add User’ button. Then, the admin will directly go to the manage user page back. For the ‘Back’ button located at the top right of the page, an admin will go back to the manage user page if they click the button.

6.3.10 Edit User Information Design

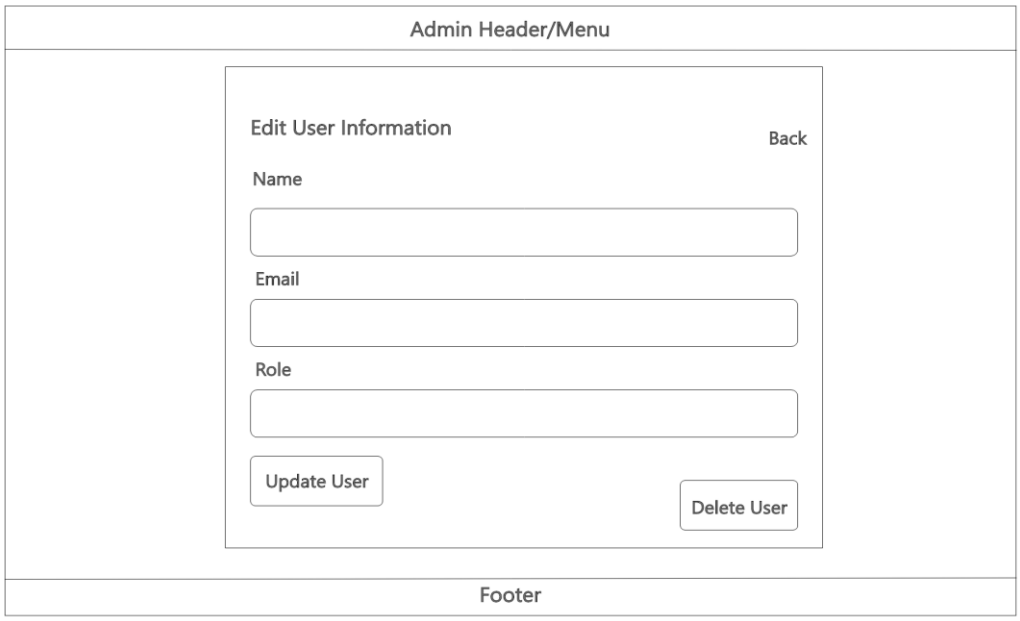


Figure 6.10 Edit User Information Design

Figure 6.10 above shows the edit user information page design for this system. This page is shown when administrators click the ‘Edit’ button on the manage user page. For this edit user information page design, the system will display user information that needs to be edited by the admin. Thus, this page will provide three information that able to be edited by the administrator which are name, email and role. Then, if some information has been edited, the admin can successfully update the user information by clicking the ‘Update User’ button and after that admin will directly go to the manage user page back. For the ‘Delete User’ button, an admin could delete the user from the system by clicking the button. And for the ‘Back’ link located at the top right of the page, an admin will go back to the manage user page if they click the button.

6.3 Database Design

6.3.1 Data Dictionary

Table 6.1 Data Dictionary for File Hiding Web App

Table Name	Data Item	Data Type	Data Format	Description	Example	Validation
users	_id	ObjectId	Alphanumeric: “60041ee4206de134131”	Unique identifier for user	“60042ae23b03421430760590”	
	name	String	“This is a string”	Name of user	“Amirul Naim”	
	email	String	“This is a string”	Email of user	amirulnaim@gmail.com	Email format, must have @
	role	String	“This is a string”	Role of user	“admin”	Accept only [“admin”, “user”]
	password	String		Password of user	“Amirul12345”	At least 6 characters
	createdAt	Date	MM/DD/YYYY	Date created	12/1/2018	
	updatedAt	Date	MM/DD/YYYY	Date updated	5/31/2018	

Table 6.1 shows the data dictionary for this file hiding web application. For the database, this system requires only one table of data which is users. It is because the main feature of this system which is hiding and reveal the files inside the image does not send any data to a server, it uses only client-side JavaScript.

Thus, for the data dictionary, it has table users. In the table users, it provides seven data which is _id, name, email, role, password, createdAt and updatedAt. The data type of _id is ObjectId and its data format is alphanumeric such as “60041ee4206de134131”. This data act as a unique identifier for users. For name data, the data type is a string and this field is to store a user name. Next, for email data, the data type is a string and this data is to store user email. Email data has validation where it must have @, for example, a user must input their email such as “amirulnaim@gmail.com”. Then, for role data, its data type is a string and it is to stores the role of a user. The system can store only specific role, which is “admin” and “user”. For password data, its data type is a string and it will store user password. The password must be at least 6 characters, for example, “Amirul12345”. For createdAt and updatedAt data, both data types are date. This data is to store the date created and date updated of user information. Its data format is MM/DD/YYYY.

6.3.2 Data Flow Diagram

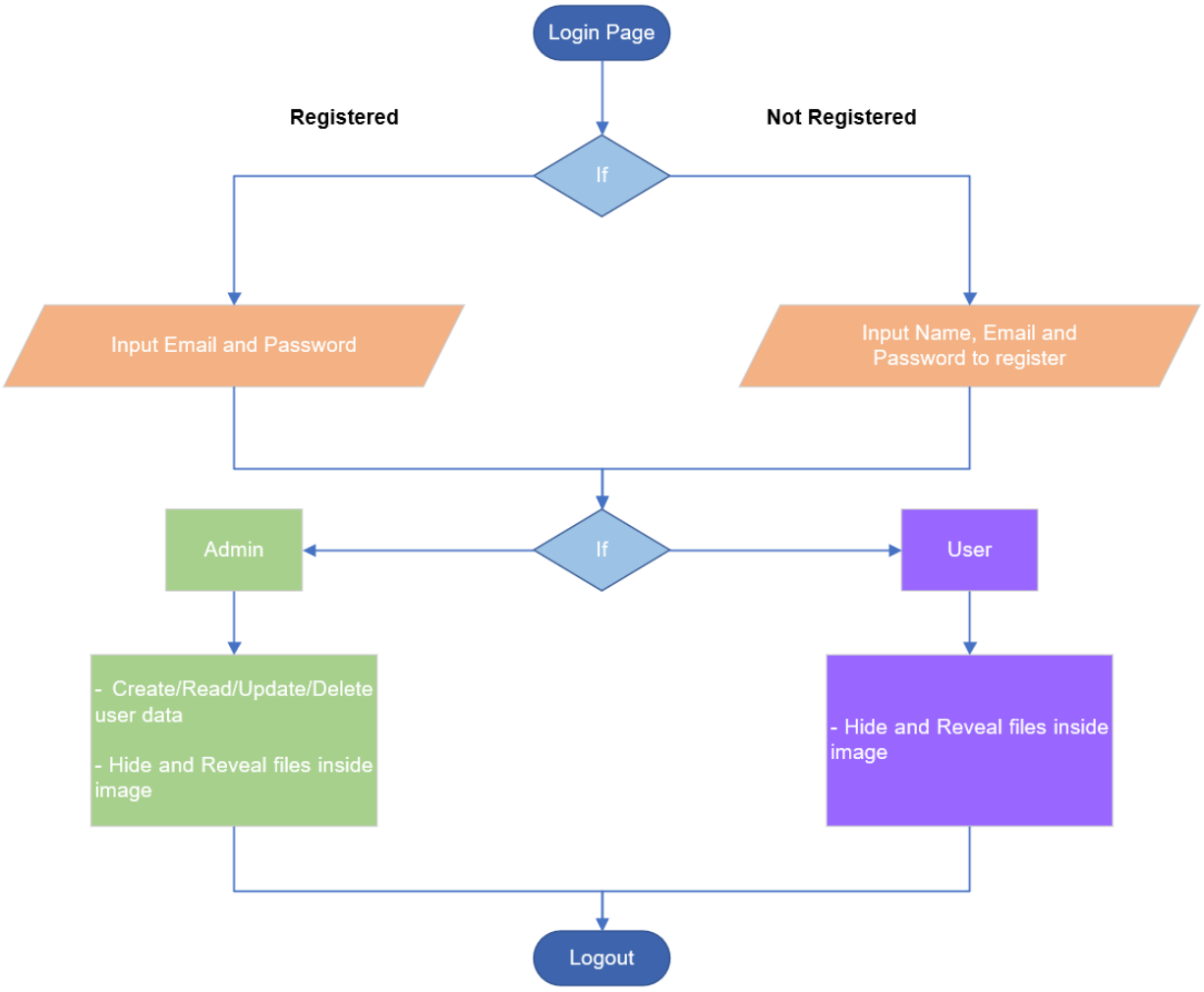


Figure 6.11 Data Flow Diagram

Figure 6.11 above shows a data flow diagram for this system. The user only requires an email and password from the database to access the system. Based on Figure 6.11 above, a user must go to the system login page. Next, if they have been registered to the system, they must input email and password, then successfully access the system. However, if a user did not register to the system, they must go to the sign-up page and register to the system by entering their name, email and password. After successfully registered, the user will automatically access the system. After granted access to the system, if the user has an admin role, they can create, read, update and delete user data. Also, the admin can use the main feature of this system which is to hide and reveal files inside the image. Then, if the user has a user role, they only can use the main feature of the system which is to hide and reveal files inside the image. Then to end the session, both admin and normal user must logout from the system.

6.3.3 Entity-Relationship Diagram (ERD)

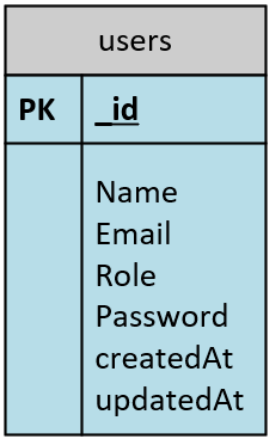


Figure 6.12 Entity-Relationship Diagram

Figure 6.12 above presented an Entity-Relationship Diagram (ERD) for the file hiding web application. Based on Figure 6.12, this system only has one table in the database which is users. The user of this system should be anyone who wants to hide their secret file inside the image file. Other than that, the user of this system is the owner of this website or the developer which will hold the admin roles for this system. Thus, the database of this system only has one table which is users is because the main features of this system, which hides and reveals a file inside the image, do not send any data to a database server, it only uses JavaScript on the client-side. This means that all the user files that have been hide and reveal will not be stored in the system database. Thus, the data will be processed on the browser only.

Therefore, the system database only will be stored users' detail such as id, name, email, role, created date and update date. The primary key for this 'users' data is _id. Thus, to get other user details, users _id must be called first. This 'users' data is used for the authentication process to access the system. Thus, a user must fetch data such as email and password from this 'users' data. This 'users' data also needed to store the details of a new user that has been registered for this system. The system database is secure and trusted because the password is stored in hash code. This means the developer cannot view the actual user's password. Other than that, since users with the admin roles can manage user's details such as name, email and role, 'users' data is needed to fetch all the user's data that have been registered. Thus, this 'users' data is used for the authentication process, registration process and managing the user's details.

6.4 Security System Framework

The security system framework is important in this system since we may protect users' important files. Since the system also stored user details in the database server, the security element is needed to protect the user data. Therefore, the security element framework is provided and will be discussed more in the next section.

6.4.1 Security Element Framework

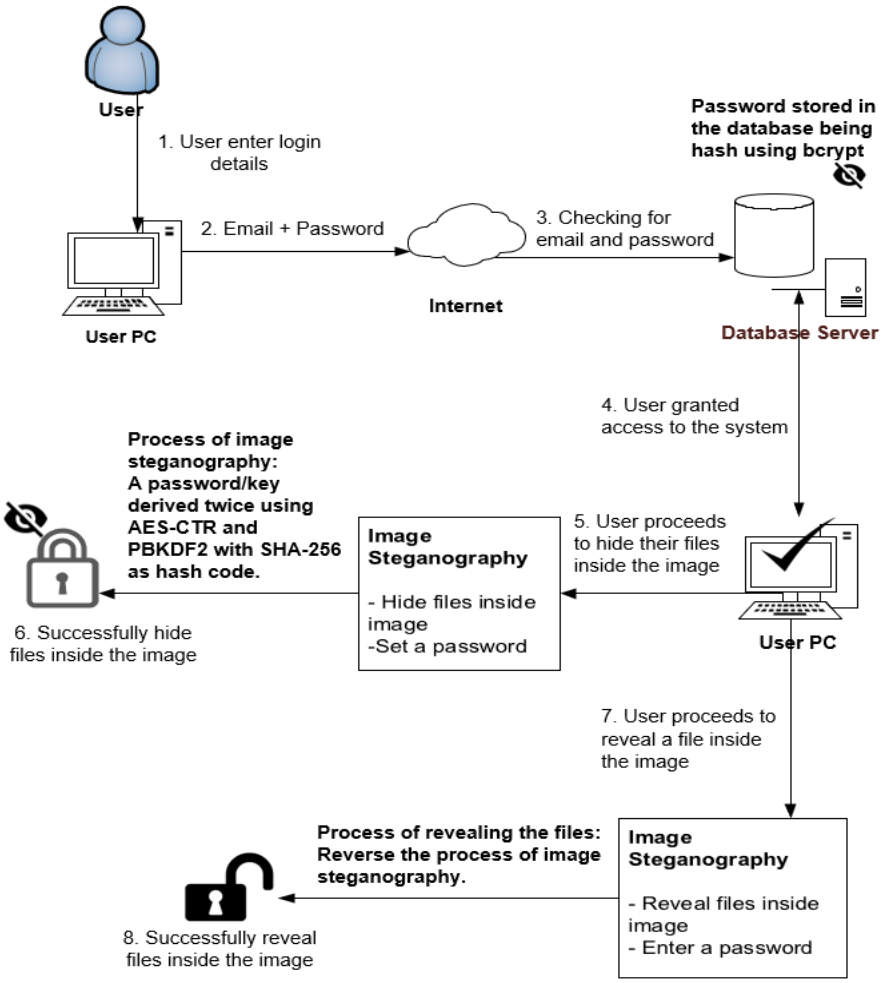


Figure 6.13 Security Element Framework

Figure 6.13 above shows the security element framework involves in the system. This system actually provides the security element framework on the authentication process, database and hide and reveal files inside the image process. Based on Figure 6.13, to access the system a user must enter the login details which are email and password. The user device or PC must connect to the internet to make a request to the server. After the user enters the login details, the system will check for the email and password either it is valid or not. The database server is secured and trusted since the user may store the password in the database. Therefore, to make it secure, the password that is stored will be hash using 'bcrypt' (a password-hashing function), based on the Blowfish cipher. Then, if the login details are valid, a

user may grant access to the system and they can perform the feature of the system which is hiding and reveal a file inside the image.

Next, if the user wants to proceeds to hide their files inside the image, they can go to the steganography page and proceed with the steps. To avoid unauthorized users to view the hidden files inside the image, a user can set a password for the files to be revealed. So, during the hiding or image steganography process, the files will be hidden and encrypted inside the image files. Then, the password that has been set by the users will be derived twice using AES-CTR and PBKDF2. The PBKDF2 will use the SHA-256 as their hash function along with the input password and salt value to produce a derived key. Thus, with this security element, unauthorized users difficult to crack the password and view the secret files that have been hide in the image file since the password has been encrypted. After this process complete, users successfully hide their secret files inside the image.

Then, if the user wants to proceeds to reveal their files inside the image, they can go to the steganography page and proceed with the steps. To reveal the hidden files inside the image file, a user must add the image file and then enter the password that has been set to hide the files. If the user did not possess the actual password, they cannot view or decrypt the hidden files. Thus, the process of revealing or decrypting the hidden files is the reverse process of the hiding process. This means the system will decrypt the hidden files by reversing the process of hiding and encrypting the secret files that may include the use of SHA-256, PBKDF2 and AES-CTR. After the reveal process complete, users successfully reveal the secret files inside the image.

6.5 Flow of the System

The flow of the system is easy to understand since all the process has been described in the analysis chapter. The flow of the system is based on the user requirement and analysis that has been made. The developer should understand and know the flow of the system and the features that the system should provide. Thus, the application flowchart is illustrated first to ease the developer developed this file hiding web application.

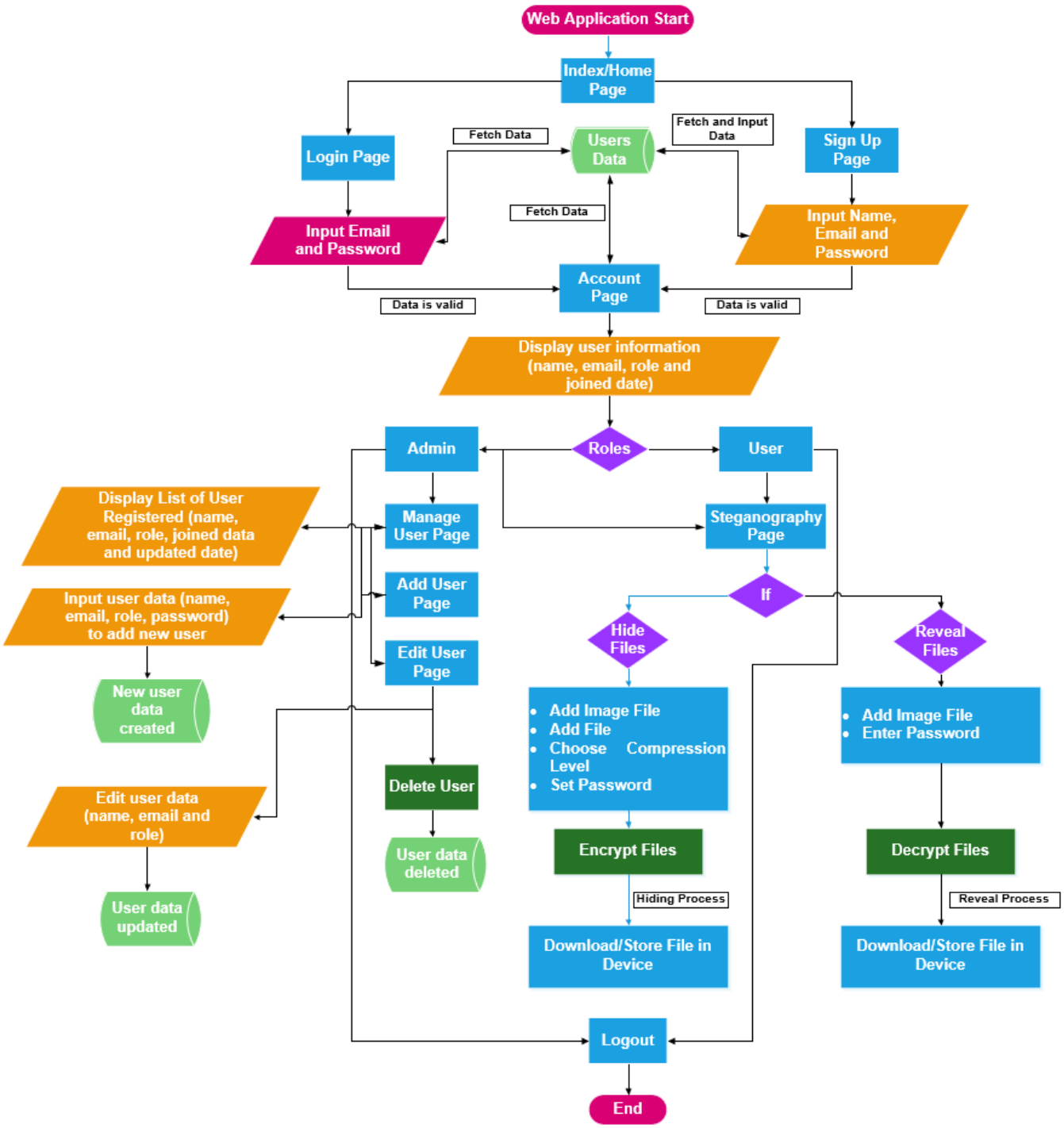


Figure 6.14 Application Flowchart

Figure 6.14 above shows the flow of the system for this project. Based on the figure, the system of file hiding web application start when a user visits the home page of the website. The home page provides a login and sign-up menu. If a user has registered to the system, they can go to the login page. On the login page, a user needs to input login details which are email and password. After inputting the details, the system will fetch the data from the database server and if the input data is valid, the user will grant access to the system and will automatically go to the user account page. However, if the user is not registered to the system, they must go to the sign-up page. On the sign-up page, a user must enter the details such as name, email and password. After entering the details, the system will fetch and add the input data into the database and if the input data is valid, a user should successfully register into the system and will automatically proceed to the user account page. The account pages will display the user information such as name, email, role and joined date.

Then, if the user role is user, they can only go to the steganography page which is the main feature of this system. On the steganography page, users can choose either they want to hide or reveal the file inside the image. If they choose to hide a file, they must perform a hiding step by adding the image file, adding the files that they want to keep hidden, choose the compression level to compress the file and set a password to protect the file. After completed follow the step, they can proceed to the hiding process by clicking the button given on the page. Then, the hiding process is done and users can download and store the image files in their devices or local storage. Next, if they choose to reveal a file, they must perform a revealing step by adding the image files that contain secret files and enter the password that has been set to hide the secret files. After completed follow the step, they can proceed to the reveal process by clicking the button given on the page. Then, the reveal process should be done and users can download and save the revealed files in their devices or local storage.

Admin should be the owner of the website or the developer of the website. Thus, if the user role is admin, instead of access to the steganography page or the main feature, they will be having permission to manage the user’s details. Thus, the admin can access the manage user page. On the manage user page, the system will display the list of users that has been registered into the system. User details such as name, email, role, joined date and created date also will be displayed on this page. This manages user page allows the admin to add a new user by inputting the user data such as name, email, role and password. Then, if the input data is valid, a new user will be created and the data will be stored on the database. Other than that, the manage user page also allows the admin to edit user information such as user name, email and role. Then, if the changed data is valid, user data should successfully be updated and will be stored on the database.

Lastly, to end the session, both user and admin must click the logout menu in the header of the page. Thus, the system should be end and they can use the services again by visit the file hiding web application home page.

6.6 Conclusion

In conclusion, the design phase plays an important role in the project making phase. This chapter presented how the developer sketch and illustrate the project design such as the interface design, database design and flow of the system. The system design is build based on the user requirement and result in an analysis that has been made. The database design helps the developer to understand what data need to be stored on the server. System flow design helps the developer and user to understand what the system can do. Thus, this design phase is important because it will be a guide for the developer to build and implement the requirement of the system during the implementation process. Also, through designing, users will be able to understand the flow of the system and meet the system requirements.

7 Implementation

7.1 Introduction

Implementation is conducted after the design document has been constructed. All the components of the software are being developed at this phase. Thus, the design that has been designed will be translated into the source code. This implementation phase is where the developers start implementing the code for this system.

In this chapter, the purpose is to show the development and implementation of the File Hiding Web Application. This includes the execution platform that will be used for this system. The implementation tools include software and hardware such as programming language and devices specification also will be explained in this chapter. Then, the actual system interface that has been constructed based on the design plan will be presented in this chapter. Other than that, this chapter will describe the significant function or the security element of the system by presenting the important code on this system. Thus, the developer may perform the implementation process based on this chapter.

