ENCRYPTION AND DECRYPTION TECHNIQUE WITH SMS SUPPORT FOR DIGITAL IMAGE SECURITY

Jumoke Soyemi
Department of Computer Science
The Federal Polytechnic Ilaro
Jumoke.soyemi@federalpolyilaro.edu.ng

ABSTRACT

With the rise in the use of digital techniques of transmitting and storing images, it becomes an important issue to look into how to protect the confidentiality, integrity, and authenticity of such images. There are various techniques to encrypt images and make them more secure, including Image encryption techniques that scramble the pixels of images and decrease the correlation among the pixels so that there are lower correlations among the pixel of the encrypted image. Encryption generally converts data or information from its original form to another in order to hides the information in it. The protection of images from unauthorised access is critical and essential. In this study, in order to address the issue of image security, an application was developed using encryption and decryption algorithm with SMS technology. This application sends messages containing the encryption and decryption key to the mobile phone of the intended/final owner of the image specifying the key for opening the file sent and the key is shared by both encrypted and decrypted image. The application developed using this algorithm is intended to provide the security so desired.

Keywords: encryption and decryption technique, image security, unauthorised access, SMS technology

1.0 INTRODUCTION

Security is the major problem when it concerns files that are sent to the internet. Such files stand the chance of being tampered with by unauthorised users, and some of these files are confidential files intended to be viewed only by the original owner. The rapid progress in the use of digital information and its communication demands ideal security mechanisms with images, being an integral part of online communication (Cheddad *et al*., 2010). Images are not only just meant for recreation and sharing, but images have now become a necessitated mode of distribution in diverse domains.

Image encryption is a method that ensures the security of images through the conversion of the original image to another version that will be difficult to decode (Singh, Hassan and Kumar, 2015). In the ever-increasing growth of multimedia applications, security is an important issue in communication and data storage, and such security is provided through encryption. The time taken to perform the process of encryption is reduced through fast image encryption algorithms (Wang *et al*., 2011).

There are other ways to preserve confidential information, they include image steganography (Amirtharajan and Rayappan, 2012; Aarthie and Amirtharajan, 2014; Amirtharajan *et al*., 2013; Zhu *et al*., 2011), watermarking (Stefan and Fabin, 2000; Zeki *et al*., 2011) apart from Image. Image steganography is also useful in hiding the confidential information of any digital media in spatial or transform domain coefficient and watermarking is useful for copyright protection and authentication.

In this study, encryption and decryption algorithm is employed with SMS technology to secure images sent across the internet and ensure that only the owner of the images has the key to unlock and access such images.

2.0 RELATED STUDIES

The image encryption and decryption algorithm are designed and implemented to provide confidentiality and security in the transmission of the image-based data as well as in storage. Image encryption is a powerful application for sending images through the internet to mobile phones. There are various algorithms employed for encryption/decryption implementation. They include but not limited to Color Signal, DCT and Stream Cipher, Modified AES Based Algorithm, In-Compression Encryption, chaos and improved DES, Hash Function, and others.

The study by Qaid and Tallbar (2012), carried out encryption and decryption of images using colour signal. This technique provided high security for digital images using an encryption algorithm that ensures accuracy and safety features and maintaining image data from getting lost during the decryption process.

Securing Image Transmission Using In-Compression Encryption algorithm by Shaimaa, Khalid and Mohamed (2010), discovered a new OMHT compression-encryption technique which is a modification to the MHT scheme. It generates different Huffman tables for each type of images instead of using fixed Huffman tables for all which is the main advantage the MHT technique. The advantage of OMHT technique over other compression technique is that it produces a much smaller compressed file than any compression method, while still meeting the advantage of encryption.

Modified AES Based Algorithm for Image encryption technique was proposed by Zeghid, *et a*l. (2007). The study designed a secure symmetric image encryption technique using a modified version of the Advanced Encryption Standard (AES). The key issue identified in AES encryption is that textured zones existed in the encrypted image. This problem was taken care of with the support of keystream generator for image encryption.

Image Encryption Using DCT and Stream Cipher algorithm by Sharma, Godara and singh,(2012), used the Discrete Cosine Transform (DCT) which is a mathematical transformation that takes a signal and transforms it from the spatial domain into frequency domain. Many digital images and video compression schemes use a block-based DCT because this algorithm minimizes the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images (Sharma, Godara and singh, 2012; Lala *et al.*, 2009).

