An image encryption tool for securing digital evidence in the National Police Service.

Student No: 095108

Group: C

An Information Systems Project Proposal Submitted to the Faculty of Information Technology in partial fulfillment of the requirements for the award of a Degree in Business Information Technology

Date of Submission: 27th January 2021

Declaration and Approval

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the research proposal contains no material previously published or written by another person except where due reference is made in the research proposal itself.

Student:

Sign:

Date: ___27th June 2021___ .

Supervisor:

Abstract

Following the global advancement of technology in the recent years, digital evidence has become an important tool in the preparation of court cases and also the solving of crime. Digital evidence is any kind of information that is stored or transmitted in binary form that may be depended upon in a court of law. Digital evidence can be found on any electronic device. On the contrary, there has been a rise in the number of cybercrime cases which poses a threat to the success of digital evidence in the process of case solving. An official cybercrime report predicted that cases will be quadruple and will cost $6 trillion dollars by 2021. Protecting the integrity of digital evidence in court cases is important as it helps the courts in delivering fair judgements.

The aim of this research was to develop an automated tool that assists law enforcement agencies in Kenya to conserve the integrity of digital evidence during the process of sharing evidence with other collaborating agencies. The developed tool preserves integrity of evidence using a 128 bits *Advanced Encryption Standard* (AES) image encryption algorithm that is accompanied by a user interface that helps the user select files to be shared and also assists the user to encrypt and decrypt the files. This makes sure the evidence is not tampered with before it reaches its destination. This project ensured the development of an efficient and reliable system that takes less computational time and consumes less power.

The study used waterfall methodology since it follows a list of phases whereby each phase has to be accomplished before going on to the next phase. This methodology was of benefit to the study since it was easy to manage, and it also works best for small projects. Tools used in the project development included, java programming language, MySQL database tool, Eclipse IDE, cryptographic Java packages and the AES algorithm.

Table of Contents

List of Figures

List of Tables

Abbreviations/Acronyms

NPS	National Police Service
DES	Data Encryption Standard
RSA	Rivest-Shamir-Adleman
AES	Advanced Encryption Standard

Chapter 1: Introduction

1.1 Background Information

Cybercrime is the activity related to the exploitation of data, computers, information systems and cyberspace for personal, economic or psychological gain (Mohd, Arief, & Gross, 2015). Cybercrime which is also known as computer crime exists in three different forms namely computer as a target, computer as a tool or computer as an accomplice to crime (Clough, 2015). Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. This is a result of the development and improvement of information technology over the years.

The development and improvement of information technology has had an impact on the openness of various forms of cybercrimes committed by individuals and groups. A significant number of cyber-related crimes include; denial of services, phishing, spying, spoofing, sniffing, attacks, masquerade and hijack (Warner, 2011). It is estimated that cybercrime damages will cost the world an amount equivalent to six trillion dollars annually by 2021, up from three trillion dollars in 2015 (The 2020 Cybercrime Report, 2020). However, this only pertains to what is reported, and a lot remains unreported. The fast growth of the internet and other shared networking systems and their respective applications has brought about a high request to protect communities and other public entities against vicious malware and cybercrime acts (Kimberly & Dhruba, 2016). According to the Overseas Security Advisory Council Report there are an estimated 3000 cyber-crime incidences that are reported in Kenya every month.

As a result of technological advancements, digital evidence has become an important factor in the solving of crimes by law enforcers (Sean & Robert, 2015). Security officers rely broadly on digital evidence for crucial intelligence concerning both suspects and victims. In cases where digital evidence is limited, the probability of solving the case becomes low thus signifying the importance of digital evidence.

Digital evidence largely consists of digital images. The advancement of digital imaging technologies has brought about various threats to the credibility and purity of digital images since they can now be generated, edited or even tampered with. All this can be done without one leaving a trace of their cybercrime (Dehnie, 2006).

On the seventh day of January the year 2019, the Kenyan National Police Service for the first time in its history launched an Information Management System that aims at digitizing all Police records including the Occurrence Book, Personnel management, Crime Management and Administrative Systems (NPS, 2019). Though one of the goals of the system is to facilitate ease of sharing information, especially criminal records between the Police and Judiciary, no advanced technological strategy has been implemented to ensure the security of the information sharing process. Evidence must be sufficiently reliable in order for it to be admissible in the solving of a case. Evidence that is of questionable integrity can't be used in case solving thus the need to ensure its security.

1.2 Problem Statement

The National Police Service Information Management System lacks a tool that provides security while also ensuring privacy and credibility during the process of sharing of evidence that is in a digital image format. This makes the National Police Service prone to attacks from hackers or even malicious software which may jeopardize the solving of cases thus causing a backlog. This might also result in unfair conclusion of cases if the credibility of the evidence is not affirmative.

1.3 Aim

In order to address the problem identified in Section 1.2, this project aimed at developing an image encryption tool that ensures high security levels, less computational time and power in the most reliable and efficient manner during the sharing of evidence within a shared network.

1.4 Specific Objectives

i. To identify common challenges faced by law enforcement agencies in sharing of digital evidence.

ii. To review existing solutions used in ensuring the security of evidence that is being shared electronically in a shared network.

iii. To design a tool that helps police officers share evidence securely.

iv. To test the proposed image encryption tool and validate its effectiveness.

1.5 Justification

This project will help ensure the security of digital evidence since it will be inaccessible to unauthorized personnel. It will also ensure credibility of digital evidence thus assisting criminal suspects and victims experience a fair hearing of cases at the courts of law. The project will help reduce backlogs of cases in courts of law since the evidence will be easy to retrieve and credible.

1.6 Scope and Limitations

1.6.1 Scope

Although there are many image encryption techniques only a couple of them are suitable for the shared network systems. The main scope of my project was to provide security for the images in the networking systems. My project provides a safe means of the transfer of images between the networking systems confidentially.

1.6.2 Limitations

It was challenging to obtain extensive information concerning the systems in place in the National Police Service due to their confidentiality protocols. However, I went to my local police station and explained to the officer in-charge about my final year project. Luckily enough, the officer granted my request of answering of a limited number of research questions related to my project.

Chapter 2: Literature Review

2.1 Introduction

This chapter discusses the present system of evidence handling at the NPS, the challenges faced by law enforcement agencies in sharing evidence, the existing solutions used to secure data in a shared network and the proposed image encryption tool. The chapter concludes with a conceptual model for the study. A review of significant research and publications by accredited scholars will help understand the concept of digital evidence and investigate the research problems.

2.2 Evidence handling at the National Police Service

A police information system comprises of people, computer equipment and related programs, accompanied by institutional procedures interacting in a defined systems design. One of the important functions of an information system in the police service is to facilitate the exchange of information among government units such as law enforcement agencies, criminal justice agencies and with the public (Whisenand, 1971).

On the 7th of January 2019, the National Police Service set in motion the implementation of an information management system aiming at the digitization of all police records (NPS, 2019). This system was meant to replace the physical occurrence book (O.B) and physical case file management systems. According to the Inspector General of Police, Mr. Hilary Nzioki Mutyambai, the previous system was burdensome and difficult to retrieve data on nature of predominating crimes in different locations across the country (Mutwiri, 2019). The implementation of the information management system is still ongoing which means that the analogue case management system is still in use in most parts of the country.

In the analogue case management system, the majority of evidence handled is physical thus is tiresome to work with. The evidence is recorded manually in books and later on stored in the relevant security facilities.

All recorded evidence data in the analogue case management system is in the process of being digitized and afterwards being saved in a database. This will ensure transparency in the conduct

of police operations since all files and police records will be available at the click of a mouse button thus ensuring no loss of files. All facilities equipped with the system are to be connected to a shared network to facilitate the ease of sharing information, especially criminal records between the law enforcement agencies and Judiciary.

2.3 Challenges faced by law enforcement agencies in the sharing of evidence.

The police service is seen as the most corrupt institution in Kenya. According to the East Africa Bribery Index (EABI) 2012, the National Police service still leads as the most corrupt public sector with the likelihood of bribery being at 60% The police service is seen as the most corrupt institution in Kenya. According to the East Africa Bribery Index (Transparency International, 2017), the National Police service still leads as the most corrupt public sector with the likelihood of bribery being at 60% The police service is seen as the most corrupt institution in Kenya. According to the East Africa Bribery Index (EABI) 2012, the National Police service still leads as the most corrupt public sector with the likelihood of bribery being at 60%.