7.2 Execution Platform

The execution platform is a platform or software that will be used to implement, test and run or execute the system code. The execution platform is important since it is used to present the system that has been developed. Without the execution platform, the design and function of the system could not be run. Thus, below are the execution platform that will be used for this project.

7.2.1 Windows 10

Figure 7.1 Windows 10 Logo
(Wikimedia.org, 2021)

The File Hiding Web Application will be run on the personal workstation which is a PC or laptop. Thus, Windows 10 is used as the operating system of the personal workstation. Windows 10 is used to run other software and tools to develop this system. It is because Windows 10 operating system is compatible with any kind of software, thus this operating system is recommended for testing and developing this project.

7.2.2 Google Chrome

Figure 7.2 Google Chrome Logo
(Google, 2021)

The system that will be developed is a web application, thus to run and present the website, a web browser is needed. Therefore, this system will be present in the Google Chrome web browser. This Google Chrome is used to present the front end of the system. This web browser is chosen since the browser is popular and mostly used by all people. However, other web browsers such as Microsoft Edge and Mozilla Firefox also could run the system, but Google Chrome is chosen as our official web browser to run the system.

7.3 Implementation Tools

7.3.1 Software

7.3.1.1 Visual Studio Code

Figure 7.3 Visual Code Studio Logo
(Wikimedia.org, 2020)

Visual Studio Code is a software that the developer will used to write, test and run the code. This software is an open-source editor created by Microsoft for Windows, Linux, and macOS. The developer will write all the code on this editor. This editor also provides a terminal or Windows PowerShell which will be used to open a file, install libraries and run the development on the server. Thus, the developer used this software to write the code on the editor provided. Then, the developer may go to the terminal section and type some commands to run the code.

7.3.1.2 MongoDB Compass Community

Figure 7.4 MongoDB Compass Community Logo
(mongodb, 2021)

MongoDB Compass Community software is used to set up the system database server and store the information and data from the system. This software is a cross-platform document-based database program. It is a NoSQL database and uses JSON-like documents with optional schemas. Thus, the developers will use this software as the system back-end to store the user's system information. By using this software, users will create the system database and input a new table or field on it. Other than that, the developers could manage and edit the data on the database that has been created.

7.3.1.3 JavaScript Programming Language

Figure 7.5 JavaScript Logo
(Wikimedia.org, 2021)

The programming language that will be used for this project is JavaScript. JavaScript is popular with the web-based client-side scripting language. It is a scripting or programming language that helps developers to implement complex functions on web pages. It allows developers to dynamically update content, manage multimedia and animate images. Since this programming language is compatible with web development, the developers use this programming language to develop the File Hiding Web Application. The developers may build a script such as loading a new page and validating input values of a web form. JavaScript also provides a JavaScript library or web application framework for the client-side or front-end of the system.

7.3.1.4 Node.js

Figure 7.6 Node.js Logo
(Wikimedia.org, 2021)

Node.js is a server-side platform based on the Google Chrome JavaScript Engine (V8 Engine). It is an open-source, cross-platform runtime environment for creating server-side or back-end and networking applications. It is also able to run a JavaScript library and framework. The server-side can create complex web page content before the page is presented to the user's web browser. The reason Node.js is used in this system is that to allow the developer to install the npm package which provides multiple libraries and frameworks. Then, the developer may use a JavaScript library and web framework for the system such as ReactJS and Next.js. Thus, the developer used this Node.js as a back-end of the system that acts as the runtime environment or server of the system.

7.3.2 Hardware

Hardware is needed in order to develop and build a system. Without the hardware, this project could not achieve its objective. Thus, to complete this project, the developer uses a personal workstation which is a laptop to build the system. The developer will use this laptop to do all the tasks related to this project including designing and implementing the system. Below is the laptop specification that is used by the developer to develop the system.

Table 7.1 Laptop Specification

Model	Nitro AN515-52
Processor	Intel(R) Core™ i5-8300H CPU @ 2.30GHz
RAM Memory	12GB
Hard Drive	475GB (SSD) + 931GB(HDD)
Graphic Card	NVIDIA GeForce GTX 1050
Display Resolution	1920 x 1080 pixels
Operating System	Windows 10 Home 64-bit
Battery Capacity	3220mAh

According to the Table 7.1 above, the developer uses a laptop model Nitro AN515-52. The processor used is Intel(R) Core™ i5-8300H CPU which the speed of microprocessors can reach to 2.30GHz. The Random-Access Memory (RAM) installed in the laptop is 12GB which is enough to build a system smoothly. The laptop uses two hard drive which is 475GB for Solid-State Drive (SSD) and 931GB for Hard Disk Drive (HDD) which is enough to store the system file. The graphic card use is NVIDIA GeForce GTX 1050 and the display of the laptop is 1920 x 1080 pixels. Thus, the laptop should be comfortable to use. The operating system installed is Windows 10 and its battery capacity is 3220mAh which can last at least 4 hours.

7.4 System Interface

7.4.1 Homepage Interface

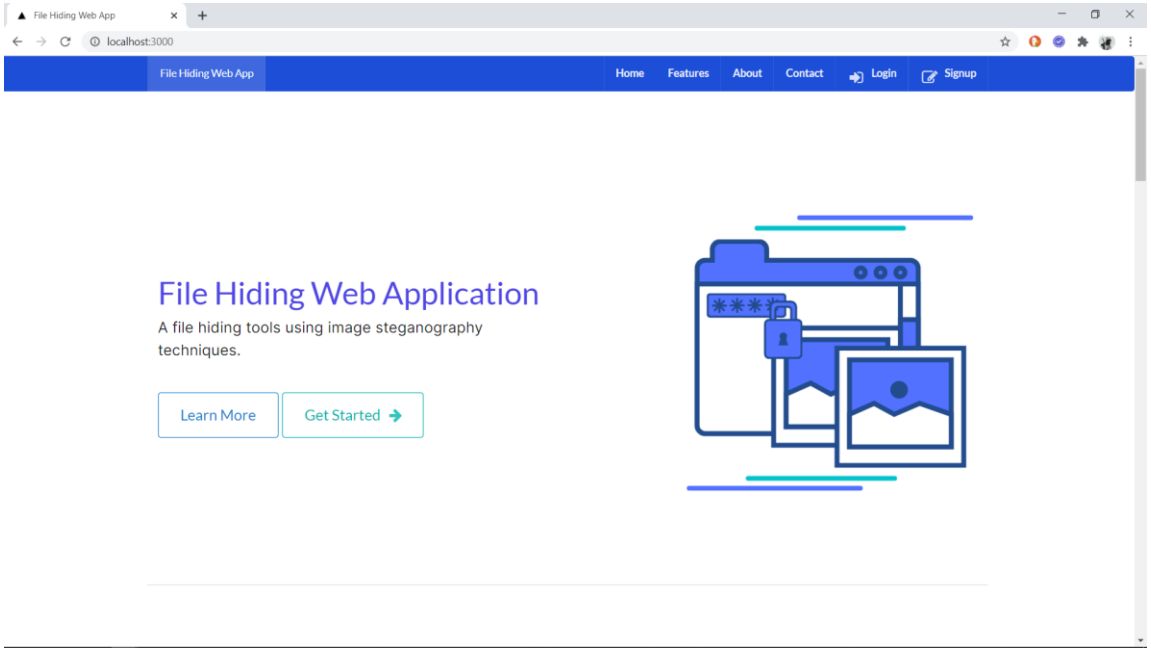


Figure 7.7 Homepage Interface

Figure 7.7 above shows the homepage interface of this system. This homepage provides a menu or navigation bar for their header. This header will be presented on each page of the website. The menu consists of ‘Home’, ‘Features’, ‘About’, ‘Contact’, ‘Login’, and ‘Sign Up’. Users will go to the login page if they click the ‘Login’ menu, while for the ‘Sign Up’ menu user will go to the sign-up page. If users click the ‘About’ menu, they will go to the about page. For the menu ‘Features’ and ‘Contact’, the user will automatically scroll down to the features or contact section whenever they click the menu. Then, this homepage also provides a banner that presents the title of the website. If users click the button ‘Learn More’, they will scroll down to the features section. While if the user clicks the button ‘Get Started’, they will go to the sign-up page.

7.4.2 About Interface

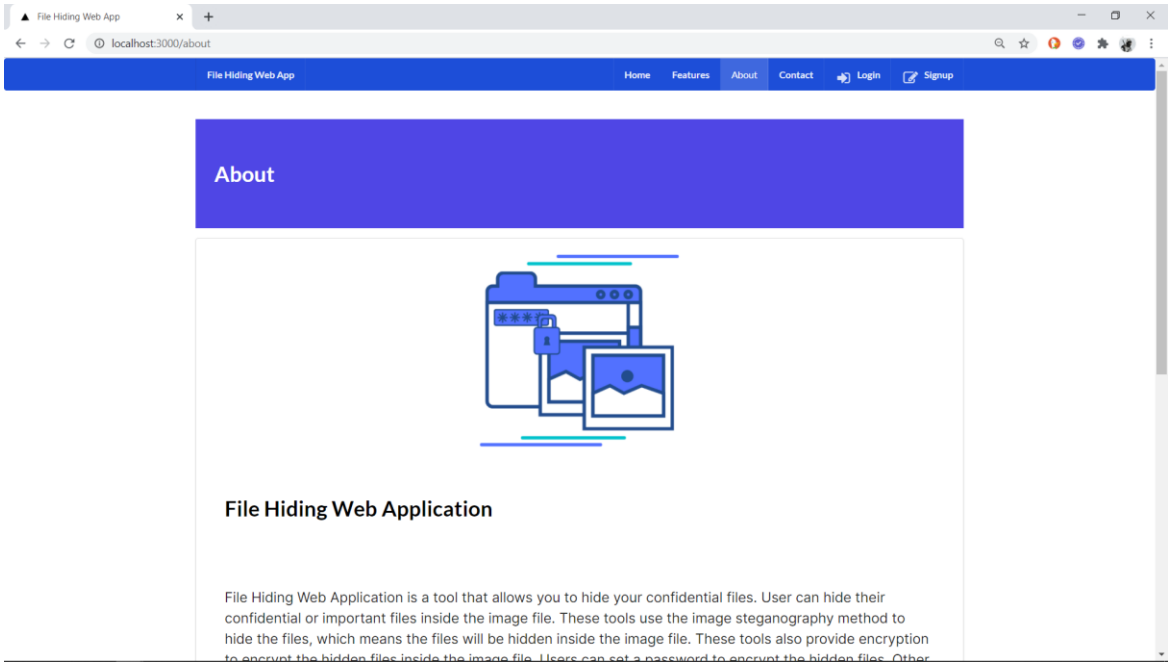


Figure 7.8 About Interface

Figure 7.8 shows the about interface. This page will be displayed if the user clicks the 'About' menu. This about page provides an explanation about this web application. Then, this page also presents the features and services they provide to the users.

7.4.3 Sign-up Interface

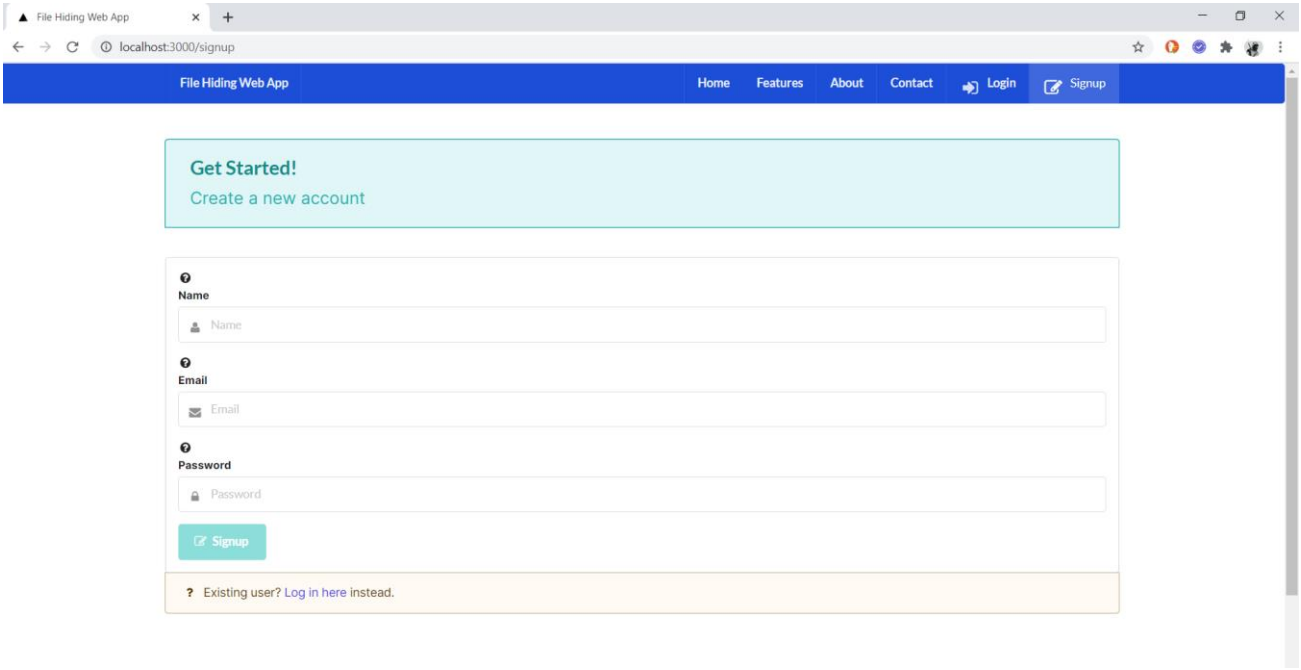


Figure 7.9 Sign-up Interface

Figure 7.9 above shows the sign-up interface for this system. This page is shown when a user clicks on the 'Signup' menu. This sign-up page allows the user to register into this system and enables them to use the feature of this system. Based on this figure, this sign-up page provides three information that needs to be filled in by the users which are the name, email, and password. Then, if all the information that has been filled in is valid, a user should successfully be registered into the system after they click the 'Signup' button and they will directly go to the account page. Other than that, if users already registered to the system, they can click the 'Log in here' below the registration form and they will directly go to the login page.

7.4.4 Login Interface

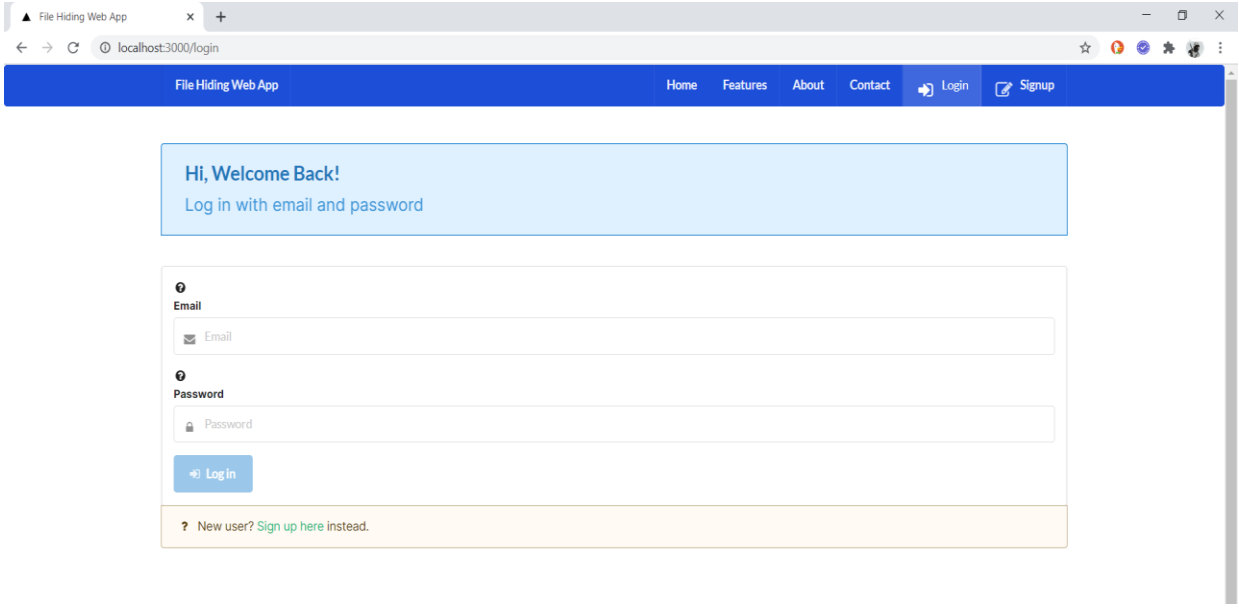


Figure 7.10 Login Interface

Figure 7.10 above presented the login page interface for this system. This page is shown when a user clicks on the 'Login' menu. This login page provides two information that needs to be filled in which are email and password. Both users, which is normal users and administrators, need to fill in the email and password that have been registered to access the features of this system. Then, if the email and password are valid, the users will directly go to the account page after they click the 'Login' button. However, if users did not register to login into the system, they should go to the sign-up page by clicking the 'Sign up here' which is located below the login form.

7.4.5 Login Validation Error Interface

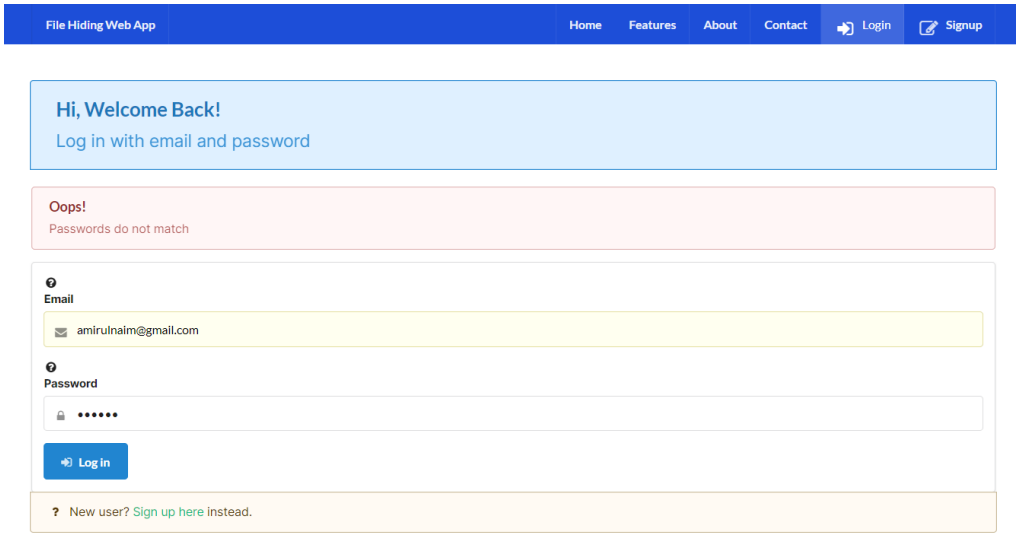


Figure 7.11 Login Validation Error

Figure 7.11 above shows the login validation error interface for this system. Based on this figure, the validation error message will occur if users enter the wrong password or email. If users enter the wrong password or wrong email, the system will show the error message. This validation error message has also been implemented on the other pages that contain a form section.

7.4.6 User Account Interface

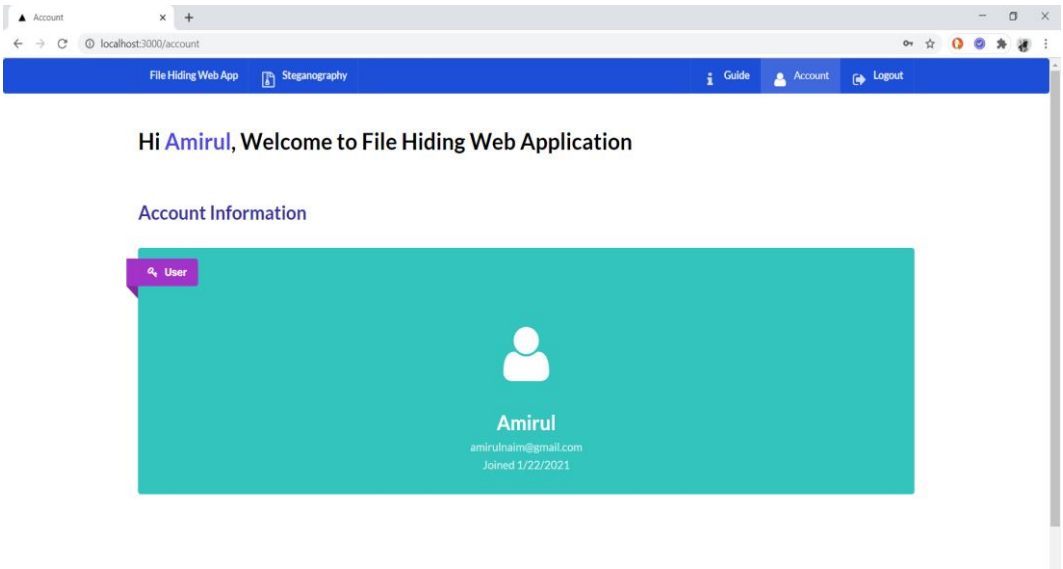


Figure 7.12 User Account Interface

Figure 7.12 above shows the normal user account page interface. This page will be displayed when a normal user successfully logged in to the system. Since this page is for normal users, they only can use the main feature which is Steganography tools. On this account page, the system provides a banner that

displays a user name, email and joins date. At the top left of the banner, the user's role is shown. Thus, for a normal user, the display of the role is 'User'. Other than that, if users click the 'Steganography' menu, they will go to the steganography page. And for the 'Logout' menu, if they click it, users will end their session and directly go to the login page.

