IMAGE ENCRYPTION “FIENDEC”

by

MUHAMAD FAIZ BIN MUHAMAD LATIF (WEK060071)

A thesis submitted in partial fulfillment of the requirements for the degree of

Bachelor Degree of Computer Science

University of Malaya

2009
## TABLE OF CONTENTS

ACKNOWLEDGEMENT ............................................................................................................... 1

ABSTRACT .................................................................................................................................. 2

CHAPTER 1: Introduction .......................................................................................................... 3
  1.1 Problem Statement ........................................................................................................ 4
  1.2 Project Objectives ...................................................................................................... 5
  1.3 Project Scopes ............................................................................................................ 5
  1.4 Project Significance .................................................................................................. 6
  1.5 Project Schedule ....................................................................................................... 6

CHAPTER 2: Literature Review ................................................................................................. 7
  2.1 Previous Works ......................................................................................................... 7
  2.2 Programming Language .......................................................................................... 10
  2.3 Cryptosystems: Hash Functions and One-Time Pad ............................................... 11

CHAPTER 3: System Methodology .......................................................................................... 13
  3.1 System Analysis ....................................................................................................... 15
  3.2 System and Object Design ...................................................................................... 15
  3.3 System Implementation ............................................................................................ 16
  3.4 System Testing ......................................................................................................... 16
  3.5 System Deployment .................................................................................................. 17
  3.6 Maintenance ............................................................................................................ 17
  3.7 Advantages and Disadvantages of Waterfall Model ................................................ 18

CHAPTER 4: System Analysis .................................................................................................. 20
  4.1 System Requirements .............................................................................................. 20
    4.1.1 Functional Requirements .................................................................................. 20
    4.1.2 Non-Functional Requirements ......................................................................... 21
  4.2 Hardware Requirement ............................................................................................. 23
  4.3 Software Requirement ............................................................................................... 24
  4.4 Tools and Technology to be Used .......................................................................... 24

CHAPTER 5: System Design ...................................................................................................... 26
  5.1 System Architecture ................................................................................................. 26
LIST OF ILLUSTRATIONS

Figure 2.1 Image Encryption Algorithm Property Comparison Table ........................................ 8
Figure 2.2 An Overview Diagram of the Proposed Technique ................................................. 9
Figure 2.3 The Architecture of the Image Encryption and Decryption Model ..................... 10
Figure 3.1 General Overview of Waterfall Model .................................................................... 14
Figure 5.1 Combinations of Image and Password .................................................................. 26
Figure 5.2 Blocks in Original Image ....................................................................................... 27
Figure 5.3 Blocks in Encrypted Image ...................................................................................... 27
Figure 5.4 System Flow ............................................................................................................ 30
Figure 5.5 Encryption Flowchart ............................................................................................. 30
Figure 5.6 Decryption Flowchart ............................................................................................ 31
Figure 5.7 Encryption Tab .......................................................................................................... 32
Figure 5.8 Decryption Tab .......................................................................................................... 33
Figure 5.9 Open File Window ................................................................................................... 33
Figure 5.10 Wrong Password Warning ................................................................................... 34
Figure 6.1 Netbeans IDE 6.7.1 workspace ............................................................................. 36
Figure 6.2 Basic Java application template .............................................................................. 37
Figure 6.3 Image Jumbling Coding ......................................................................................... 38
Figure 6.4 Image Flipping Coding ............................................................................................ 39
Figure 6.5 Embedding Hash in Image ...................................................................................... 40
Figure 6.6 Acquire an Image and Set The Preview ................................................................. 41
Figure 6.7 Hash Generation ...................................................................................................... 41
Figure 6.8 Hash Saving Into The Image ................................................................................... 41
Table 7.1 Unit Testing Done .................................................................................................... 46
Figure 8.1 Original Lena picture .............................................................................................. 49
Figure 8.2 Normal Image Encryption Result ........................................................................... 49
Figure 8.3 The Application Encryption Result ......................................................................... 49
Table A.1 Project Schedule ...................................................................................................... 55
Figure B.1 NetBeans IDE with the File > New Project menu item selected ......................... 56
Figure B.2 NetBeans IDE, New Project wizard, Choose Project page ................................. 57
Figure B.3 NetBeans IDE, New Project wizard, Name and Location page ......................... 57
Figure B.4 NetBeans IDE with the HelloWorldApp project open ........................................ 57
ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious, the Most Merciful

All praise is due to Allah

In completing this thesis entitled Image Encryption, I owed much kindness and thoughtfulness from my devoted project advisor, Mrs. Hannyzura Pal @Affal. Without her supervision and guidance it will be more difficult to me to finish the research and the documentation. I also admired her passionate assistance in encouraging me to work on the thesis as it has in the paper. The paper contains much of her positive criticism, sharing thoughts and sincere advice. My greatest my respectfulness and gratefulness are belong to her.

The sincere thankfulness and credit are given to my beloved parents and supporting friends. I have to admit that I will never have the guts to finish the thesis without their encouragements and assistances. To my parents even though they did not support me academically, they help me financially and morally. It is to them also I seek advice and pamper whenever difficulties arise in finishing the thesis. My kindness friends also support me faithfully in assisting me matters that I did not understand and to them also I asked for help and guidance. There is a lot labour that my friends and I have worked out in the thesis.