Image Encryption Using Block-Based Transformation Algorithm was proposed by Mohammad, Younes, and Aman (2008). Here, transformation technique works as follows: the original image is divided into a random number of blocks, then these blocks get shuffled within the image. The generated (or transformed) image serve as an input to the Blowfish encryption algorithm. The intelligible information present in an image is due to the Correlation among the image elements in a given arrangement. So this technique reduced the correlation among the image elements using certain transformation techniques (Sharma, Godara and singh, 2012). The secret key to this approach is used to determine the seed. The seed plays the main role in building the transformation table, which is then used to generate the transformed image with a different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

Zhang *et al*. (2009), carried out a study on the chaotic encryption, DES encryption and a combination of image encryption algorithm. Here, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement on DES. Their result shows high starting value sensitivity, and high security and the encryption speed.

Image Encryption Algorithm Based on Hash Function employed a novel way of encrypting digital images with password protection using ID SHA-2 algorithm coupled with a compound forward transform. A spatial mask is generated from the frequency domain by taking advantage of the conjugate symmetry of the complex imagery part of the Fourier Transform. This mask is then XORed with the bit stream of the original image. Exclusive OR (X0R), a logical symmetric operation, that yields 0 if both binary pixels are zeros or if both are ones and 1 otherwise (Cheddad, Condell, Curran and Kevitt, 2010).

Sinha and Singh (2003), proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-ChaudhuriHochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature can be used to verify the authenticity of the image.

The study here employed encryption and decryption algorithm that uses encryption and decryption key with SMS technology to notify the original owner of progress status of the encryption and decryption images, providing a higher level of security.

3.0 SYSTEM DESIGN

3.1 System Overview

There are many types of digital image formats like .bmp, .gif, .jpg, pict, .eps and .png. This study designed an application that uses mainly the gif format. The Graphics Interchange Format (GIF) was originally invented by CompuServe in 1987. It was mainly used as file formats for web graphics and exchanging graphics files between computers. GIF format supports 8 bits of colour information. This information is limited to 8 bits palette and 256 Colors. Therefore, 256 different colours are available in this format to represent the picture. GIF also supports transparency, interlacing, and animation (Saraf, Jagtap and Mishra, 2014). The main feature of the encryption and decryption program implementation is the generation of the encryption key. Other features are related to the design of the GUI, progress of encryption details, and user notification of the status of encryption.

3.2 Encryption/Decryption Algorithm

A symmetric Encryption key is used for this application, which means the same key is shared for both Encryption and decryption. A copy of the generated key is saved in a file named .ekf. During the Encryption process, the same key is used as the decryption key to retrieve the encrypted file. The technique of generating the key uses two methods: random number generation and combination. First, a long number with only digit values called A is generated, then another long number with character values called B is generated. The size of B is twice the size of A. Then an insertion operation is performed such that each digit of A is inserted after two characters of B. The result of the insertion is called C. Then another only digit number called D is randomly generated. C is combined with D by placing alternately one character or digit from C after a character or a digit from D.

The result of the combination is a relatively strong key. Then, an odd and even partitioning is performed on the key. The position of each character in the key decides the p to be an even or an odd character. For example, the character at position 0 is an even one while the character at position 1 is an odd character. Similarly, position 2 is an even position while position 3 is an odd one. The even part of the key is combined with the odd part of the key. Finally, the two parts of the key are joined as an even part followed by an odd part to produce one final encryption key. Since the final key is a key that consists of all character another key with only ASCII values of each character is obtained. The result is very long decimal key.