7.4.7 Steganography Hiding Files Interface

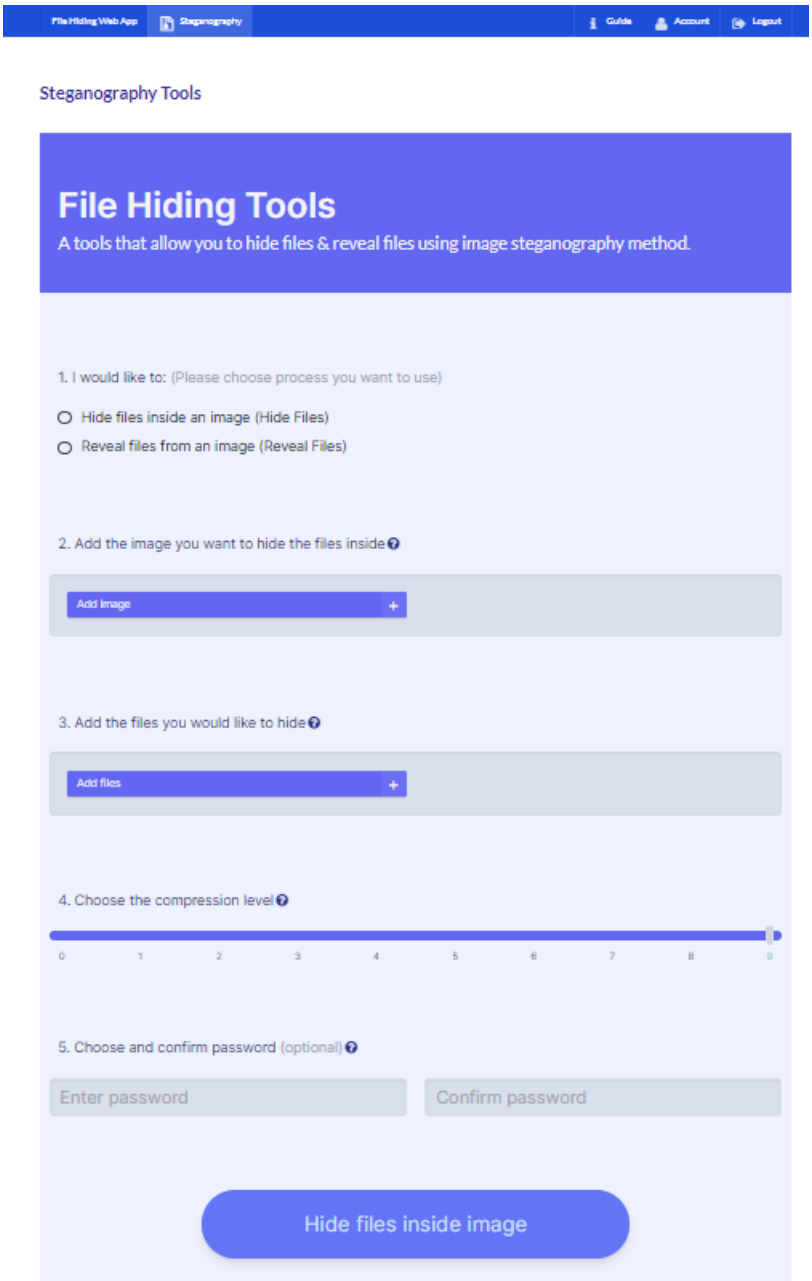


Figure 7.13 Hiding Files Interface

Figure 7.13 above presented the steganography hiding files page interface. This page is shown when users click the 'Steganography' menu. The system allows normal users and administrators to use

this feature. This page provides the main function of this system which is to hide and reveal files inside the image using image steganography techniques. To hide the files inside the image, users must click a radio button that is provided in question one which is the 'hide files inside an image'. After click it, the system will provide a form to hide a file inside the image that needs to be filled by the users. Based on Figure 7.13, the page design provides 'Add image' button to add the image that user wants to hide the files inside. Then, users must click the 'Add files' button to add the files that they want to hide and choose the compression level to compress the files. The system also provides the user to set the password to encrypt the files. Then, to proceed with the hiding process, 'Hide files inside image' button is provided. After that, a button to download the image will be available and the user needs to click the button to download and store the image files that contain hidden files into the user's devices or local storage.

7.4.8 Steganography Revealing Files Interface

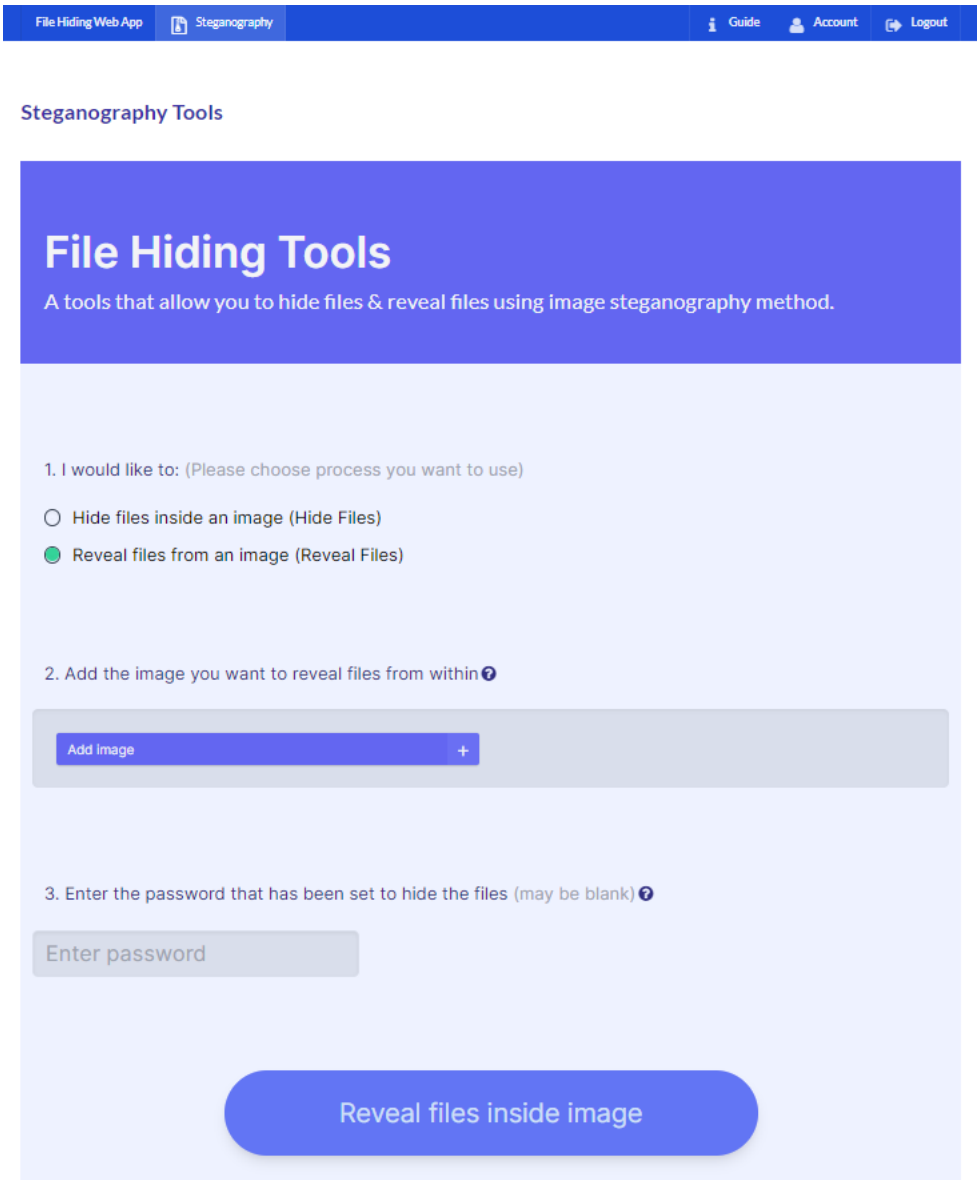


Figure 7.14 Revealing Files Interface

Figure 7.14 above presented the steganography revealing files page interface. This page interface is also displayed on the steganography page. The form that needs to be filled is difference from the steganography hide files interface. To run the revealing files process, users must click a radio button that is provided in question one which is the ‘Reveal files from an image’. After users click it, the system will provide a form that is different from hiding a file inside the image form that needs to be filled by the users. Based on Figure 7.14, the system provided only two forms that need to be filled by the users. First, it provides ‘Add image’ button for the user to add the image that they want to reveal the files from within. Second, users just need to enter the same password that has been set or used to hide the files. After that, proceed with the reveal process by clicking the ‘Reveal files inside image’ button. Then, button download will be available and user must click the download button to download and store the hidden or revealed files into the user's devices or local storage.

7.4.9 Guide Interface

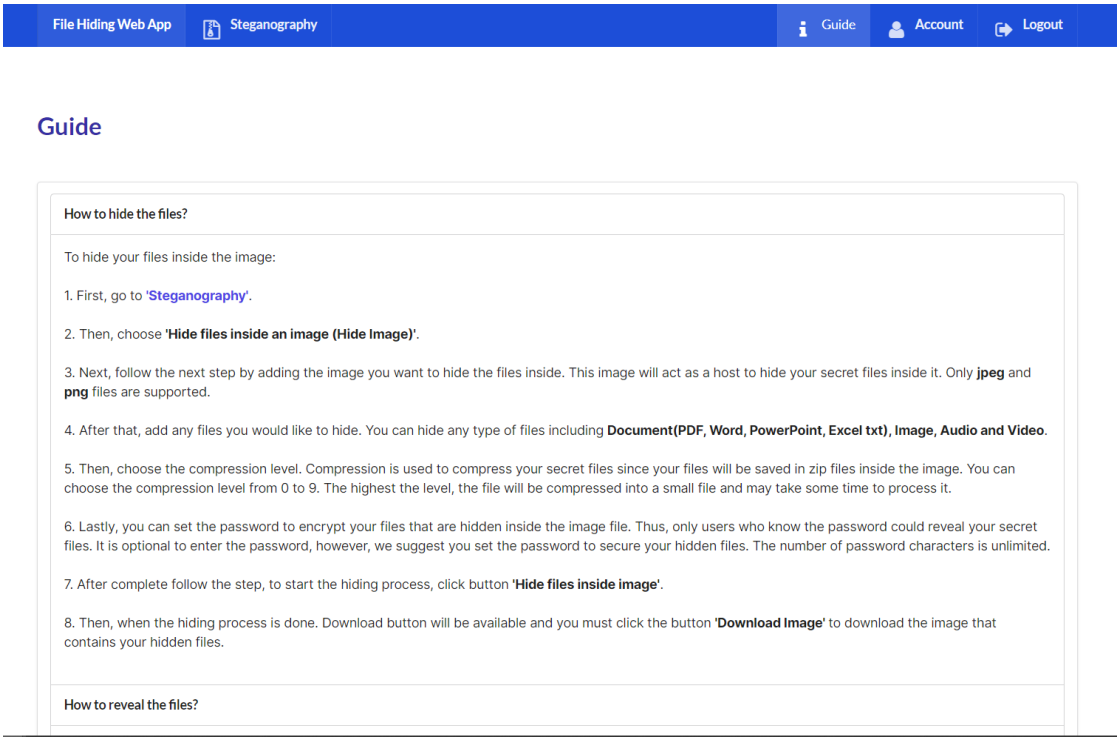


Figure 7.15 Guide Interface

Figure 7.15 shows the guide page interface of this system. This page will be shown when users click the ‘Guide’ menu. This guide page gives information to the users about how to use the main feature of this system. Thus, this page will guide and show the step to the user on how to hide their confidential files inside the image. Other than that, this page also shows the step to the users on how to reveal their confidential files from the image file.

7.4.10 Admin Account Interface

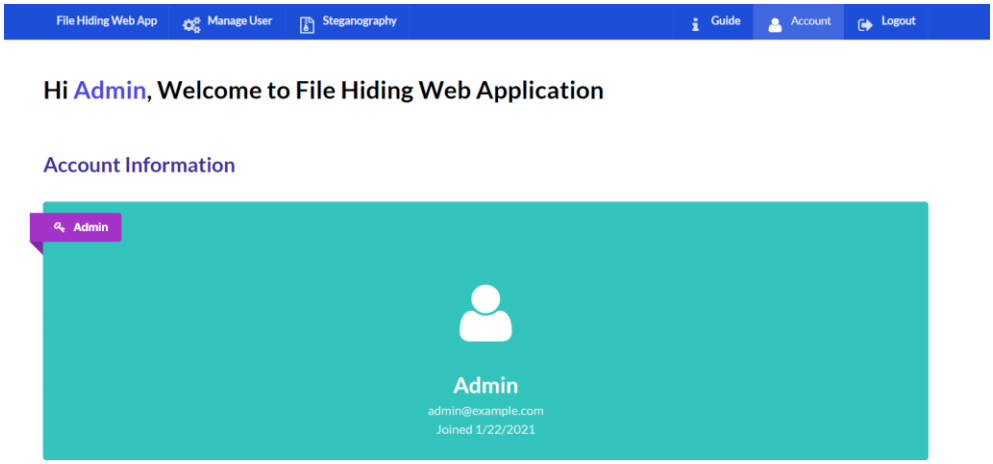


Figure 7.16 Admin Account Interface

Figure 7.16 above shows the administrator account page interface for this system. This page is shown when an admin successfully logged in to the system. Since this page is for administrators, an additional feature is provided in the header which is 'Manage User' that makes it different from normal users. On this interface, the system provides a banner that displays the administrator name, email and joins date. At the top left of the banner, the user's role is shown. Since this account page is for administrators, the display of the role is 'Admin'. Other than that, if users click the 'Manage User' menu, they will proceed to the manage user page. Then, for the 'Steganography' menu, they will proceed to the steganography page. And for the 'Logout' menu, if they click it, the admin will end their session and directly go to the login page.

7.4.11 Manage User Interface

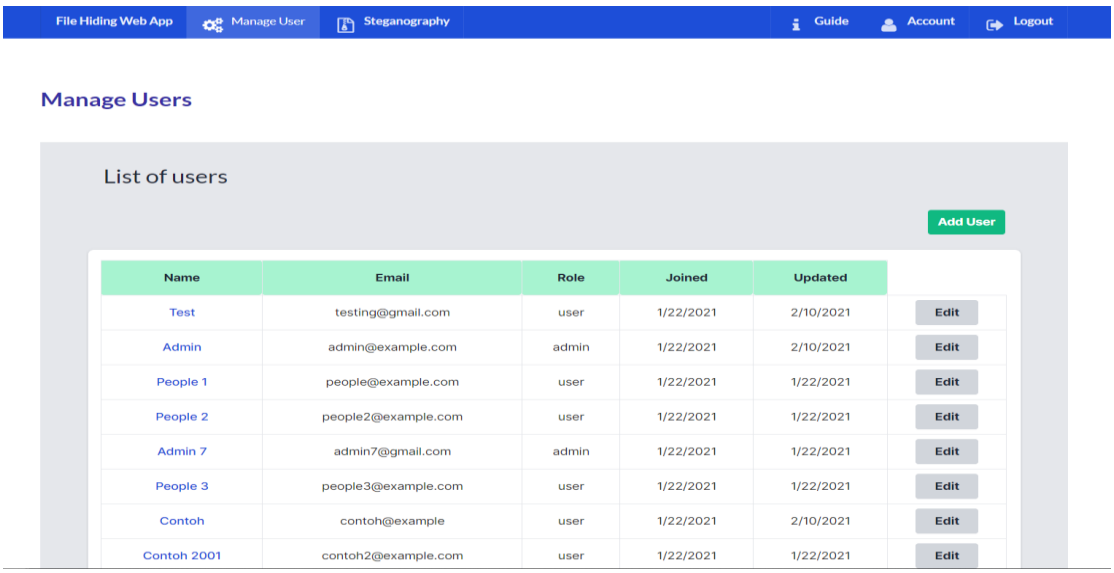


Figure 7.17 Manage User Interface

Figure 7.17 above shows the manage user page interface for this system. This page is shown when users with admin role click the 'Manage User' menu. Thus, this feature only available for administrators. For this page interface, the system displays a dashboard that provides a list of users that has been registered in the system. Thus, the details of registered users such as name, email, role, joined date and updated date is displayed on this page. Then, the admin can edit the user's information by clicking the 'Edit' button and they will proceed to the edit user information page. Other than that, an admin also can add a new user by clicking the 'Add User' and directly proceed to the create new user page.

7.4.12 Add New User Interface

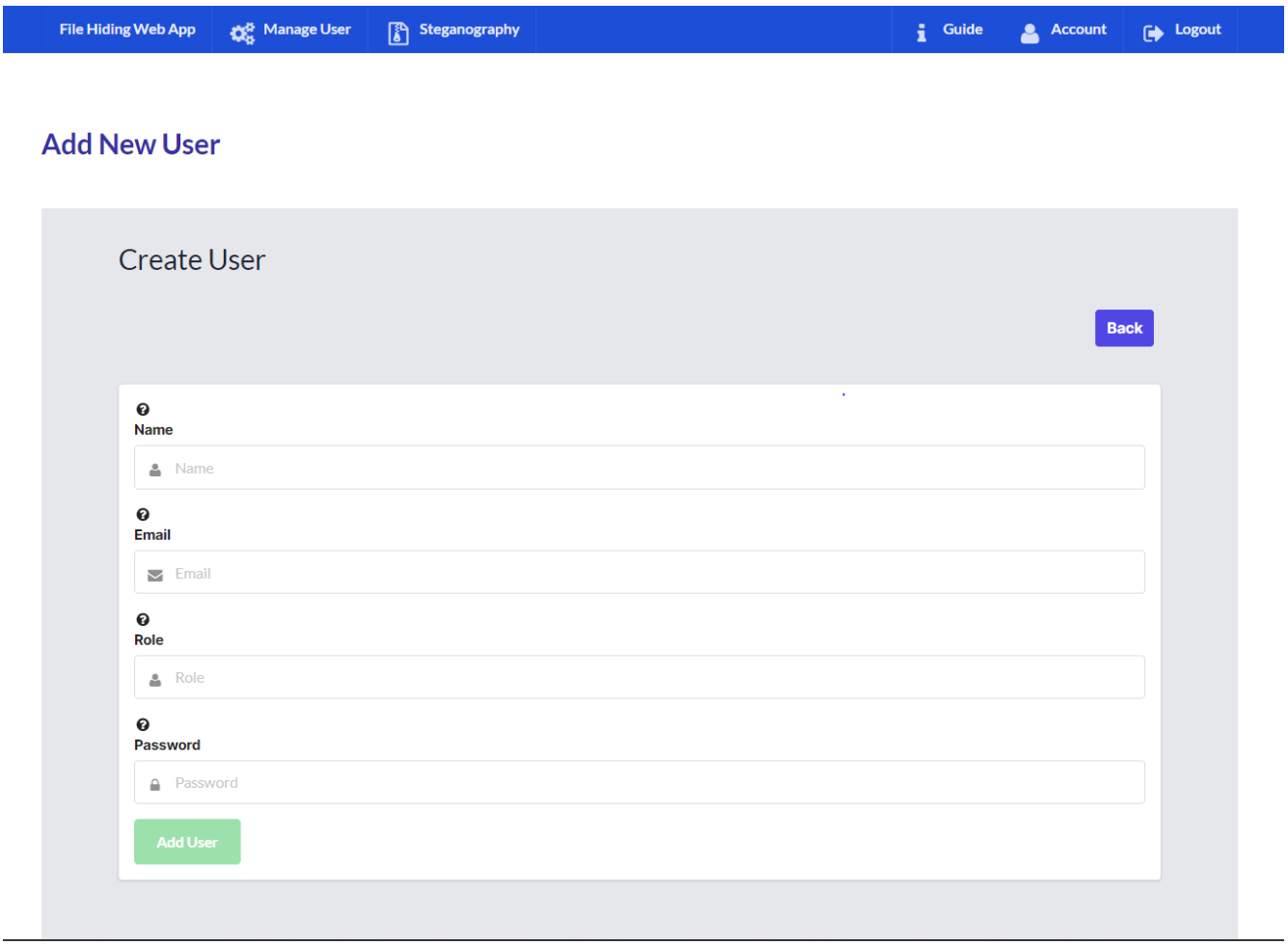


Figure 7.18 Add New User Interface

Figure 7.18 above shows the add new user page interface for this system. This page will be displayed when administrators click the 'Add User' button on the manage user page. For this page interface, the system displays a form that needs to be filled in by the admin to add a new user to the system. This page provides four information that needs to be filled in by the admin which are name, email, role, and password. Then, if all the information that has been filled in is valid, a new user should successfully be registered into the system after the admin clicks the 'Add User' button. Then, the admin

will directly go to the manage user page back. For the 'Back' button located at the top right of the page, an admin will go back to the manage user page if they click the button.

7.4.13 Edit User Information Interface

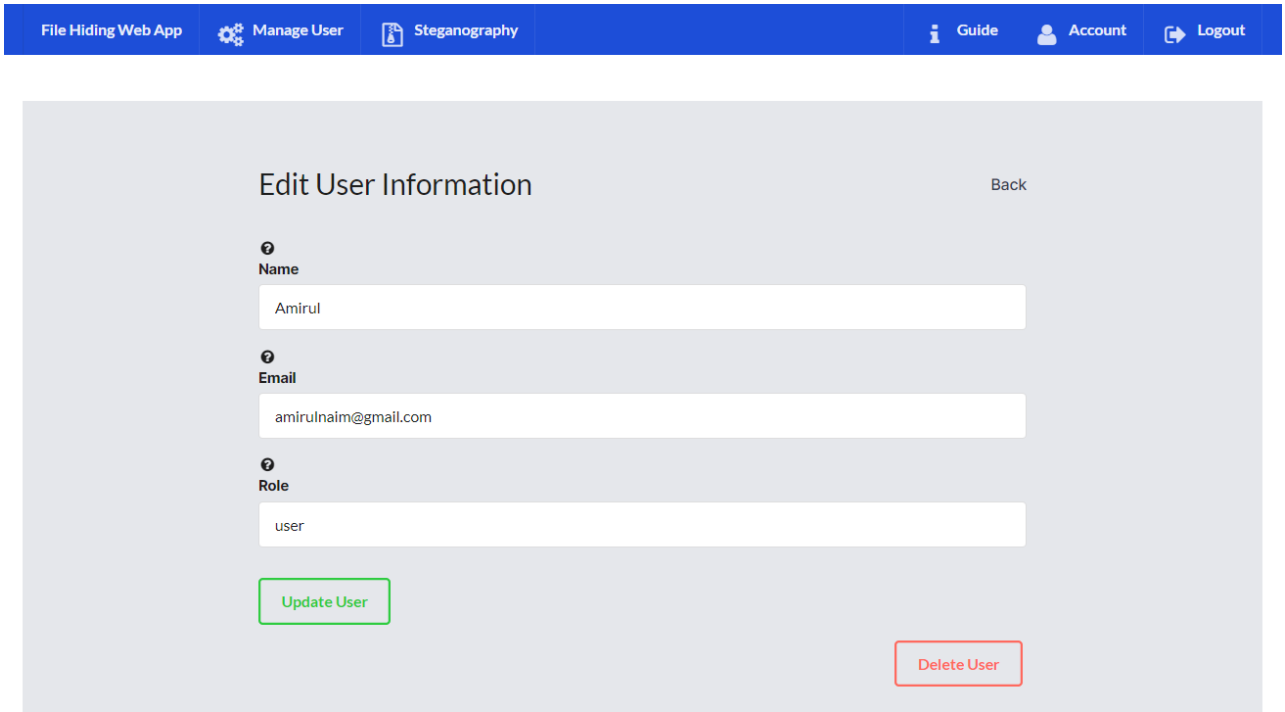


Figure 7.19 Edit User Information Interface

Figure 7.19 above shows the edit user information page interface for this system. This page will be displayed when administrators click the 'Edit' button on the manage user page. For this page interface, the system displays user information that needs to be edited by the admin. This page provides three information that able to be edit by the administrator which are name, email, and role. Then, if some information has been edited, the admin can successfully update the user information by clicking the 'Update User' button and after that admin will directly go to the manage user page back. To delete the user from the system, an admin must click the 'Delete User' button. And for the 'Back' link located at the top right of the page, an admin will go back to the manage user page if they click the button.

7.5 Significant Function

The reason why users should use this File Hiding Web Application is because of the implementation of the security element on the system. Users may use this system to hide their confidential files such as financial information, health information, and other important information from unauthorized users. Therefore, this system provides users to secure their confidential files by allowing them to hide their important files inside the image file using image steganography techniques. This system also allows users to reveal the hidden files inside the image files. Other than that, the system allows the user to set the password to encrypt their hidden files. Encryption has also been used to hash the user password who are registered into the system. Thus, the system implements the steganography and cryptography method for their security element. Below is the algorithm that has been implemented to secure user confidential files.