Rank	Sector	2017(%)	2014(%)	Variance
1	Police	41.6	71.7	-30.1
2	Civil Registration	23.6		
3	Land Services	19.6	19.4	0.2
4	Business Licensing	17.7		
5	Judiciary	17.7	15.7	2
6	Medical and Health Services	9.6	10.5	-0.9
7	Tax Services	8.8	31.4	-22.6
8	*Huduma* Centers	7.6	-	0
9	Educational Institutions	7.9	13.4	-5.5
10	Utilities (Water and Electricity)	5.9	5.7	0.2

Table 2.1 East Africa Bribery Index Survey *Source (Transparency International, 2017)*

Corruption in the Police Service has been the root of various problems affecting the daily operations in the service including the security of case evidence. Allegations related to the loss, destruction and manipulation of multiple evidence some of which were vital in ongoing cases have been made against the NPS. This has exposed the impunity that the police service has embraced over the years. Previous case files have shown that police officers often decline to produce evidence to investigators and repeatedly fail to show up in court (Fick, 2018).

According to an undercover agent who has worked with the Kenya Police for eight years, suspects collude with vulnerable police officers to carry out mediocre investigations. This leads to the suspect(s) not being charged in court because of inadequate evidence through witness accounts thus weakening the charges (Mwololo, 2016). Once evidence is shared with other parties in an improper manner, its potential to resolve the case decreases.

2.4 Existing solutions used to secure data in a shared network

All digital services require reliable security in storage and transmission of digital images. To fulfill such security and privacy needs in various applications, encryption of images is important to minimize malicious attacks from unauthorized parties. Encryption means that the data or bits of any source are alternated in a specific pattern which is known to only the sender and receiver (Narasimhan & Rengarajan, 2014).

There are three ways in which encryption is implemented; symmetric cryptography, asymmetric cryptography and hash functions. In symmetric cryptography, a single secret key is used for both encryption and decryption. In asymmetric cryptography, one key is used for encryption and a different key used for decryption. Hash functions use a mathematical transformation to irreversibly encrypt information. Some of the encryption techniques used in network systems are Advanced Encryption Standard(AES), Rivest-Shamir-Adleman(RSA), Triple Data Encryption Standard(TripleDES), Twofish just to mention some (Stallings, 1999).

2.5 Proposed image encryption tool

This research proposes to come up with an automated tool that encrypts image evidence that is being transmitted from one user to another in a shared network. The proposed tool will use a chaos-based cryptographic algorithm. “Chaos is a branch of study in mathematics, physics and philosophy that reviews the ways of powerful systems which are highly sensitive to initial conditions” (Shyamala, 2011).

Chaotic-based encryption algorithms entail two processes; chaotic confusion and pixel diffusion. During the chaotic confusion stage, a combination of chaotic maps is used to implement the confusion of pixels in the image. The parameters of the chaotic maps are used for the confusion key. In the pixel diffusion stage, the value of each pixel changes one by one with using of the chaotic confusion stage. The parameters of the diffusion function are used for the diffusion key.

Many scientists have worked on chaos-based image encryption (symmetric cryptography) algorithms thus making it popular for image encryption. Chaotic cryptographic algorithms have suggested new ways to develop effective image encryption schemes. This method transforms the statistical characteristic of original image information. This makes it difficult for an unauthorized party to break the encryption. It provides an efficient way for real-time applications and transmission (Shyamala, 2011).

In the proposed symmetric key cryptography technique, a typical coupled map will be mixed with a one-dimensional chaotic map and used for high degree security image encryption while its speed is acceptable. This mixture application of chaotic maps shows advantages of large key space and high-level security. The cipher generated by this method is the same size as the plaintext. Similarly, a scientist by the name Jessica Fridrich showed how to adapt certain invertible chaotic two-dimensional maps on a square to create symmetric block encryption schemes (Fridrich, 1998).

The schemes are useful for encryption of large amounts of data, such as digital images or electronic databases. In this, a chaotic map is first generalized by introducing parameters and then sampled to a fixed square frame of points which represent pixels or some other data items. The sampled map is further extended to three dimensions and composed with a simple diffusion

mechanism. As a result, a block product encryption scheme is obtained. To encrypt an N x N image, the ciphering map is iteratively applied to the image. The main features of the encryption scheme studied are a variable key length, a relatively large block size, and a high encryption rate. The cipher is based on two dimensional chaotic maps, which are used for creating complex, key-dependent permutations.

Unlike most of today's symmetric encryption schemes, which rely on complex substitution rules while somewhat neglecting the role of permutations, the cipher is based on complex permutations composed with a relatively simple diffusion mechanism. A unique chaotic maps-based image encryption method has been proposed to improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps and design a key scheme for the resistance to cipher attack, differential attack and grey code attack. Because of the floating-point analytical computation outcome of the chaotic system, unauthorized users or attackers can attack cryptosystems effectively through certain structures. To increase the security level of the cryptosystem, combined approaches of chaotic and conventional crypto-graphic methods will be implemented.

To achieve high encryption speed, cryptographic methods using algebra-based transformation scrambling techniques will be used. Since the operations are simple, the encryption does not require high computation, but recent research suggests that Chaos-based transformations naturally have affine linearity while algebra-based transformations have fixed scrambling matrices for data encryption.

A related study to the proposed system is where a Poker shuffle is used for scrambling image, which is controlled dynamically by a chaotic system. This scrambling technique belongs to the position permutation and it has several features like non-linearity, non-analytic formula and large key space. In addition, it can deal with a non-square image while many scrambling methods with analytic formulas only work with square images and can be integrated into the existing image encryptions (Sarode, 2014).

To overcome these limitations in Logistic maps the nonlinear chaotic algorithm (NCA) map uses power function and tangent function instead of linear function. The chaotic secure system can be

used in applications that do not require a high level of information security such as remote keyless entry system, video phone, and wireless telephone.

2.6 Conceptual Framework

This is a conceptual diagram that shows how the proposed system functions. The user logs into the system according to their access level. Upon successful authentication of the user credentials, the user will be able to add an image to be encrypted, apply the chaotic algorithm and send it to the receiving client through a shared network. The receiving client will receive the shared file and will be able to decrypt it using the key provided by the host.