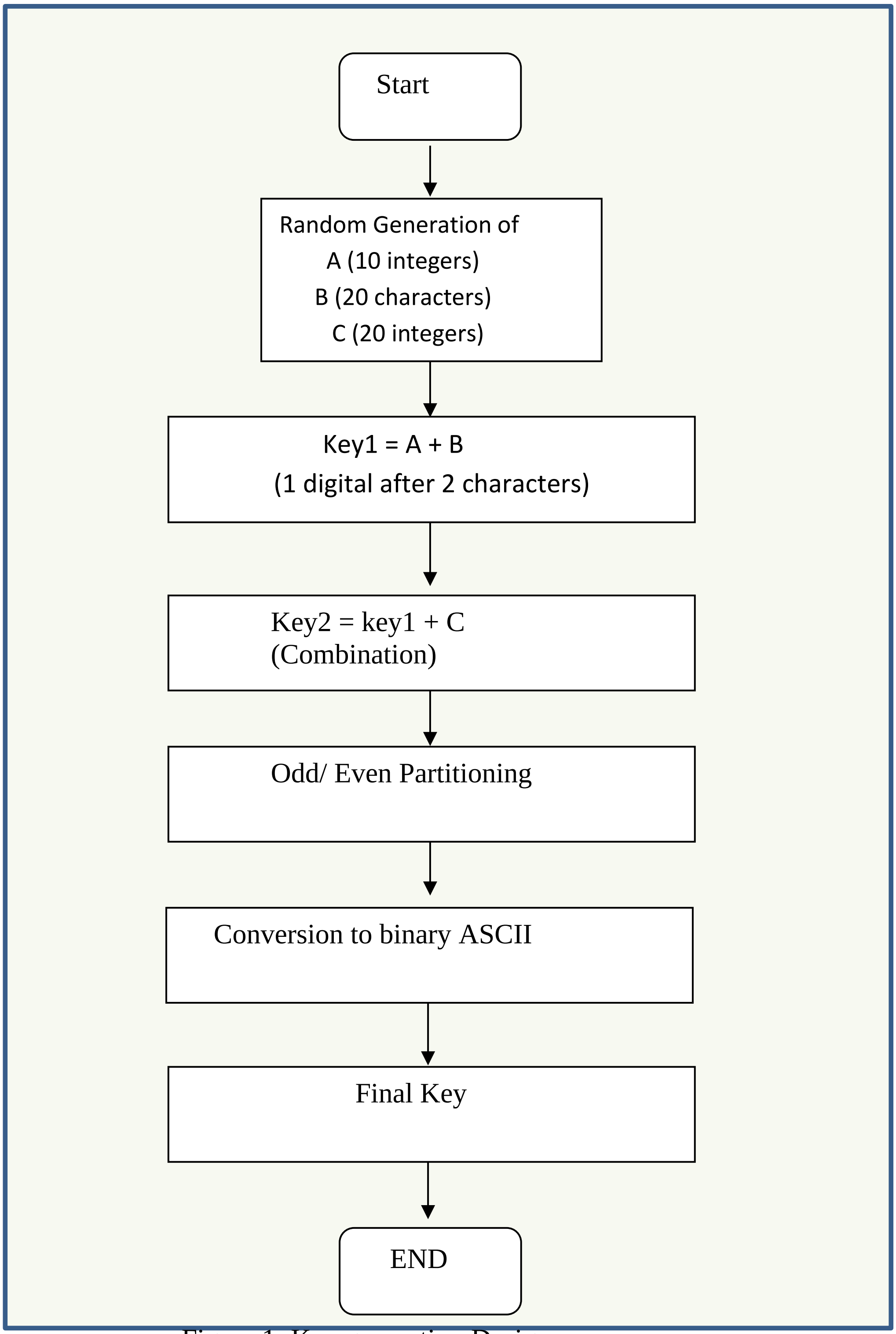


Figure 1: Key generation Design

3.3 System Flowchart Design

Encryption of image starts with the loading of the image and converting it to cipher which is then, sent to the receiver who now decrypts the cipher using a specific key. For image decryption to take place, encryption is retrieved from the database and then decryption using a specific key sent via SMS to the intended owner. The decrypted image is then, saved in the database.