7.5.1 Encrypting Algorithm

workers > Hide.worker.js > encryptZip

```
import JSZip from "jszip";

//Hiding files inside image function
const encryptZip = async (zipUint, imageUint, password) => {
    const passwordUint = new TextEncoder().encode(password);
    const baseKey = await crypto.subtle.importKey(
        "raw",
        passwordUint,
        "PBKDF2",
        false,
        ["deriveBits", "deriveKey"]
    );

    //hash the derivation key variables
    const cryptoKey = await crypto.subtle.deriveKey(
        {
            name: "PBKDF2",
            salt: imageUint.slice(0, 16),
            iterations: 10000,
            hash: "SHA-256",
        },
        baseKey,
        {
            name: "AES-CTR",
            length: 128,
        },
        false,
        ["encrypt"]
    );

    //encrypt the key/password using AES-CTR
    const zipEncrypted = await crypto.subtle.encrypt(
        {
            name: "AES-CTR",
            counter: new Uint8Array(16),
            length: 128,
        },
        cryptoKey,
        zipUint.buffer
    );
    return new Uint8Array(zipEncrypted);
};
```

Figure 7.20 Encrypting Algorithm

Figure 7.20 shows the encrypting algorithm to encrypt the user's hidden files. Based on this figure, the system uses PBKDF2 and SHA-256 to encrypt the password that user has entered to secure their hidden files. The password that the user entered is imported to create a derivation key. Then the

derivation key is hashed using SHA-256 and a salt. After being hashed by SHA-256, the new key is given and then will be derived again using the PBKDF2 algorithm. Finally, the hidden files will be encrypted using a new encryption key which is obtained by the derivation process. Thus, the system will encrypt the data or the hidden files using symmetric AES-CTR algorithm.

7.5.2 Hiding the Files Algorithm

workers > JS Hide.worker.js > ...

```
//accept input/data from user
onmessage = async ({
    data: {
        image: [{ contents, type }],
        files,
        compression,
        password,
    },
}) => {
    //function to create a zip file
    const zip = new JSZip();
    files.forEach((file) => {
        const { name, contents, date } = file;
        zip.file(name, contents, {
            date,
        });
    });

    const imageUint = new Uint8Array(contents);

    //compression level function
    const zipUint = await zip.generateAsync(
        {
            type: "uint8array",
            compression: compression === 0 ? "STORE" : "DEFLATE",
            compressionOptions: {
                level: compression,
            },
        },
        ({ percent }) => {
            postMessage({ progress: percent });
        }
    );

    const zipEncryptedUint = await encryptZip(zipUint, imageUint, password);
    const resultUint = new Uint8Array([...imageUint, ...zipEncryptedUint]);

    //a blob which contains image file is created
    postMessage({
        result: new Blob([resultUint], { type }),
    });
    close();
};

export default encryptZip;
```

Figure 7.21 Hiding the Files Algorithm

Figure 7.21 shows the algorithm for hiding the files. Based on this figure, the system implements the image steganography method since the system required users to add an image to hide their confidential files inside it. The system requires the user to input the image file to act as a host, files that they want to hide, compression level and a password to encrypt their hidden files. This figure shows that the system will

read all the files as an array buffer. The image will be converted into a Uint8Array (an array of 8-bit unsigned integers). The system will store the user's confidential files inside the zip file. And compression is used to compressed the user's hidden files. After all the hiding process is done, the user's confidential files will be hidden inside the image. Then, the image is converted to a Blob and a URL is created to allow users to download the resulting image.

7.5.3 Decrypting Algorithm

```
workers > JS Find.worker.js > onmessage

//Revealing files inside image function
const decryptZip = async (zipUint, imageUint, password) => {
    const passwordUint = new TextEncoder().encode(password);
    const baseKey = await crypto.subtle.importKey(
        "raw",
        passwordUint,
        {
            name: "PBKDF2",
        },
        false,
        ["deriveKey"]
    );

    //hash the derivation key variables
    const cryptoKey = await crypto.subtle.deriveKey(
        {
            name: "PBKDF2",
            salt: imageUint.slice(0, 16),
            iterations: 10000,
            hash: "SHA-256",
        },
        baseKey,
        {
            name: "AES-CTR",
            length: 128,
        },
        false,
        ["decrypt"]
    );

    //decrypt the AES-CTR
    const zipDecrypted = await crypto.subtle.decrypt(
        {
            name: "AES-CTR",
            counter: new Uint8Array(16),
            length: 128,
        },
        cryptoKey,
        zipUint.buffer
    );
    return new Uint8Array(zipDecrypted);
};
```

Figure 7.22 Decrypting Algorithm

Figure 7.22 shows the decrypting algorithm to decrypt the user's hidden files. Based on this figure, the decryption of the hidden files uses the same technique as is used for encryption. The system must use the PBKDF2 and SHA-256 to decrypt the password that user has set to encrypt their hidden files. However, the derivation key or the password is used to derive a decryption key. Finally, the hidden files will be decrypted using a decryption key which is obtained by the derivation process. Thus, the system will decrypt the data or the hidden files using symmetric AES-CTR algorithm.

7.5.4 Revealing the Files Algorithm

```
workers > JS Find.worker.js > ...
//accept input/data from user
onmessage = async ({
    data: {
        image: [{ contents, type }],
        password,
    },
}) => {
    //function to read the image file to reveal the hidden files
    const imageUint = new Uint8Array(contents);

    const marker = {
        "image/png": [174, 66, 96, 130],
        "image/jpeg": [255, 217],
        "image/gif": [59],
    }[type];

    const indexOfZip =
        imageUint.findIndex(
            (_, index) =>
                imageUint.slice(index, index + marker.length).toString() ===
                marker.toString()
        ) + marker.length;

    const zipEncryptedUint = imageUint.slice(indexOfZip);
    const zipUint = await decryptZip(zipEncryptedUint, imageUint, password);

    //a blob which contains hidden files is created
    postMessage({
        result: new Blob([zipUint], { type: "application/zip" }),
    });
    close();
};
```

Figure 7.23 Revealing the Files Algorithm

Figure 7.23 shows the algorithm for revealing the files. Based on this figure, revealing the files is a similar process to hiding but in reverse. The hidden files will be read and will be converted to a Uint8Array. The EOF marker is used to allow the files to follow it. If there is no content matching the EOF marker, the image does not contain any hidden files. After all the revealing process is done, the user's confidential files will be revealed. Then, the zip file which contains hidden files is converted to a Blob and allows users to download the zip file that contains all the user's hidden files.

7.5.5 Hashed the User Password

```
27        // 3) --if not, hash their password
28        const hash = await bcrypt.hash(password, 10);
29        // 4) Create user
30        const newUser = await new User({
31            name,
32            email,
33            password: hash
34        });
35        newUser.save();
36
```

Figure 7.24 Hashed User Password

Figure 7.24 shows the code which hashed the user password. Based on this figure, the password of the user who registered into the system will be hashed using bcrypt. Bcrypt is an efficient hash function based on a Blowfish symmetric block crypto algorithm. This hash is important to avoid unauthorized users including the admin to view the user's password. Thus, all the user's password that has been stored in the database server will be encrypted and will be view in hash code. This means that the admin or the developer will not able to view the user's actual password.

7.6 Conclusion

In conclusion, the implementation phase provides a specific overview of the development and implementation of File Hiding Web Application. This phase presents how the system will be developed. These including the use of hardware and software such as application tools and programming language to execute the system that needs to be developed. This phase also provides a detailed component of the interface design, functionality, and security element used in this system. Thus, the implementation phase is one of the important phases since all the resources, equipment, design, and tools being specified in this phase. As a result, this phase could ease the developer to develop the system since all the requirement has been described in a specific way. Thus, by referring to all the requirements needed, the developer could achieve the objective of this project.

8 Testing

8.1 Introduction

In this chapter, all the component and element of the system that has been developed will be tested by the users. Testing is a systematic procedure focused on identifying bugs in a software system. The purpose of this testing is to evaluate how the system works either it is working properly or not. Other than that, testing is important since it is to evaluate the system if there is some bug or error in it.

This chapter will implement a series of testing to make sure that the system that we will develop working properly. One of the testing that we will implement is unit testing. In unit testing, the developer will evaluate and test the functionality of an individual component of a software. Other than that, integration testing also will be implemented in order to evaluate possible errors or bugs in the interaction between integrated units. System testing such as functionality and non-functionality testing also be implemented in this chapter. Then, acceptance testing including alpha and beta testing is implemented in this chapter to ensure that our system ready to deploy or used. Thus, this phase may involve the user since the beta testing, requires a user to give feedback or comment or any suggestion during the testing. This phase will determine whether actual result fits the requirement of the system and to ensure that the system meets their objectives.

8.2 Unit Testing

Unit testing is a method of software testing where individual software units or components are evaluated. This testing is to validate that each of the component or unit in the system performs as expected. This unit testing was implemented during the development of the system. Unit testing is important because the developer may find an error and bugs which help them to fix any issue occur on the code. Below are the individual units or components that have been tested.

Table 8.1 Unit Testing

Unit/Function	Input	Output	Expected Error/Error Handling
Login Page Process of user authentication by entering valid email and password.	Email and Password (string and must at least 6 characters). e.g.- Email:	Error message “Password do not match” will be displayed to inform the password do not match.	An error message will be displayed if user enter wrong username and password.

	testing@gmail.com Password: t123		
	Email and Password (string and must at least 6 characters). e.g.- Email: testing@gmail.com Password: test123	Users will be directed to the account page of the application.	
Signup Page Process of user registration by fill a valid form such as name, email, and password.	Name (3-10 characters), Email (not been registered yet), and Password (at least 6 characters). e.g.- Name: Ts Email: testing2@gmail.com Password: testing123	Error message "Name must be 3-10 characters long" will be displayed to inform the name is invalid.	An error message will be displayed if user enter invalid name, email, and password.
	Name (3-10 characters), Email (not been registered yet), and Password (at least 6 characters). e.g.- Name: Test Email: testing@gmail.com (has registered into the system) Password: testing123	Error message "User already exist with email "testing@gmail.com" will be displayed to inform the email has been registered into the system.	
	Name (3-10 characters), Email (not been registered yet), and Password (at least 6 characters).	Error message "Password must be at least 6 characters" will be displayed to inform the password are invalid and less than 6	

	e.g.- Name: Test Email: testing2@gmail.com Password: 123	characters.	
	Name (3-10 characters), Email (not been registered yet), and Password (at least 6 characters). e.g.- Name: Test Email: testing2@gmail.com Password: testing123	Users successfully registered into the system and will be directed to the account page of the application.	
Steganography Page (Hiding Files) Process of hiding a file inside an image by following the valid step to begin the process.	Image File (jpeg, png), Secret Files (any type of file), Compression Level (0-9), Password (unlimited characters). e.g.- Image File: empty Secret File: empty Compression Level: 9 Password: empty	Users cannot begin the hiding process and download the image file because the user did not upload the image file and the secret file they want to hide. Thus, the system unable to start the hiding process.	A popup message will be displayed during revealing the hidden files if the user enters invalid image file.
	Image File (jpeg, png), Secret Files (any type of file), Compression Level (0-9), Password (unlimited characters). e.g.- Image File: image.gif Secret File: files.pdf Compression Level: 9	Users successfully begin the hiding process and able to download the image file that contains secret files, but cannot reveal it since the system did not support other image file formats except jpeg and png.	

	Password: 12345 or [empty]	Thus, error message “filename.zip, the archive is either is unknown format or damaged” will be displayed to inform the file is not valid.	
	Image File (jpeg, png), Secret Files (any type of file), Compression Level (0-9), Password (unlimited characters). e.g.- Image File: image.jpeg or image.png Secret File: files.pdf Compression Level: 9 Password: 12345 or empty	Users successfully begins the hiding process and able to download the image file that contains secret files and able to reveal the hidden files inside the image.	
Steganography Page (Revealing Files) Process of revealing the hidden files inside an image by following the valid step to begin the process.	Image File (jpeg, png) and Password (same as the password that has been set to hide the files or may be blank). e.g.- Image File: empty Password: empty	Users cannot begin the revealing process and download the image file because the user did not upload the image file which contains hidden files. Thus, the system unable to start the revealing process.	A popup message will be displayed during revealing the hidden files if the user enters invalid image file.
	Image File (jpeg, png) and Password (same as the password that has been set to hide the files or may be blank).	Users successfully begin the revealing process and able to download the image file that contains secret files, but cannot reveal it since the system	

	e.g.- Image File: image.gif Password: empty	did not support other image file formats except jpeg and png. Thus, error message “filename.zip, the archive is either is unknown format or damaged” will be displayed to inform the file is not valid.	
	Image File (jpeg, png) and Password (same as the password that has been set to hide the files or may be blank). e.g.- Image File: image.jpeg or image.png Password: 12345 or empty	Users successfully begins the revealing process and able to download the image file that contains secret files and able to reveal the hidden files inside the image.	
Edit User Information Page (Admin) Process of updating user information by editing valid name, email and role.	Name (3-10 characters), Email (email format) and Role (must be ‘admin’ or ‘user’). e.g.- Name: Ts Email: testing@gmail.com Role: user	Error message “Name must be 3-10 characters long” will be displayed to inform the name is invalid.	An error message will be displayed if the admin enters the invalid name, email, and role.
	Name (3-10 characters), Email (email format) and Role (must be ‘admin’ or ‘user’).	Error message “Email must be valid” will be displayed to inform the email is invalid.	

	e.g.- Name: Test Email: testing Role: user		
	Name (3-10 characters), Email (email format) and Role (must be ‘admin’ or ‘user’). e.g.- Name: Test Email: testing@gmail.com Role: userss	Error message “Role is required [admin, user]” will be displayed to inform the role that admin filled is invalid.	
	Name (3-10 characters), Email (email format) and Role (must be ‘admin’ or ‘user’). e.g.- Name: Test Email: testing@gmail.com Role: user	Admin successfully updated user information and will be directed back to the manage user page.	
Add New User Page (Admin) Process of creating new user into the system by fill a valid form such as name, email, role, and password.	Name (3-10 characters), Email (email format and not been registered yet), Role (must be ‘admin’ or ‘user’), and Password (at least 6 characters). e.g.- Name: Te Email: testing3@gmail.com Role: user Password: testing123	Error message “Name must be 3-10 characters long” will be displayed to inform that the name is invalid.	An error message will be displayed if the admin enters the invalid name, email, role, and password.

	Name (3-10 characters), Email (email format and not been registered yet), Role (must be ‘admin’ or ‘user’), and Password (at least 6 characters). e.g.- Name: Test 3 Email: testing@gmail.com (has registered into the system) Role: user Password: testing123	Error message “User already exists with email testing@gmail.com” will be displayed to inform that the email has been registered into the system.	
	Name (3-10 characters), Email (email format and not been registered yet), Role (must be ‘admin’ or ‘user’), and Password (at least 6 characters). e.g.- Name: Test 3 Email: testing3@gmail.com Role: usersss Password: testing123	Error message “Role must be ["user" or "admin"]” will be displayed to inform that the role is invalid.	
	Name (3-10 characters), Email (email format and not been registered yet), Role (must be ‘admin’ or ‘user’), and Password (at least 6 characters). e.g.- Name: Test 3 Email: testing3@gmail.com	Error message “Password must be at least 6 characters” will be displayed to inform that the password characters are invalid and less than 6 characters.	

	Role: user Password: tes12		
	Name (3-10 characters), Email (email format and not been registered yet), Role (must be 'admin' or 'user'), and Password (at least 6 characters). e.g.- Name: Test 3 Email: testing3@gmail.com Role: user Password: testing123	New users successfully registered into the system and the admin will be directed to the manage user page back.	

Table 8.1 shows the unit testing that has been tested by the developers. Based on the table, each unit or component that requires a user to input the data has been tested. The unit includes are the login page, signup page, steganography page for hiding files, steganography page for revealing files, edit user's information page, and add new user page. The table provides input and expected output for each unit that has been tested. Other than that, the table also provide expected error or error handling that may occur for each unit that has been tested. This unit testing will help the developers to find any error that may occur in each unit and may ease them to troubleshoot the error and improvise the system.

8.3 Integration Testing

Integration testing is identified as a method of testing where the software modules are logically combined and evaluated as a group. This testing aims to identify any faults or errors in the interaction between each component or module when they are integrated. Thus, this integration testing will ensure the system could integrate each component on the system work properly. Below is the combination of the individual units available in the system that has been tested.

Table 8.2 Integration Testing

Module	Input	Output	Expected Error/Error Handling
User Authentication A process of user login by entering valid	Correct email and password (string and at least 6 characters).	User will be directed to the account page of the application and receive a	Users will receive an error message if they enter the wrong email

username and password. Once successful, user will be directed to the account page and receive welcome message.	e.g.- Email: testing@gmail.com Password: testing123	welcome message.	and password.
	Wrong email or password (string and at least 6 characters). e.g.- Email: testing111@gmail.com (unregistered email) Password: testing1111 (wrong password)	Error message “No user exists with that email” will be displayed to inform that emails are not registered into the system. Error message “Passwords do not match” will be displayed to inform that the password is incorrect.	
User Registration A process of user registration by filling the valid name, email, and password. Once successful, user will be registered into the system and directed to the account page and receive welcome message.	Correct name (3-10 characters), email, and password (string and at least 6 characters). e.g.- Name: Test Email: testing12@gmail.com Password: testing123	Users will be registered into the system and will automatically direct to the account page of the application and receive a welcome message.	Users will receive an error message if they enter an invalid name, email, and password.
	Invalid name (3-10 characters), email, or password (string and at least 6 characters). e.g.- Name: Te Email:	Error message “Name must be 3-10 characters long” will be displayed to inform that the name entered is invalid. Error message “User already exist with email	

	testing@gmail.com (registered email) Password: test1	testing@gmail.com" will be displayed to inform that emails already registered into the system. Error message "Password must be at least 6 characters" will be displayed to inform that the password entered is invalid.	
Account Page For normal user, check the interface link between the account page and steganography page. For administrator, check the interface link between the account page with manage user and steganography page.	From account page click the 'Steganography' menu.	Normal user and admin will be directed to the steganography page.	
	From account page click the 'Manage User' menu.	Admin will be directed to the manage user page.	
Steganography Page (Hiding Files) Process of hiding a file inside an image by following the valid step to begin the process. Once the step is valid, users will successfully hide their secret files inside the image and	Valid image file (jpeg, png), secret files (any type of file), compression level (0-9), password (unlimited characters). e.g.- Image File: image.jpeg or image.png Secret File: files.pdf Compression Level: 9	Users will be successfully executing the hiding process and able to download the image file that contains secret files and able to reveal the hidden files inside the image.	A popup message will be displayed during revealing the hidden files if the user enters invalid image file.

able to download the image.	Password: 12345 or empty		
	Invalid image file (jpeg, png), secret files (any type of file), compression level (0-9), password (unlimited characters). e.g.- Image File: image.gif Secret File: files.pdf Compression Level: 9 Password: 12345 or [empty]	Users successfully begin the hiding process and able to download the image file that contains secret files, but cannot reveal it since the system did not support other image file formats except jpeg and png. Thus, error message “filename.zip, the archive is either is unknown format or damaged” will be displayed to inform the file is not valid.	
Steganography Page (Revealing Files) Process of revealing the hidden files inside an image by following the valid step to begin the process. Once the step is valid, users will successfully reveal their secret files inside the image and able to download the secret files.	Valid image file (jpeg, png) and password (same as the password that has been set to hide the files or may be blank). e.g.- Image File: image.jpeg or image.png Password: 12345 or empty	Users successfully begins the revealing process and able to download the image file that contains secret files and able to reveal the hidden files inside the image.	A popup message will be displayed during revealing the hidden files if the user enters invalid image file.
	Invalid image file (jpeg, png) and password (same as the password that has been set to hide	Users successfully begin the revealing process and able to download the image file that contains	

	the files or may be blank). e.g.- Image File: image.gif Password: empty	secret files, but cannot reveal it since the system did not support other image file formats except jpeg and png. Thus, error message "filename.zip, the archive is either is unknown format or damaged" will be displayed to inform the file is not valid.	
Manage User Page (Admin) Check the interface link between the manage user page with add user page and edit page. Once the integration is successful, the admin will direct to the page selected.	From manage user page, click the 'Edit button.	Admin will be directed to the edit user information page.	
	From manage user page, click the 'Add User button.	Admin will be directed to the add new user page.	
Edit User Information Page (Admin) Process of updating user information by editing valid name, email and role. Once the data entered is valid, user information successfully updated and the admin will be	Valid name (3-10 characters), email (email format) and role (must be 'admin' or 'user'). e.g.- Name: Test Email: testing@gmail.com Role: user	Admin successfully updated user information and will be directed back to the manage user page.	An error message will be displayed if the admin enters the invalid name, email, and role.
	Invalid name (3-10	Error message "Name	

directed to the manage user page back.	characters), email (email format) and role (must be ‘admin’ or ‘user’). e.g.- Name: Ts Email: testing@gmail Role: userss	must be 3-10 characters long” will be displayed to inform that the name is invalid. Error message “Email must be valid” will be displayed to inform that the email is invalid. Error message “Role is required [admin, user].” will be displayed to inform that the role is invalid.	
	Admin clicked the ‘Delete User’ button.	Admin successfully delete user from the system and will be directed back to the manage user page.	
Add New User Page (Admin) Process of creating new user into the system by fill a valid form such as name, email, role, and password. Once the data entered is valid, a new user will be added into the system and the admin will be directed to the manage user page back.	Valid name (3-10 characters), email (email format and not been registered yet), role (must be ‘admin’ or ‘user’), and password (at least 6 characters). e.g.- Name: Test 3 Email: testing3@gmail.com Role: user Password: testing123	Admin successfully registered new user into the system and the admin will be directed to the manage user page back.	An error message will be displayed if the admin enters the invalid name, email, role, and password.
	Invalid name (3-10 characters), email (email format and not been registered yet), role (must be ‘admin’ or	Error message “Name must be 3-10 characters long” will be displayed to inform that the name is invalid.	

	'user'), and password (at least 6 characters). e.g.- Name: Te Email: testing3@gmail Role: users Password: tes123	Error message "Email must be valid" will be displayed to inform that the email is not valid. Error message "Role must be ["user" or "admin"]" will be displayed to inform that the role is not valid. Error message "Password must be at least 6 characters" will be displayed to inform that the password is not valid and less than 6 characters.	
Logout Menu Check the interface link between the logout menu that provides on any page on the system and the login page. Once the integration is successful, the users including normal users and admin will end their session and will be direct to the login page.	From any page on the system, click the 'Logout' menu.	Normal user and admin will end their session and will be directed to the login page.	

Table 8.2 shows the integration testing that has been tested by the developers. Based on this table, each main component of the system that integrated with each module has been tested. The main module

includes are the user authentication, user registration, account page, steganography page for hiding files, steganography page for revealing files, manage user page, edit user's information page, add new user page, and logout menu. The table also provides input and expected output for each module that has been tested either it is successfully integrated or not. Then, this table also provides error handling that may occur for each module that has been tested. This integration testing will ensure that no error occurs during the interaction between each module.

