AN APPROACH TO ENHANCE IMAGE ENCRYPTION USING BLOCK-BASED TRANSFORMATION ALGORITHM

by

MOHAMMAD ALI MOH'D BANI YOUNES

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

UNIVERSITI SAINS MALAYSIA
2009

ACKNOWLEDGMENTS

"All praises and thanks to ALLAH"

I would like to express my sincere appreciation and heartfelt thanks to my supervisor, Dr. Aman Jantan, for his creative guidance, intellectual support, stimulating discussions and inspiring words. I am grateful for his excellent hospitality and wonderful attitude.

Also, I would like to thank Dr. Omar Abu Shqeer, Dr. Ahmed Abdel Raouf Younis, Dr. Samer Al-Dhalli, Dr. Ahmed Manasrah, and Dr. Ahmad Alzoubi for their constructive contribution, invaluable advice, critical comments and patience.

A great thanks from my heart to my parents for their prayers, my wife for her patience and support, my sons and daughter for their patience too, and my father in law, mother in law, brothers, sisters, friends, and colleagues for their encouragements.

Finally, I would like to thank all lecturers, administration, and staff of Universiti Sains Malaysia and all academic and non academic staff of the School of Computer Science for Graduate Studies for their help and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF APPENDICES

SUATU PENDEKATAN UNTUK MENINGKATKAN PENYULITAN IMEJ MENGGUNAKAN ALGORITMA TRANSFORMASI BERASASKAN BLOK

ABSTRAK

Penyulitan data (data encryption) telah digunakan secara meluas untuk menjamin keselamatan dalam rangkaian terbuka (open network), contohnya internet. Setiap jenis data mempunyai cirinya yang tersendiri. Oleh itu, teknik yang berbeza sepatutnya digunakan untuk melindungi data imej rahsia (confidential image data) daripada dicapai oleh pihak yang tidak berkenaan. Kebanyakan algoritma penyulitan digunakan untuk data teks. Walau bagaimanapun, disebabkan saiz data yang besar dan kekangan masa sebenar (real time constrains), algoritma yang sesuai untuk data teks mungkin tidak sesuai bagi data multimedia.

Dalam penyelidikan ini, satu algoritma transformasi berasaskan blok dicadangkan untuk keselamatan imej iaitu dengan menggunakan gabungan transformasi imej dan teknik penyulitan. Algoritma ini akan digunakan sebagai transform prapenyulitan (pre-encryption transform) untuk mengelirukan hubungan di antara imej biasa (original images) dan imej yang dijana (generated images). Imej yang dijana (ditransformasi) kemudiannya disesuaikan pada algoritma penyulitan Blowfish. Korelasi, histogram dan entropi digunakan untuk menentukan tahap keselamatan imej.

Hasil daripada eksperimen yang dijalankan menunjukkan bahawa teknik gabungan menghasilkan korelasi yang rendah, nilai entropi yang tinggi dan histogram yang seragam. Sedangkan keputusan daripada penggunaan algorithma Blowfish menunjukkan peningkatan dalam tahap keselamatan imej yang disulitkan (encrypted images). Kedua-dua teknik (gabungan transformasi imej dan teknik penyulitan) menunjukkan kesamaan yang tinggi (high similarity) serta kualiti yang baik daripada imej yang dipulihkan, jika dibandingkan dengan teknik asal. Ciri lain bagi teknik gabungan adalah keteritlakkan (generality). Keputusan eksperimen menunjukkan bahawa penggunaan teknik gabungan bersama dengan algoritma lain memberikan prestasi yang lebih baik, jika dibandingkan dengan penggunaan algoritma lain secara bersendirian.

Dalam usaha meningkatkan kekuatan penyulitan imej yang ditransformasikan, suatu pendekatan steganografi baru bagi penyembunyian data (data hiding) juga dicadangkan. Keputusan eksperimen menunjukkan bahawa korelasi dan nilai entropi daripada imej yang disulitkan sebelum sisipan (insertion) adalah sama dengan nilai korelasi dan entropi selepas sisipan. Oleh kerana korelasi dan entropi tidak berubah semasa penyembunyian maklumat yang perlu, maka keadah ini memberikan perlindungan (concealment) data yang baik dalam imej yang disulitkan serta mengurangkan peluang ia dikesan. Data yang disembunyikan akan digunakan untuk membolehkan penerima membangunkan semula (reconstruct) jadual transformasi rahsia yang sama selepas mengekstraknya, dan imej asal boleh dihasilkan semula dengan menyongsangkan (inverse) proses transformasi dan proses penyulitan.

