CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The advent of personal Computers and Internet facilities has made digital communication, processing and distribution of information easy, economical and available globally all day long. Several applications have been developed to ensure information processing reliable, efficient, fast and secure. In the Information Technology Industry, there has been a series of bridge in the information security of individuals and companies which has led to the fall of many companies and industries. As a result of this bridge in information security, various means has been tried to curb this criminal act leading to many research theories propounded.

Amidst these various theories propounded, the most advanced theory developed was the Cipher-Stream technique, which uses a set of undefined keys generated randomly by a key generator and it has been effectively implemented in all language to ensure Text files were kept secure. The Cipher-Stream Technique seems to be an effective technique but as years will pass, the need for information to be stored in images (Simon,2001). The Cipher-Stream Technique seems to be ineffective as a random generator could be used to break and defile the technique to extract the Information. Various theories have emerged in which the Image Steganography stands to excel using a combination of Cipher-Steam Techniques and embedding algorithms, but the advent of Steganography was not all that was needed because it could also be infiltrated and defile. To enable information processing secure and difficult to read for intruders, Cryptography was introduced in the Babylonia era about 4000 B.C (Thwate, 2013).

As Technology advances, many developed countries have adopted the use of images in information processing in systems such as database, biometrics and security system among many

others. In ensuring the security and validity of information seen via the Internet and every other communication medium, various applications have been developed using various Cryptography Algorithms and Techniques to avoid intrusive attack with one notion in mind that no security system is safe for eternity, it is only safe the day it was developed (Kaur, 2013).

Cryptography is the process of rendering a meaningful piece of data/information difficult, meaningless and useless unless it is rightly decoded. Cryptography measures have long been used by militaries and governments to facilitate secret communication. Cryptography as it stands to useful for civilian activities and also in protecting data in transit, for example data being transferred via networks (for example, the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. When a message is decrypted, it is returned to its original readable form. Cryptography/Encryption can provide strong security for data to give sensitive data the highest level of security (Sharma et al, 2012). The goal of cryptography is to make data unintelligible to unauthorized readers and extremely difficult to decipher when attacked hereby affirming the given definition of encryption given above and Kwang (1967) states that "Cryptography as a process of encoding/enciphering so that its meaning is not obvious." According to Kwang (1967) he regarded Cryptography as the Grandfather of Encoding and Enciphering (Sharma et al, 2012).

Digital Image Cryptography systems differs from the plain text cryptography system such the image size is often larger/bigger than the text size, any tiny change in the pixel of an image doesn't necessarily affect the image unlike the plain text in which any distortion, the whole message is altered and unrecoverable unless via the use of Advanced Data Recovery Algorithms; there is a

high level of data redundancy which is found otherwise in plaintext; there is a strong correlation among adjacent pixels (Sharma et al, 2012).

The scope of the project is to ensure3-Dimensional (3D) images are encrypted, render them unreadable for the intruders and decrypt the message encrypted message through the use of Discrete Cosine Transformation technique

Due to the scope of this study, the focus of this project shall be on the Image Encryption and it will be necessary to understand that the Discrete Cosine Transformation Technique deals with images as numerical values with a distinctive set of integer values representing the image pixels in a matrix form of 8 blocks (i.e. 8x8 matrix).

1.2 Statement of the Problem

The inadequacy of the existing Encryption and Decryption System to produce encrypted and decrypted data with little or no loss of data quality hereby causing insecurity, incorrect delivery of data, poor data quality among many others. To improve the existing system, there is a need for an adequate and a secure system with the capacity to distort the image and re-align the set of images via a mathematical formula to enable decryption move in a reverse array.

1.3 Motivation

Discrete Cosine Transformation Technique stands to be one of the most effective and efficient cryptographic technique for image cryptography. However, it has been implemented only in the 2Dimensional images (black and white). The desire to implement it on 3D images is the motivation for this project work.

1.4 Project Aim and Objectives

The aim of the research is to carry out image encryption using 2-D and 3-D images. The objectives are as follows:

(i) Design an image encryption system using discrete cosine transformation technique

(ii) Implement the digital image encryption design in (i) above.

1.5 Project Report Structure

This report consists of five (5) chapters, each descriptively explaining its designated details. Chapter one consists of the introduction which in concise details explains the content, approaches and methodology to be employed in the project work. It provides the background knowledge of the project, documenting the foundation of the project work. The other arms of the chapter contain statement of the problem, the project motivation, its broad aim and several objectives and also this project report structure.

Chapter two is the literature review; it gives an expository knowledge of the research done into relevant problem domain, appropriate methodologies, proposed solutions and the appropriate technologies that support them. It also documents development of existing systems in the research area or other research area that have tackled similar problems are also documented. It justifies how the overview of related literature has helped the project in view develop or choose its techniques or methodologies.

Chapter three entails the Methodology; it shows the methods, techniques, data collection approach, tools and materials used in achieving the project. It also highlights the requirements specification section which in expanse gives birth to the functional and non-functional requirements gathering process. The analysis phase which describes business process model or other high-level conceptual

view of the required system is also a part of the chapter. Design section describes the system architecture and displays relevant design diagrams which include interesting features of the project design.

Chapter four enumerates Implementation, Result and Discussion; this section of the project documentation presents the implementation related issues such as the approach, materials, platform, languages, tools used and project status as at time of submission. The details of system testing and performance evaluation are documented here. This chapter explains with details the testing, project management and schedule. It highlights other subsections which contain information such as risk management (identification, analysis and mitigation plan), quality management and social, legal, ethical and professional considerations made in completing the project.

Chapter five summarizes and concludes the project report; showing its contribution to knowledge, limitations and envisaged future works. This chapter also critically appraises the project work demonstrating the knowledge and expertise gained from it. Bibliography, references and appendix concludes the project report.

CHAPTER TWO

LITERATURE REVIEW

2.1 Image Cryptography

Cryptography as its meaning denotes, its serves as a strong pillar of information security. As times have passed by, Cryptography has become a vital aspect in information system and is being exploited in many computing fields and areas such as remote access, certificate based authentication, e-commerce, network messaging(e-mails) among many others (Sara and Al-Najdawi, 2012).

Image cryptography is a means of storing, manipulating and transmitting image data in a form that only the targeted personnel can only read or process. The Image Cryptography System stands to replace the old and existing text cryptosystems as text to be sent are converted to images via various methods. The Image Cryptography System ensures images are totally distorted and unreadable for the third party to visualize unless it passes through the process of cryptanalysis, which in many instance it's difficult to break through unless it goes through the reverse order of the cryptography technique used (Sara and Al-Najdawi, 2012).

The Image Cryptography provides series of advantages over the text cryptography system given as follows (Sara and Al-Najdawi, 2012);

(i) Cost for transmitting an image as data reduces at much extent as cost depends upon duration for which data is being transmitted.

(ii) It saves computing power as execution of image transmission takes very less time if the size is lesser.

(iii) It reduces the transmission errors since fewer bits are transferred.

(iv)Secure level of transmission is possible due to encoding and compressing the image.

I will like to note that the Image Cryptography differs from the Image Steganography. In the light of this the Image Steganography involves the Embedment of data or to be precise text into an Image using mediums such as digital signature, image bar code, the quick response code (QR code), captcha etc.

2.2 Image Cryptography Techniques

No security system ever succeeds without an algorithm or a technique because they serve as the basis of the system giving a detailed understanding of how the system should be implemented. As technology and times has passed by, researchers from various angles in the field of computing and information security have made a direct and straight manipulation of the existing old text cryptosystems (Cryptography algorithms and methods) to directly encrypt and decrypt images (Sandeep et al, 2013). Among this algorithm and methods used are:

(i) Advanced Encryption Standard

(ii) Digital Encryption Standard

(iii) The Blowfish Encryption Standard

(iv) Triple DES (3DES) which emanated from the DES where it is stands to replace the DES because of its ability to withstand cryptanalysis.