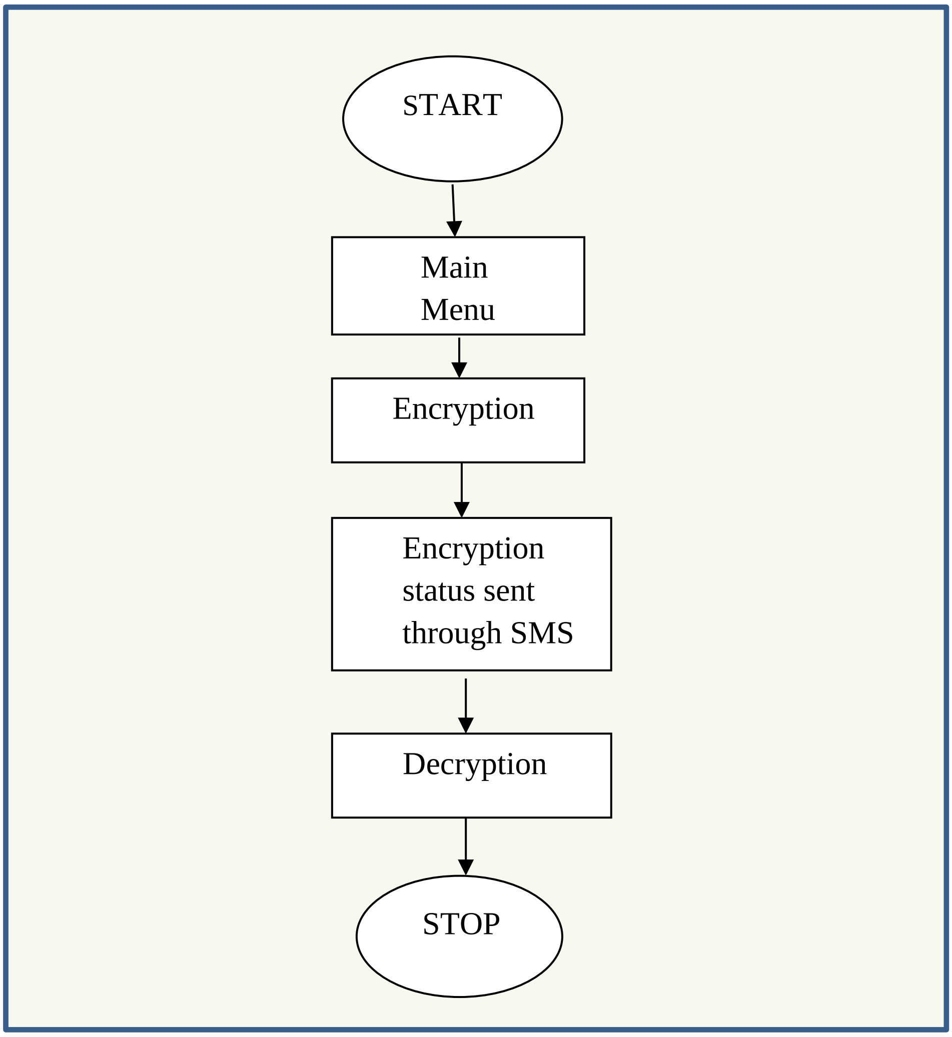


Figure 2: System Design flowchart

3.4 Image Encryption/Decryption Flowchart

This flowchart explains how encryption takes place; image is loaded from image database if it is a valid image, then encryption can take place. The encryption image is then saved in the database for easy retrieval for decryption.