AN APPROACH TO ENHANCE IMAGE ENCRYPTION USING BLOCK-BASED TRANSFORMATION ALGORITHM

ABSTRACT

Data encryption is widely used to ensure security in open networks such as the internet. Each type of data has its own features, therefore, different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

In this research, a block-based transformation algorithm is proposed for image security using a combination of image transformation and encryption techniques. This algorithm will be used as a pre-encryption transform to confuse the relationship between the original images and the generated ones. The generated (transformed) images are then fed to the Blowfish encryption algorithm. Correlation, histogram, and entropy have been used to measure the security level of the images.

The experimental results have shown that the combination technique resulted in a lower correlation, a higher entropy value, and a more uniform histogram, compared to using the Blowfish algorithm alone; resulting in an enhancement to the security level of the encrypted images. This implies a high similarity and a good quality of the retrieved image compared to the original one. Another feature of the combination technique is its generality; it can be applied with any other traditional algorithm to enhance its performance. Experimental results have shown that using the combination technique along with the other algorithms resulted in a better performance compared to using the other algorithms alone.

In order to further strengthen the encryption of the transformed image, a steganography approach for data hiding is also proposed. Experimental results have shown that the correlation and entropy values of the encrypted image before the insertion are similar to the values of correlation and entropy after the insertion. Since the correlation and entropy have not changed while hiding necessary information, the method offers a good concealment of the data in the encrypted image, thus reduces the chance of the encrypted image being detected. The hidden data will be used to enable the receiver to reconstruct the transformation table after extracting it and hence the original image can be reproduced by the inverse of the transformation and encryption processes.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. Encryption and steganography techniques of digital images are very important and should be used to frustrate opponent attacks from unauthorized access (Mitra et al, 2006), (Shujun et al, 2002), (Lee et al, 2003).

Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data (Hossam El-din et al, 2006). There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types (Shujun and Zheng, 2002), (Mohammed Husainy, 2006).

In general, most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data (Yas A. Alsultanny, 2008), (Droogenbroech and Benedett, 2002), (Fong and Singh, 2002). According to Xun (2001) and Wang (2005), even though triple-data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications (Xun et al, 2001), (Wang et al, 2005). Therefore, encryption algorithms such as data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA) were built for textual data (Lee et al, 2003), (Syed, 2002), (Xun et al, 2001).

Although we can use the traditional encryption algorithms to encrypt images directly, this may not be a good idea for two reasons. First, the image size is often larger than text. Consequently, the traditional encryption algorithms need a longer time to directly encrypt the image data. Second, the decrypted text must be equal to the original text but this requirement is not necessary for image data. According to Chang (2001), due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable (Chang et al, 2001), (Jiri Jan, 2005), (David Salomon, 2005). The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. According to Mitra (2006), this perceivable information can be reduced by decreasing the correlation among image elements using certain transformation techniques (Mitra et al, 2006).

In addition to cryptography, steganography techniques are getting significantly more sophisticated and have been widely used. The steganography techniques are the perfect supplement for encryption that allows a user to hide large amounts of information within an image. Thus, it is often used in conjunction with cryptography so that the information is doubly protected, that is, first it is encrypted, and then it is hidden so that an adversary has to find the hidden information before the decryption takes place (Kisik Chang et al, 2004), (Kessler, 2001), (Kathryn Hempstalk, 2005).

1.2 Research Motivations

Most of the algorithms specifically designed to encrypt digital images were proposed in the mid-1990s. According to the Maniccam and Bourbakis (2004), there are two major groups of image encryption algorithms: (a) Non-chaos selective methods, and (b) Chaos-based selective or non-selective methods (Maniccam and Bourbakis, 2004). However, most of these algorithms are designed for a specific image format, either compressed or uncompressed. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption. According to Borko (2005), the user is expected to choose a method based on its properties, which will be best for image security (Borko Furht et al, 2005).