(v) Twofish Algorithm

(vi) Rivest, Shamir and Adelman algorithm (RSA)

Although there exist various algorithms are used for image cryptography but all other algorithms were established based on the foundation of the above algorithms or combination of two or more of the algorithms (Sandeep et al, 2013).

The digital techniques for image cryptography serve as the basis of the creation of the algorithms above and they are of three (3) major categories (Sharma *et al.*, 2012):

(i.) Position permutation based technique: the order of the pixels of an image is changed hereby transforming the image into an invisible image.

(ii.) Value transformation based technique: the weights and biases of the network are set according to the binary sequence generated from a chaotic system.

(iii.) Visual transformation based technique: this is a combination of both value transformation and position permutation by recording the first pixels and a substitution of values occur using the binary sequence generated via a key generator (chaotic system).

Many other algorithms/techniques have emerged after the existence of the above given algorithm but still the security and the integrity of images encrypted have been found lagging due to the size (N-1 blocks) and the characteristics of the images which differs in a larger part form the text. Due to this lagging discrepancy, research has shown that researchers have used various methods and techniques to ensure image cryptography are of a standard and a guaranteed measure providing the five objectives of security. These techniques though are not 100 percent guaranteed but they earn a maximum guarantee level of 85 percent, no security system/technique is 100 percent secure, it is only 100 percent secure the day it was developed (Sharma *et al.*, 2012).

2.2.1 Image Cryptography Using Hash Function

The Hash Function is a mapping of but strings of an arbitrary finite length to a string of fixed length. A hash function is a mathematical function that takes an input message M of a given length and creates a unique fixed length output code. The code, usually 128-bit or 160-bit stream, is commonly referred to as a hash or a *message digest* (Pethe and Pande, 2016).

A one-way hash function, a variant of the hash function, is used to create a signature or fingerprint of the message - just like a human fingerprint. On input of a message, the hash function compresses the bits of a message to a fixed-size hash value in a way that distributes the possible messages evenly among the possible hash values. Using the same hash function on the same message always results in the same message digest. Different messages always hash to different message digests A cryptographic hash function does this in a way that makes it extremely difficult to come up with two or more messages that would hash to a particular hash value. It is conjectured that the probability of coming up with two messages hashing on the same message digest is on the order of 264**,** and that of coming up with any message hashing on a given message digest is on the order of 212.

In ensuring data integrity and authenticity, both the sender and the recipient perform the same hash computation using the same hash function on the message before the message is sent and after it has been received. If the two computations of the same hash function on the same message produce the same value, then the message has not been tampered with during transmission. There are various standard hash functions of message digest length including the 160-bit (Message Digest 5(MD5), Secure Hash Algorithm (SHA-1)) and 128-bit (RSA, MD2, and MD4) in which the hash data strings (occur mostly to be integers) change their state from the natural image state to a set of unnatural state. Message Digest hash algorithms MD2, MD4, and MD5 were developed by Ron Rivest, while the Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST). The most popular of these hash algorithms are the SHA and MD5. The Hashing Algorithm encrypts digital images with password protection using 1D SHA-2 algorithm coupled with a compound forward transform (Pethe and Pande, 2016).

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 (XOR), a logical symmetric operation, that yields 0 if both binary pixels are zeros or if both are ones and 1 otherwise (Abbas et al, 2010). The security system built using this algorithm use an increasing strong cryptographic methods that put to void all patterns and statistical analysis attempts. This approach to Image Cryptography retains the structures readily available in the unencrypted bit for a little while and these structures always comply with the standard multimedia codec such as the Jpeg or MPEG-1/2/4 standards.

Although the Hash Function is safe and secure but it doesn't give an image as it results because it converts and get the hash values of each and every data into a set of hash values. It has its short comings in the area of providing an encrypted Image distorted in characteristics and pixel. The Hash Algorithm is best used in a Steganography System than a Cryptography System.

The Hashing Algorithm remains unreliable and secure due to the lack of a general database system which will store all hash value and their equivalent images. And if there exist a database there is little or no more guarantee on Image Information encrypted because a database system is prone to attack via the brute force.

2.2.2 Image Cryptography Using the Chaotic Algorithm

The Chaotic Algorithm is a symmetric key stream cipher algorithm that makes use of the sensitivity of the initial condition as well as on system parameter also regarded as the chaos (Ismail, Amin and Diab, 2010). This System uses a chaotic map to derive its secret key and this secret key is generated following the procedures given below (Ismail, Amin and Diab, 2010):

(i.) Mixing property: Mixing property of chaotic maps is closely related to property of diffusion in encryption transformations (algorithms). If we think of the set of possible (sensible) plaintexts as an initial region in the phase space of the map (transformation), then it is the mixing property (or in other terms, sensitivity to initial conditions) that implies \spreading out of the influence of a single plaintext digit over many ciphertext digits".

(ii.) Robust chaos: A good encryption algorithm spreads also the influence of a single key digit over many digits of ciphertext. The keys of an encryption algorithm represent its parameters. Therefore, we should consider only such transformations in which both parameters and variables are involved in a sensitive way.

(iii.) Parameter set: One should consider only systems that have robust chaos for large set of parameters (keys), larger parameter space of the dynamical system implies that its discriminated version will have larger *K*. In this paper, we design the proposed cipher using logistic chaotic maps.

2.2.3 Image Cryptography Using the Block Based Transformation Algorithm

Younes and Janat (2008) proposed this transformation technique in which the *original* image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers

to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels' keep their neighbors (Komal and Sonal, 2011). In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. A general block diagram of the transformation method is shown in Figure 2.1.

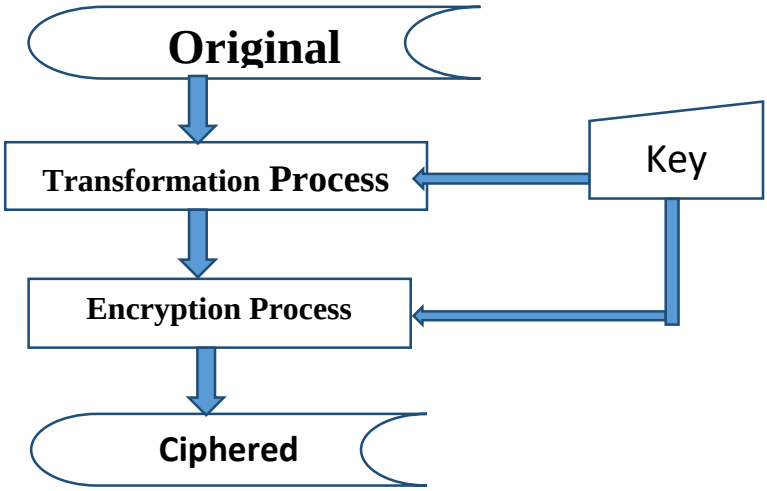

Figure 2.1 General Block Based diagram for Image Encryption (Younes and Jantan, 2008).

The block-based transformation algorithm is based on the combination of image transformation followed by encryption (that is, transformation algorithm followed by the Blowfish algorithm). The transformation algorithm and the Blowfish algorithm use the original image to produce three output images (Sandeep, Sukhpreet and Sonia,2013):

(i.) A ciphered image using Blowfish

(ii.) A transformed image using the Block Based transformation process and

(iii.) A transformed image encrypted using Blowfish.

The correlation and entropy of the three images are computed and compared with each other. This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value. The experimental results of Block Based Algorithm indicate visibly that there exists an inverse relationship between blocks and correlation, and direct relationship between number of blocks and entropy. The comparative analysis also identifies that the Block Based Algorithm has its best performance in the lowest correlation and highest entropy (Sandeep, Sukhpreet and Sonia,2013).