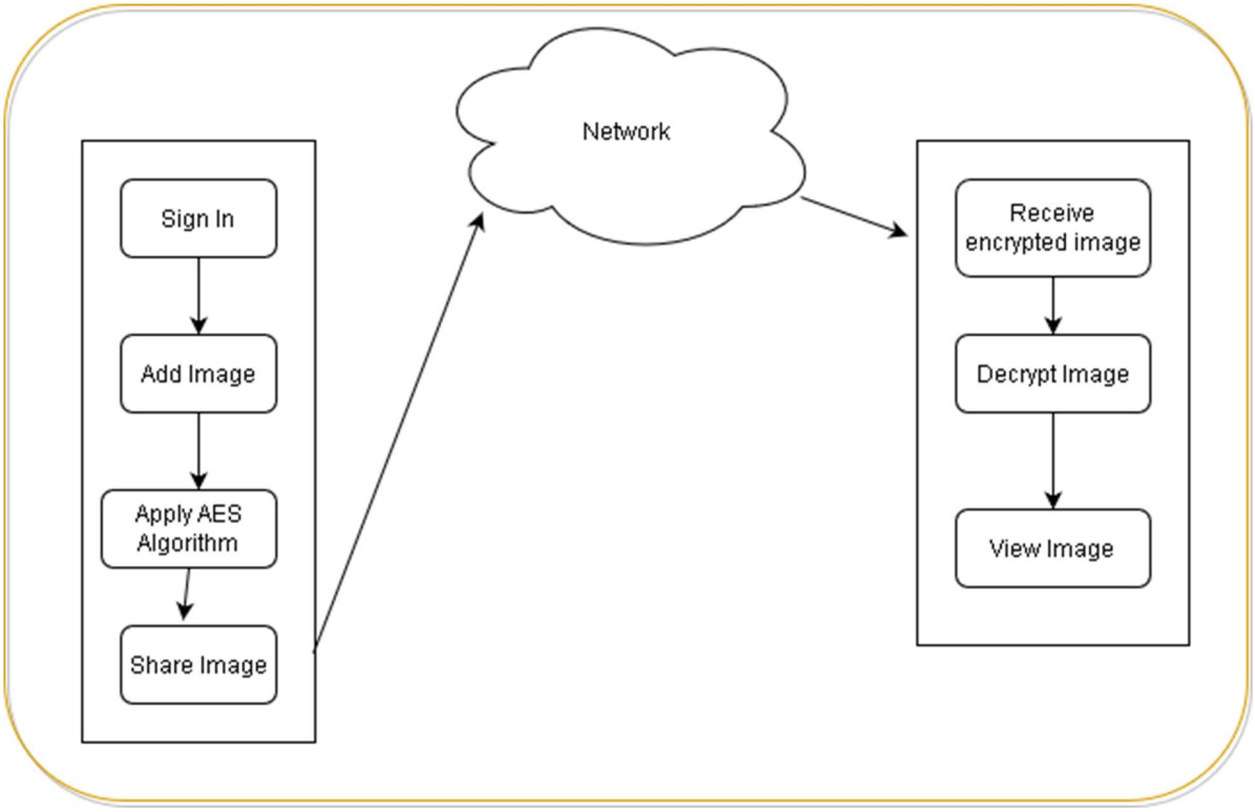

Figure 2.1 Conceptual Diagram of the proposed system

Chapter 3: Methodology

3.1 Introduction

This chapter presents the analysis and design methods that were used to meet the research objectives aimed at solving the problem.

The developed system applied the Object-Oriented Analysis and Design (OOAD) approach due to its data orientation. Object Oriented Analysis and Design was used through its various Unified Modelling Language (UML) diagrams. The goal of object-oriented design (OOD) was to design the classes identified during the analysis phase and illustrate the relationships and the responsibilities that these different classes have.

3.2 Development approach to be used

The project was developed using the linear sequential model which is also known as the waterfall model. The reasons for settling on this model was motivated by the fact that it suggested a systematic, sequential approach to software development that began at the system level and progressed through analysis, design, coding, testing and support.

The figure below shows the waterfall model for software engineering.

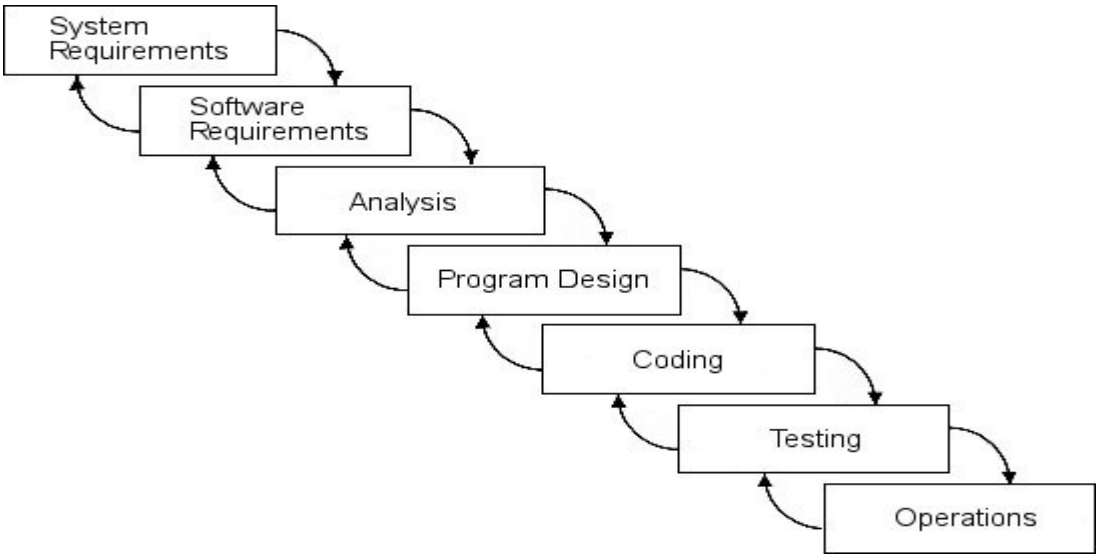

Figure.3.1 Waterfall development methodology source (Bassil, 2012)

3.2.1 System/Information engineering

Since a software is always a part of a larger system, this section worked on establishing requirements for all system elements and then allocating some subset of these requirements to software. System engineering and analysis encompassed requirements gathering at the system level with a small amount of top-level design and analysis. Information engineering encompassed requirements gathering at the strategic business level and at the business area level.

3.2.2 Software requirements analysis

This process entailed the gathering of requirements and was intensified and focused specifically on software.

The process assisted in understanding the nature of the program to be built. The software engineer must understand the information domain for the software as well as required function behavior performance and interface. Software requirements are documented and reviewed with the client.

3.2.3 Design

The design process translated requirements into a representation of the software that could be assessed for quality before coding began. Like requirements, the design was documented and became a part of the software configuration

3.2.4 Coding

The design must be translated into a machine-readable form. The code generation step performed this task. If the design is performed in a detailed manner, code generation can be performed mechanically.

3.2.5 Testing

After the code had been generated, testing of the program began. The process focused on the logical internals of the software, ensuring that all statements were tested, and on the functional externals. Tests were conducted to uncover errors and ensure that defined inputs would produce actual results that agree with required results.

3.2.6 Operations/Maintenance

The software will undergo changes after it is delivered to the client. Software support/maintenance re-applies each of the preceding phases to an existing program rather than a new one.

As the linear sequential model is the oldest and the most widely used paradigm for software engineering, it can be used efficiently for small projects that require less customer communication, it has been in development of data security project.

3.3 System Development Tools and Techniques

The tools that were found to be suitable for the success of this project are:

3.3.1 Eclipse IDE

This integrative development environment will provide the platform where coding will take place.

3.3.2 Java

This is the programming language that will be used since it allows one to create modular programs and reusable code. It is also easy to write compile and debug. Java is also platform-independent since it is compiled into platform independent byte code. This makes it run on a variety of platforms such as Windows, Mac OS and the various UNIX versions.

3.3.3 MySQL Database

This database is used in the creation, storage and management of data related to the system.

3.3.4 Apache Tomcat Webserver

This will be used to process the network requests of the user.

3.3.5 Advanced Encryption Standard Algorithm

AES is a symmetric key block cipher encryption algorithm which is implementable in Java .

3.3.6 Microsoft Office

Microsoft office tool will be used in the documentation of the project.

3.3.7 Rational Rose

This tool was used to draw the Unified Modeling Language (UML) diagrams.

3.3.8 Windows Operating System

This is the platform where the above tools were installed. It is owned by Microsoft Corporation.

Chapter 4: System Analysis, Design and Architecture

4.1 Analysis

According to (Peersman, 2014) data analysis techniques must be selected to match the specific assessment in terms of its key evaluation questions and the resources available. It goes further to state that the techniques must be able to complement each other's strength and weaknesses.

In order to identify the system requirements, an interview was conducted with a top-level user to determine the current operations in the process of sharing evidence. Questionnaires were also used to gain more insight on the research.

4.1.1 Functional Requirements

This section describes activities and services the system provides.

ID	Description
FR1	The system should be able to maintain a register of users and their roles.
FR2	The user should be able to login with their credentials to access the system and logout after completing their tasks.
FR3	The system should be able to encrypt image files in order to protect data being shared in the network.
FR4	The system should be able to decrypt image files that have been encrypted.

Table 4.0.1 A Table of the System's Functional Requirements

4.1.2 Non-Functional Requirements

ID	Description
NFR1	The system should have a simple user interface which is easy to use.
NFR2	The system should ensure controlled access to its resources
NFR3	The system should be stable and available anywhere and at all times
NFR4	The system should have a fast response time during the encryption/decryption process
NFR5	The system should be able to back up its data on a regular

Table 4.0.2 A Table of the System's Non-Functional Requirements

4.2 System Designs

System design refers to the procedure of designing the components of a system such as the modules and architecture, the different interfaces of those components and the data that goes through that system.