Image encryption has applications in internet communication, multimedia systems, medical and military imaging systems. Each type of multimedia data has its own characteristics such as high correlation among pixels and high redundancy. Thus, different techniques should be used to protect confidential image data from unauthorized access (Hossam El-din et al, 2006), (Ozturk and Sogukpinar, 2004).

The motivation behind this research is the ever-increasing need for harder-to-break encryption and decryption algorithms as the computer and network technologies evolve. We believe that by proposing the block-based encryption and decryption algorithm, it will help to reduce the relationship among image elements by increasing the entropy value of the encrypted images as well as lowering the correlation.

However, in order to increase the robustness of the proposed encryption technique, a steganography method using the least significant bit insertion will be applied without impacting the quality of the image.

Considering the above points, we will divide this research into three parts: a new transformation algorithm, a combination technique (transformation and encryption), and a steganography approach that will be used to hide a secret information (that is, the number of horizontal and vertical blocks of the transformed image) in the encrypted image data before transmission to the receiver. A general block diagram of the transformation and encryption techniques is shown in Figure 1.1.

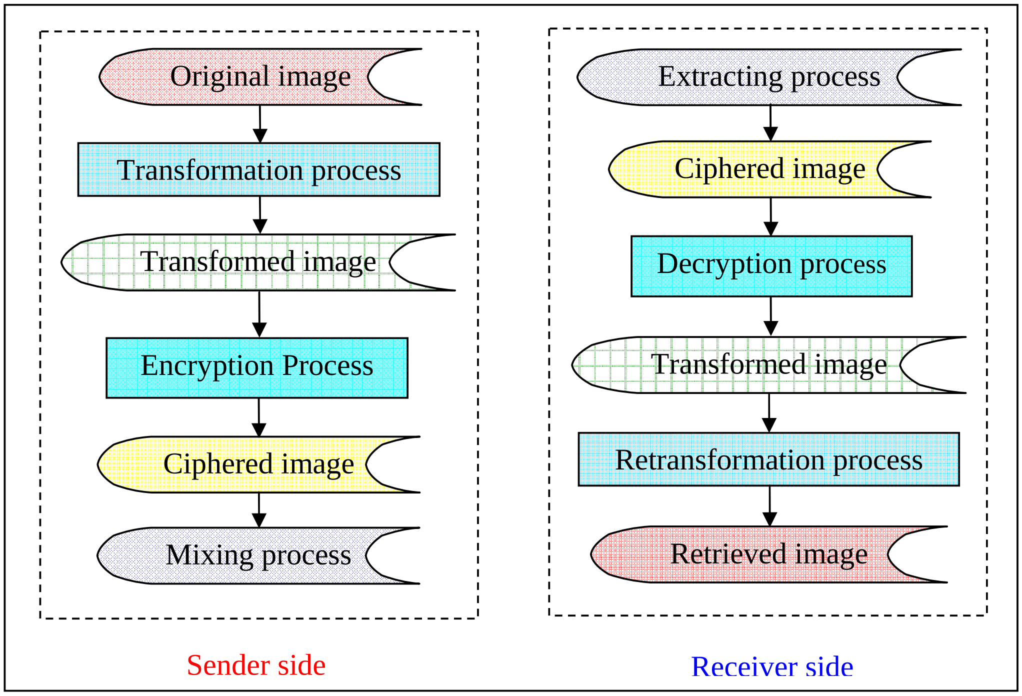

Figure 1.1 General block diagram of the proposed technique

The next section will explain more about the adopted algorithm and the methodology used.

1.3 Symmetric Key Algorithms

In general, symmetric key algorithms use a single, shared secret key. The same key is used for both encrypting and decrypting the data. There are two primary types of symmetric algorithms: block and stream ciphers. A block cipher is used to encrypt a text to produce a ciphertext, which transforms a fixed length of block data size into same length block of ciphertext in which a secret key and algorithm are applied to the block of data. For example, a block cipher might take a 64-bit block of plaintext as input, and output a corresponding 64-bit block of ciphertext. This transformation process should be conducted by a user providing a secret key and the decryption process is the inverse transformation to the ciphertext using the same key (April, 2005). Blowfish, Data Encryption Standard (DES), Triple-DES, IDEA, Rijndael and RC2 are examples of symmetric block cipher. The symmetric key algorithms use a single key for encryption and decryption processes as shown in Figure 1.2.