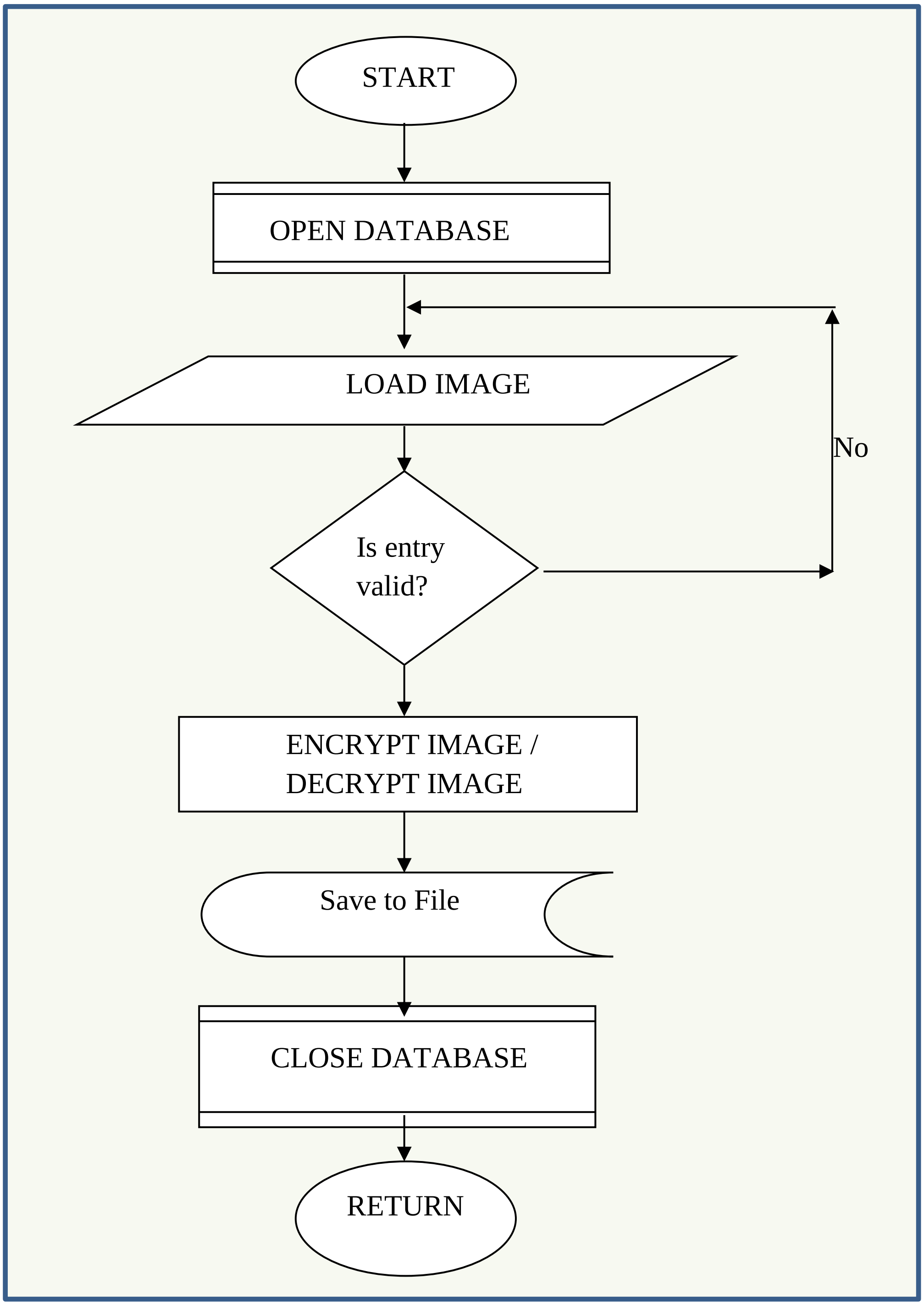


Figure 3: Image Encryption/Decryption Flowcharts.

4.0 SYSTEM IMPLEMENTATION

4.1 Software Requirements

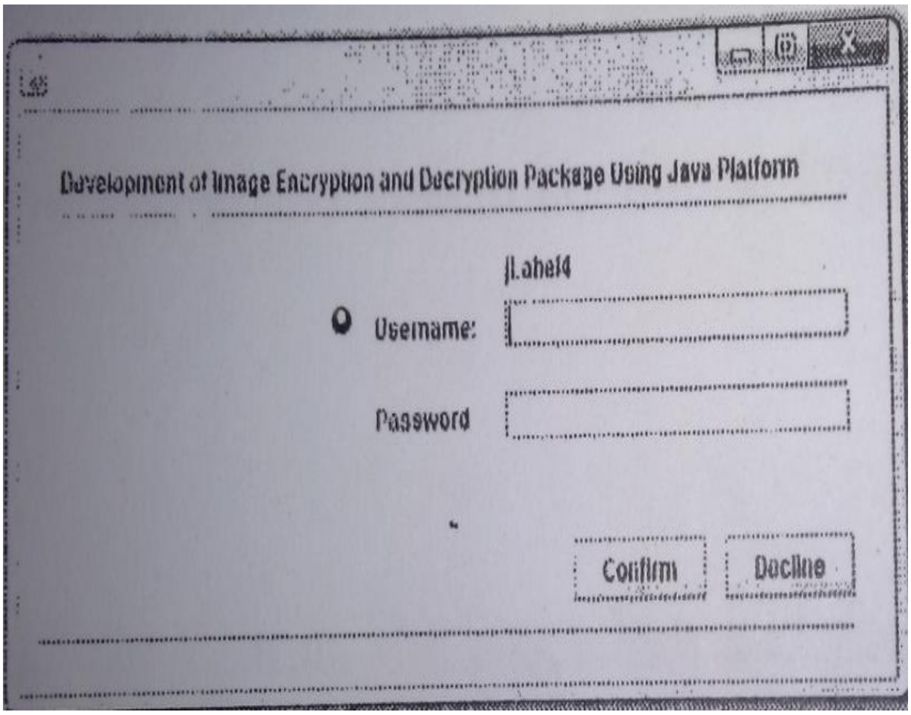
The implementation of Image Encryption and Decryption demands the use of Java Platform although other Programming languages can be used for the same purpose. Here, in this study, Java Programming language is used for the implementation. Images are loaded into the system, and the system encrypted the image by performing a series of process on it. In the process of encryption, an 8x8 blocks technique is used. Java platform is used for its security. The new system was implemented using Java platform and Mysql database application. This is because the programming language has the advantage of easy development, flexibility and ability to provide the developer/programmer with possible hints and also the availability of graphical user interface.