4.2.1 Class Diagram

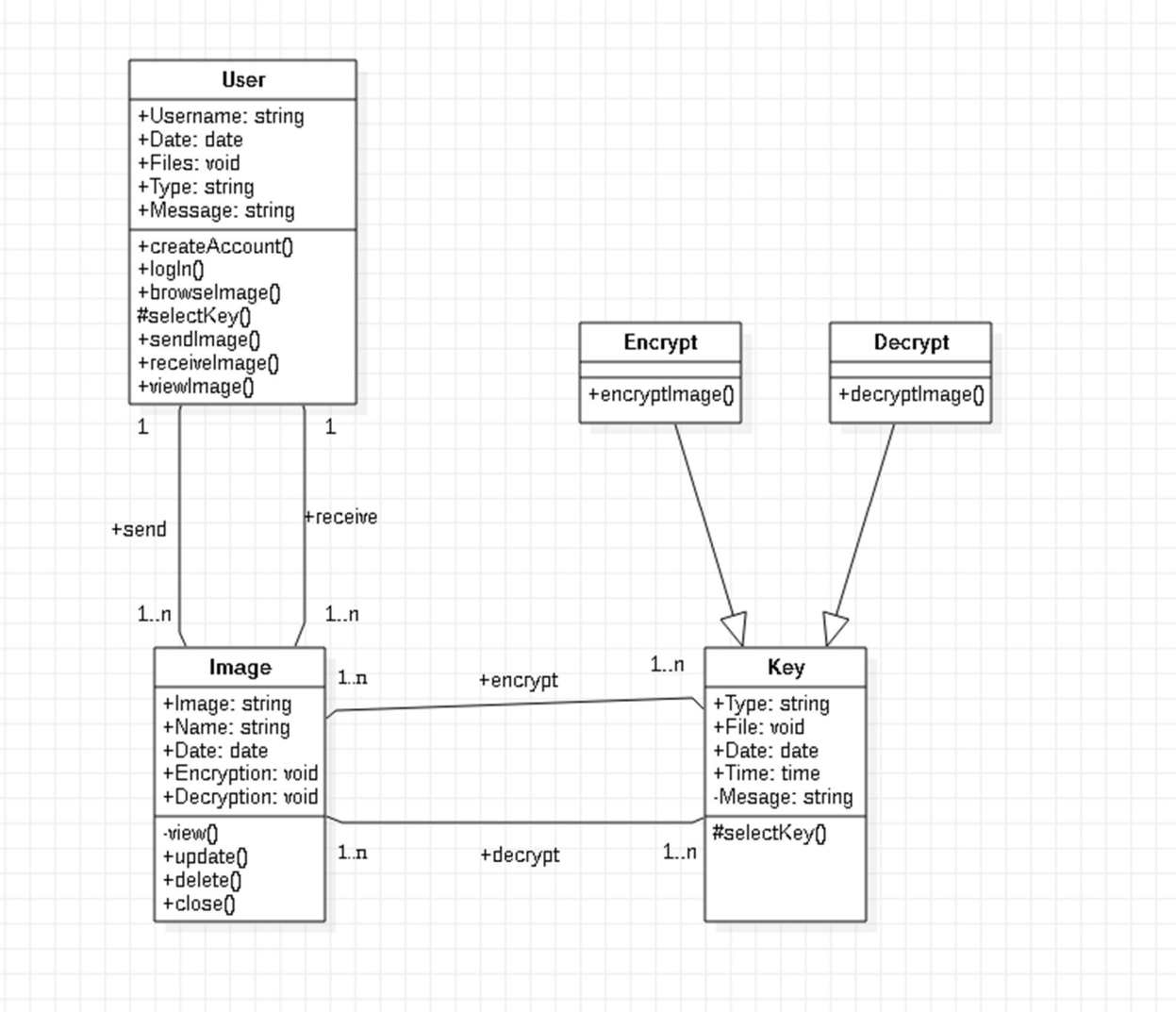

Figure 4.1 The Class Diagram

The diagram above describes the system structure by showing the system's classes, their attributes and the relationships between the classes.

4.2.2 Interaction Diagram

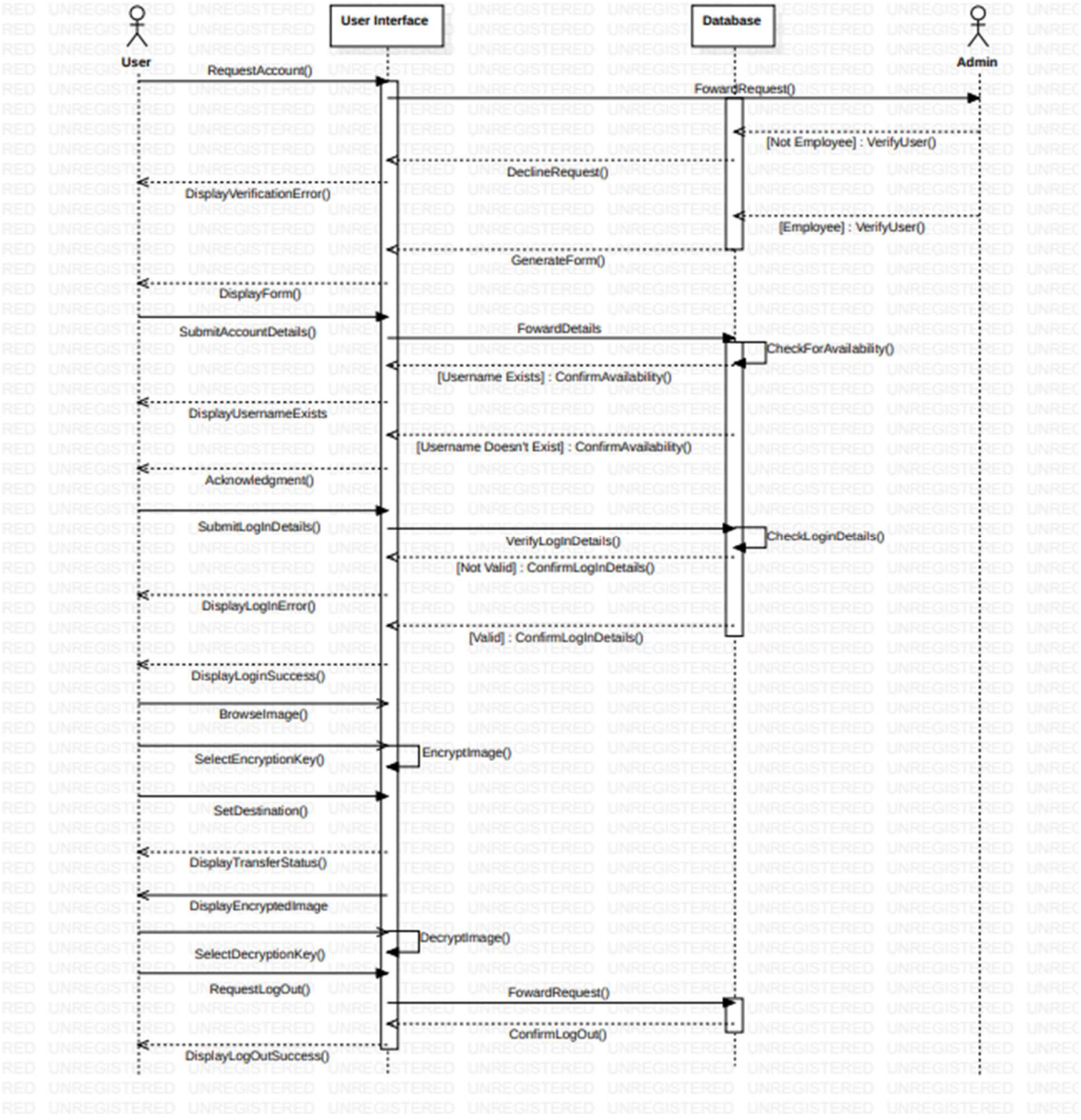

Figure 4.2 The Sequence Diagram

The interaction diagram above is the sequence diagram. This shows how objects in the system connect and communicate with each other.

4.2.3 Use case Diagram

Figure 4.3 The Use Case Diagram

The above use case diagram represents a graphical overview of the functionality provided by the system such as actors, objectives of the actors and their dependencies.