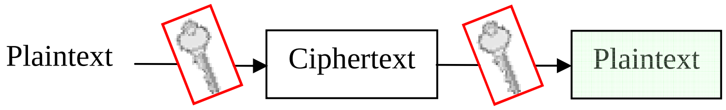

Figure 1.2 Symmetric key algorithms

The Blowfish algorithm is one of the symmetric block cipher algorithms that was designed in 1993 by Bruce Schneier as a fast alternative of the existing encryption algorithms, whereby it can be used as a replacement for the Data Encryption Standard (DES) or the International Data Encryption Algorithm (IDEA). The Blowfish encryption algorithm has been analyzed considerably, and is gaining acceptance as a strong encryption algorithm. Its source code is also available and it is not subjected to any patent royalties (Bruce Schneier, 1993), (William Stallings, 2003). Hence, this algorithm will be used mainly in this research as part of the new combination encryption technique.

The Blowfish algorithm consists of two parts: a key-expansion part and a data-encryption part. It encrypts the data by using the block cipher method, which breaks the text into 64-bit blocks before encrypting them. It takes a variable-length key from 32 bits to 448 bits of length, which implies flexibility in its security strength (John and James, 2005), (Bruce Schneier, 1993), (William Stallings, 2003).

1.4 Image Encryption Using Block-Based Transformation Algorithm

In this research, we propose a new transformation algorithm to be used as a pre-encryption transform, where the original image is divided into a random number of blocks which are shuffled and placed randomly within the image to build a newly transformed image. The generated transformed image is then fed to the Blowfish encryption algorithm. Thus, we expect that the combination of the transformation and encryption techniques will enhance the security level of the encrypted images.

This combination technique uses the original image to produce two output images:

a) a transformed image, using the proposed transformation algorithm.

b) a ciphered image of the transformed image, using the Blowfish algorithm.

A block diagram of the proposed technique versus Blowfish algorithm is shown in Figure 1.3.