2.2.4 Image Cryptography Using the Genetic Algorithm

Rasul and Abdul (2011) proposed the Genetic algorithm based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In this technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

2.2.5 Image Encryption Using the Hyper Chaotic Algorithm

The Hyper chaotic algorithm uses a Hyper Chaos map employed to confuse the relationship between the encrypted image and plain-image. The shuffling process is made plain-image dependent and confusion process through hyper-chaotic map is made encrypted image dependent, by executing it in the cipher-block-chaining mode of encryption. This makes the algorithm robust

against cryptographic potential chosen-plaintext and known-plaintext attacks (Ahmad and Al-Sharari, 2013).

The Hyper Chaotic algorithm is based on the concept of inter-component shuffling of image pixels using Arnold transform, then changing the gray values of the shuffled image using hyper-chaotic map. The control parameters of shuffling are extracted from the pending plain-image. The shuffling is inter-component scrambling that is, the content of whole scrambled image doesn't change after scrambling, but it alters the contents of each component. The scrambled image is then encrypted using the preprocessed sequences generated by a 2D hyper-chaotic system. To get good encryption quality, the two key values are utilized to encrypt one pixel. The encryption is executed in CBC mode to make the process of confusion to encrypted image dependent. This way, the whole algorithm is made dependent to the pending plain-image, to make the potential cryptographic attacks infeasible, thereby improving the robustness of the algorithm against cryptanalysis (Ahmad and Al-Sharari, 2013).

The experimental analysis and results demonstrate that the proposed algorithm has desirable properties like: high sensitivity to a small change in secret keys and plain-image, low correlation coefficients, low chi-square scores and large information entropy. All these features verify that the proposed algorithm is robust and effective for practical color image encryption (Huang and Nien, 2009).

This Algorithm will have served to be it best and one of the secure algorithm for Image Cryptography but it focuses more on the Color image format neglecting the aspect of Mono colored image. The Figure below shows the experimental results derived after implementation:

Figure 2.2a: Original Image

Figure 2.2b: Image in the Encrypted Form

Figure 2.2c: The Decrypted Image

2.2.6 Image Cryptography Using Digital Holography

A Hologram is a three-dimensional image formed by the interference of light beams from a laser or other coherent light source. It is also a photograph of an interference pattern which, when suitably illuminated, produces a three-dimensional image. Javidi and Nomra proposed the Holography System that uses the Fourier Transformation Technique both for the Forward Encryption and the backward Decryption.

The Fourier Transformation uses the technique of randomly generating a matrix value for the images to be encrypted only to be displayed by the ray of light shine on the Image to be Encrypted and vice versa.

All images obtained by the inverse Fourier transforming of the digital hologram of the encrypted data renders the original images unrecognized which is majorly a setback in the Image Cryptography standard (Javidi and Nomra).

2.3 Image Cryptography Using Image Compression Technique

Image Compression is the process of giving out a compact representation of an image, as a result hereby reducing the image storage, transmission requirements and visual characteristics. Compression is achieved by the removing one of the following redundancy (Dinesh *et al.*, 2015):

(i) Coding

(ii) Inter-pixel

(iii)Perceptual

(Dinesh et al, 2015) Coding redundancy emerges when the codes assigned to a set of events such as the pixel values like position, intensity of illumination, of an image have not been selected to take full advantage of the probabilities of the events. It is only possible to represent an image having compressed resolution by taking these three redundancies approach into consideration. Decoding is done to get the original image explicitly, Decoding is the process of reversing the cryptography scheme to get the image whether through the proper decoding algorithm or otherwise and this process is often referred to as Cryptanalysis. The major objective of compression is to reduce the number of bits to much possible extent, while keeping the resolution and the quality of the reconstructed image as close to the original image as possible.

Image compression systems always consist of two blocks: an encoder and a decoder. Image in the form of 2-D matrix denoted as f (x, y) is fed into the encoder. If we let n and m denote the number of units that carry information (both actual) in the original and preprocessed images respectively, the compression that we get is calculated through the compression ratio, CR = n/m. The encoder reduces all three redundancies of input image in three phases (Kaur, 2013).

The first phase is where the Image mapper translates the input image into a format suitable to reduce inter-pixel loop-holes.

In the second phase is often regarded as the Quantization process, the quantizer reduces the mappers output accuracy in accordance with a predefined value.

In the third phase, a symbol decoder generates a random code for quantizer output and maps the output in accordance with the given code. These blocks when operates in reverse order, the inverse operations of the encoders symbol coder and mapper block are performed. These techniques majorly known as the Image Compression technique have been broadly divided into two major areas (Kaur, 2013);

(i) Lossy Compression Technique

(ii) Lossless Compression Technique

2.3.1 Lossless Compression

The lossless compression (as the name suggests) ensures Images are reconstructed after compression without errors, i.e. no information is lost. One reason why the lossless coding schemes are preferred to the lossy coding scheme is that the lossless compression has a lower computational demand to the lossy compression. For all lossless compression techniques, there is a well-known trade-off: Compression Ratio-Coder Complexity-Coder Delay. Lossless Compression typically is a process with three stages:

(i) The model: the data to be compressed is analyzed with respect to its structure and the relative frequency of the occurring symbols.

(ii) The encoder: produces a compressed bit stream / file using the information provided by the model.

(iii) The adaptor: uses information extracted from the data (usually during encoding) in order to adapt the model (more or less) continuously to the data.

The basic idea in lossless compression is to use code words which are shorter (in terms of their binary representation) than their corresponding symbols in case the symbols do occur frequently. It is also known as entropy coding as it uses decomposition techniques to minimize loopholes. The original image can be perfectly recovered from the compressed image, in lossless compression techniques. These do not add noise to the signal. It is also known as entropy coding as it uses decomposition techniques to minimize redundancy. The following techniques are included in lossless compression:

(i.) Huffman encoding: Huffman Coding is a popular technique using the idea of variable length coding combined with a constructive algorithm how to build the corresponding unique code words. Suppose we have given a source S with an alphabet of size n. The two least frequent symbols are combined into a new virtual symbol which is assigned the sum of occurrence probabilities of the two original symbols. Subsequently, the new alphabet of size n−1 is treated the same way, which goes on until only two symbols are left. If we know the code words of the new symbols, the code words for the two original symbols are obtained by adding a 0 and 1 bit to the right side of the new symbol. This procedure is applied recursively, i.e. starting with the two most frequent symbols which are assigned code words 0 and 1, we successively add corresponding bits to the right until code words for all original symbols have been generated. The example has entropy H(S) = 2.15, the generated Huffman code have average code length of 2.2 bits/symbol, an ad-hoc generated code like shown before, like e.g. {0, 10, 110, 1110, 1111} has average code length of 2.25 bits/symbol.

The Huffman coding is not the best for Image encryption as it encounters the following problem while encrypting:

(a.) In case a source has a symbol with p(s) close to 1 and many others with small probability of occurrence we result in an average code length of 1 bit/symbol since the smallest length for a code word is of course 1 bit. The entropy is of course much smaller (recall the coding of differences).

(b.) In case of changing statistics of the source one can easily obtain a data expansion.

(c.) Since a fixed codebook is of poor quality in many cases we have a two stage algorithm: building statistics (the model), generate the code.

(d.) It is difficult to implement its Adaptation characteristics, since changes in the statistics affect the entire tree and not just a local part. We can either store corresponding Huffman tables (trees) in the data [which is inefficient in terms of compression] or compute them on the fly from decoded data [which is inefficient in terms of compression speed].