8.4 System Testing

System testing is a testing process that evaluates a complete and fully integrated software system. The main objective of system testing is to determine the end-to-end requirements of the system. This process will test fully functional systems, including external peripherals, to evaluate how modules integrate with each other and with the system as a whole. Then, this process also ensures that any input in the system has been thoroughly tested to evaluate the desired outputs. Other than that, system testing also involves its users reviewing the user's experience with the system. System testing has different types, however, for this project, the developer will conduct functional and non-functional testing for the system testing. Below is the functional and non-functional testing that has been tested.

8.4.1 Functional Testing

Table 8.3 Functional Testing

Function	Expected Result	Actual Result
User Authentication	Users including normal users and admin should be able to login into the system using their email and password.	Working properly. Users can log in to the system using their email and password.
Users Registration	Users must be able to register to get their login credentials to log into this system.	Working properly. Users can register into the system.
Add Files	Users must be able to add any type files that they want to keep hidden.	Working properly. Users can add any type of files that they want to keep hidden.
Add Image	Users must be able to add the image that they wish to hide the files within.	Working properly. Users can add the image that they wish to hide the files within.
Compression Level	Users must be able to choose the compression level for the file.	Working properly. Users can choose the compression level for the file.

Password and Confirm Password	Users must be able to enter a password to encrypt and decrypt the hidden files.	Working properly. Users can enter a password to encrypt and decrypt the hidden files.
Hiding and Encrypting	Users must be able to click the hiding button to proceed with the process of hiding the files.	Working properly. Users can click the encrypt button to proceed with the process of hiding the files.
Add Image Contains Hidden Files	Users must be able to add the image that contains a secret file to be decrypted.	Working properly. Users can the image that contains a secret file to be decrypted.
Revealing and Decrypting	Users must be able to click the reveal button to proceed with the process of revealing the secret files.	Working properly. Users can click the reveal button to proceed with the process of revealing the secret files.
Download	Users must be able to download the image that contains a secret file or a file that has been decrypted into their devices or local storage.	Working properly. Users can download the image that contains a secret file or a file that has been decrypted into their devices or local storage.
Add and Update	The administrator must be able to add and update user information that has been registered.	Working properly. The administrator can add and update user information that has been registered.
Delete	The administrator must be able to delete a user that has been registered in the system	Working properly. The administrator can delete a user that has been registered in the system
Save	The administrator must be able to save the user's information that has been updated.	Working properly. The administrator can save the user's information that has been updated.
Logout	Users including normal users and admin must be able to end the session from the system.	Working properly. Users including normal users and admin can end the session from the system.

Table 8.3 shows the functional testing that has been tested. These tables show that each unit or function on the system has been tested. The function tested are user authentication, user registration, add files, add image, compression level, password and confirm password, hiding and encrypting, add image

contains hidden files, revealing and decrypting, download, add and update, delete, save, and logout. Based on the table, each function meets the expected result. This means, all the functionality that has been tested is working properly. Thus, the system meets their functional requirement for this project.

8.4.2 Non-Functional Testing

Table 8.4 Non-Functional Testing

Testing	Requirement	Actual Result
Performance	The system should be run smoothly. Each function must work well with no error occurred during system executing.	System performance works properly. The system run smoothly, each function work well and no error occurred during system executing.
Availability	The system should be able to use by the user anytime. User that has been registered into the system should able to use the feature of the system.	System availability works properly. The system will be available for 24 hours a day. However, if there are some enhancement and adjustment in this system, the system will take several hours for maintenance break. User that has been registered into the system can use the feature of the system.
Security	The system should provide different routes for normal users and administrators. The user's login credential information should be secure. Steganography and cryptography method should be used to secure user secret files.	The systems provide security. Normal users and admin have different routes. Users login credential such as password is stored in hash code in a database server. Then, the steganography and cryptography method are used to secure user secret files.
Reliability	The system should not have an issue, bugs, and technical errors in each module in the system. Error handling should be provided to inform the user if there is any invalid data being inputted.	System reliability works properly. The system has no issues, bugs, and technical errors in each module. Error handling is provided if the user enters invalid data into the system.
Portability	The system should be able to run on a PC, laptop, tablet, or smartphone. The system design should be user-friendly to desktop and mobile users.	System portability works properly. The system can run on PC, laptops, tablets, and smartphones. The design and layout of the system are user-friendly to desktop and mobile users.

Table 8.4 shows the non-functional testing that has been tested. These tables show that some non-functional requirement for this system has been tested. The non-functional being tested are the performance, availability, security, reliability, and portability. Based on the table, all the non-functional that have been tested is meet the expected result. Thus, the system can be considered to meets their non-functional requirement for this project.

8.5 Acceptance Testing

Acceptance testing is the final phase of testing an application. The main purpose of this test is to evaluate the operating process of the system by complying with the requirements needed which is acceptable for delivery. For acceptance testing, the developer will conduct user acceptance testing (UAT), a type of testing performed by the end-user or the client to evaluate the system architecture before transferring the system to the production environment. The main objective of UAT is to evaluate the end of system flow. Thus, for this project, the developer will conduct alpha and beta testing for the acceptance testing.

8.5.1 Alpha Testing

Alpha testing is conducted to evaluate and identify all possible errors and issues before the final product or the system will be released to the end-users. The purpose of this testing is to define and test the functionality or features of the system that the end-user might perform on the system. This testing will be conducted before the developer conducts the beta testing. Thus, alpha testing will be performed by the developer.

For this project, the developer has conducted the alpha testing early on. The testing includes unit testing and integration testing. All the code, design, and functionality of the system have been tested first. The test is to ensure that each function and module on the system work properly. Thus, the developer may find any bugs or errors on the system during the testing execution. With the inspection during testing, the developer will fix the error and improvise the function or module that has an error. After this alpha testing is completely done, the system will be ready to proceed to the beta testing which involves the end-users.

8.5.2 Beta Testing

Beta testing is carried by end-users of the software application in a real environment and it can be defined as a form of external User Acceptance Testing. This means this testing will involve actual users. It

is the final test before the end product is published. Beta testing helps us to improvise our system since we will get feedback from the users.

For this project, the beta version of the system will be released to a limited number of end-users in order to get feedback on the system quality. The number of end-users to test the beta version is around 10 to 20 respondents. The respondents then will send feedback by answering the online survey that has been given to them. From the survey, we will analyze the result if the system meets its objective or not and improvise the system if there are certain things on the system that need to be improved

8.5.3 Analysis of Acceptance Testing

Beta testing has been tested by potential users who want to hide their confidential files. During this beta testing, 20 respondents have tested the system and give feedback by answering the questionnaire given. The feedback by the respondent is crucial since it will help developers to improve and produce better outcomes for this project. Below is the result analysis obtained during the beta testing.

8.5.3.1 Part A: System Design

Question 1: Does the layout and design of the application is simple and easy to understand?

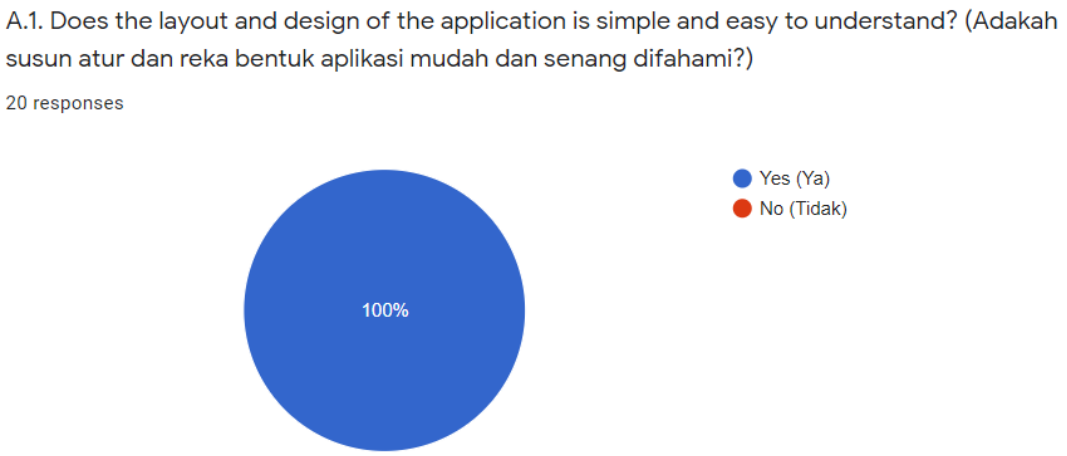


Figure 8.1 Result of Question 1 for Section A

Figure 8.1 shows the result of question 1 for section A. From the figure above, we found that all of the respondents voted yes for the understanding and simplicity of the layout and design of the application. This is because the design and layout of the application are very simple and allow any user to understand how the application should work.

Question 2: Does the navigation or interaction between each page in the application work properly?

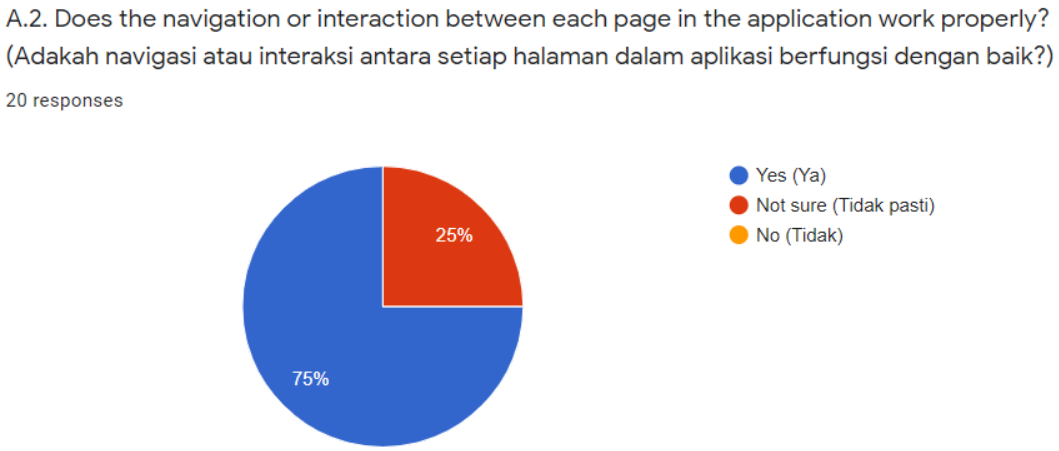


Figure 8.2 Result of Question 2 for Section A

Figure 8.2 shows the result of question 2 for section A. From the figure above, we found that 75% of respondents agreed that the navigation or interaction between each page in the application works properly. And only 25% of respondents are not sure if the interaction between each page works properly. The reason why a large number of respondents answered for yes is that the system can interact with each page as expected.

8.5.3.2 Part B: System Functionalities

Question 1: Does the application run smoothly?

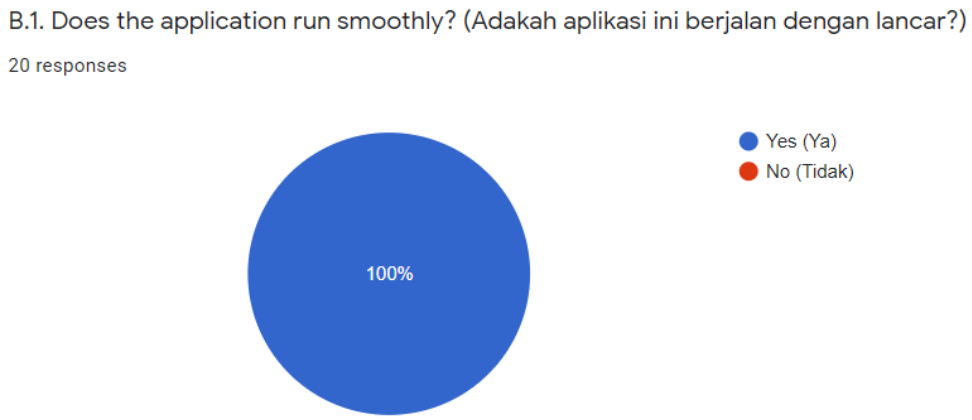


Figure 8.3 Result of Question 1 for Section B

Figure 8.3 shows the result of question 1 for section B. Based on this figure, we found that all of the respondents agreed that the application runs smoothly. The reason why they answered yes to this question is that the system actually can run smoothly and all the functions work properly.

Question 2: Users can login and register into the application.

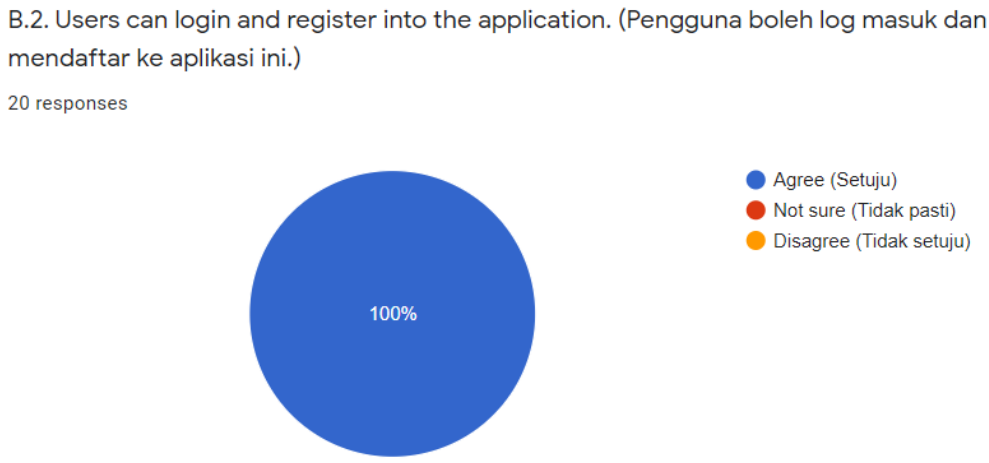


Figure 8.4 Result of Question 2 for Section B

Figure 8.4 shows the result of question 2 for section B. Based on this figure, we found that all of the respondents agreed that users can login and register into the application. The reason why they answered yes to this question is that the system actually provides a login page and register page for the users. All the user who wants to hide their confidential files can register into the system and use the feature of the system.

Question 3: Users can perform the main features and all the functions provided in the application.

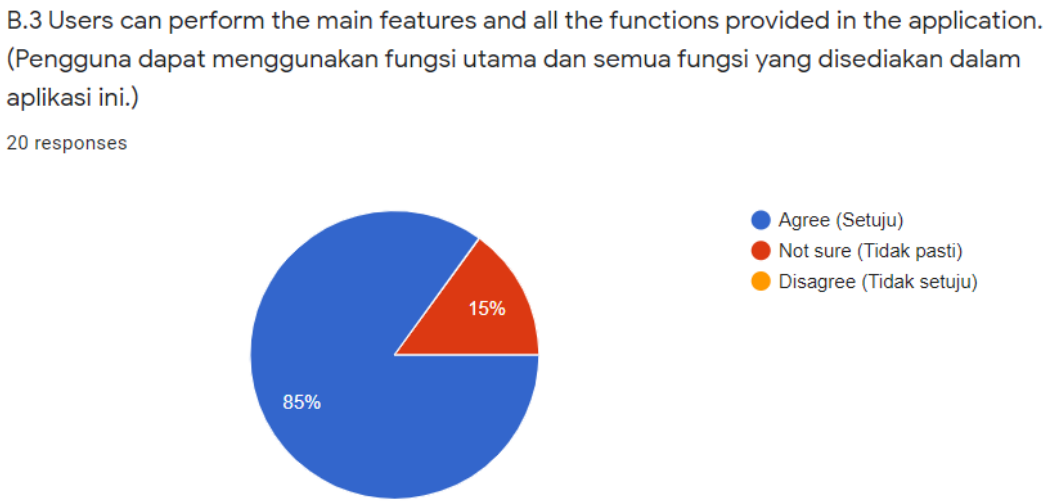


Figure 8.5 Result of Question 3 for Section B

Figure 8.5 shows the result of question 3 for section B. From the figure above, we found that 85% of the respondents agreed that users can perform the main features and all the functions provided in the application. And only 15% of respondents answered for not sure. The reason why a large number of respondents agreed is that all the features and functions provided on the system actually work properly. And why some of them are not sure is because they not sure either they have used all the features on this system or not.

8.5.3.3 Part C: System Security

Question 1: User must have an email that has been registered into the system and password to login into the system.

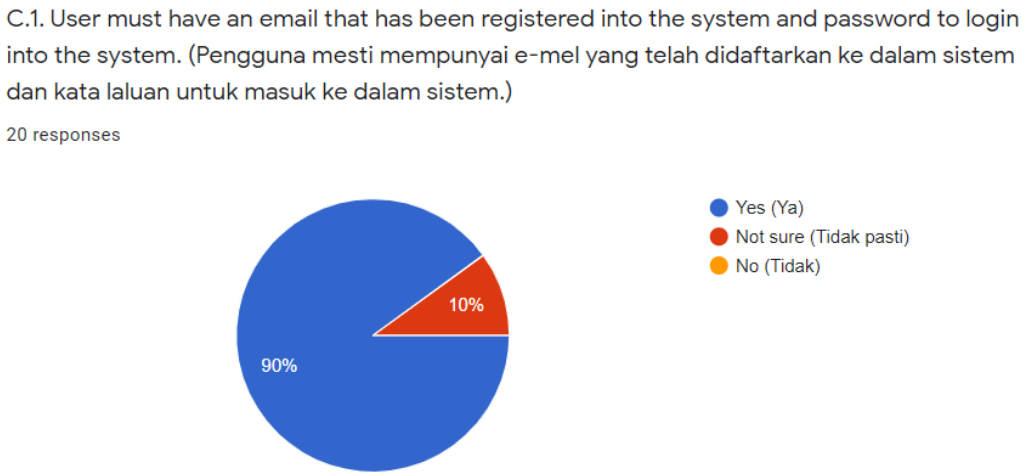


Figure 8.6 Result of Question 1 for Section C

Figure 8.6 shows the result of question 1 for section C. From the figure above, we found that 90% of the respondents agreed that users must have an email that has been registered into the system and a password to login into the system. And only 10% of respondents answered for not sure. The reason why a large number of respondents agreed with this statement is that the system actually required users to register first into the system and required a user to enter an email and password to log on to the system.

Question 2: User can hide their confidential files inside an image.

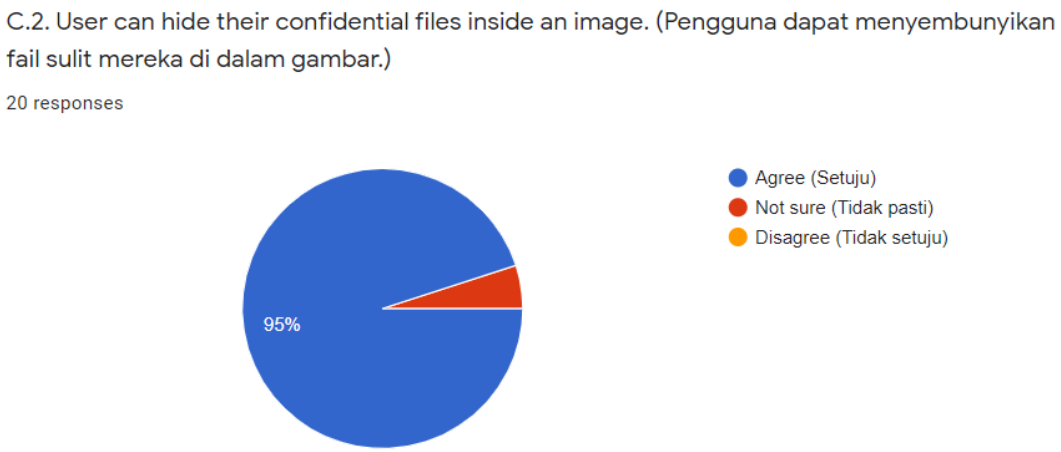


Figure 8.7 Result of Question 2 for Section C

Figure 8.7 shows the result of question 2 for section C. Based on this figure, we found that 95% of respondents agreed that user can hide their confidential files inside an image. And only 5% of respondents answered not sure about this statement. The reason why a large number of respondents agreed with this statement is that the system actually provides a feature that allows a user to hide their files inside an image file.

Question 3: User able to set a password to encrypt their hidden files inside the image.

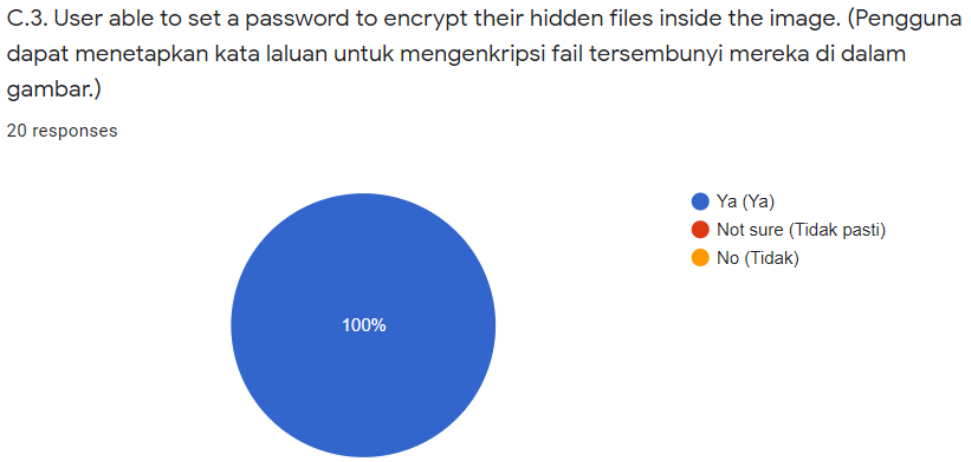


Figure 8.8 Result of Question 3 for Section C

Figure 8.8 shows the result of question 3 for section C. From the figure above, we found that all of the respondents answered yes that users able to set a password to encrypt their hidden files inside the image. The reason why all of the respondents answered yes with this statement is that the system actually provides a feature that allows the user to set a password to encrypt and secure their hidden files inside the image.

Question 4: User cannot reveal the hidden files inside the image without entering the correct password.

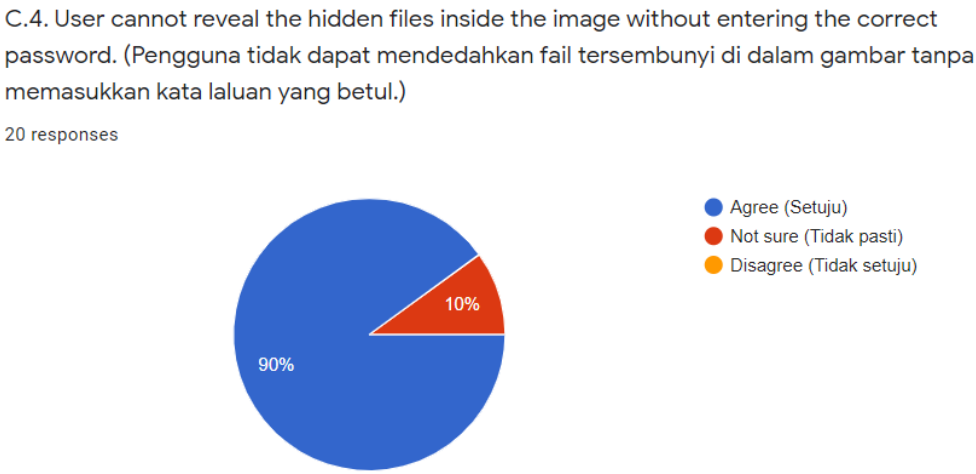


Figure 8.9 Result of Question 4 for Section C

Figure 8.9 shows the result of question 4 for section C. Based on this figure, we found that 90% of respondents answered yes that users cannot reveal the hidden files inside the image without entering the correct password. And only 10% of respondents answered not sure about this statement. The reason why a large number of respondents agreed with this statement is that the system actually provides a feature that allows a user to reveal their hidden files inside an image by entering the password that has been set. Without entering the correct password, the hidden files cannot be revealed.