4.2.4 Entity Relationship Diagram(ERD)

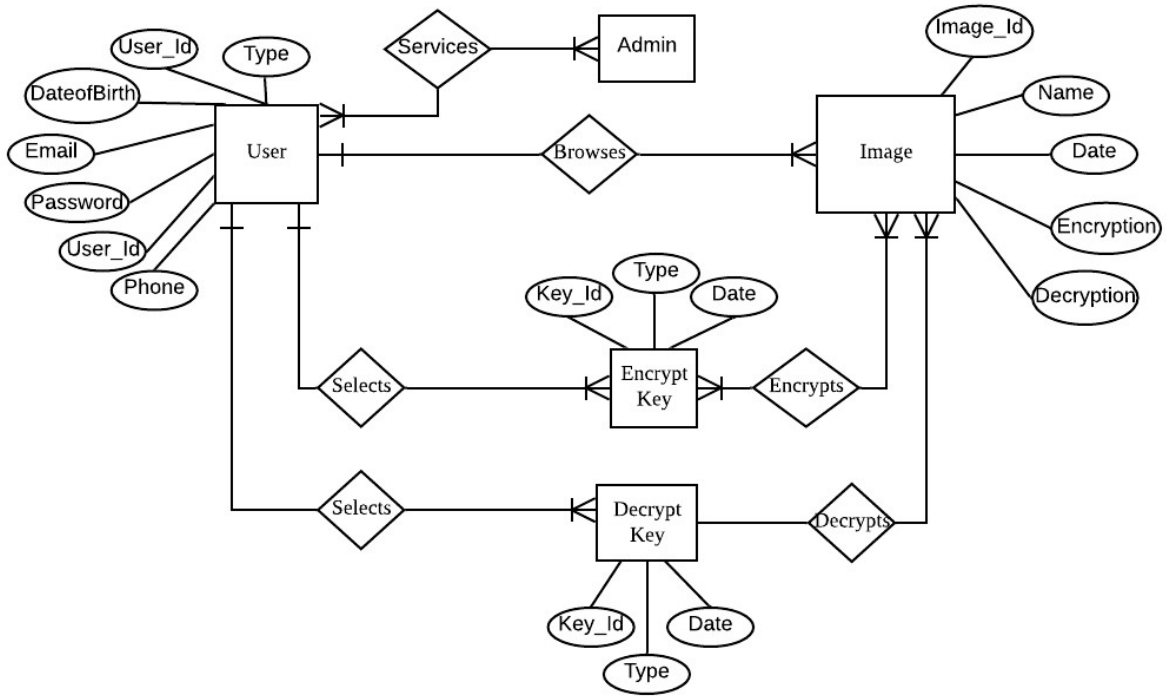

Figure 4.4 The ERD Diagram

For the client to manipulate the system information or data, they have to be conscious of the basic attributes that constitute the system (Li, 2009).

The ERD diagram above represents the system data in terms of entities and relationships as illustrated by data.

4.2.4 Database Schema

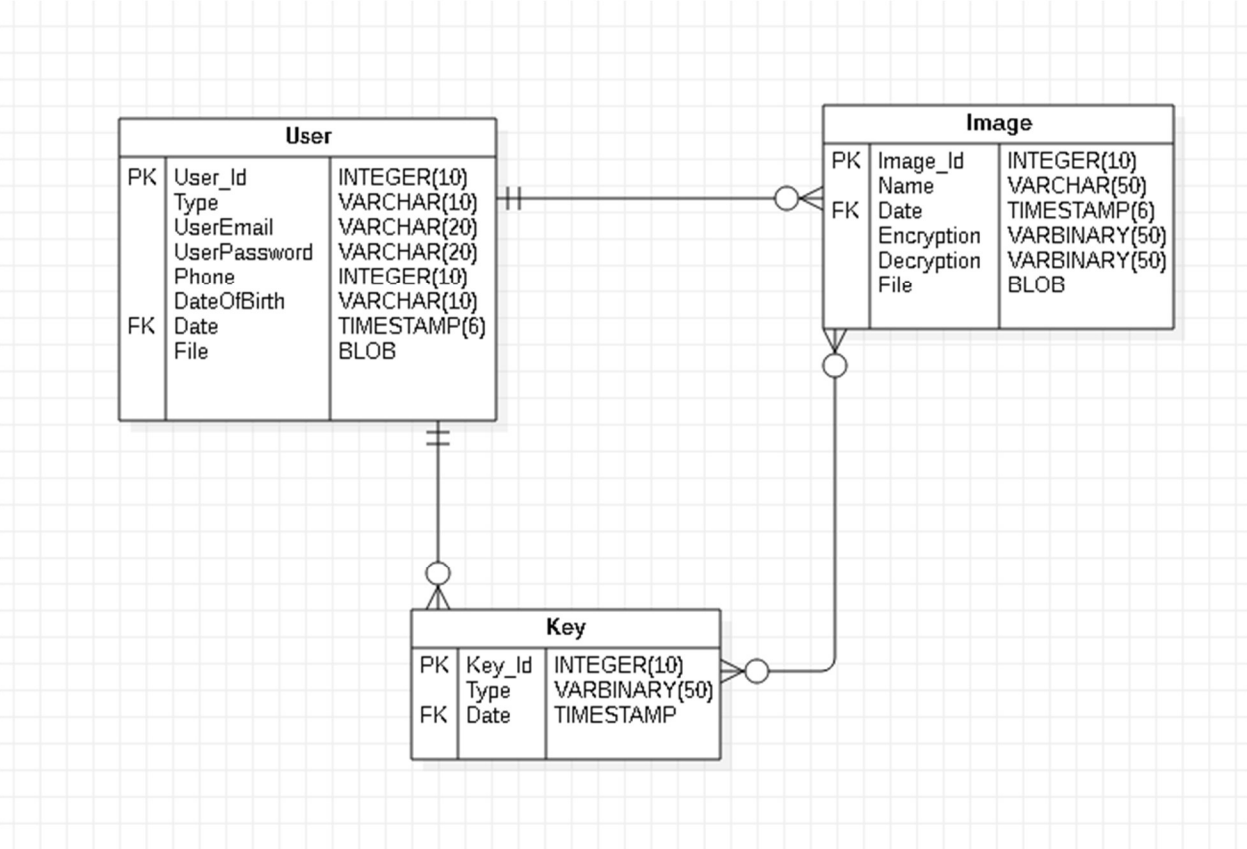

Figure 4.5 The Database Schema Diagram

The above diagram represents the structure of the entire database. It shows how data in the database is organized and how the different entities relate with each other.

4.3 Architecture

The deliverables and modules in the system are:

4.3.1 User Interface

This enables the system users to select, encrypt, decrypt and share image evidence with each other. It also enables registration of the system users.

4.3.2 Administrator Module

The administrator has all the rights to access the portal. The administrator can view all the encrypted image files in the shared database and the registered users in the system. He will be able to manage the system users.

4.3.3 User Module

The people who use this system to provide security for confidential images are the users. The user has to first register themselves on the system in order to be able to use it. The user loads an image and encrypts it by setting a shared key. The user then shares the image with a different user who uses the shared key to decrypt the image and view it.

4.3.4 File Upload/Download Module

This enables the system user to have the ability to share or receive the encrypted image files.

4.3.5 An object-relational database management system of MySQL

This assists in the storage of user credentials and also assists the administrator in the storage and retrieval of data.

Chapter 5: System Implementation and Testing

5.1 Introduction

The next step after coding of the system with guidance from the analysis and design phases, was its implementation and testing. This chapter discusses the implementation of the image encryption

tool and highlights its significant functionalities. System testing was also done to ensure the system met its functionality and also user requirements.

5.2 Implementation Environment

5.2.1 Hardware Requirements

The minimum hardware requirement specifications for developing this project are as follows:

Processor	Standard processor with a speed of 1.6GHz
Hard Disk	at least 20GB
RAM	At least 256MB
Monitor	Standard color monitor
Keyboard	Standard keyboard
Mouse	Standard mouse

Table 5.1 The System's Hardware Requirements

5.2.2 Software Requirements

The minimum software requirement specifications for developing this project are as follows:

Operating System	Windows 8
IDE	My Eclipse 3.3 and above
Frontend	Core Java
Coding Language	Java
Database	MySQL
Server	Tomcat server
Database Layer	JDBC

Table 5.2 The System's Software Requirements

5.3 System Installation and User Manual

5.3.1 Introduction

Considering the fact that the system is a desktop application. The installation procedure is quite simple. This chapter will include installation of the various software requirements and a user manual. It will also include screenshots of some of the important system interfaces and tests that were carried out.