(ii.) LZW coding: The Lempel-Ziv-Welch algorithm is named after the three inventors and is usually referred to as the LZW algorithm. The original idea is due to Lempel and Ziv and is used in the LZ77 and LZ78 algorithms. LZ78 constructs a code book(dictionary)during compression, with entries for combinations of several symbols as well as for individual symbols. If, say, the ten next symbols already have an entry in the code book as individual symbols, a new entry is added to represent the combination consisting of these next ten symbols. If this same combination of ten symbols appears later in the text, it can be represented by its code. The LZW algorithm is based on the same idea as LZ78, with small changes to improve compression further. LZ77 does not store a list of codes for previously encountered symbol combinations. Instead it searches previous symbols for matches with the sequence of symbols that are presently being encoded. If the next ten symbols match a sequence 90 symbols earlier in the symbol sequence, a code for the pair of numbers (90,10) will be used to represent these ten symbols. This can be thought of as a type of run-length coding. One problem with the LZW Algorithm that makes it unreliable is that the

dictionary can get too large and eventually the code word formed mix up and there is confusion in the system.

2.3.2 Lossy Compression Technique

Lossy compression methods have larger compression ratios as compared to the lossless compression techniques. By this the output image that is reconstructed image is not exact copy but somehow resembles it at larger portion.

As shown in Figure 2, this prediction – transformation – decomposition process is completely reversible. There is loss of information due to process of quantization. The entropy coding after the quantizing, is lossless. When decoder has input data, entropy decoding is applied to compressed signal values to get the quantized signal values. Then, de-quantization is used on it and the image is recovered which resembles to the original (Kaimal and Manimurugan, 2013). The Lossy compression methods include some basic consideration from the angle of performance as given below (Dinesh et al, 2015):

(i.) Speed of encoding and decoding: the speed at this level of encoding and decoding is at its peak performing the work of compression and decompression.

(ii.) Compression ratio

(iii.) SNR ratio.

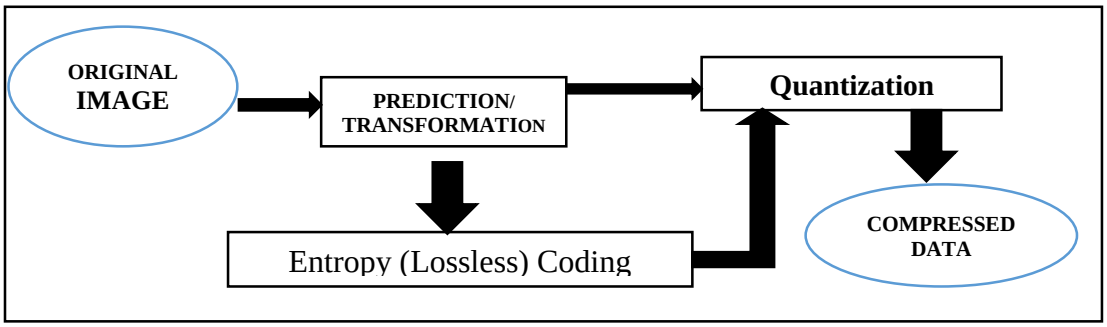

Figure 2.3: Lossy Image Compression (Kaimal and Manimurugan, 2013).

Lossy compression includes following methods (Dinesh et al, 2015):

(i) Block truncation coding

(ii) Code Vector quantization

(iii) Fractal coding

(iv) Transform coding

(v) Sub-band coding

2.3.2.1 Block Truncation Coding

In this, image is divided into blocks like we have in fractals. The window of N by N of an image is considered as a block. The mean value of all values of that window consisting a certain number of pixel. The threshold is normally the mean value of the pixel values in the vector. Then a bitmap of that vector is generated by replacing all pixels having values are greater than or equal to the threshold by a 1. Then for each segment in the bitmap, a value is determined which is the average of the values of the corresponding pixels in the original code vector (Dinesh et al, 2015).

2.3.2.2 Code Vector Quantization

The basic idea in Vector Quantization is to create a dictionary of vectors of constant size, called code vectors. Values of pixels composed the blocks called as code vector. A given image is then parted into non-recurring vectors called image vectors. Dictionary is made out this information and it is indexed. Further, it is used for encoding the original image. Thus, every image is then entropy coded with the help of these indices (Dinesh et al, 2015).

2.3.2.3 Fractal Compression

The basic thing behind this coding is to divide image into segments by using standard points like color difference, edges, frequency and texture. It is obvious that parts of an image and other parts

of the same image are usually resembling. Here, there is a dictionary which is used as a look up table called as fractal segments. The library contains codes which are compact sets of numbers. Doing an algorithm operation, fractals are operated and image is encoded. This scheme is far more effective for compressing images that are natural and textured (Dinesh et al, 2015).

2.3.2.4 Subband Coding

In this scheme, quantization and coding is applied to each of the analyzed sub-bands from the frequency components bands. This coding is very useful because quantization and coding is more accurately applied to the subbands (Dinesh *et al*, 2015).

2.3.2.5 Transform Coding

In this coding, transforms like Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT), Discrete Cosine Transform are used to alter the pixel specifications from spatial domain into frequency domain. One is the energy compaction property; some few coefficients only have the energy of original image signal that can be used to reproduce itself. Only those few significant coefficients are considered and the remaining is discarded. These coefficients are given for quantization and encoding. DCT coding has been the most commonly used in transformation of image data (Dinesh *et al.*, 2015). The rationale behind transform coding is that If Y is the result of a linear transform T of the input vector X in such a way that the components of Y are much less correlated, then Y can be coded more efficiently than X. If most information is accurately described by the first few components of a transformed vector, then the remaining components can be coarsely quantized, or even set to zero, with little signal distortion (Dinesh et al, 2015).

The Discrete Cosine Transformation(DCT) and the Discrete Fourier Transformation (DFT) uses the mathematical approach to Image Encryption and Decryption. The DCT and the DFT converts

the image into a matrix and converts the matrix values into a set of distinguished values which distorts the original image and makes it difficult to read (Dinesh *et al.*, 2015).

Sara and Nijad (2012) proposed the Discrete Cosine Transformation after carrying out several researches on other various cryptography algorithm to be the most efficient and secure algorithm for encryption. The aim of the experiment was to determine the most secure, efficient method of acquiring the visual quality of each encryption algorithm both during the encryption process and after the encryption process (Dinesh *et al*., 2015).

2.4 Image Encryption using The Discrete Cosine Transformation

The Discrete Cosine transformation (DCT) is a mathematical transformation technique for converting a signal and transform it from its spatial domain into a frequency domain (Lala *et al*.,2009). The Spatial domain indicates how many times the pixel values of an image change across a block. It expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. It is a Fourier related transformation technique similar to the discrete Fourier transformation but it stands to be distinguished as it only deal with real numbers.

In the Discrete Cosine transformation, the following process occurs (Li and Drew 2003):

(i) The image is broken into m x n blocks of pixels. Where m is the number of row and n is the number of column.

(ii) Working from left to right, top to bottom, the DCT formula is applied to each pixel values in a block.

(iii) Each block is compressed through quantization into an array.

(iv)The array of the compressed block that constitutes the image is stored into a drastically reduced amount of space in an array.

(v) When desired, the image is reconstructed through decomposition.

The DCT is applied in so many dimension but for the scope of this research, I will be considering the 3-dimensional form.

2.4.1 Definition of DCT

Given an input function *f(i,j)* over two integer variables i and j (a piece of an image), the DCT transforms it into a new function F(u,v), with integer u and *v* running over the same range as *i* and *j*. the DCT transformation is defined generally as(Li and Drew,2003):

$$D(u,v) = \frac{2}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} .P(x,y).\cos\frac{(2x+1)\times u\pi}{2\times M} \cdot \cos\frac{(2y+1)\times v\pi}{2\times N} \quad (2.1)$$

where M, N is the number of blocks on the row and column of an image block, u = 0, 1……, M-1, v = 0, 1, ..., N-1.

