CHAPTER 5: System Design

The objective of system design is to pass on the requirements as stated in system analysis. System design consists of logical and physical design where the logical design explains the structure and activities in the system like designing the system’s input and output while physical design shows the actual system. The system design plays a significant role for the application. This is because a proper design is needed when it comes to the image and security as these two matters are sensitive and indifferent.

5.1 System Architecture

An important feature that is used to generate an encrypted image is the blocks position in the image. Blocks positions are measured based on their relations of dimensions and quantity of block that determined earlier. This process is shown in Figure 5.1.

Figure 5.1 Combinations of Image and Password

Once the image is acquired, it will be divided into a few blocks depending on the image dimensions.
For example, an image is divided into 100 blocks as shown in Figure 5.2 below.

![Figure 5.2 Blocks in Original Image](image)

The location of the new blocks based on the given array of encryption, namely

\[ \text{rie} = \{54, 19, 6, 69, 32, 16, 57, 38, 26, 44, 4, 49, 56, 36, 41, 66, 20, 14, 82, 43, 86, 80, 85, 90, 58, 59, 18, 53, 52, 40, 15, 45, 25, 96, 68, 2, 88, 17, 47, 28, 71, 22, 48, 78, 84, 12, 83, 79, 34, 75, 9, 67, 1, 70, 95, 76, 8, 5, 10, 64, 91, 93, 98, 72, 92, 97, 62, 30, 73, 65, 29, 51, 39, 31, 35, 42, 13, 0, 81, 24, 99, 50, 74, 89, 23, 27, 77, 7, 11, 46, 21, 94, 55, 33, 63, 3, 60, 87, 37, 61\}, \]

is shown in Figure 5.3.

![Figure 5.3 Blocks in Encrypted Image](image)
For this particular rie, only specific complementary decryption array can be used to reassemble back the position of the blocks. Based on the value and the result in Figure 5.3, the value of complement array, rid should be, \( r_i d = \{77, 52, 35, 95, 10, 57, 2, 87, 56, 50, 58, 88, 45, 76, 17, 30, 5, 37, 26, 1, 16, 90, 41, 84, 79, 32, 8, 85, 39, 70, 67, 73, 4, 93, 48, 74, 13, 98, 7, 72, 29, 14, 75, 19, 9, 31, 89, 38, 42, 11, 81, 71, 28, 27, 0, 92, 12, 6, 24, 25, 96, 99, 66, 94, 59, 69, 15, 51, 34, 3, 53, 40, 63, 68, 82, 49, 55, 86, 43, 47, 21, 78, 18, 46, 44, 22, 20, 97, 36, 83, 23, 60, 64, 61, 91, 54, 33, 65, 62, 80\} \\

Due to time constraint, the relation between rie and rid cannot be translated in terms of mathematical formula. This thesis is only covered selected rie and rid that has been provided earlier. Further studies should be done to determine its formula to increase efficiency and effectiveness as the current application hardcode both rie and rid into the coding.

There are four classes in the application that has been used in for the system architecture. The classes are the FrontPage.java, HashHandler.java, Jumble.java, and MD5.java. Each of these classes brings specific function of architecture that develops the application further. The system architecture for this application is as below;

The FrontPage.java is the parent class that connects all the other classes for the application to work in the application built. From the figure above, it can be seen that it is divided by two tab, encryption and decryption tab. The application contains the GUI of the application where there are a button, a tab, and a preview pane for the picture. It is functioning to browse the particular picture, preview the original and result pictures, column for inserting password, and save button. Such system architecture is made easy because it will ease the function of the application. The application also can be classified as user friendly according to the system architecture.
Futhermore, HashHandler.java class acts as intermediary to the MD5.java class. It has to handle hashing process, comparing, saving and retrieving, the hash result from the image selected. When the MD5.java does all the calculation of the MD5 hash algorithm, the Jumble.java class will be used to load, flip and then jumble the selected image. These architectures are based on the programming and functioning of the application. The proposed architecture gives smooth process when it comes to the building of the application in the latter process.

5.2 Program Design

The program design for the system must guarantee to satisfy the user requirement stated in the previous section. Besides that, the program design is suppose to be easy to read and understand by others. This is to allow if any adjustment are needed to be made in the future. Speaking of adjustment, the system must be design to have room for changes.

In the Image Encryption’s design for the thesis, it has guaranteed to satisfy the requirement because it is easy to read and understand by the user and even the user from non-computer background.

5.2.1 System Flowchart

Figure 5.4 illustrates the conceptual flows of the processes that will be involved in the proposed image encryption application. In the image encryption process, the user will browse for a specific image file that they would like to transfer securely. Once it has been selected, the user is required to enter a password. The password will be used to encrypt the selected image file and it is the very same password that required when the image needs to decrypt once it reached its intended recipient.
5.2.1.1 Encryption Flowchart

Figure 5.5 will illustrate the flow of encryption process.
5.2.1.2 Decryption Flowchart

Figure 5.6 will illustrate the flow of decryption process.

![Decryption Flowchart](image)

Figure 5.6 Decryption Flowchart

5.3 User Interface

The application user interface is designed using Java Swing feature provided by Netbeans. The user interfaces help the users to navigate through the application. Provided that most of the users are familiar with simple application navigation, this application is easy to be used. User interface also provides a transparent layer between the system and the users.

Each interface have distinctive and standardize features so that the system will not be complicated to understand. Every single interface lies in the system has its own functions which are shown directly and clearly for the users’ ease.
5.3.1 Screen Design

The screen is designed with user friendly and simple function yet powerful security. Some of the screen shot are provided in this section.

Interface for Encryption Tab (Main Menu)

In this tab, encryption process takes place. The function available is acquiring an image, display/preview it on preview pane, insert password, encrypt the image, and save the result image. Figure 5.7 below show the encryption tab.

![Encryption Tab](image)

Figure 5.7 Encryption Tab
Interface for Decryption Tab

In this tab, decryption process takes place. The function available is acquiring an encrypted image, display/preview it on preview pane, insert password, decrypt the image, and save the result image. Figure 5.8 below show the decryption tab.

![Decryption Tab](image)

Figure 5.8 Decryption Tab

Interface for Opening an Image

Figure 5.9 below is the interface for opening/selecting image file browser. The window is called when the user is clicking the browse button.

![Open File Window](image)

Figure 5.9 Open File Window
Warning for Wrong Password

When the user receiver input the wrong password, the warning as shown in the Figure 5.10 below will be shown.

Figure 5.10 Wrong Password Warning