5.3.2 Software Installation

The first step is to download the Java development platform (version 8.0 and above) on to your desktop machine. This can be downloaded from https://www.java.com/en/download/manual.jsp. Select the appropriate version for your operating system and follow the instructions given. Make sure to set the correct path to the Java folder location on the system environment variables settings on your desktop machine. The user should also download the MySQL connector JDBC driver that will enable communication between the system and the database. This driver can be downloaded from https://www.mysql.com/products/connector/. The MySQL connector's location should also be specified in the system's environment variable settings same way as done on the Java platform.

The second step is to download any cross-platform web server solution that supports the MySQL database and Apache server. The recommended web server solution is XAMPP since it is easier to install and operate. This can be downloaded from https://www.apachefriends.org/download.html. Make sure to download the appropriate version related to the system you are using and follow the installation guidelines provided.

The system administrator then needs to navigate to the localhost and create a database that will store registered users in the system so as to enable them to access the system's resources. The database will also act as a storage for some of the encrypted files. The database will consist of two tables with various columns as indicated below.

Table	**Columns**							
users	u_fname	u_lname	u_uname	u_pass	u_bdate	u_address		
file	filesID	name	filesName					

Table 5.3 The Database Tables and their respective columns

The final step will be to copy the entire system folder to any desired location on the desktop machine and everything will be good to go.

5.3.3 User Manual

(a) In order to launch the application, one has to ensure that the XAMPP application has been launched and the Apache and MySQL modules are running. This is important since it will enable the application to communicate with the database. The figure below shows the XAMPP instance running.

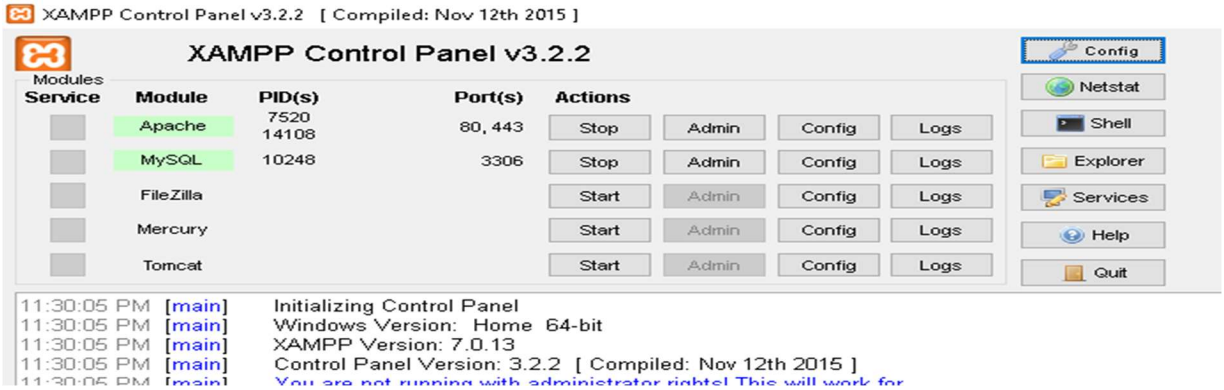

Figure 5.1 The XAMPP web server Application

(b) The next step is to open the command prompt and navigate to the directory where the system folder is located. Once in the system folder, navigate to the folder named ***src.*** This folder contains the main files of the application. Once in the src folder, the command prompt will almost be similar as shown in the screenshot below.

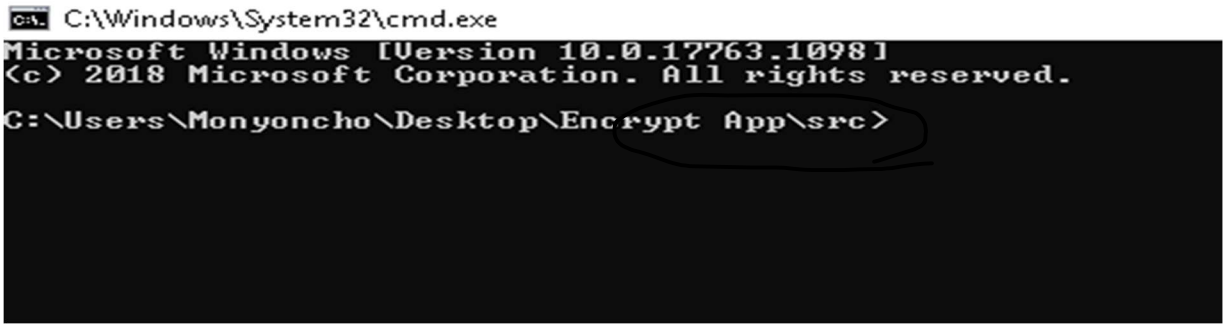

Figure 5.2 A snippet of the command prompt in the application's folder directory

If the current directory is the ***src*** folder, type the command ***java HOME_JFrame*** in the command prompt and it will immediately launch the application. The application interface will appear as shown below.

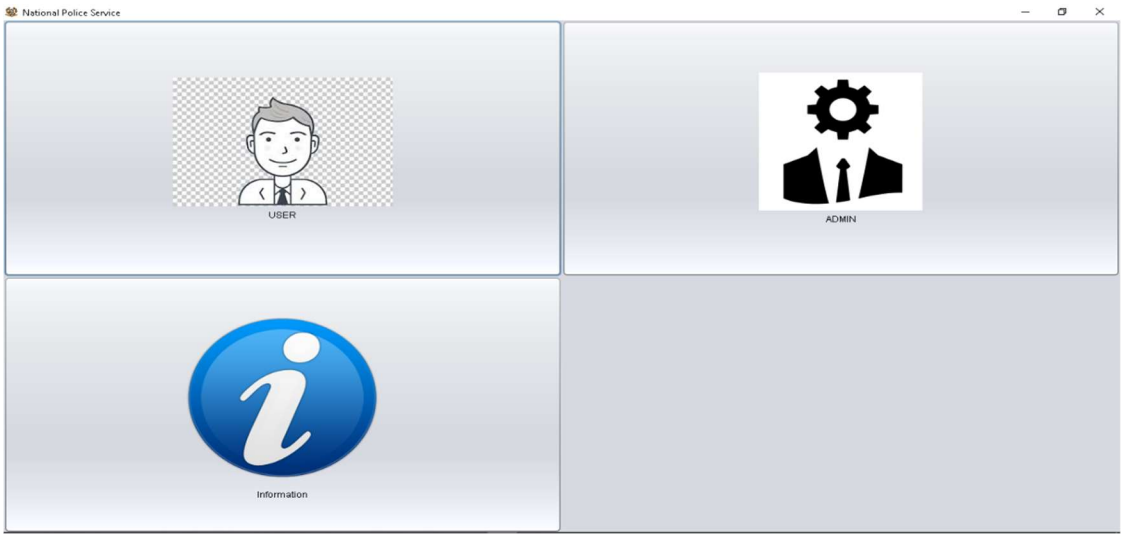

Figure 5.3 A screenshot of the applications Home Page interface

(c) After successful launch of the application, the user should then click on the user button in order to be able to register themselves to the system. If the registration is a success, the user now has the ability to log into the system and use its resources. The figures below show the Registration and Log in pages of the system.

Figure 5.4 A screenshot of the Application's user registration interface

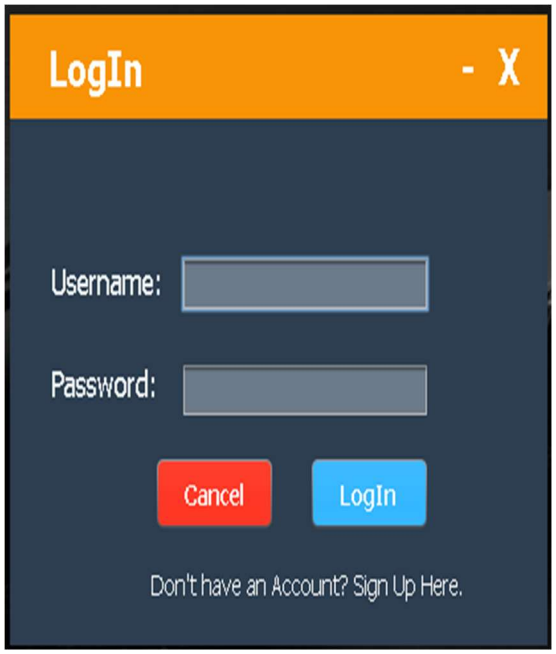

Figure 5.5 A screenshot of the Applications user Log In interface

(d) Once the user is logged into the system, they can now be able to load an image into the application and either encrypt or decrypt it by the use of a pass key. The main interface consists of four items on the menu bar which are straightforward to understand and use. Firstly, the user has to select the ***File*** menu and open an image they wish to either encrypt/decrypt. After the image has loaded on the interface, the following step will be to open the ***encrypt/decrypt*** menu and set a pass key that they will use to encrypt the image. This same pass key will also be used in the decryption of the image. After setting of a pass key, the user should then select the ***Encrypt Image*** menu item under the ***encrypt/decrypt*** menu. The appropriate action will be taken by the application and the image will be encrypted.