P (x, y) is the image matrix of m-columns by n-rows.

if u, v=0 the equivalent cos(u) and cos(v) = cos (0) =1, therefore we have the DCT formula to be;

$$D(u,v) = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} P(x,y) \quad (2.2)$$

After the transformation process the matrix P(x,y) has been transformed and the transformed values are stored in a new image matrix D(u,v). the new matrix D(u,v) is then transposed, multiplied by P(i,j) and the inverse of its transpose.

$$P(i,j) = P(x,y) - pixel \quad (2.3)$$

Where pixel is as determined by the user and its constant throughout the operation.

$$DC(x,y) = D(u,v) \cdot P(i,j) \cdot D(u,v)' \quad (2.4)$$

DC (x, y) now consists of MxN Discrete Cosine Transformation coefficient, with the top leftmost coefficient DC (x, y) correlating to the lowest frequency of the original image block. Moving forward and downward from the DC (0,0) the DCT coefficients correlate to higher frequencies of

the image block. It is important to identify the fact that the human eye is most sensitive to low frequencies, although this fact cannot but be affirmed as the quantization step will reflect and ascertain this fact (Li and Drew, 2003).

2.4.2 Quantization

Quantization is the process of reducing the number of possible bits needed to represent the encrypted image to be. This serves to be the major function of the Lossy compression and it is distinguished in three forms as follows (Li and Drew,2003):

(i) Uniform Quantization: this partition the domain of input values into a set of equally spaced intervals with the exception of the two outer intervals. The output or reconstruction value corresponding to each interval is taken to be the midpoint of the interval, and the length of each interval is referred to as the step size denoted by Δ. The Uniform quantization exhibits in two form, the Midrise (at output level all numbers are even) and the Midtread (at output level all numbers are even) quantizers (Li and Drew,2003).

(ii) Non-uniform Quantization

(iii)Vector Quantization: Unlike the Uniform and the Compound which uses the scalar quantization method, its makes use of the vector quantization. It uses a Vector Quantization code vectors with *n* components. The collection of these code vectors form the *codebook*. This vectors are formed by concatenating a number of consecutive samples into a single vector sample.

According to Shannon's (1948) he emphasized that any compression system performs better if it operates on vectors or groups of samples rather than individual symbols or samples. The DCT compression technique employs the Vector quantization technique to improve its performance capabilities (Li and Drew,2003).

Quantization in DCT is achieved by dividing each element in the transformed image matrix DC(x,y) by the corresponding element in the quantization matrix(*Q*), then rounding off to the nearest integer value that can be represented in just three bits. The Quantization matrix(*Q*) is derived by rounding off the D (*u, v*) into the nearest integer that can be represented in 3 bits and divide by a weight(w) constant of ¼ then round off(Li and Drew 2003).

DCT quantized matrix is now represented as:

$$C_{i,j} = round\left(\frac{DC(x,y)}{Q(i,j)}\right) \tag{2.5}$$

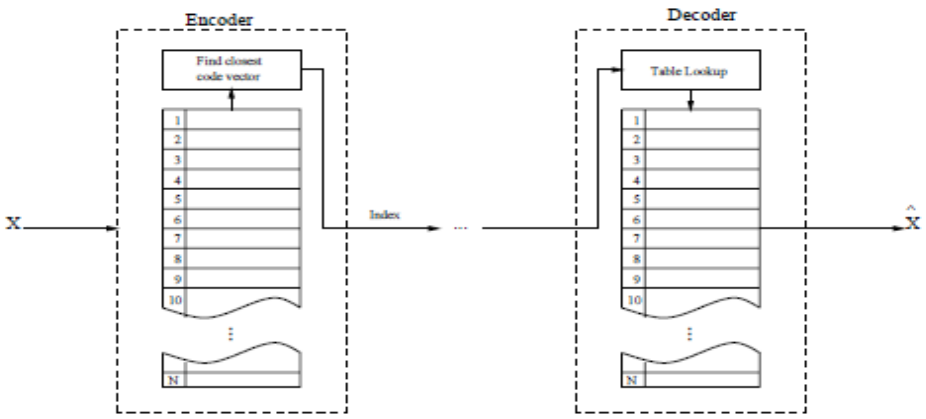

Figure 2.4: Basic DCT vector quantization process table (Li and Drew,2003).

After the quantization it is of a high priority to note that the image will have lost most of its high frequencies of pixel values to become zero and the remaining non-zero's value will be used to construct the image.

2.4.3 Coding

After the process of quantization, the image matrix C is ready for the final lap of compression, and this is performed simply by converting all coefficients of C by an encoder to a stream of binary data representing the pixel value of the Image Matrix. The coding aids the combination of several

and relatively large data of zeros which are easily compressed. The following sequence or order of compression is continuous for a M by N block (Li and Drew 2003).

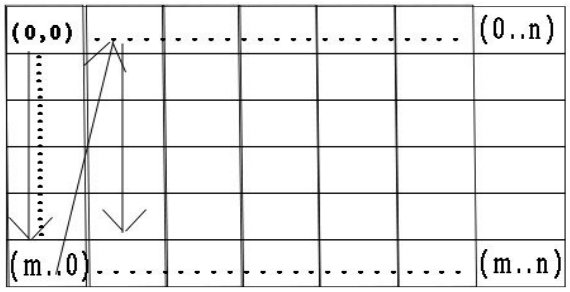

Figure 2.5 Sequential movement for M by N block (Li and Drew,2003).

During this process the DCT formalizes this notion with a measure of how much the image contents(pixels) change in correspondence to the number of cycles of a cosine wave per block (refer to the cosine function in equation (i)). Mathematically, the cosine waves flows from the range of -1 to +1 depicting an assurance of an unstable range of numerical values between -1 to +1. From this knowledge we can ascertain that as the number of rows and columns increase the DCT cosine function produces a relatively odd numeric figure of 0's than 1's (Li and Drew,2003).

CHAPTER THREE

METHODOLOGY

Methodology is the underlying principles and rules that govern a system method; on the other hand it is a systematic procedure for a set of activities. Thus, from these definitions a methodology encompasses the methods used within a study.

3.1 Requirements Specification

3.1.1 Requirement Gathering Technique

This was done via proper analysis of the existing the system. Reference was also made to some existing documents gotten from existing systems. Some materials were also downloaded from the internet for the purpose of reviewing the work.

3.1.2 Functional Requirement Specification

The functional requirements describe the essential functionality of the system. It gives a descriptive detail of what the system must possess and what necessary and important action at it shall perform.

Requirement	Requirement Specification
Input	a. The system is developed to allow the users select their desired image to be encrypted. b. The system is developed to accept images of only .Jpeg Format.
Encryption	The system is developed to convert the selected Images into a set of images difficult to understand.

Decryption	The system is developed to reverse the encrypted image back into its original form without little or no loss of image quality.

Table 3: Functional Requirement of the System

3.1.3 Non-functional Requirement Specification

Non-functional requirements refer to behavioral properties that the system must have, such as performance and usability. Non-functional requirements may influence the rest of analysis (functional, structural, and behavioral models). They help to make decision useful decisions such as the user interface, the hardware and software, and the system's underlying physical architecture.

Non-functional Requirement	Specifications
Operational Requirements	a. The system is developed to run on all devices using the Windows Operating System. b. The system will be able to read Images and write Images to File i.e. Save Images. c. The system will be able to import Images only in JPEG format. d. The system is developed to operate on a the Java Virtual Machine (JVM) called the Java Mission Control.
Performance Requirements	a. Response time is less than 10 seconds. b. The system is developed to Save File in JPEG formats.