8.5.3.4 Part D: Opinion

Question 1: Does this application solve the user problem to hide their confidential files from unauthorized users?

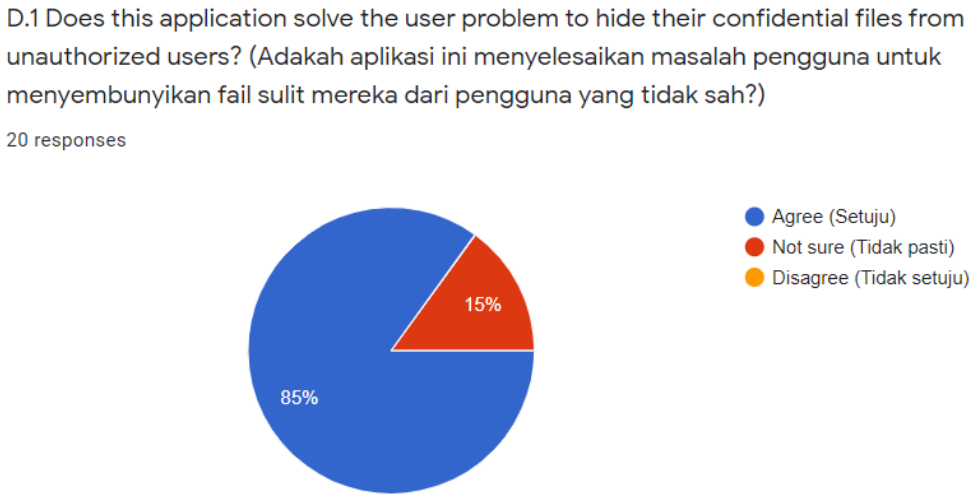


Figure 8.10 Result of Question 1 for Section D

Figure 8.10 shows the result of question 1 for section D. From the figure above, we found that 85% of respondents agreed that this application solves the user problem to hide their confidential files from unauthorized users. And only 15% of respondents answered not sure about this statement. The reason why a large number of respondents agreed with this statement is that the system actually could solve the user problem to hide their confidential files. The system provides users to hide their confidential files inside an image and will be secured by enabling them to set a password to encrypt their hidden files. And why some of them are not sure is because they not sure either this system actually could hide and secure their confidential files or not.

8.6 Conclusion

In conclusion, this chapter is important in developing this system. By making several testing such as unit testing, integration testing, system testing and, user acceptance testing (alpha and beta), the File Hiding Web Application could produce a better result after completed developed this web application. This testing allows the developer to find out the weakness of the system and allow them to resolve and improvise the system. According to the result of the survey, this system meets its requirement and ready to be deployed to potential users. Thus, this testing crucial and with the testing, the developer could improve the system to reach user satisfaction and relevant to be on the market for the user.

9 Project Management

9.1 Introduction

Project management is an important structure that applies process expertise, skills, resources, deliverables and plans to the development of the project to ensure that the project deliverable fulfilling its priorities and criteria. Thus, the development of an application must be organized and schedule by conducting project management to ensure the development run smoothly.

In this chapter, the management of this project will be discussed according to the planned approach. This project management will act as guidance for File Hiding Web Application development from the beginning until the deployment of the project. Thus, to ensure the development of this project to meet its criteria, the project schedule and risk management will be structured in this chapter. The project schedule will guide a developer to complete each task during the development and must be complete before the deadline. The risk management will ensure that the project achieves its objective and follow the plan if any dangers occur during the project life cycle. Thus, this project management will organize the developer to complete this project according to the plan.

9.2 Project Schedule

A project Schedule is a procedure that indicates what work should be done, which element of the project would execute the work and the time period in which the work should be completed. It provides an outline of the timeframe of the project and usually contains a specific start and finish date and lists all objectives, tasks, and deliverables necessary for the project. Thus, the developer will create an appropriate schedule that suits this project.

For this project, the project schedule will be structured based on the Work Breakdown Structure (WBS) and Gantt Chart. The WBS is used to ensure that the developers developed the system based on the phase of the project life cycle. As for the Gantt Chart, it will be structured to allow the developers to refers to the duration of the project processes. Thus, this both models will ease developer to track their progress during the development of the system.

9.2.1 Work Breakdown Structure (WBS)

The Work Breakdown Structure (WBS) describes all the activities the project needs to perform, organizes them into different stages, and presents them graphically. It is designed to establish a clear understanding of the scope of the project. The structure of the activities outlined in the WBS must be completed in order to accomplish the project's deliverables. Below is the WBS for the File Hiding Web Application.

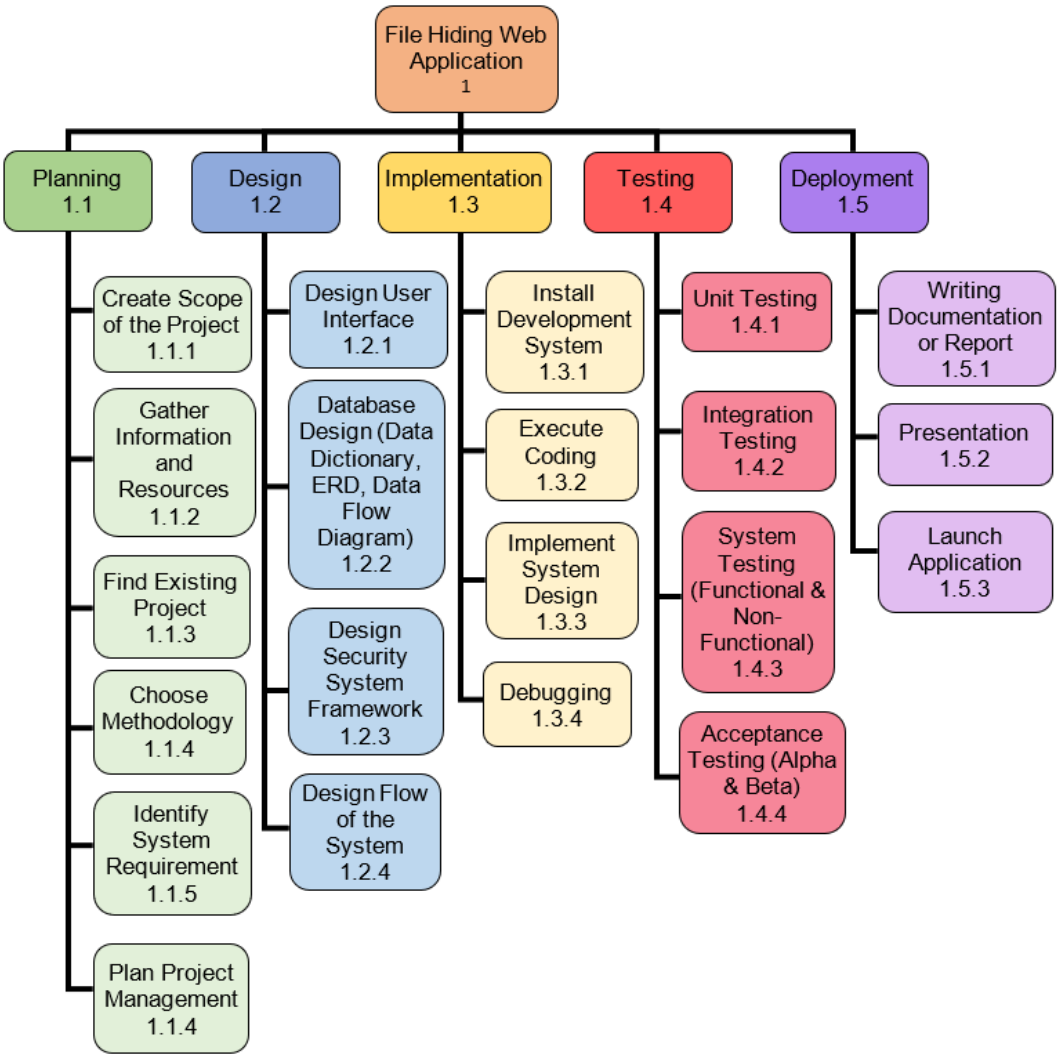


Figure 9.1 Work Breakdown Structure (WBS)

Figure 9.1 shows the Work Breakdown Structure (WBS) for the File Hiding Web Application. Based on this figure, there are five main activities or phase the developer needs to perform. The activities include the planning, design, implementation, testing, and deployment. Each of these phases has a specific task that needs to be performed. The specific task for each phase can be seen in Figure 9.1. By following this structure, the developer will understand what activities need to finish and they can easily accomplish the project deliverables in an organized way.

9.2.2 Gantt Chart

A Gantt Chart is a project management tool that assists in the planning and scheduling of this project and it is highly beneficial for simplifying types of projects. It is a horizontal, timeline-based bar chart that illustrates a time-based project schedule. This chart will help the developer to break down the project into manageable tasks, remain structured and envision the interactions between projects. Below is the Gantt Chart for the File Hiding Web Application.

Table 9.1 Gant Chart for Week 1 – 14

Activities	Weeks	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	Month	July 2020				August 2020				September 2020				October 2020	
1. Project Planning															
2. Project Brief															
3. Literature Review (Research)															
4. Project Methodology Used															
5. Project Management Planning															
6. System Requirement Planning															
7. System Analysis and Data Gathering															
8. Presenting the Project for Chapter 1-5															

Table 9.1 shows the Gant Chart of this project for week 1 until week 14. Based on this table, the activities involve during these 14 weeks are project planning, project brief, research, project methodology, project management planning, system requirement planning, analysis and data gathering, and presenting the project for chapters 1 until 5. The estimation time and progress on the project for 14 weeks are shown in the table above.

Table 9.2 Gant Chart for Week 15 – 28

Activities	Weeks	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	Month	November 2020		December 2020				January 2021			February 2021				March 2021
9. System Design															
10. Implementation															
11. Testing															
12. Maintenance, Review and Feedback															
13. Final Report Writing															
14. Final Presentation															
15. Submitting Full Project Report															

Table 9.2 shows the Gant Chart of this project for week 15 until week 28. Based on this table, the activities involve during these 15 to 28 weeks are system design, implementation, testing, maintenance, final report writing, final presentation, and submitting a full project report. The estimation time and progress on the project for 15 to 28 weeks are shown in the table above.

9.3 Risk Management

Project risk management is a process for discovering, analyzing and mitigating possible issues that could adversely impact the progress of the project. The main purpose of risk management in project management is to keep control of anything that could prevent the project from achieving its objective. Risk management is important because if the project risks are not defined, prevented or rectified, the project may end up over budget, postponed or even brought to a complete failure. Thus, this project will identify the risk that may probably occur during the development of the system. The developer provides a solution for each identified risk. With this risk management defined, the developer could easily handle the issue by taking an action to solve the issues. Thus, below is the structure of the risk management for this project.

Table 9.3 Risk Management

Risk Identification	Analysis Risk	Mitigation Plan
Software damaged	Software that is used to develop the system is damaged and not up to date. This causes the developer not to be able to develop the system and will delay the development progresses.	The developer must always check the version of the software used and update the software when the new updated version is available.
Lack of knowledge for the implementation of the system	Developer lack of knowledge to develop the system. They cannot find any material or sources used as a reference to develop the system. This issue could make the project not achieve its objective.	The developer must make research early on the information and material that is related to the project. They also must get some advice and help from the lecturer, friends and any person who is experts about the related system needs.
Data corrupted	All the data that is related to the project are corrupted or missing. They cannot retrieve it to get the data back. This issue could failure the project since they	The developer must make a backup for all the data that is related to the project. They must backup the data in any storage such as in hard drive, cloud

	cannot retrieve the data back and they might be developed the system from the scratch back.	storage, and many more.
Time constraints to complete the project	The developer might face some issues during the system development such as fixing some errors and lack of knowledge. Thus, it will take some time to solve the issue. Thus, this could cause time constraints to complete the project before the deadline.	The developer must follow the project management that has been constructed. They also must gather the data that is related to the project by following the duration time given on the project schedule. This will ensure that the developer could finished the project according the timeframe given.

Table 9.3 shows the risk management for this project. Based on the table, risk management consists of three components which are the risk identification, analysis risk, and mitigation plan. Risk identification listed all the risks that might occur during the project development. The analysis risk is the explanation of what risk the developer will be faced. And for the mitigation plan, is a plan that the developer will take to counter or solves the risk that might occur. According to the table above, there are four risks that have been identified for this project. The risk is software damaged, lack of knowledge, data corrupted and time constraints. The analysis risk and mitigation plan are being discussed in the table above. Thus, by referring to this risk management, the developer might control the risk if the risk occurs during the development of the project. This risk management will ensure that the developer completes developing the project and achieve its objective.

9.4 Conclusion

In conclusion, project management is crucial since it will guide the developer from the beginning until the last step to finished the project. Project management could organize the development of the project because it provides project schedule and risk management. Thus, the developer able to make a decision and follow the right path during the project development. Besides, this project management also will ensure the work flow of the project run smoothly and meet its requirements. As a result, project management is the best process for the team project to plan and create a strategy to concentrate on developing projects and to allow the developer to maintain the project finished on time.

10 Conclusion

10.1 Introduction

For the entire project, File Hiding Web Application has been developed by the developer. This web application was developed to provides image steganography tools to the users. This web application is important because people might want to avoid their confidential files such as financial statement, personal details and others confidential file from being viewed by an unauthorized user. Thus, this web application could help any user who wants to hide or secure their confidential files from unauthorized users. This application enable user to hide their confidential file inside the image file. Users can hide any type of file including document, image, audio and video. This application also provides an encryption by allowing user to set a password for the hidden files. Then, this application provides users to reveal the hidden files inside an image.

In the last chapter of this project, it will discuss an overview of the File Hiding Web Application development process. The developer will explain a summary of the scenario faced by them during developing the web application. This chapter will restate and answer all the project objectives as well as the findings, recommendations, scope and future research of this project. Thus, this chapter will discuss the achievements, future work and project evaluation for this project.

10.3 Achievements

The biggest achievements of this project are this project successfully met their objectives. This project finally covered all the objectives of the project. Thus, by developing the File Hiding Web Application, the objectives of the project such as enable users who want to hide their confidential files inside an image has met its requirement. Besides, this project provides encryption to secure the hidden files inside the image which is one of the objectives for this project. Then, the last objective also achieved, which is to enable users to reveal their hidden files inside the image file. The final result of the web application being delivered as expected. As a consequence, this web application may help to solve the problem when someone wants to hide their files from unauthorized users.

In addition to achieving objectives, the developer gains a lot of knowledge during the development of this project. They acquire a lot of knowledge including technical and non-technical elements. Other than that, the developer improvises their development skills by learning a programming language and framework that they never used before. Writing codes, designing interfaces, establishing resources is some of the knowledge that the developer gain from this project. On top of that, the developer also develops and improves their problem-solving skills. The skills include how to fix an error and handle the risk that occurred during the development of the project. With all the skills achieved by the developer, this project

was completed according to the schedule and timeframe that has been structured. Thus, this project successfully achieved to be finished before the deadline.

10.3 Future Work

To maintain and improvise the application, the developer plans to continue to update the application in the future. This may include adding new features, improvise security elements, and improve usability in other platforms. This improvement is important because it will satisfy the user's needs and provide better interaction and experience between the users and the application. The following details are some of the suggestions and features that will be added to enhance the application.

10.3.1 Build the system for mobile application

Even though the current application is a web-based application which able to use on any platform, a mobile application is crucial to be developed for this system. It is because, today, a smartphone is an important device in the community. People will bring it anywhere and anytime since it is used to communicate or to do a certain task. By developing the mobile application for this system, users who want to use this application will obtain better experience and interaction since the system was built for mobile application. By developing mobile applications, potential users can use the system easily since the system can be installed on their smartphones anytime and anywhere.

10.3.2 Add cloud storage feature

This system could be improvised by providing a user to save the image file that contains hidden files and the confidential files themselves inside the user’s cloud storage such as Google Drive. By providing this feature users may easily access their confidential files anytime and anywhere since the files stored in their cloud storage. Other than that, users could share confidential files with others easily since cloud storage provides sharing features. Thus, this feature could ease the user to retrieve confidential files and share their confidential files with the authorized user.

10.3.3 Add digital watermarking feature

This feature can be implemented in this system because it also uses the image steganography method. However, the main objective of this feature to maintain the originality of the data or file. Thus, by adding this digital watermarking feature, unauthorized users cannot easily duplicate the data and

distinguish the identity of the data owner or creator. This feature will help users to secure their content of the data by adding the watermarking on their data or file.

10.3.4 Improve the interface design

The improvement of the interface design for the system is needed. It is to ensure that the users will experience better interaction with the system. The user interface design pattern trending may differ and evolve over time. Thus, to follow the new or current trends, the system will update and improve the system interface design according to the current trending which makes the system more relevant and usable in the future.

10.4 Project Evaluation

File Hiding Web Application is an ideal application that applied the concept of image steganography and cryptography method. This web application was developed to allow the user to hide their confidential file from being viewed by unauthorized users. After finished this project, the project evaluation must be made to describe the outcome of the project.

This project achieves its objective because of the effort of the developer to complete this project. Even though that the project achieves its objective, there is certain limitation during this study to complete this project. One of them is the developer's lack of knowledge during the implementation of the system. This including coding and designing the system. Due to lack of knowledge, the developer needs to do research about the topic including technical and non-technical elements related to the project to understand what the system should produce. Besides, to satisfied the users, the developer provides a survey to the potential users as it helps on the finding of this project.

Other than that, developers also faced some issues and errors during the development of the system. This is because, the developer lack of experience, skills and knowledge. This problem resulting in delaying the task that needs to be completed according to the expected time given. Even though there is a slack time to finish completing the project, the developer able to tackle the problem by making certain research related to the issues and get some advice from the supervisor, lecturer, friend and social community who are experts with the related issue. Thus, the developer still able to complete the project before the deadline.

Lastly, to ensure that the File Hiding Web Application is ready to deploy, it has been tested on the potential users in order to get feedback from them. The feedback helps the developer to improvise the system and meet user requirements before it can be deployed. Thus, with the result of this project, File Hiding Web Application can be used to secure and hide user’s confidential files inside an image file.

10.5 Conclusion

In a conclusion, the development of File Hiding Web Application has fulfilled the requirements by achieving the objectives. As a student who develops this system, it is difficult to handle the project until the end of the project. A lot of research and practice need to be acquired to understand what should be delivered for the system. This project could not achieve its objective if the developers cannot handle and make a good decision for the limitation that occurs during the development of the project. Then the help from the supervisor, friend, and social community is very helpful in order to achieve the project objectives.

Besides, features of the system will be improved and updated to make File Hiding Web Application more relevant and useful. In the future, the developers hope that this web application can be used to help any user who wants to hide or secure their confidential files from being viewed by an unauthorized user. The future work should produce great output to make it different from the current system.

Finally, thanks to the faculties and supervisors who committed to the completion of this project, especially to my supervisor, Madam Noraliza Binti Azizan and Final Year Project (FYP) Coordinator, Miss Shuhadah Binti Othman who keep monitoring the progression of this project until the completion of this project. Without their advice, guidance, and suggestion, this project cannot achieve its objective and could be a failure.

References

1. Acer. (n.d.). Nitro 5 AN515-52. [online] Available at: https://www.acer.com/ac/en/GB/content/model/NH.Q3MEK.014 [Accessed 3 Oct. 2020].

2. Almuhammadi, S. and Al-Shaaby, A. (2017). A Survey on Recent Approaches Combining Cryptography and Steganography. Computer Science & Information Technology (CS & IT). [online] Available at: https://airccj.org/CSCP/vol7/csit76506.pdf [Accessed 3 Oct. 2020].

3. Al Sadi, G. (2015). Image Steganography Approach. International Journal of Computer Science and Mobile Computing, [online] 4(8), pp.166–169. Available at: https://www.researchgate.net/publication/286452501_Image_Steganography_Approach [Accessed 3 Oct. 2020].

4. Anonymous (2014). The Hacker News. [online] The Hacker News. Available at: https://thehackernews.com/2014/04/securing-passwords-with-bcrypt-hashing.html [Accessed 15 Feb. 2021].

5. Altigani, A. and Barry, B. (2013). A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and Word Shift Coding Protocol. 2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE), [online] pp.134–139. Available at: https://www.researchgate.net/figure/Combining-Cryptography-and-Steganography-with-an-Additional-Layer-of-Compression-2_fig3_261526896 [Accessed 3 Oct. 2020].

6. Arias, D. (2018). Hashing in Action: Understanding bcrypt. [online] Auth0 - Blog. Available at: https://auth0.com/blog/hashing-in-action-understanding-bcrypt/ [Accessed 15 Feb. 2021].

7. Chugh, G. (2013). IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE. Acta Technica Corvininesis-Bulletin of Engineering, [online] 6(3). Available at: http://acta.fih.upt.ro/pdf/2013-3/ACTA-2013-3-17.pdf [Accessed 3 Oct. 2020].

8. Ertaul, L., Kaur, M. and Gudise, V.A.K.R. (2016). Implementation and Performance Analysis of PBKDF2, Bcrypt, Scrypt Algorithms. In Proceedings of the International Conference on Wireless Networks (ICWN), [online] pp.66-72. Available at: http://borg.csueastbay.edu/~lertaul/PBKDFBCRYPTCAMREADYICWN16.pdf [Accessed 3 Oct. 2020].

9. Housley, R. (2004). Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP). [online] Available at: https://dl.acm.org/doi/pdf/10.17487/RFC3686 [Accessed 3 Oct. 2020].

10. Hussain Azmee (2018). Agile Methodology. [online] Academia.edu. Available at: https://www.academia.edu/4383136/Agile_Methodology [Accessed 3 Oct. 2020].

11. Ives, G. (2017). StegaPhoto. [online] Greg Ives. Available at: https://gregives.co.uk/projects/stegaphoto/ [Accessed 3 Oct. 2020].

12. Jyothi, P.S. and Ali, SK.M. (2020). A NEW SECURE DATA HIDING IN IMAGE ENCRYPTED TECHNIQUE BASED BY USING AES-CTR KEY MODULATION. International Journal For Advanced Research In Science & Technology, [online] 10(7), pp.217–224. Available at: http://www.ijarst.in/admin-panel/papers/658_approvedpaper.pdf [Accessed 3 Oct. 2020].

13. Khillar, S. (2019). Difference Between SHA-256 and SHA-1 | Difference Between. [online] DifferenceBetween.net. Available at: http://www.differencebetween.net/technology/difference-between-sha-256-and-sha-1/ [Accessed 3 Oct. 2020].