For the decryption process, the same process carried out for encryption will be used for decryption. The only difference will be that after setting of the pass key the user will select the ***Decrypt Image*** menu item under the ***encrypt/decrypt*** menu.

After successful encryption or decryption of an image, the user is required to save the manipulated image. They can either decide to overwrite the original file or save the manipulated file as a totally new file. This process is carried out under the ***File*** menu where the user can choose between the S***ave*** or ***Save as…*** menu item.

(e) Users who have successfully encrypted a file can share the manipulated file with other parties by uploading it to the system database through the ***Upload/Download*** menu. The receiving party can also retrieve shared files by accessing them through the same menu.

The figure below shows an overview of the main interface.

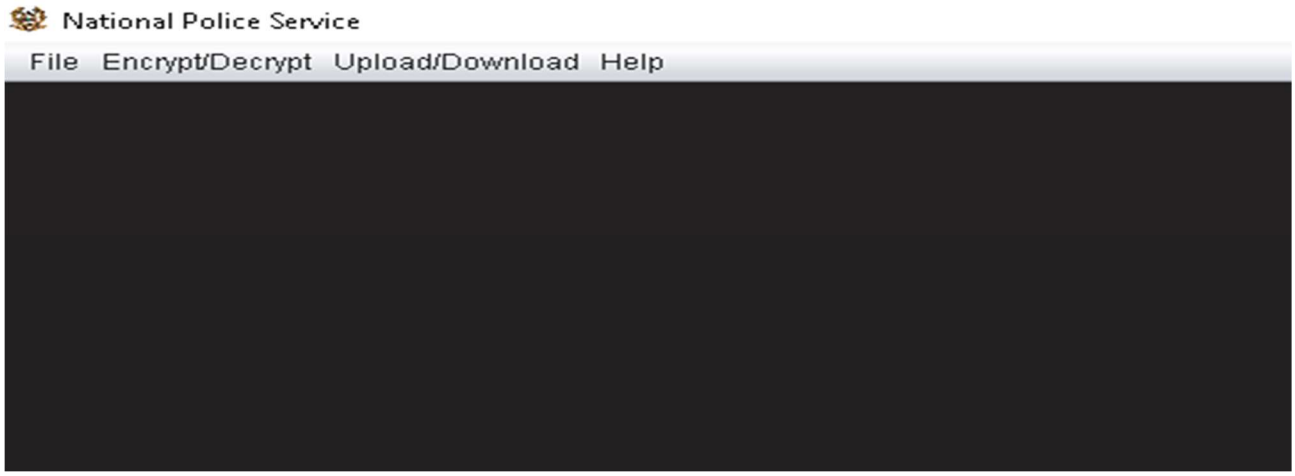

Figure 5.6 A screenshot of the Application's Main user interface

5.4 System Testing

5.4.1 Introduction

This section gives a view of the tests carried out in relation to the functionality of the system.

5.4.2 System Tests

Test ID	Requirement	Expected Result	Achieved Result
1	FR1	The system should be able to maintain a register of users and their roles.	The system successfully registered users of different roles.

2	FR2	The user should be able to login with their credentials to access the system and logout after completing their tasks.	The system was able to authenticate and allow access to registered users. Users were also able to log out of the application
3	FR3	The system should be able to encrypt image files in order to protect data being shared in the network.	The system successfully encrypted various image files.
4	FR4	The system should be able to decrypt image files that have been encrypted.	The system successfully decrypted image files using the shared key.
5	NFR4	The system should have a fast response time during the encryption or decryption process.	The system successfully encrypted and decrypted the image files in good time (in less than 15 sec).

Table 5.4 A table of the System Test details

Chapter 6: Conclusions, Recommendations and Future Works

6.1 Conclusion

Computer security has become a crucial issue with the widespread application of computers in day-to-day operations and the increasing demand for computer technology especially in the security sector such as in military or governmental services. The problem to be solved is how to assure the confidentiality, integrity and usability of the computing equipment and various software in a messaging system not to forget how the message will be processed, stored and transmitted.

There exist other various symmetric encryption algorithms such as the International Data Encryption Algorithm(IDEA) and Data Encryption Standard (DES) but a more powerful symmetric algorithm (AES) was introduced by the National Institute of Standard Technology better known as NIST which took over the other algorithms. It was demonstrated that the AES algorithm can protect messages, including those that are multimedia in nature, from known or unknown attackers under the current technical level in a safe and reliable manner. This research

has been able to validate the claims of the National Institute of Standard Technology since the developed application is fast and has a strong ability to resist attacks yet is simple in design.

6.2 Recommendations

The developed system is best suited for any kind of entity operating in the security sector. The users of the developed system should ensure that the pass key they use to encrypt an image should only be shared with the relevant personnel otherwise the objectives of this study will not have been achieved at all and all the work and effort put into the achievement of this study will all be in vain.

6.3 Future Works

Advanced Encryption Standard is a well-known block cipher that has several advantages in data encryption. However, it is not suitable for real-time applications. In the near future I hope to carry out a research that will assist in the development of a modification to the AES algorithm that will be suitable for real time applications. The modification will be facilitated by adjusting the Shift Row Transformation phase of the algorithm which will give it better encryption results in terms of security against statistical attacks.

References

Bassil, Y. (2012). A Simulation Model for the Waterfall Software Development Life Ccycle. *Internation Journal of Engineering and Technology*.

Clough, J. (2015). *Principles of Cybercrime* (2 ed.). Victoria: Cambridge University Press. doi:https://doi.org/10.1017/CBO9781139540803

Dehnie, S. (2006). DIigital Image Forensics for Identifying Computer Generated and Digital Camera Images. 2313-2316.

Fick, M. (2018). Reuters. *Special Report: Amid claims of police butality in Kenya, a watchdog fails to bite*.

Fridrich, J. (1998). Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, 1259-1284.

Kimberly, A. D.-B., & Dhruba, J. B. (2016). An overview of contemporary challenges and impending threats. *Cybercrimes*, 119-132.

Li, Q. (2009). Entity-Relationship Diagram. *Modeling and Analysis of Enterprise and Information Systems*, 125-139.

Mohd, B. A., Arief, B., & Gross, T. (2015). Cybercrime from its Stakeholers': Part 1-Attackers. *IEEE Security & Privacy, 13*(1), 71-76.

Mutwiri, D. (2019, November 22). *Kenya Police now have digital Occurence Book (OB)*. Retrieved from Citizen Digital: https://www.google.com/amp/s/citizentv.co.ke/news/kenya-police-now-have-digital-occurrence-book-ob-304948/%3famp

Mwololo, M. (2016, September 20). *Daily Nation*. Retrieved from With evidence, there is no room for false steps: https://www.google.com/amp/s/www.nation.co.ke/lifestyle/dn2/Why-cases-collapse-in-court--/957860-3388322-view-asAMP-qgjbxiz/index.html

Narasimhan, A., & Rengarajan, A. (2014). Image Encryption: An Information Security Perspective. *Journam of Artificial Intelligence, 7*(3), 123-135. doi:10.3923/jai.2014.123.135

NPS. (2019, January). (Office of the Inspector General) Retrieved May 2020, from National Police Service: http://www.nationalpolice.go.ke/2015-09-08-1756-33/news/267-national-police-servies-goes-digital.html

Peersman, G. (2014). Overview: Data Collection and Analysis Methods in Impact Evaluation. *Methodological Briefs: Impact Evaluation 10*.