Table 3.1: Non-Functional Requirements of the System

3.2 Analysis

3.2.1 Existing System

Various systems as evolved as various scholars and programmers have developed Image Encryption systems to ensure private information are kept private and vice versa. Due to the scope of this research, I will be critically analyzing a popular application for encrypting images which is known as the Aspose Imaging. The Aspose imaging functions by converting the image format and transform it into a .PSD format or at the user discretion.

After a concrete evaluation and study of the existing system, the following are the shortcomings of the existing system:

(i) Its encryption technique is easy to breach via stalling and observation of messages pattern

(ii) The authentication system is weak to withstand various

3.2.2 The Image Encryption System

The system is an application that runs on the windows operating system that allows users encrypt and decrypt images for security reasons. The application allows the user decide the format to save the encrypted and decrypted images.

3.3 Design

System design is a discipline within the software development industry which seek to provide a framework for activity and the capture, storage, transformation and dissemination of information so as to enable the economic development of computer systems that are fit for purpose.

3.3.1 System Architecture of the Image Encryption System

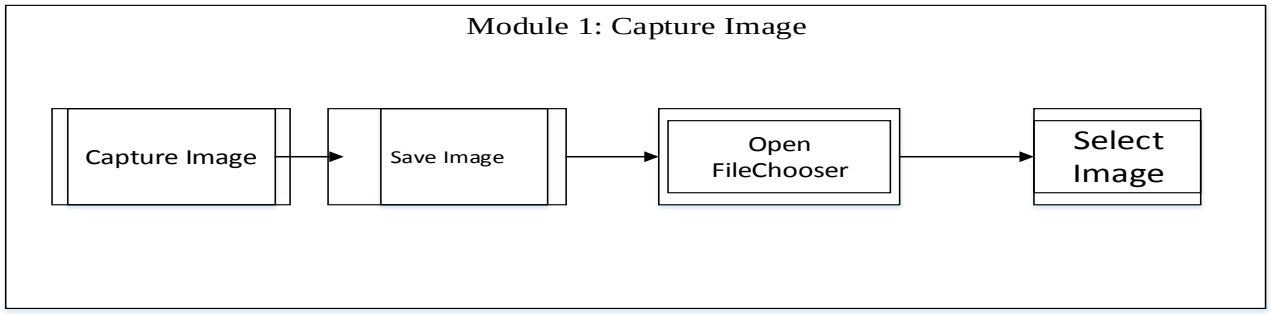

Figure 3.1: Image Capture Module

The module gives a detailed description of how the image to be encrypted is captured, stored and selected for the encryption stage.

3.3.1.1 Capture Image

In this stage, the image is capture via any image capturing medium such as photographic cameras, web cameras, electromagnetic cameras and many more. The image to be captured has no specific pixel value and it doesn't have any width and length.

3.3.1.2 Save Captured Image

The image captured is saved to the system with the Image format of, JPEG and other PEG format. The image file is saved to the user's desired location. It saves the image using the user desired name and image format.

3.3.1.3 Open File Chooser/Select Image

This is a form view selection mode prompted by the system which allows users make appropriate decision on which image they desire for the encryption operation. It is also flexible by allowing the users to change the selected image if discovered the image is not correctly selected.

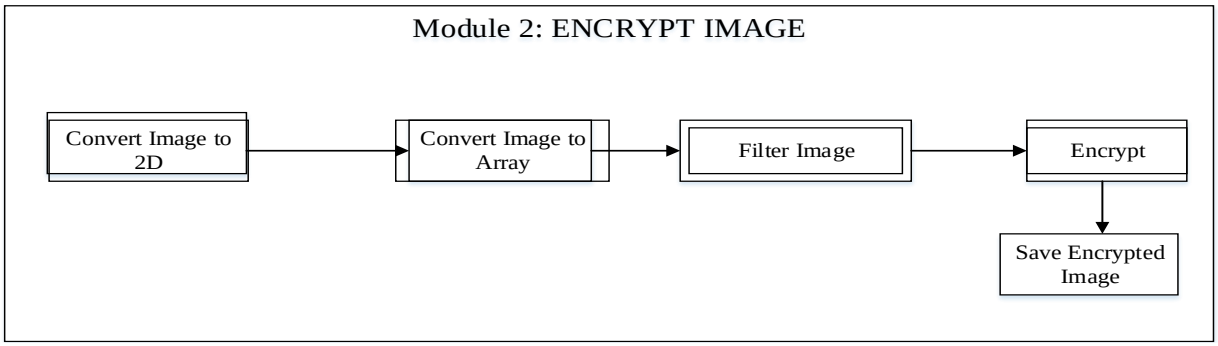

Figure 3.2: Image Encryption Module for Image Encryptor

3.3.2 Encryption Module

This stage ensures that the image selected in the Image Capture Module is secure and it is kept secret. In this module, there are various sub processes that enables the system encrypt images efficiently. These process are given below as:

3.3.2.1 Convert Image to 2-Dimensional Form

For every image captured they are restricted to the 3D form, in as much as to enable the Image ready for encryption, the image is converted to a 2D image to allow the filtering of Images. The algorithm for the module is given as follows:

Step 1: Start

Step 2: Retrieve the Captured Image

Step 3: Get the Image Width and represent it with W

Step 4: Get the Image Height and represent it with H

Step 5: Let MxN be the matrix to represent the Image

Step 6: Let M represent W and N represent H

Step 7: Image is now represented as WxH Matrix.

Step 8: End

3.3.2.2 Image Conversion Module

The selected image is converted to an array model in which the Image in 3D model is converted to 2D model to enable the system perform the DCT operation on the selected image. The algorithm for the module is given below

Step 1: Start

Step 2: Let R represent Red in the Image RGB pixel value

Step 3: Let G represent Green in the Image RGB pixel value

Step 4: Let B represent Blue in the Image RGB pixel value

Step 5: Get the Red Value in the RGB pixel value and store in R

Step 6: Get the Green Value in the RGB pixel value and store in G

Step 7: Get the Blue Value in the RGB pixel value and store in B

Step 8: Let i,j represent the counter for R,G,B

Step 9: The image is now represented as WxH(i,j)

Step 10: End

3.3.2.3 Image Filtering Module

The Image converted to an array is then filtered using the Low Pass Filter. The process of filtering is such that the ambiguous pixel values are reduced in such a way to lower values so as to produce an image quality of less than the desired value. The algorithm for this module is given as:

Step 1: Retrieve Image WxH(i,j)

Step 2: Counter i,j=R|G|B

Step 3: Perform bitwise shift on R,R= R>>16

Step 4: Perform bitwise shift on G, G=G>>8

Step 5: Perform bitwise shift on B, B=B>>0

Step 6: Store the R, G, B values in the counter i,j =R|G|B

Step 7: Image becomes WxH(i,j)

Step 8: End

3.3.2.4 Image Encryption Module

At this stage the transformation technique is applied on the Filtered Image and the image is ready to as an encrypted image. The algorithm for this module is given as:

Step 1: Start

Step 2: Retrieve image from the Image Filtering Module

Step 3: Sum all the pixel values into Pixel

Step 4: Apply the DCT equation on the Image using the pixel as its co-efficient factor.

Step 5: Encrypted image is given in WxH(i,j)

Step 6: Let the new Image be represented in W_1xH_2

Step 6: End

3.3.3 Image Encryption Flow Chart

The flowchart diagram is a pictorial illustration of how the system operates, giving a vivid understanding of its operational processes and it functional processes. Figure 3.5 gives the flowchart representation of the proposed system.