I will like to fill the rest acknowledgement with a little note of appreciation to my faculty, Faculty of Computer Science and Information Technology (FCSIT) for giving me such invaluable opportunity and experience in making the thesis. I managed to challenge my 3 years knowledge as a networking student in FCSIT to produce this thesis. The thesis also helps me to have better understanding on what I have learned in the FCSIT as well as to implement my knowledge in real situation.

It is my deepest hope that this work of thesis can benefit the society and the related area. May the security of the data images will be more secured than before with the outcome of this thesis.
ABSTRACT

With the fast progression of data exchange in electronic way, it is important to protect the confidentiality of images data from unauthorized access. This paper proposed an application of Image Encryption that can encrypt and decrypt an image file provided with password along with its algorithm. The proposed application has referred to many past literatures that related to the study. Derived from the past works implementation of programming languages such as Java and C#, Netbeans IDE 6.7.1 is used to develop a Graphical User Interface (GUI) of the Image Encryption Application. It also explains in specific manner the algorithm works as well the use of Block Based Image Transformation. The paper is strictly follow the Waterfall model as its system methodology. The paper also contains detail information of the system development, system design, system analysis, system implementation and system testing. Such details help to develop the application in correct way because it has been done step by step and in sequence manner.

Keyword – Image encryption, Block Based Image Transformation, Image Encryption Application
CHAPTER 1: Introduction

Nowadays, security issue becomes more important especially when it comes to the use of Internet and other networks. Security breaches may affect user’s privacy and reputation. Due to this risk, various measurements have already been taken to prevent security breaches in the network. One example that has been made due to this problem is an encryption. Data encryption is an important way to protect data before it can be transmitted over any networks. Encryption is defined as modifying information into a special code, especially in order to prevent unauthorized users to have access to the information. Decryption on the other hand is the opposite meaning of encryption.

As the number of the Internet users increase exponentially, the needs to protect the information on the Internet has become a high priority. The effects of security breaches are more disastrous to organizations that depending highly on the usage of the network in their daily processing. Most of the processes in medicine, engineering and military departments are dealing with data which are in the form of image. This form of data has a high risk of being retrieved by unauthorized person since it can be easily break in and up to the danger of being exposed to the public. Without any doubt, the risks of images data can bring a loss of profit, lower the integrity, violate the prestige and many other disadvantages to the company involved. To note here that it is not a problem to the high-tech sectors but also to the real world scene. In real life situation, supposedly that we want to send a picture in a contest, of course we did not want others to see it especially the other contestants.

Apart from that, picture is also an important tool to decipher meaning. Old sayings once said that a picture is worth a thousand words. This shows that pictures are important in conveying meaning. Thus, it is also important to protect it apart from protecting textual data that much of the security concern with. Most of today’s encryption algorithm is based on
textual data. These encryption algorithms may not be suitable for encrypting image data types and not give proper attention to the sensitivity of image types.

There are various data encryption systems to encrypt and decrypt data available like Advanced Encryption Standard (AES), Blowfish, Data Encryption Standard (DES), Triple DES, Serpent, and Twofish but there none of the encryption algorithms satisfy the different image types like JPEG, TIFF, PNG, and BMP. In this thesis, it uses the possibility to alter the pixel location of the picture. By using the possibility, the encryption and decryption process explain later in the paper has worked with various types of images that the previous encryption algorithms have imagined before.

An application has been developed to encrypt image data types before the image can be transmitted over the network. The application encrypts selected image based on combination of block-based transformation and pixel offset techniques.

1.1 Problem Statement

Protecting some of the images are as important as protecting the textual data and perhaps much more important. Limitations in protecting the images based on their types must be eliminated. In encrypting images, there is a need to protect its content regardless of the types. There are various image encryption algorithms but none of them can work with various image types like JPEG, TIFF, PNG, and BMP unlike this application.

This application has successfully eliminated the limitation problems. The algorithm modified the position of the pixels, which is the mutual property of the images. Thus, various image types can be encrypted using the application.
1.2 Project Objectives

There are three objectives that have been achieved from this thesis and as to make the application possible. The first one is to study the architecture of image file. The study is focused to JPG file type because it is one of the most popular image formats used. The second objective is to develop an application that can be used to encrypt an image file. This application must be simple, easy to use, and powerful. Many factors have been considered in order to develop this application such as processing speed of image, the strength of the encryption result and ease of use to end user. The last objective of this thesis is to make sure that the password handling process is not carelessly implemented. Failure of the password feature in this application will affect its integrity and reputation. All of the objectives achieved give a good outcome in the project.

1.3 Project Scopes

The idea of this project is to develop an image encryption application. The project scopes are based on Netbeans IDE 6.7.1, Java 2D™ API and MD5 (the one way encryption algorithm). All of the scopes help as below;

1. Netbeans IDE 6.7.1.
   - This application enables to edit any Java coding that is relevant for the project.

2. Java 2D™ API
   - This API is imported to the source code and enable actions such as reading/loading, drawing, creating, and writing/saving an image
3. The one way encryption algorithm (MD5)
   - MD5 is used to verify the correct password entered to decrypt the encrypted image.

1.4 Project Significance

The application has the capability to protect sensitive image file from being exposed to the unauthorized users while being transferred or when it reaches its target destination. The modification performed by the application whereby once the image file is encrypted by the application, it can only be retrieved back or decrypted by itself only. The project also provides user with the ease of use concept and faster processing time. It also introduces safer and powerful protected data.

1.5 Project Schedule

Refer to [APPENDIX A].