Sarode, T. (2014, February). Study of Perfect Shuffle for Image Scrambling. *International Journal of Scientific and Research Publications, 4*(2).

Sean, E. G., & Robert, C. D. (2015). Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. *Digital Evidence and the U.S. Criminal Justice System*, 1-31.

Shyamala, P. (2011). Chaos Based Image Encryption Scheme. *Communications in Computer and Information Science*, 312-317.

Stallings, W. (1999). *Cryptography and Network Security: Principles and Practice.* Upper Sadle River, N.J.

The 2020 Cybercrime Report. (2020). Retrieved from Herjavec Group: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Transparency International. (2017). *The East African Bribery Index*.

Warner, J. (2011). A View from Below. *Understanding Cyber-Crime, 5(1)*, 736-749.

Whisenand, P. M. (1971). Automated Police Information Systems: An argument for Vertical and horizontal Integration. *Journal of Criminal Law and Criminology, 62*(3), 422-429.

Appendix A: Time Schedule

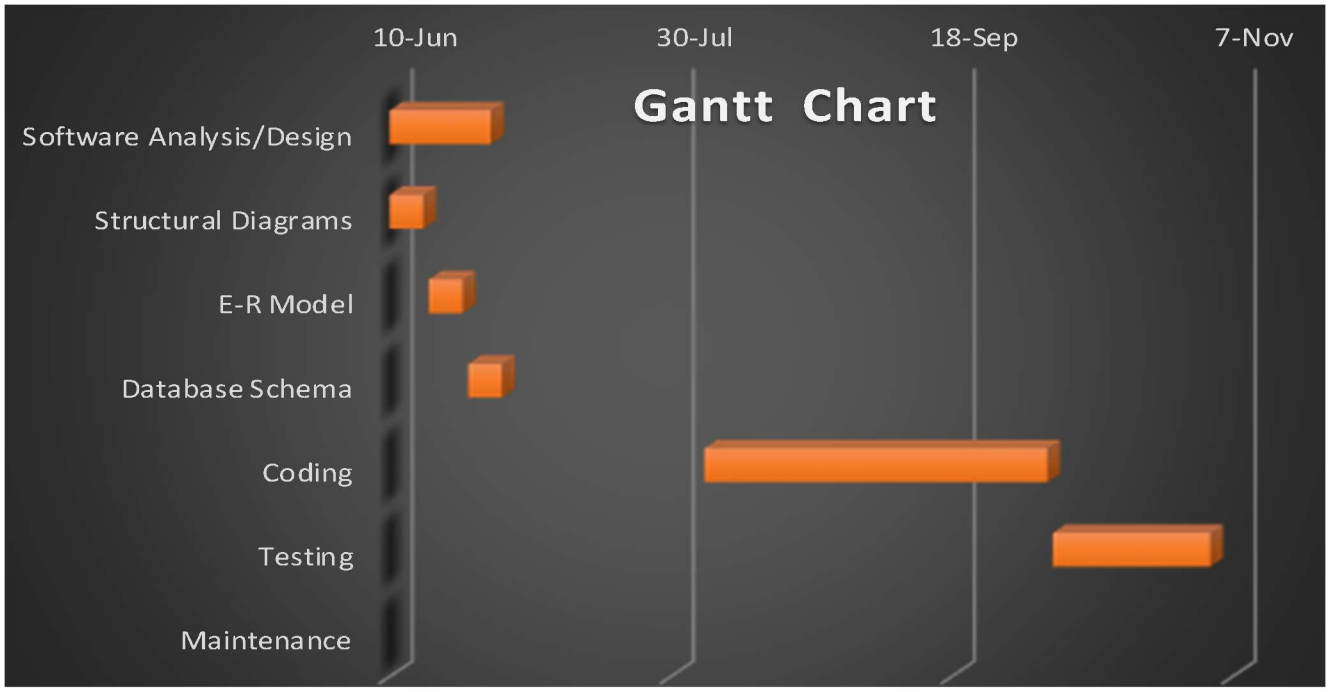

Figure A-1: The project research and development schedule

Appendix B: Core Code

```
//The image encrypt class
//this class holds methods for enrypting and decrypting images
class ImageEncrypt{

    private boolean verbose=false;
    private Random generator;

    private Cipher cipher;
    private SecretKeySpec skeySpec;

    /** Constructor */
    ImageEncrypt() {

        try{
            // Used for noise
            generator = new Random();

            KeyGenerator kgen = KeyGenerator.getInstance("AES"); //initiate with AES algorithm, can be changed to DES but the key size should be 56 bits
            kgen.init(128);
            /**initialize the encryption key with 128,
            key could be 128, 196 or 256 using AES encryption algorithm
            */
            SecretKey skey = kgen.generateKey();
            byte[] raw = skey.getEncoded();
            skeySpec = new SecretKeySpec(raw, "AES");

            cipher = Cipher.getInstance("AES/ECB/NoPadding");

        }catch(Exception e){ System.out.println("ERROR: " + e);}

    }
```

Figure A-2: The main code class used as the base for encryption and decryption

Appendix C: Interview Questions

Question 1

How long have you worked in the police service?

Question 2

What is your opinion on the recently implemented digital management system to be used in the police force?

Question 3

How do you feel about the handling of digital evidence in the police force?

Question 4

What do you think is the best technique that can be used to secure digital evidence?

Question 5

Are you computer literate? If No, are you open to the learning of basic computer skills?

Appendix D: Encrypted Image

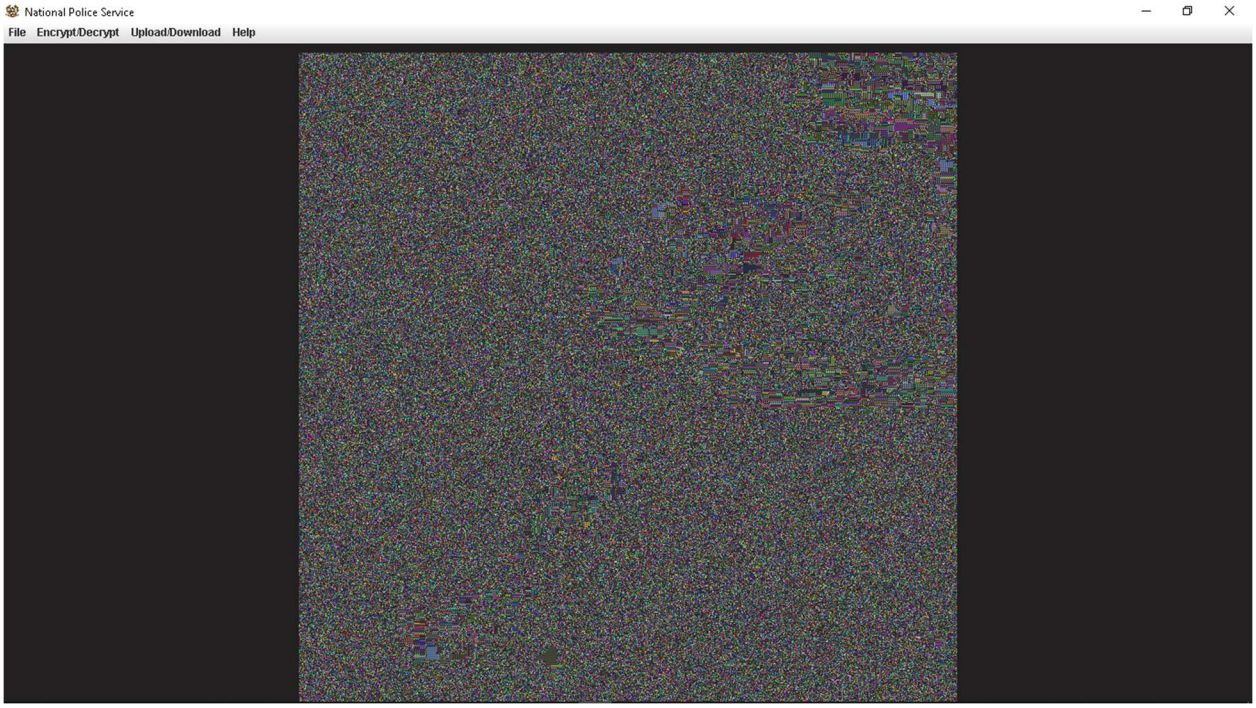

Figure A-3: A screenshot of an image after encryption