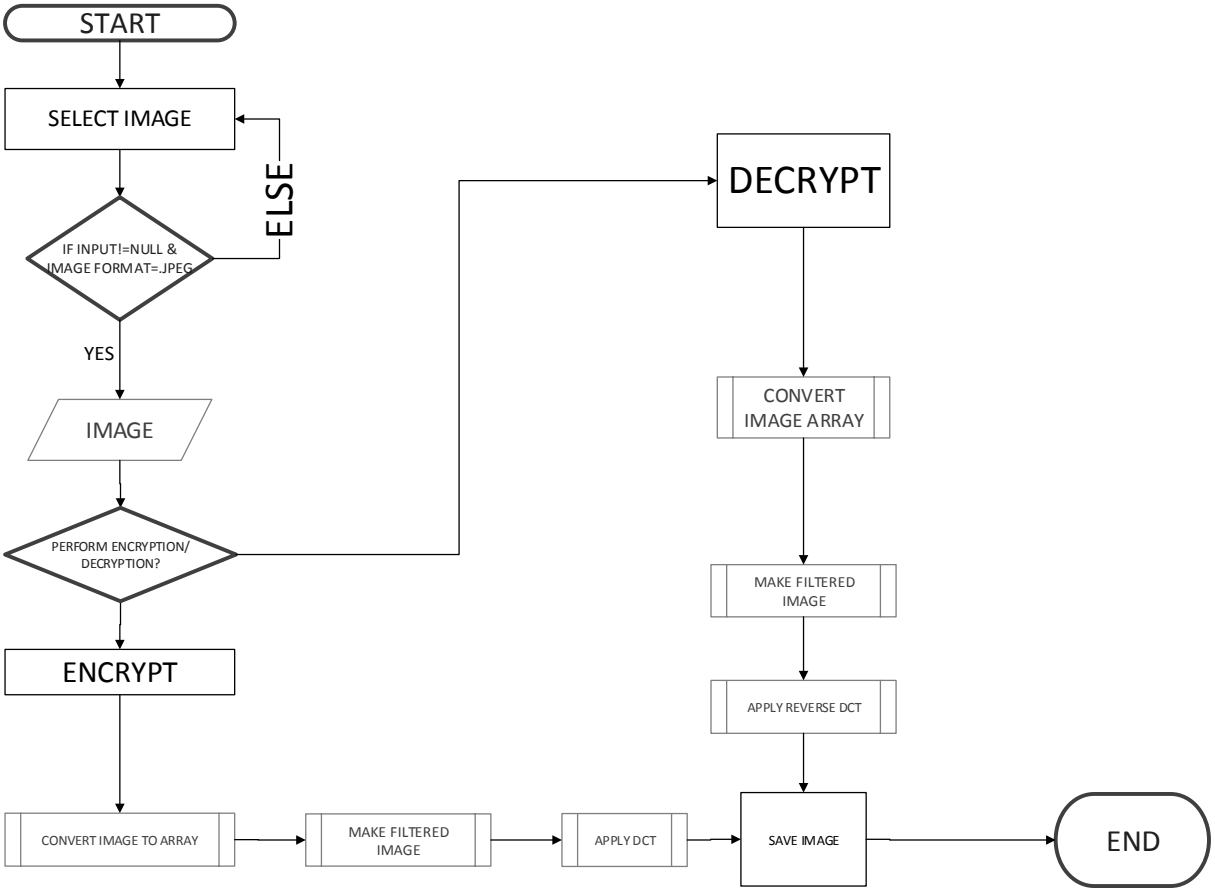

Figure 3.2: Flowchart Diagram illustrating the process of the Image Encryption System.

CHAPTER FOUR

IMPLEMENTATION, RESULT AND DISCUSSION

4.1 Interface Design

The interface design consists of the system operations that are visible to the users, the interface helps bridge the gap between the users and the system. The interface design assist users get maximum usage of the system. The system designed has a simple interface allowing the users perform all operations at the entry point as in Figure 4.1.

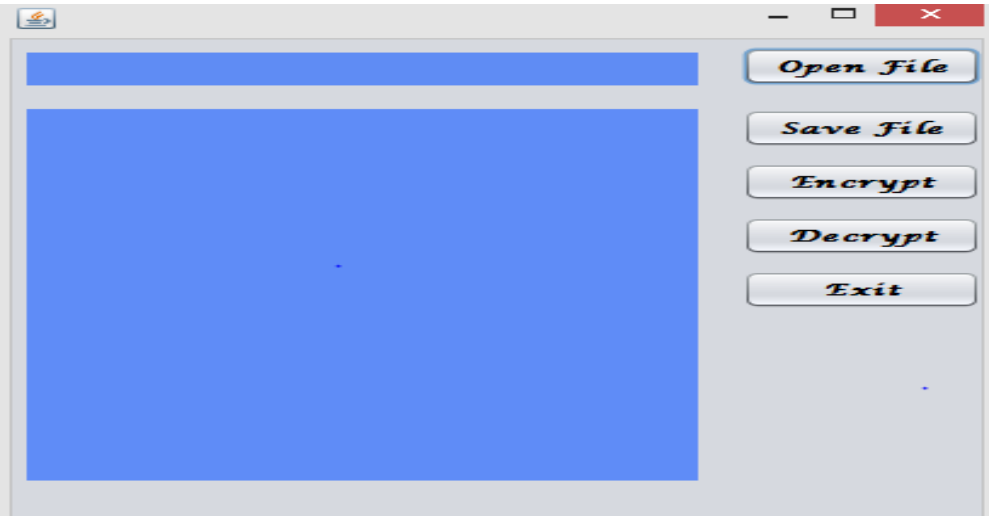

Figure 4.1: The interface design of the proposed system.

Open File

The Open File button allows the users to select their desired image to be encrypted. It performs its function by using the Abstract Windows Toolkit File Chooser as shown in Figure 4.2 below. It allows navigation from the Main Disk Drive to other locations on the system where the image is stored. It is an interactive form view where users literally maneuver around the system.

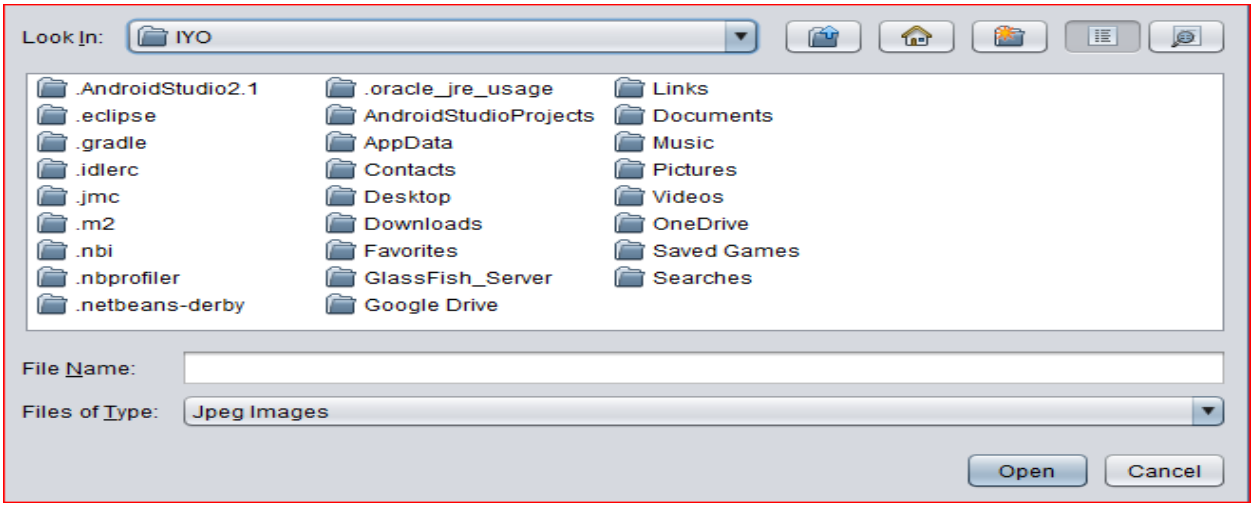

Figure 4.2: The Abstract Windows Toolkit File Chooser

Save File Button

The Save File button allow the users to save their decrypted and encrypted images. It uses the same form view as shown in Figure 4.2 only that the Open button changes to Save.