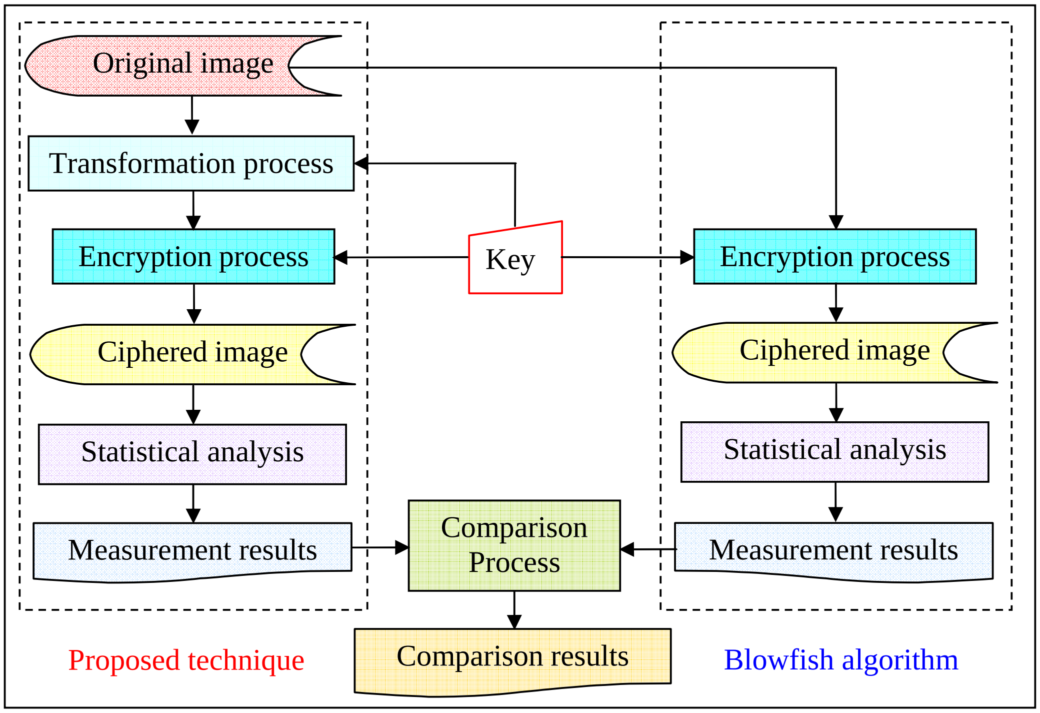

Figure 1.3 A block diagram of the proposed technique versus Blowfish algorithm

The measurements of correlation, entropy and histogram will be used to measure and compare the security level of the original image, transformed and encrypted images using the combination technique, and the encrypted image using the Blowfish algorithm alone. Encrypted images produced by the combination technique are expected to have lower correlation and higher entropy values, compared to those produced by the Blowfish algorithm alone.

In addition to transformation technique, we also present a steganography approach to be used for hiding secret information within encrypted image before being transmitted to the receiver.

1.5 Hiding Technique

Steganography techniques can be used for hiding information within other information. The least significant bit (LSB) insertion is one of the most widely used methods for embedding a message in a digital image. Steganography involves hiding information so it appears that no information is hidden at all. Therefore, it is expected that the person will not be able to decrypt the information (Shujun and Zheng, 2002), (Neil and Zoran, 2001), (Sushil, 2001). An alteration of the least significant bit of the color value of some pixels in an image will not change the quality of the image significantly. Therefore, a message can be sent within an image using these bits (Stallings, 2003).

In this research, the number of horizontal and vertical blocks of the transformed image, produced by the proposed algorithm, represents the secret information to be mixed (hidden) with the encrypted image before being transmitted to the receiver. This secret information will be needed at the receiver. Instead of sending the whole transformation table, which is usually big, only the secret information is sent. At the receiver side, the hidden information allows the receiver to regenerate the transformation table. Thus, the original image can be retrieved by the retransformation and decryption processes.

1.6 Goal, Scope, and Objectives of the Research

The goal of this research is to enhance the security level of the encrypted images using the proposed transformation algorithm. The scope is limited to the image encryption using the combination technique (block-based transformation algorithm and Blowfish encryption algorithm) on Microsoft windows based machine. This combination technique is applied to divide and shuffle the positions of the blocks of the original image, encrypt the transformed image, and then embed secret information (the number of horizontal and vertical blocks) in the encrypted image data prior to transmission to the receiver. Furthermore, the focus of this research was concerning a bit mapped (bmp) images using the standard Cipher Block Chaining (CBC) mode of the Blowfish algorithm.

To achieve the above goal, the objectives of this research will be as follows:

1. To introduce a new algorithm for image transformation, and to test and evaluate it.
2. To compute and compare correlation, entropy and histogram of different images with and without the proposed algorithm.
3. To compare the security levels of the encrypted images generated by the combination technique and the Blowfish algorithm..
4. To introduce a steganography method to exchange the secret information between the sender and the receiver that will be used for producing the transformation table.

1.7 Thesis Structure

This thesis will be organized into six chapters. Chapter 1 provides an introduction to the work, the motivations of this research, and explains important goal, scope, and objectives of this study. Image encryption using block based transformation algorithm is explained to provide a general aspects of symmetric encryption algorithm, then the most important features of the blowfish encryption and decryption algorithm are presented. A precise description of the proposed technique and its diagram is presented. Furthermore, the important use of the steganography technique is also presented.

In chapter 2, we will provide an overview of the concepts of digital image encryption. The general aspects of digital images and image file formats will also be discussed. We will also provide the explanations on cryptographic systems in general; block cipher with its modes of operation, stream cipher and some of the most commonly used or well known encryption and decryption algorithms such as DES, Blowfish, Rijndael-AES and IDEA. This chapter also highlights a background of the current research in image encryption. Steganography technique for digital images is also presented. At the end of this chapter, the image measurements; the correlation among image elements, image entropy, and image histogram as well as image similarity are discussed in certain degree of details.