14. Knight, M. (2017). What is Data Modeling? [online] DATAVERSITY. Available at: https://www.dataversity.net/what-is-data-modeling/# [Accessed 3 Oct. 2020].

15. Lake, J. (2019). What is steganography and how does it differ from cryptography? [online] Comparitech. Available at: https://www.comparitech.com/blog/information-security/what-is-steganography/ [Accessed 3 Oct. 2020].

16. Mishra, N. (2019). Types of Cryptography. [online] The Crazy Programmer. Available at: https://www.thecrazyprogrammer.com/2019/07/types-of-cryptography.html [Accessed 3 Oct. 2020].

17. mongodb (2021). [online] Mongodb.com. Available at: https://webassets.mongodb.com/_com_assets/cms/MongoDB_Logo_FullColorBlack_RGB-4td3yuxzjs.png [Accessed 19 Jan. 2021].

18. Pal, P. and Dubey, S. (2016). Various JPEG Image Steganography Techniques: A Review. [online] www.semanticscholar.org. Available at: https://www.semanticscholar.org/paper/Various-JPEG-Image-Steganography-Techniques%3A-A-Pal-Dubey/a1c5bd6230c4d08e0408fb9707af50eeae3f41d3#references [Accessed 3 Oct. 2020].

19. Rout, H. and Mishra, B.K. (2014). Pros and Cons of Cryptography, Steganography and Perturbation techniques. IOSR Journal of Electronics and Communication Engineering, [online] pp.76–81. Available at: https://www.researchgate.net/profile/Brojo_Mishra2/publication/286092142_Pros_and_Cons_of_Cryptography_Steganography_and_Perturbation_techniques/links/56660a3208ae418a786f3afb.pdf [Accessed 3 Oct. 2020].

20. Saleh, M.E., Aly, A.A. and Omara, F.A. (2016). Data Security Using Cryptography and Steganography Techniques. IJACSA) International Journal of Advanced Computer Science and Applications, [online] 7(6), pp.390–397. Available at: http://13.233.42.234/Downloads/Volume7No6/Paper_51-Data_Security_Using_Cryptography_and_Steganography_Techniques.pdf [Accessed 3 Oct. 2020].

21. Semusheva, O. (2016). Requirements. Why is it important? [online] Steelkiwi.com. Available at: https://steelkiwi.com/blog/requirements-why-it-important/ [Accessed 3 Oct. 2020].

22. Sharief, K. (2020). What is Cryptanalysis? - Definition, Methods, and More. [online] Computer Tech Reviews. Available at: https://www.computertechreviews.com/definition/cryptanalysis/ [Accessed 3 Oct. 2020].

23. softpedia. (n.d.). Download Steganofile 1.0. [online] Available at: https://www.softpedia.com/get/Security/Encrypting/Steganofile.shtml [Accessed 3 Oct. 2020].

24. softpedia. (n.d.). Download SteganPEG 1.0. [online] Available at: https://www.softpedia.com/get/Security/Encrypting/SteganPEG.shtml [Accessed 3 Oct. 2020].

25. ssl2buy. (2019). Symmetric vs. Asymmetric Encryption – What are differences? [online] Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences [Accessed 3 Oct. 2020].

26. Taha, M.S., Mohd Rahim, M.S., lafta, S. abdulsattar, Hashim, M.M. and Alzuabidi, H.M. (2019). Combination of Steganography and Cryptography: A short Survey. IOP Conference Series: Materials Science and Engineering, [online] 518(5), p.5. Available at: https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf [Accessed 3 Oct. 2020].

27. Techopedia. (2018). What is Hash Function? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/19744/hash-function [Accessed 3 Oct. 2020].

28. Telsy. (2020). Steganography: from its origins to the present. [online] Available at: https://www.telsy.com/steganography-from-its-origins-to-the-present/ [Accessed 3 Oct. 2020].

29. Thattamparambil, Dr.N. (2020). How to choose the research methodology best suited for your study. [online] Editage Insights. Available at: https://www.editage.com/insights/how-to-choose-the-research-methodology-best-suited-for-your-study [Accessed 3 Oct. 2020].

30. Tryfanava, D. (2020). Functional vs Non-functional Requirements: Examples and Types. [online] VironIT. Available at: https://vironit.com/functional-vs-non-functional-requirements/ [Accessed 3 Oct. 2020].

31. Wikimedia.org. (2019). [online] Available at: https://upload.wikimedia.org/wikipedia/commons/thumb/5/5f/Microsoft_Office_logo_%282019%E2%80%93present%29.svg/1024px-Microsoft_Office_logo_%282019%E2%80%93present%29.svg.png [Accessed 3 Oct. 2020].

32. Wikimedia.org. (2020). [online] Available at: https://upload.wikimedia.org/wikipedia/commons/thumb/9/9a/Visual_Studio_Code_1.35_icon.svg/1024px-Visual_Studio_Code_1.35_icon.svg.png [Accessed 3 Oct. 2020].

33. Wikimedia.org. (2019). [online] Available at: https://upload.wikimedia.org/wikipedia/commons/thumb/8/8d/Windows_darkblue_2012.svg/1024px-Windows_darkblue_2012.svg.png [Accessed 3 Oct. 2020].

34. www.pelock.com. (n.d.). Steganography Online Codec - Hide Message in Image. [online] Available at: https://www.pelock.com/products/steganography-online-codec [Accessed 3 Oct. 2020].

35. Yoon, S. (2019). Steganography in the Modern Attack Landscape. [online] VMware Carbon Black. Available at: https://www.carbonblack.com/blog/steganography-in-the-modern-attack-landscape/ [Accessed 3 Oct. 2020].

Appendix A – Requirements Specification Document

Questionnaire for File Hiding Web Application Using Image Steganography Techniques

Dear Respondent,

I am Amirul Naim Bin Mohd Shafiee, final year student of Bachelor of Information Technology (Honours) in Information Security, Kolej Universiti Poly-Tech MARA Kuala Lumpur. The main purpose of this questionnaire is to do analysis in developing the file hiding web application using image steganography techniques. This survey is important to my research since this is for my final year project. I really appreciate you for taking the time to participate in this survey. The data collected would be used only for academic purposes and all related information will be kept confidential.

Thank you for your participation and cooperation!

(Kepada Responden,

Saya Amirul Naim Bin Mohd Shafiee, pelajar tahun akhir Sarjana Muda Teknologi Maklumat (Kepujian) dalam Keselamatan Maklumat, Kolej Universiti Poly-Tech MARA Kuala Lumpur. Tujuan utama penyelidikan soal selidik ini adalah untuk melakukan analisis dalam mengembangkan aplikasi web penyembunyian fail menggunakan teknik steganografi gambar Tinjauan ini penting bagi kajian saya kerana ini adalah untuk projek tahun akhir saya. Saya sangat menghargai anda kerana meluangkan masa untuk mengambil bahagian dalam tinjauan ini. Data yang dikumpulkan hanya akan digunakan untuk tujuan akademik dan semua maklumat yang berkaitan akan dirahsiakan.

Terima kasih atas penyertaan dan kerjasama anda!)

SECTION A: Respondent Information

Gender (Jantina): _____

Age (Umur): 15-18 ☐ 19-22 ☐ 23-26 ☐ -30 O ☐ 30 ☐

Race (Bangsa): _____

Occupation Status (Status Pekerjaan): _____

SECTION B: Image Steganography Techniques

Please tick [/] in the box to answer the question.

1. Have you ever heard of Image Steganography Technique? (Pernahkah anda mendengar Teknik Steganografi Gambar?)

Yes (Ya) ☐ No (Tidak) ☐

2. Have you ever heard of Image or Visual Cryptography Technique? (Pernahkah anda mendengar Teknik Kriptografi Gambar atau Visual?

Yes (Ya) ☐ No (Tidak) ☐

3. Do you know that Steganography and Cryptography techniques can be combined to secure your confidential file? (Adakah anda tahu bahawa teknik Steganografi dan Kriptografi dapat digabungkan untuk melindungi fail sulit anda?)

Yes (Ya) ☐ No (Tidak) ☐ Not sure (Tidak pasti) ☐

SECTION C: Use of File Hiding Application

Please tick [/] in the box to answer the question.

1. Confidential file should not be viewed by unauthorized user (Fail sulit tidak boleh dilihat oleh pengguna yang tidak dibenarkan).

Strongly Agree ☐ Agree ☐ Moderate ☐ Disagree ☐ Strongly Disagree ☐
(Sangat Bersetuju) (Setuju) (Sederhana) (Tidak bersetuju) (Sangat Tidak Setuju)

2. Password is normally required to protect the authorization of a system or access to a system. (Kata laluan biasanya diperlukan untuk melindungi keizinan sistem atau akses ke sistem.).

Strongly Agree ☐ Agree ☐ Moderate ☐ Disagree ☐ Strongly Disagree ☐
(Sangat Bersetuju) (Setuju) (Sederhana) (Tidak bersetuju) (Sangat Tidak Setuju)

3. Have you ever used any file hiding application or software to hide your confidential file? (Adakah anda pernah menggunakan aplikasi atau perisian menyembunyikan fail untuk menyembunyikan fail sulit anda?)

Yes (Ya) ☐ No (Tidak) ☐

4. If you use a file hiding tool, what type of file you want to kept it hidden? (Sekiranya anda menggunakan alat penyembunyian fail, jenis fail apa yang ingin anda rahsiakan?)

☐ Document (Dokumen) - PDF, Words, PowerPoint, Excel, text
☐ Image (Gambar)
☐ Video
☐ Audio
☐ All of the above (Semua di atas)

5. Where do you usually store your confidential files? (Di manakah anda biasanya menyimpan fail sulit anda?)

- [ ] Personal Computer PC (Komputer Peribadi)
- [ ] Laptop (Komputer Riba)
- [ ] Smartphone (Telefon Pintar)
- [ ] Tablet
- [ ] Cloud storage (Penyimpanan Awan)
- [ ] Other (Lain).. _____

6. Cloud storage makes it easy for users to store and share their confidential files (Penyimpanan awan memudahkan pengguna menyimpan dan berkongsi fail sulit mereka)

Strongly Agree	Agree	Moderate	Disagree	Strongly Disagree
(Sangat Bersetuju)	(Setuju)	(Sederhana)	(Tidak bersetuju)	(Sangat Tidak Setuju)

7. In your opinion, is it necessary to develop an application that can hide confidential files? (Pada pendapat anda, adakah perlu untuk mengembangkan aplikasi yang dapat menyembunyikan fail sulit?)

Yes (Ya) ☐ No (Tidak) ☐ Not sure (Tidak pasti) ☐

Questionnaire for Feedback on File Hiding Web Application (Beta Testing)

Feedback on File Hiding Web Application (Beta Testing)

Dear Respondent,

The purpose of this survey is to get feedback from users after testing the File Hiding Web Application. This application is developed to allow any user to hide their confidential files inside an image using the image steganography method. Users can hide any type of file including Document(PDF, Word, PowerPoint, Excel, txt), Image, Audio, and Video inside an image file. This feedback helps to get a result for the Beta Testing of this application. I really appreciate you for taking the time to participate in this survey. The data collected would be used only for academic purposes and all related information will be kept confidential.

Thank you for your participation and cooperation!

(Kepada Responden,

Tujuan tinjauan ini adalah untuk mendapatkan maklum balas daripada pengguna setelah selesai menguji File Hiding Web Application. Aplikasi ini dibina untuk membolehkan pengguna menyembunyikan fail sulit mereka di dalam gambar menggunakan kaedah steganografi gambar. Pengguna dapat menyembunyikan semua jenis fail termasuklah Dokumen (PDF, Word, PowerPoint, Excel, txt), Imej, Audio dan Video di dalam fail gambar. Maklum balas ini membantu mendapatkan keputusan Beta Testing untuk aplikasi ini. Saya sangat menghargai anda kerana meluangkan masa untuk mengambil bahagian dalam tinjauan ini. Data yang dikumpulkan hanya akan digunakan untuk tujuan akademik dan semua maklumat yang berkaitan akan dirahsiakan.

Terima kasih atas penyertaan dan kerjasama anda!)

Next

Feedback on File Hiding Web Application (Beta Testing)

* Required

Respondent Information

Gender (Jantina) *

- Male/Lelaki
- Female/Perempuan

Age (Umur) *

- Aged 15-18
- Aged 19-22
- Aged 23-26
- Aged over 27

Occupation Status (Status Pekerjaan) *

- Employed (Bekerja)
- Not Employed (Tidak Bekerja)
- Student (Pelajar)

Back Next

Feedback on File Hiding Web Application (Beta Testing)

* Required

Part A: System Design

A.1. Does the layout and design of the application is simple and easy to understand? (Adakah susun atur dan reka bentuk aplikasi mudah dan senang difahami?) *

- ◯ Yes (Ya)
- ◯ No (Tidak)

A.2. Does the navigation or interaction between each page in the application work properly? (Adakah navigasi atau interaksi antara setiap halaman dalam aplikasi berfungsi dengan baik?) *

- ◯ Yes (Ya)
- ◯ Not sure (Tidak pasti)
- ◯ No (Tidak)

Back Next

Part B: System Functionalities

B.1. Does the application run smoothly? (Adakah aplikasi ini berjalan dengan lancar?) *

- ◯ Yes (Ya)
- ◯ No (Tidak)

B.2. Users can login and register into the application. (Pengguna boleh log masuk dan mendaftar ke aplikasi ini.) *

- ◯ Agree (Setuju)
- ◯ Not sure (Tidak pasti)
- ◯ Disagree (Tidak setuju)

B.3 Users can perform the main features and all the functions provided in the application. (Pengguna dapat menggunakan fungsi utama dan semua fungsi yang disediakan dalam aplikasi ini.) *

- ◯ Agree (Setuju)
- ◯ Not sure (Tidak pasti)
- ◯ Disagree (Tidak setuju)

Back Next

Part C: System Security

C.1. User must have an email that has been registered into the system and password to login into the system. (Pengguna mesti mempunyai e-mel yang telah didaftarkan ke dalam sistem dan kata laluan untuk masuk ke dalam sistem.) *

- ◯ Yes (Ya)
- ◯ Not sure (Tidak pasti)
- ◯ No (Tidak)

C.2. User can hide their confidential files inside an image. (Pengguna dapat menyembunyikan fail sulit mereka di dalam gambar.) *

- ◯ Agree (Setuju)
- ◯ Not sure (Tidak pasti)
- ◯ Disagree (Tidak setuju)

C.3. User able to set a password to encrypt their hidden files inside the image. (Pengguna dapat menetapkan kata laluan untuk mengenkripsi fail tersembunyi mereka di dalam gambar.) *

- ◯ Ya (Ya)
- ◯ Not sure (Tidak pasti)
- ◯ No (Tidak)

C.4. User cannot reveal the hidden files inside the image without entering the correct password. (Pengguna tidak dapat mendedahkan fail tersembunyi di dalam gambar tanpa memasukkan kata laluan yang betul.) *

- ◯ Agree (Setuju)
- ◯ Not sure (Tidak pasti)
- ◯ Disagree (Tidak setuju)

Back Next

Part D: Opinion

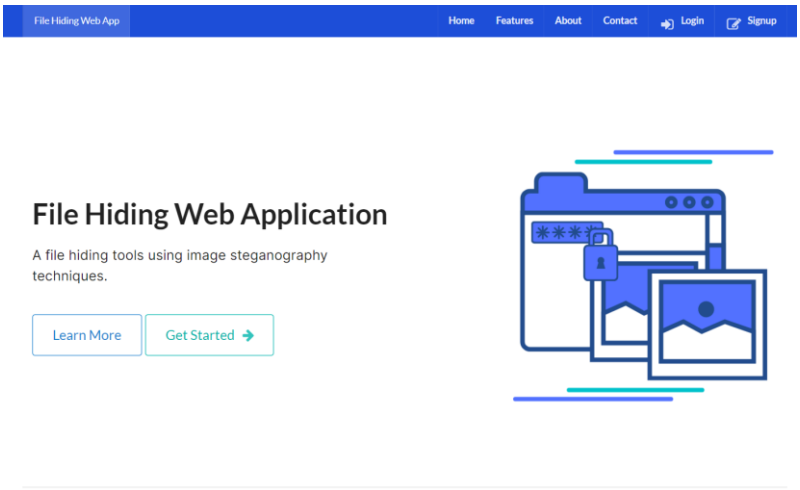
D.1 Does this application solve the user problem to hide their confidential files from unauthorized users? (Adakah aplikasi ini menyelesaikan masalah pengguna untuk menyembunyikan fail sulit mereka dari pengguna yang tidak sah?) *

- ◯ Agree (Setuju)
- ◯ Not sure (Tidak pasti)
- ◯ Disagree (Tidak setuju)

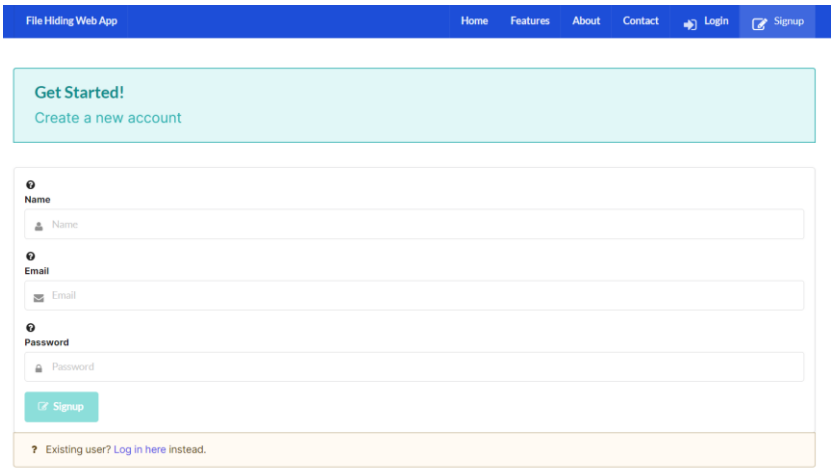
Back Submit

Appendix B – User Manual

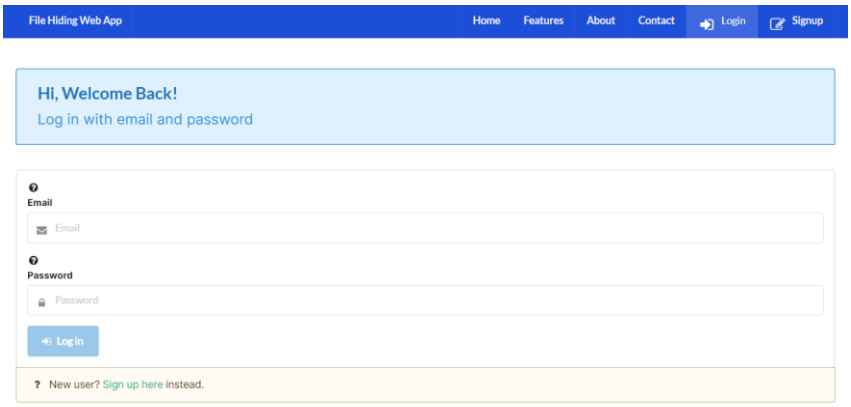
Step 1: Users will directly go to the File Hiding Web Application homepage when they open this website.



Step 2: To register into the system, users must click the 'Signup' menu that has been provided on the header of the website. Users must fill the form given and the data must be valid to successfully register to the system.

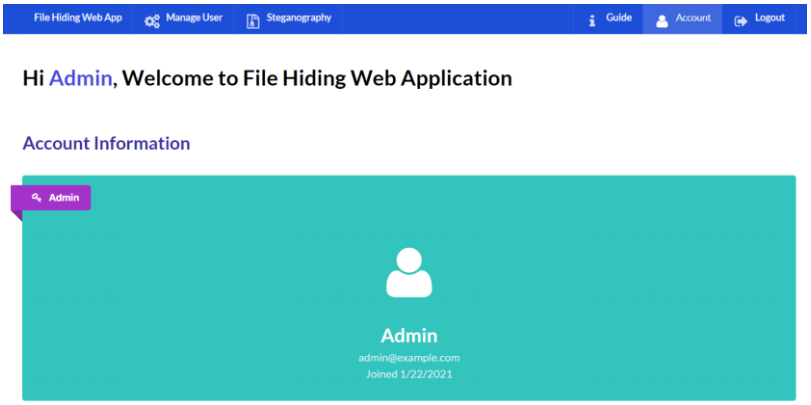


Step 3: If the user already registered into the system. Users must click the 'Login' menu that has been provided on the header of the website. Then, users must enter the email that has been registered and the password to log in to the system.

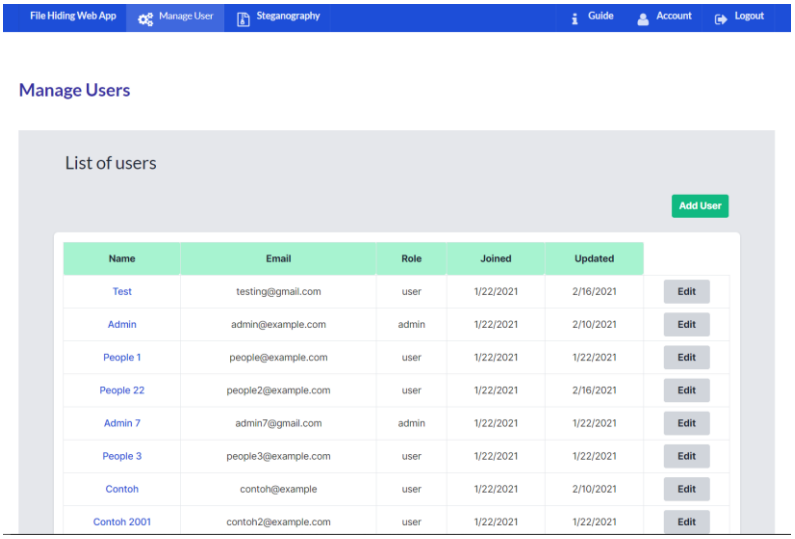


- **Logged in as an administrator**

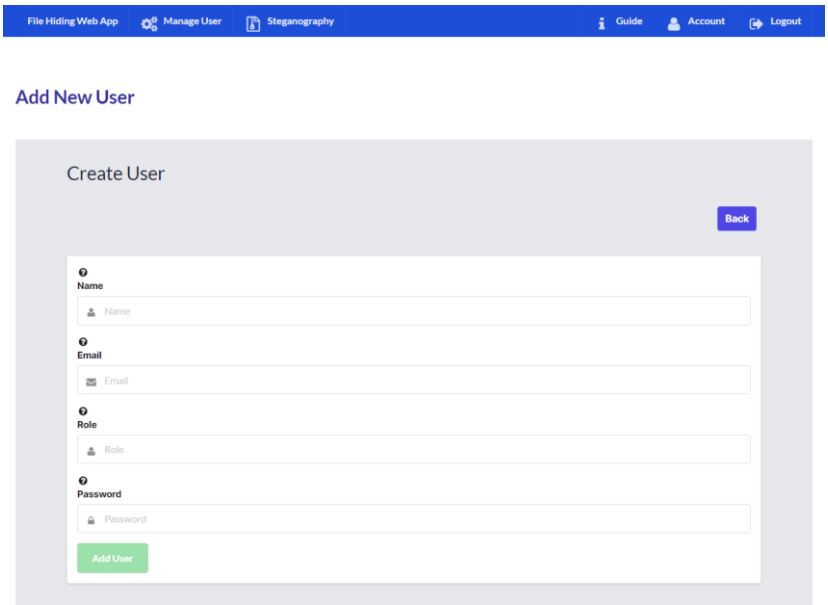
Step 1: After successfully log into the system, an admin will directly go to the account page.