Encrypt/Decrypt Button

The Encrypt and Decryption button allows the users to perform encryption and decryption process.

Exit Button

The Exit button allows the user excuse themselves from the system at any time they desire to.

Labels

The small Blue Textbox serves as an indicator setting the user aware of each process of system while operating so as not to keep the users in a state of confusion not knowing what to do next. The Large blue label serves as the medium of view for the users allowing them to view the desired

image, encrypted and decrypted images, saved images, also allow users verify if they are actually working on their desired image as shown in Figure 4.3.

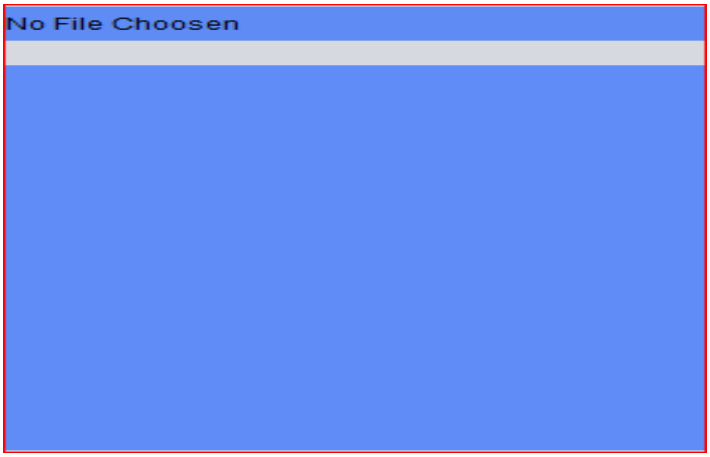

Figure 4.3: Labels indicating system activities

4.2 Result

After various evaluation and constant checkup, the system gives a certain pattern of encrypted image as shown below in Figure 4.2. The encrypted image follows a specific pattern because the transformation technique implemented uses a constant value declared by the developer of the system to avoid inconsistency and error while in operation. The encrypted image is advised to be saved in the JPEG format but this can be disregarded and ignore.

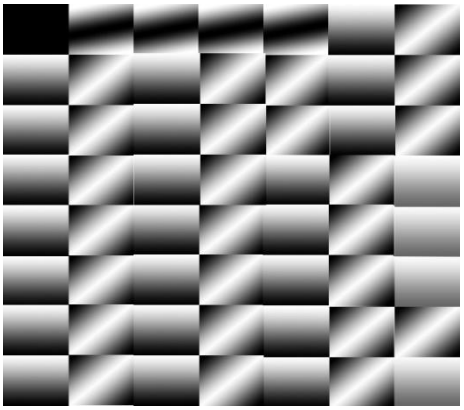

Figure 4.2: Encrypted Result of the Image.

Figure 4.3 Image to Be Encrypted

CHAPTER FIVE

CONCLUSION

5.1 Introduction

This chapter concludes the project report as it summarizes the work done, techniques employed and the final achieved. It details the project contribution to knowledge, its limitations, and possible developments to be made to the current project work. Its critically analyzes the projects aims and objectives, checkmating it to the outcome of the project and considers the reasons and the effectiveness of the employed solution.

5.2 Contributions to Knowledge

The system designed by implementing the discrete cosine transformation technique is a cryptography system. It details the use of cryptographic tools to ensure images are secured and are kept secret.

5.3 Limitations

The following are the limitations of the system:

i. The system has no standard cosine coefficient to determine the quality of the image at each point in time.

ii. The system is only developed to perform encryption and decryption activities on 3D-Images.

5.4 Future Works

I recommend that in the future the aspect of 7 Dimensional Images should be considered and encrypted using advanced Cosine Transformation technique to ensure images are well encrypted using the Discrete Cosine Transformation Technique

5.5 Critical Appraisal

Considering the aim and objectives of this project, the outcome of the project matches the highlighted goals and this is hallmark in any research work. Although, the project schedule might not have been fully adhered to, it is very important that the project work was concluded within the given deadline presenting a fully designed, implemented and tested system that was proposed.

The technique employed in this project work demanded and spurred me to obtain a level of expertise in mathematical studies and also improve my existing knowledge in Java Programming. The project also challenged me to give in my best into studying more and wide making a vast use of the Internet Facilities around me.

REFERENCES

Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt (2010) "A Novel Image Encryption

Ahmad M and Al-Sharari H.D, (2013). An Inter-Component Pixels Permutation Based Color Image Encryption Using Hyper-Chaos Algorithm Based on Hash Function.

Aspose Imaging for Java master (2016). Retrieved October 10, 2016 from http://www.asspose.com/java/imaging-component.aspx.

Gwang-hui CAO, Hu, K. Yang, H and Xu, E (2010). Algorithm of Image Encryption based on Permutation Information Entropy. *3rd International Conference on Computer and Electrical Engineering 53(2013), pp 1-7*

History of Cryptography: *an easy way to understand cryptography*. (2013). Thawte

Huang C K and Nien H H., 2009, "Multi chaotic systems based pixel shuffle for image encryption", Optics Communications 282, pp. 2123–2127.

Ismail, A. Amin, M. and Diab, H. 2010. A Digital Image Encryption Algorithm Based On a Composition of Two Chaotic Logistic Maps. *International Journal of Network Security, Vol 11, No 1, (2010) pp.1-10.*

Javidi, B and Nomura, T. Securing information by the use of digital holography

Kaimal, B. and Manimurugan, S. - *Image Compression Techniques: A Survey‖ International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISBN: 2319-6491 Vol 2, Issue 4 (2013) pp: 26-28.*

Kaur P. (2013. Image Compression- A Succinct Review. *International Journal of Engineering Associates Vol 2. 2013.*

Komal, D. P. and Sonal, B. (2011). Image Encryption Using Different Techniques: A Review. *International Journal of Emerging Technology and Advanced Engineering 1(1), pp,30-34*

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

Li and Drew (2003). Lossy Compression Algorithm.In Li and Drew fundamentals of multimedia (chapter 8). Prentice Hall

M.Younes and A.Janat ,2008. Image encryption using block based transformation algorithm

Pethe H. B and Pande S. R (2016). An overview of Cryptographic Hash Function MD-5 and SHA. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661*.

Rasul Enayatifar, Abdul Hanan Abdullah, Image Security via Genetic Algorithm‖, 2011 *International Conference on Computer and Software Modeling IPCSIT vol.14.*

Sandeep K, Sukhpreet S and Sonia (2013). A review on Image Encryption Techniques. *International Journal of Emerging Trends and Technology in Computer Science vol. 2, issue 3.* ISSN 2278-6856

Sara T and Al-Najdawi N. (2012). Lossless Image Cryptography Algorithm Based on Discrete Cosine Transformation. *The International Arab Journal of Information Technology vol. 9.*

Shannon, C.E and Weaver, W. W. (1949) *The Mathematical Theory of Communication*. University of Illinois Press, Urbana, IL.

Sharma P, Godara M and Singh R (2012). Digital Image Encryption Techniques: A Review. *International Journal of Computing and Business Research ISSN (Online): 2229-6166*

Simon Singh, "The Code Book" (2001, Shinchosha).

Vemuri, B. C. Sahni, S. Chen, F. Kapoor, C. Leonard, C. and Fitzsimmons, J. Image Compression ND,pp 82-112