In chapter 3, we will present and discuss in details the description of the model and methodology that will be applied to enhance the security level of the encrypted images by using the newly proposed approach. Hiding information in image using steganography technique is also presented in this chapter.

In chapter 4, we will discuss the implementation, testing and results analysis of the proposed technique. Hiding efficiency will also be presented in this chapter with the focus on mixing and extracting data within the encrypted image. How the sender will hide the secret information in the image data that enables the receiver to rebuild the transformation table using the secret key will also be discussed.

In chapter 5, we will present the technical contribution; strength and efficiency of the technique by comparing the combination technique with three commonly used encryption algorithms; Blowfish, Twofish, or RijnDael. Economical contribution of the research; knowledge gain and security enhancement will also be explained. Some suggestions for future work will also be provided. Chapter 6 will summarize the main points of the thesis and list the main conclusions of the work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides a detail description of the cryptographic systems used in this research. Section 2.2 presents general aspects of the digital image encryption. Section 2.3 defines fundamental concepts of cryptography systems and image encryption. Categories of cryptography systems are also discussed; symmetric key cryptography and public key cryptography. Some important symmetric key algorithms such as block cipher and stream cipher algorithms are also introduced in this section. Furthermore, we will discuss modes of operation; Electronic Code Book Cipher (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB).

Section 2.4 presents some of the recently developed or well-known encryption and decryption algorithms in cryptography, such as DES, Blowfish, Rijndael-AES and IDEA. These algorithms define and cover the rules of encryption and decryption that are used to provide security in image encryption. Section 2.5 presents an overview of the research in the image encryption area. Section 2.6 provides an overview of the steganography techniques for digital images.

Section 2.7 explains the image security measurements; the correlation among image elements, image entropy, image histogram, and image similarity in a certain degree of detail. These security measurements will be used in this research to compute and evaluate the encrypted images produced by the combination technique.

Finally, section 2.8 summarizes the main points presented and discussed in this chapter.

2.2 Digital Images

A digital image is defined by an array of individual pixels and each pixel has its own value. The array, and thus the set of pixels, is called a bitmap. If we have an image of 512 pixels × 512 pixels, it means that the data for the image must contain information about 262144 pixels (Steinmetz and Nahrstedt, 2002), (Kristian Sandberg, 2000).

Digital images are produced through a process of two steps: *sampling* and *quantization*. Sampling is the process of dividing the original image into small regions called pixels, whereas quantization is the process of assigning an integer value (i.e. color) to each pixel (David Salomon, 2007).

The number of colors (i.e. color space) that can be assigned to any picture element or pixel is a function of the number of bits, which is sometimes referred to as the color depth or bits resolution. This concept is also known as bits per pixel (bpp) that represents the color for each value. The color space is computed using the following equation:

$$ColorSpace = 2^{b} \quad \text{….……………………….……………....}\textit{Equation 1}$$

where:

b: the bit depth

The color values used in each bitmap depend on the specific bitmap format. This means that each pixel in a bitmap contains certain information, usually interpreted as color information. The information content is always the same for all the pixels in a particular bitmap. Thus, each color value in a bitmap is a binary number. A binary number is a series of binary digits that can be either 0 or 1 and called bits. This binary number in a given format will differ in length depending on the color depth of the bitmap, where the color depth of a bitmap determines the range of possible color values that can be used in each pixel. For example, each pixel in a 24-bit image can be one of roughly *16.8* million colors. This means that each pixel in a bitmap has three color values between 0 and 255 and then those colors are formed by mixing together varying quantities of three primary colors: red, green and blue (Vaughan, 2004), (Rafael and Richard, 2002), (Sander, 2000). Table 2.1, illustrates the image color space.