4.2 Hardware Requirements

The designed application will operate effectively by using the following minimum specifications in term of hardware. Computer system that is internet ready with random access memory (RAM) of at least 512MB, a hard disk of at least 50GB and an uninterruptible power supply (UPS) units. The application would run perfectly with the minimum requirement stated above. A higher configuration will cause the program to run faster and better.

4.3 Display of Graphical User Interface

Figures 4 – 7 display the graphical user interface of the developed system



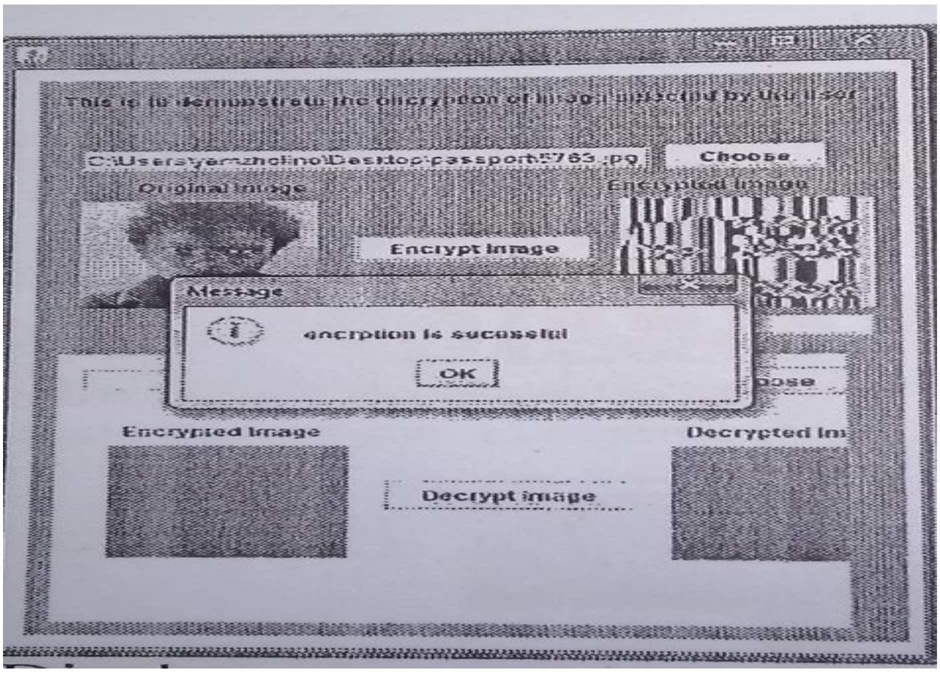
Development of Image Encryption and Decryption Package Using Java Platform

jLabel4

Username:

Password

Figure 4: Login interface of the application



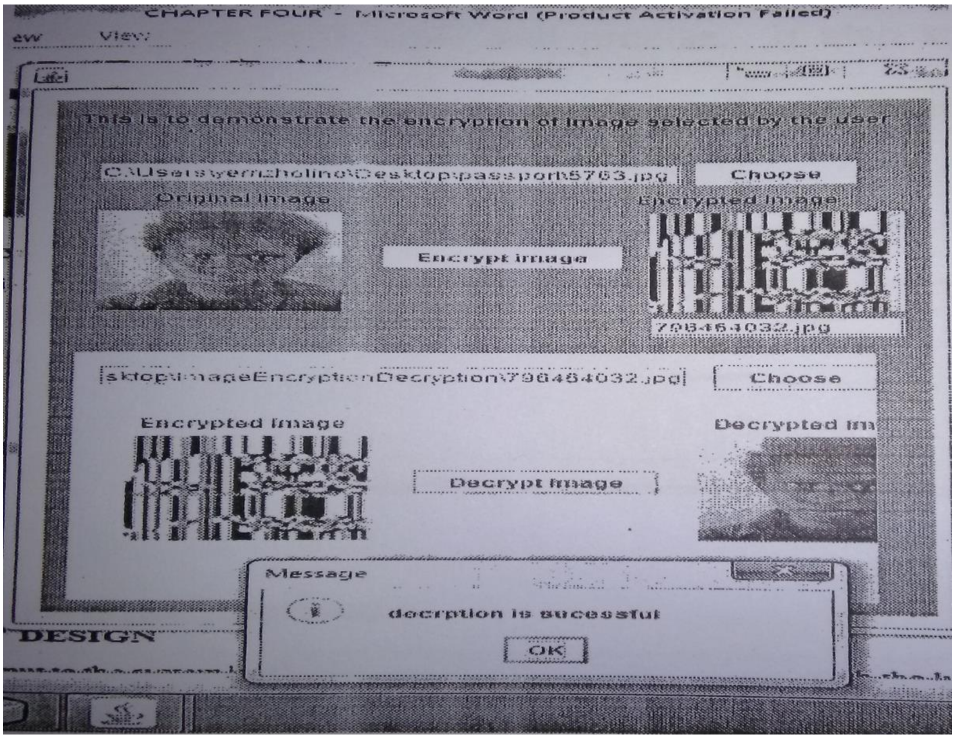
This is to demonstrate the encryption of image selected by the user

C:\Users\yemzholino\Desktop\passport5763.jpg

Message

encrption is sucessful

Figure 5: Encryption output Display



CHAPTER FOUR - Microsoft Word (Product Activation Failed)

This is to demonstrate the encryption of image selected by the user

C:\Users\yemzholino\Desktop\passport5763.jpg

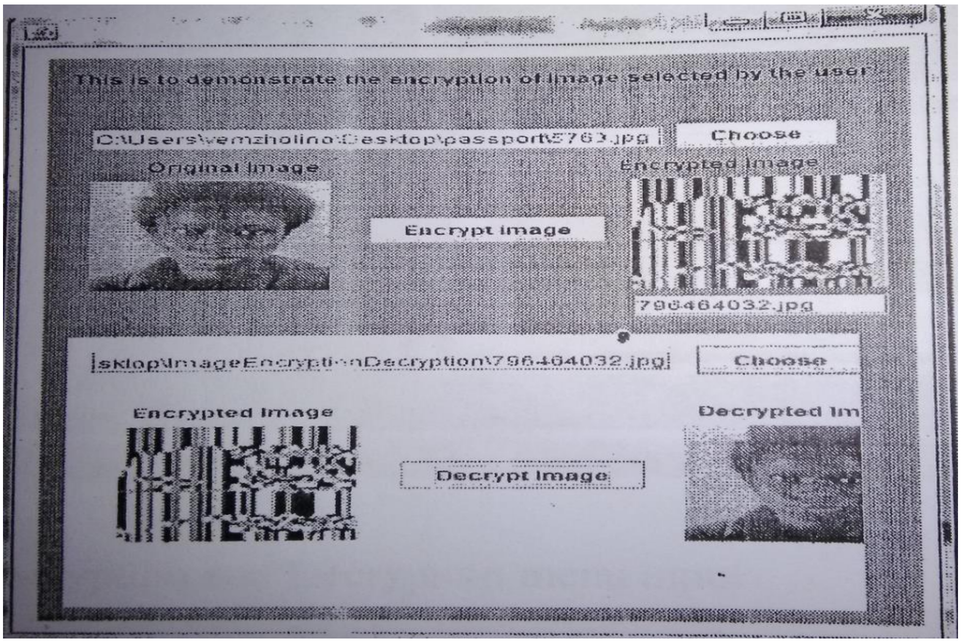
798464032.jpg

sktop\ImageEncryptionDecryption\798464032.jpg

Message

decrption is sucessful

Figure 6: Decryption Output display



This is to demonstrate the encryption of image selected by the user

C:\Users\vemzholino\Desktop\passport\5763.jpg

796464032.jpg

sktop\ImageEncryptionDecryption\796464032.jpg

Figure 7: Complete encrypted and decrypted image process

4.4 Program Description

When the application is launched, a splash screen of the system is displayed with the login page to authenticate the user as in figure 4. The login page, therefore grants access to the main menu of the application. The main menu bar shows the encryption and decryption menu. When the encryption menu is selected, encryption of image starts with the loading of the image and converting it to cipher which is then sent to the receiver who now decrypts the cipher using a specific key. Figure 5 shows a typical image that has successfully been encrypted. Figure 6 is a graphical user interface interaction menu of a successfully decrypted image previously encrypted. Meanwhile, before this is achieved, a text message containing the encryption and decryption key would have been sent to the intended/final owner of the mage. The same key is shared for both encrypted and decrypted image. The process of generating the key is shown in figure 1. Figure 7 shows the complete encryption and decryption interface of the application.