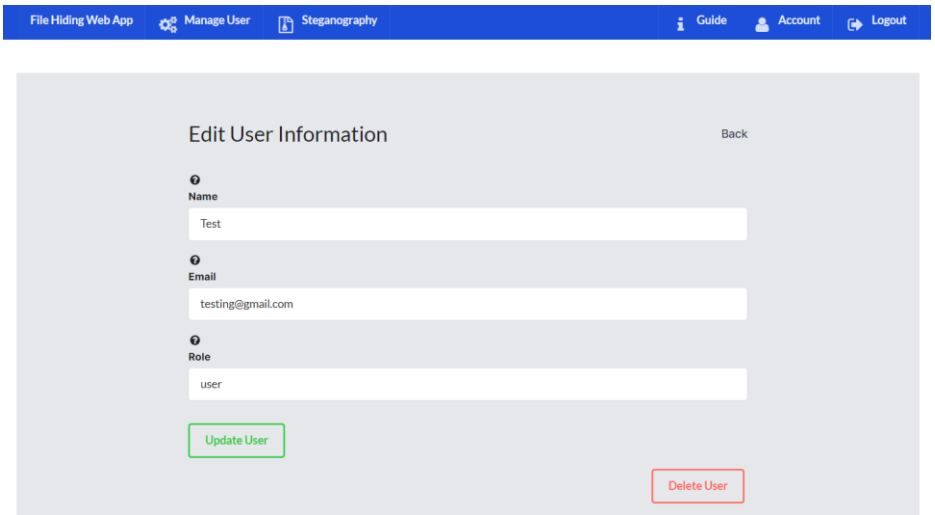
Step 2: To manage any user that has been registered into this system, an admin must click the 'Manage User' menu provided on the header of the website. Then a list of users can be viewed by the admin. To add a new user to the system, an admin must click the 'Add User' button. And to edit the user information, an admin must click the 'Edit' button.



Step 3: When the admin clicks the 'Add User' button on the manage user page, the admin will go to this page. Then the admin needs to fill the form given and after finished fill the form, the admin must click the 'Add User' button to successfully register a new user into this system.

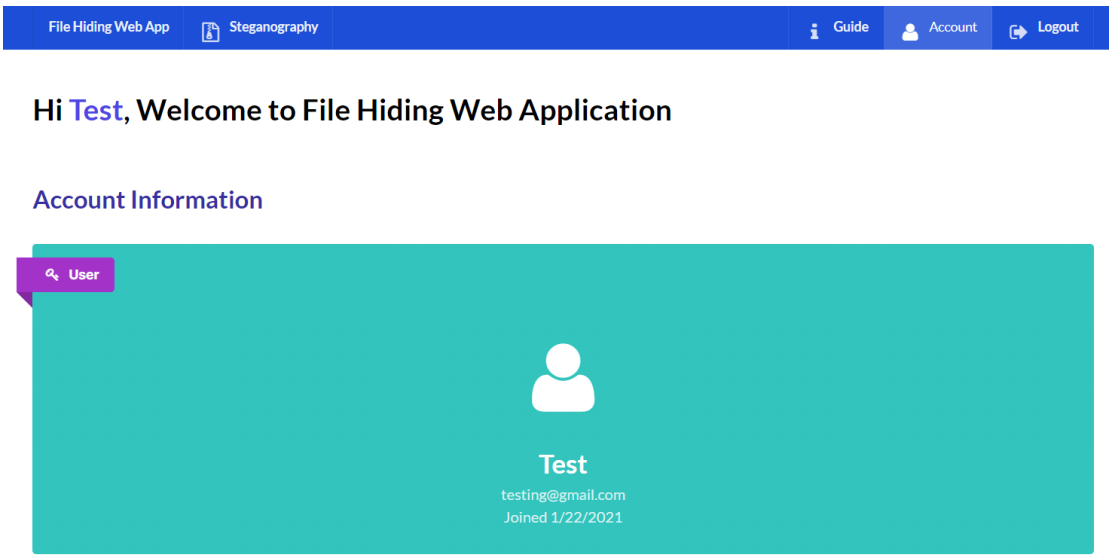


Step 4: Then, when the admin clicks the ‘Edit button’ on the manage user page, the admin will go to this page. Admin can edit user information such as name, email, and role. After finished edit the user information, the admin must click the ‘Update User’ button to successfully update user information. Other than that, the admin can delete users from this system by clicking the ‘Delete User’ button.



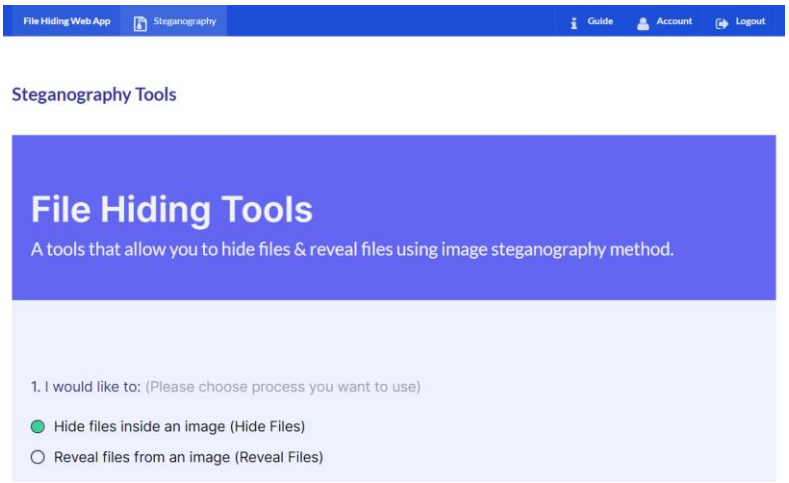
- **Logged in as normal users**

Step 1: After successfully log into the system, users will directly go to the account page.

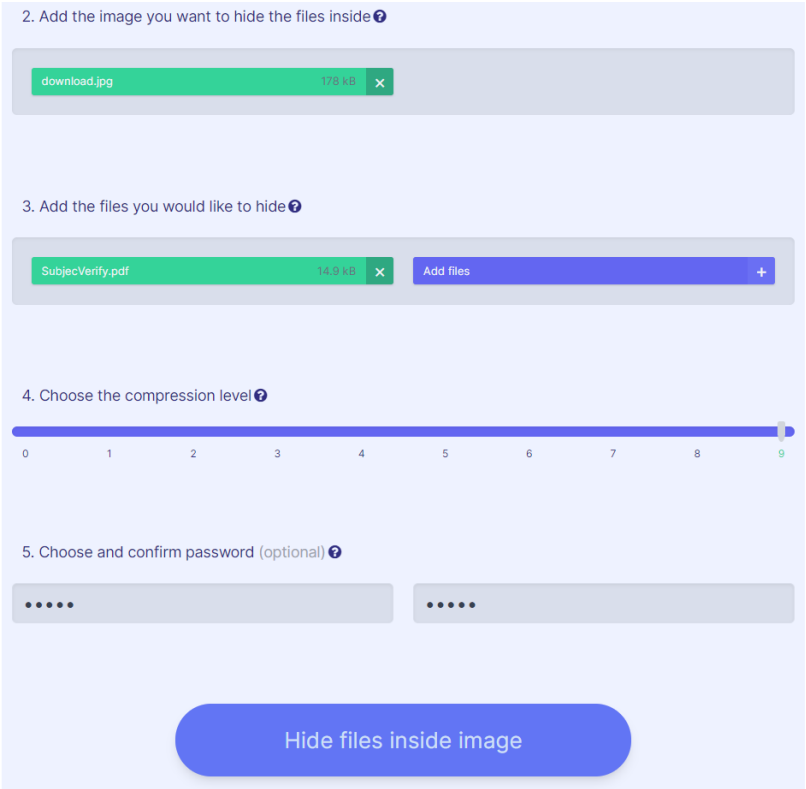


- **Hiding the files inside an image**

  Step 1: To hide the files inside an image, users must click the 'Steganography' menu first, then they will go to the steganography page. Then, users must choose the hiding process which is 'Hide files inside an image (Hide Files)'.



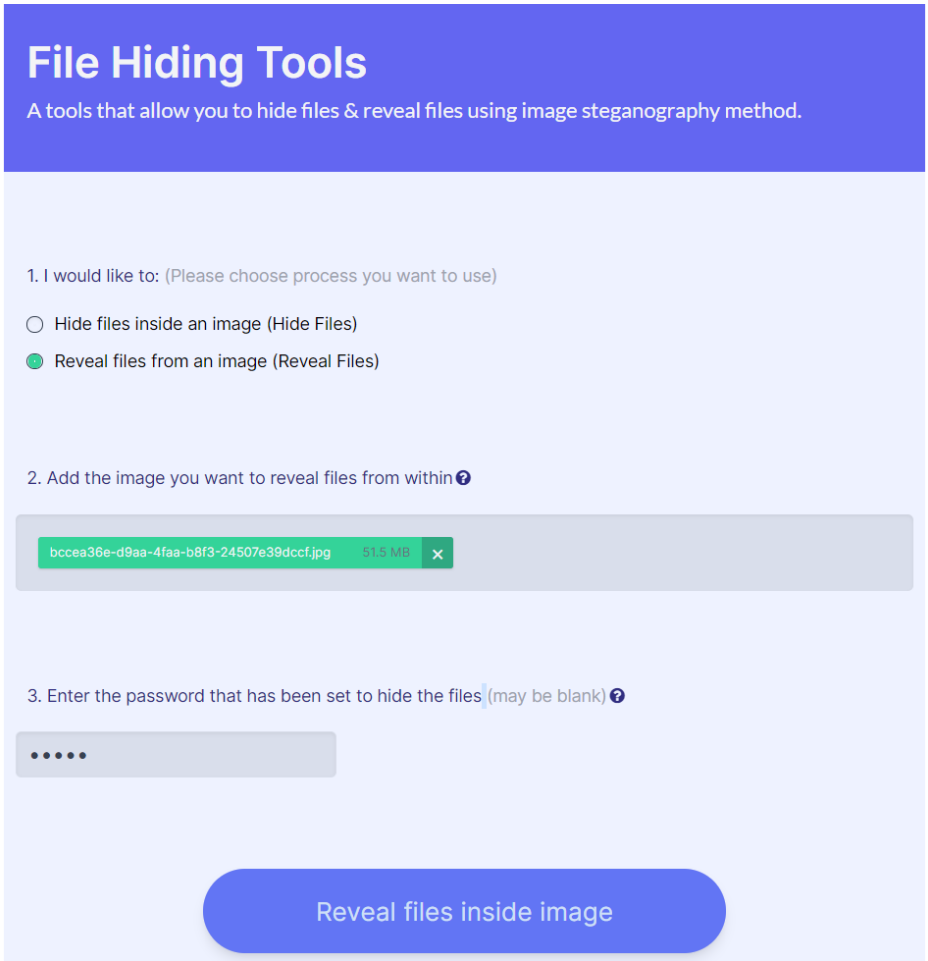
  Step 2: Then, follow the step given such as add the image files, add the files that you want to hide, choose the compression level, and lastly enter the password to encrypt the hidden files. After finished follow the step, the user must click the 'Hide files inside image' button to proceed with the process of hiding the files. After the process completed, the system will provide a download button and users need to click it to download and save the image files which contained the hidden files.



- **Revealing the files inside an image**

  Step 1: To reveal the files contained inside an image, users must click the 'Steganography' menu first, then they will go to the steganography page. Then, users must choose the revealing process which is 'Reveal files inside an image (Reveal Files)'.

  Step 2: Then, follow the step given such as add the image files which contained hidden files and enter the password that has been set to encrypt the hidden files. After finished follow the step, the user must click the 'Reveal files inside image' button to proceed with the process of revealing the files. After the process is completed, the system will provide a download button and users need to click it to download and save the hidden files that have been revealed.



Appendix C – Turnitin Result

Full Report of FYP

ORIGINALITY REPORT

5%	4%	2%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.scribd.com Internet Source	<1 %
2	auth0.com Internet Source	<1 %
3	www.ermt.net Internet Source	<1 %
4	www.fool.com Internet Source	<1 %
5	www.thecrazyprogrammer.com Internet Source	<1 %
6	www.geeksforgeeks.org Internet Source	<1 %
7	www.pelock.com Internet Source	<1 %
8	en.wikibooks.org Internet Source	<1 %
9	deenoverduniya.wordpress.com Internet Source	<1 %

10	eprints.utem.edu.my Internet Source	<1 %
11	Marcus Kim, Eddy Krygiel, Lance Kirby. "Mastering Autodesk® Revit® for Architecture", Wiley, 2017 Publication	<1 %
12	www.thedigitalmentor.com Internet Source	<1 %
13	dspace.fsktm.um.edu.my Internet Source	<1 %
14	vibdoc.com Internet Source	<1 %
15	tutorsonspot.com Internet Source	<1 %
16	repositorio.uam.es Internet Source	<1 %
17	wdc65xx.com Internet Source	<1 %
18	M.M. Amin, M. Salleh, S. Ibrahim, M.R. Katmin, M.Z.I. Shamsuddin. "Information hiding using steganography", 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings., 2003 Publication	<1 %

19	Afnan Alsadhan, Asma Alotaibi, Lulu Altamran, Majd Almalki, Moneera Alfulaij, Tarfa Almoneef. "Manar: An Arabic Game-based Application Aimed for Teaching Cybersecurity using Image Processing", International Journal of Advanced Computer Science and Applications, 2020 Publication	<1 %
20	en.wikipedia.org Internet Source	<1 %
21	rhimrj.com Internet Source	<1 %
22	www.uniqwa.ac.za Internet Source	<1 %
23	studentsrepo.um.edu.my Internet Source	<1 %
24	Timothy "Thor" Mullen. "The Interface", Elsevier BV, 2016 Publication	<1 %
25	etd.aau.edu.et Internet Source	<1 %
26	Petros Zaris, Harald Gjermundrod. "NoteLocker: Simple Secure Storage Service", 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and	<1 %

	Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS), 2014 Publication	
27	Yili Luo, Jia Fan, Chunhua Deng, Yixin Li, Yue Zheng, Jianwei Ding. "Accountable Data Sharing Scheme Based on Blockchain and SGX", 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019 Publication	<1 %
28	Alessandro Del Sole. "Visual Studio Code Distilled", Springer Science and Business Media LLC, 2019 Publication	<1 %
29	mafiadoc.com Internet Source	<1 %
30	"Managing Technology-Based Projects", Wiley, 2014 Publication	<1 %
31	www.carbonblack.com Internet Source	<1 %
32	student.blog.dinus.ac.id Internet Source	<1 %
33	argon.ess.washington.edu Internet Source	<1 %

34	opus.govst.edu Internet Source	<1 %
35	go2kennewick.com Internet Source	<1 %
36	Tony Steidler-Dennison. "Mac for Linux Geeks", Springer Science and Business Media LLC, 2009 Publication	<1 %
37	link.springer.com Internet Source	<1 %
38	hdl.handle.net Internet Source	<1 %
39	ethesis.nitrkl.ac.in Internet Source	<1 %
40	Gautam Siwach, Amir Esmailpour. "LTE Security potential vulnerability and algorithm enhancements", 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 2014 Publication	<1 %
41	Balakrishnan Ramalingam, Rengarajan Amirtharajan, John Bosco Balaguru Rayappan. "Multiplexed stego path on reconfigurable hardware: A novel random approach", Computers & Electrical Engineering, 2016 Publication	<1 %

42	www.etutorialspoint.com Internet Source	<1 %
43	medium.com Internet Source	<1 %
44	"Transactions on Computational Collective Intelligence VIII", Springer Science and Business Media LLC, 2012 Publication	<1 %
45	vuir.vu.edu.au Internet Source	<1 %
46	Jamie O'Brien. "Reasoning with graphs", Elsevier BV, 2014 Publication	<1 %
47	repozitorij.etfos.hr Internet Source	<1 %
48	Aya Y. AlKhamese, Wafaa R. Shabana, Ibrahim M. Hanafy. "Data Security in Cloud Computing Using Steganography: A Review", 2019 International Conference on Innovative Trends in Computer Engineering (ITCE), 2019 Publication	<1 %
49	Joe Micallef. "Beginning Design for 3D Printing", Springer Nature, 2015 Publication	<1 %
50	Nihad Ahmad Hassan, Rami Hijazi. "Data Hiding Using Steganographic Techniques",	<1 %

	Elsevier BV, 2017 Publication	
51	www.tara.tcd.ie Internet Source	<1 %
52	laptopunderbudget.com Internet Source	<1 %
53	www.netbooknews.com Internet Source	<1 %
54	www.diva-portal.org Internet Source	<1 %
55	rspublication.com Internet Source	<1 %
56	www.guru99.com Internet Source	<1 %
57	www.mts-recovery.com Internet Source	<1 %
58	www.masteringblockchain.com Internet Source	<1 %
59	kb.vircom.com Internet Source	<1 %
60	"A Glossary of Blockchain Terms*", Emerald, 2021 Publication	<1 %
61	repository.tudelft.nl Internet Source	<1 %

62	commons.wmu.se Internet Source	<1 %
63	scholar.uwindsor.ca Internet Source	<1 %
64	"Advances in Networks and Communications", Springer Science and Business Media LLC, 2011 Publication	<1 %
65	B WHITLOCK. "Grounding and InterfacingHandbook for Sound Engineers by Bill Whitlock", Audio Engineering Explained-for professional audio recording, 2010 Publication	<1 %
66	www.slideshare.net Internet Source	<1 %
67	istqbquestionbank.blogspot.com Internet Source	<1 %
68	etheses.dur.ac.uk Internet Source	<1 %
69	download.cnet.com Internet Source	<1 %
70	Alan G. Konheim. "Hashing in Computer Science", Wiley, 2010 Publication	<1 %
71	actionresearch.net Internet Source	<1 %

72	Dan Rahmel. "Advanced Joomla!", Springer Nature, 2013 Publication	<1 %
73	Alan P. Parkes. "Phrase Structure Languages and Turing Machines", Undergraduate Topics in Computer Science, 2008 Publication	<1 %
74	duepublico.uni-duisburg-essen.de:443 Internet Source	<1 %
75	epubs.surrey.ac.uk Internet Source	<1 %
76	www.techsource.com Internet Source	<1 %
77	www.coursehero.com Internet Source	<1 %
78	R KITCHEN. "X-rays and X-ray measuring instruments", RF and Microwave Radiation Safety, 2001 Publication	<1 %
79	www.softwaretestingclass.com Internet Source	<1 %
80	researchonline.ljmu.ac.uk Internet Source	<1 %
81	"Information Systems and Management in Media and Entertainment Industries",	<1 %

	Springer Science and Business Media LLC, 2016 Publication	
82	Benkwitz, Alexander(Lütkepohl, Helmut and Uhlig, Harald). "<> software JMulTi", Wirtschaftswissenschaftliche Fakultät, 2002. Publication	<1 %
83	epdf.tips Internet Source	<1 %
84	Rachel Andrew, Rob Turnbull, Alan Foley, Drew McLellan. "ASP Web Development with Macromedia Dreamweaver MX 2004", Springer Science and Business Media LLC, 2004 Publication	<1 %
85	vaskoedo.wordpress.com Internet Source	<1 %
86	"The Death of the Internet", Wiley, 2012 Publication	<1 %
87	Anna Mette Fuglseth, Siri Pettersen Strandenes. "NorshipS: A decision support system for analyses of bulk shipping markets", Computers in Human Behavior, 1997 Publication	<1 %
88	gnanavelrec.files.wordpress.com Internet Source	<1 %

89	xml.coverpages.org Internet Source	<1 %
90	bvucoepune.edu.in Internet Source	<1 %
91	inspire.redlands.edu Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Appendix D – Log Book

KOLEJ UNIVERSITI POLY-TECH MARA KUALA LUMPUR

FACULTY OF COMPUTING & MULTIMEDIA (FCOM)

INFORMATION SECURITY PROJECT 2
(NET403)

LOG BOOK

STUDENT'S NAME : **AMIRUL NAIM BIN MOHD SHAFIEE**
ID NO. : **AM1901005018**
SUPERVISOR : **NORALIZA BINTI AZIZAN**
PROJECT TITLE : **FILE HIDING WEB APPLICATION USING IMAGE STEGANOGRAPHY TECHNIQUES**

Week		Date	Agenda	Next Agenda	Signature (Supervisor / Coordinator)
23/11/2020 – 27/11/2020	1	25/11/2020	Final Year Project 2 Briefing.	Lecture on Chapter 6 and 7.	Coordinator
30/11/2020 – 4/12/2020	2	2/12/2020	Lecture on Chapter 6 and 7.	Lecture on Chapter 7 and 8.	Coordinator
7/12/2020 – 11/12/2020	3	9/12/2020	Lecture on Chapter 7 and 8.	Lecture on Chapter 8, 9 and 10.	Coordinator
14/12/2020 – 18/12/2020	4	16/12/2020	Lecture on Chapter 8, 9 and 10.	Start writing a report for Chapter 6 and developed the project.	Coordinator
21/12/2020 – 25/12/2020	5	21/12/2020	Writing a report for Chapter 6 and developed the project	Finished Chapter 6 report and deliver to Supervisor to evaluate.	Supervisor
28/12/2020 – 1/1/2021	6	1/1/2021	Receive feedback for report Chapter 6 from Supervisor.	Continue developing the system and writing report for Chapter 7 and 8.	Supervisor
4/1/2021 – 8/1/2021	7	4/1/2021	Devloped the system and writing report for Chapter 7 and 8.	Continue developing the system and writing report for Chapter 9 and 10.	Supervisor
9/1/2021 – 17/1/2021	**Mid Term Break**				
18/1/2021 – 22/1/2021	8	18/1/2021	Devloped the system and writing report for Chapter 9 and 10.	Show report and development progress to the Coordinator.	Supervisor
25/1/2021 – 29/1/2021	9	27/1/2021	Present the progress of the project to the Coordinator.	Review of the system development from Supervisor.	Coordinator
1/2/2021 – 5/2/2021	10	1/2/2021	Suggestion for the system development by Supervisor	Making Questionnaire for Beta Testing and Report for Chapter 8.	Supervisor
8/2/2021 – 12/2/2021	11	11/2/2021	Deliver Questionnaire to Supervisor to be evaluate and distribute it.	Lecture on the preparation of final presentation.	Supervisor
15/2/2021 – 19/2/2021	12	17/2/2021	Lecture on the preparation of final presentation.	Deliver completed report and completed system to Supervisor	Coordinator
27/2/2021 – 26/2/2021	13	26/2/2021	Report and system feedback received and proceed to making a correction.	Submission of Hardbound Final Report and System to Coordinator.	Supervisor
1/3/2021 – 5/3/2021	14	Submission of Hardbound Final Report to Coordinator ***(5/3/2021)			