5.0 CONCLUSION

Security in these contemporary times is a must. The built-in protections may not be adequate in most cases and for images as in this case here to be secure; it is necessary to add protections not provided by the computer operating systems. If intruders never tried to break into or steal data from a particular computer, its data will be safe, or if intruders never learned how to get around the simple default mechanisms, additional security might not be necessary. Unfortunately, many attackers do have the skills and resources to break various built-in security systems. One of the most important tools for protecting data from unauthorised access is Encryption, and this study has demonstrated how encryption could be used by developing an application using JAVA platform to secure images.

REFERENCES

Aarthie and Amirtharajan (2014). Image encryption: An information security perspective. *Journal of Artificial Intelligence,* 7:123-135.

Amirtharajan, R., Qin J. and Rayappan, J.B.B. (2012). Random image steganography and steganalysis: Present status and future directions. *Inform. Technol. J*., 11: 566-576.

Amirtharajan, R. Rajesh, V. Archana P.and Rayappan, J.B.B. (2013). Pixel Indicates Standard Deviates: A Way for Random Image Steganography. *Research Journal of Information Technology,* 5: 383-392.

Cheddad A., Condell J. Curran K. and Kevitt P.M. (2010). Digital image steganography: survey and analysis of current methods. *Elsievier, Signal processing* 90: 727-752.

Lala K., Sami B., Thawar A. and Zyad S. (2009). Image encryption using DCT and Stream Cipher. *European Journal of Scientific Research*, 32(1):48-58.

Mohammed A., Bani Y. and Aman Jantan (2008). Image encryption using block-based transformation Algorithm. International Journal of Computer Science, 35(1):1-9.

Qaid, G.R.S. and Talbar, S.J. (2012). Encryption and Decryption of digital Images using color signal. *International journal of computer science*, 9(2):588-592.

Saraf K.R., Jagtap V.P. and Mishra A.K. (2014). Text image encryption decryption using advanced encryption standard, *International Journal of Emerging Trends & Technology in Computer Science*, 3(3): 118-126.

Shaimaa A.E., Khalid K.F.A. and Mohamed M.F. (2010). Securing image transmission in-compression encryption technique. *Journal of computer science and security*, 4(5): 366-381.

Singh J., Hasan H. and Kumar R. (2015). Enhance security for image encryption and decryption by applying hybrid technique using MATLAB. *International Journal of Innovative in Computer and Communication Engineering*, 3(7):6414-6422.

Sharma, P., Godara M. and Singh R. (2014). Digital Image Encryption Techniques: A Review, *International journal of Computing & Business Research*. Pp. 1-6.

Sinha A. and Singh K. (2003). A technique for image encryption using digital signature. *Optics Communications*, 218:229-234.

Stefan, K. and Fabin A. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, London, UK.

Wang, Y., Wong, K.W. Liao X. and Chen, G. (2011). A new chaos-based fast image encryption algorithm. *Applied Soft Comput*., 11: 514-522.

Zeghid M., Machhout M., Khriji I, Baganne A. and Tourki R. (2007). A modified AES based

Algorithm for image encryption. World Academy of Science, Engineering and Technology, 27:206-211.

Zeki, A.M., Manaf A.A. and Mahmod, S.S. (2011). High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373

Zhang Y., Liu W., Cao S., Zhai Z., Nie X. and Dai W. (2009). Digital image encryption algorithm based on Chaos and improved DES. *Proceedings of the IEEE International Conference* on Systems, Man and Cybernetics, San Antonio, TX, USA, 480-485.

Zhu, J. Wang, RD., Li J. and Yan, D.Q. (2011). A huffman coding section-based steganography for AAC audio. *Inform. Technol. J.*, 10: 1983-1988.