Table 2.1 Image color space versus bit depth (bpp)

Image properties	Bits resolution	Color space
Binary image (black and white)	1	2 colors
Gray scale (monochrome)	8	256 gray levels
Colored image	8	256 colors
Colored image	16	65536 colors
True color (RGB)	24	16,777,216 colors

As seen from Table 2.1, as the number of bits increases, the image quality is also increased. However, storage requirements will increase, resulting in a direct relationship between the image storage size and the bits resolution. Image storage size for an uncompressed image is computed using the following equation:

$$IMGSS = IMGR \times BR \quad \text{…………….………………………..} \textit{Equation 2}$$

where:

IMGSS: Image storage size

IMGR: Image resolution (i.e. image width × image height)

BR: Bits resolution (bits depth)

For example, the storage size of a 640 pixels × 480 pixels, true colored image is given as follows:

$IMGSS = W \times H \times BR = 640 \times 480 \times 24$ bits = (7372800/1024/8) = 900 *KB*.

2.2.1 Digital Image Formats

Basically, there are three types of image files: bitmap, vector, and metafiles. When an image is stored as a bitmap file, its information is stored as a collection of pixels, manifest as colored or black-and-white dots. When an image is stored as a vector file, its information is stored as mathematical data. The metafile format can store image information as pixels (bitmap), mathematical data (vector), or both (Betcher and Gardner, 2006), (Sander, 2000). There is no single format that is appropriate for all types of images. According to Glouglim (2001), larger files take longer to load, require more disk space and can take longer to print, whereas small file sizes means greater performance (McGlouglim, 2001). The most common file formats are discussed below:

a) BMP Files

According to Bourke (1998), the BMP Bitmaps are defined as a regular rectangular mesh of cells called pixels (Bourke, 1998). Each pixel contains a color value as shown in Figure 2.1

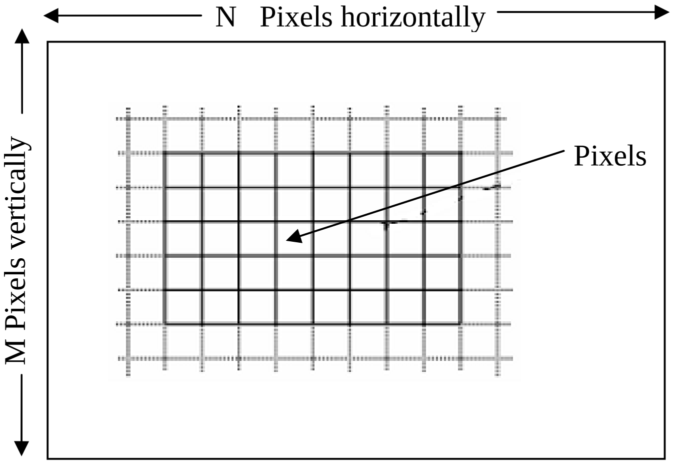

Figure 2.1 Image pixels

Bitmaps are characterized by only two parameters: the number of pixels, and the information content (color depth) per pixel, and they are the most commonly used type to represent images on the computer.

BMP is the native bitmap format of Windows. BMP is a general format that stores images in different color depths without compression (Betcher and Gardner, 2006), (Paul Bourke, 1998), (James and William, 1996).

The BMP advantages are that each pixel is independently available for any alteration or modification, and that repeated use of them does not normally degrade the image quality (Lancaster, 2003). The main disadvantage of this format is due to the size of the files, which is usually larger compared to other formats or other lossy compression schemes. In general, a BMP file consists of a header, descriptive information about the image (such as width, height, etc), an optional Color Lookup Table (CLUT) area which contains the actual colors of the image pixels, and a pixel data area (Shalini, 2004). The parts of the BMP file are illustrated in Table 2.2.

Table 2.2 BMP file header

Header	Stores general information about the BMP file.
Information header	Stores detailed information about the bitmap image.
Optional palette	Stores the definition of the colors being used for indexed color bitmaps.
Image data	Stores the actual image, pixel by pixel.

Color Lookup Tables (CLUTs) follow the header for those lower performance modes in which they are used such as (1, 4, 8 or 16 lookup colors). These, in turn, are followed by the actual pixel data. The main interest lies in the 24-bit uncompressed RGB color mode. In this mode, there are no color lookup tables used. Each pixel consists of an 8-bit red value, an 8-bit green value and an 8-bit blue value (Lancaster, 2003).

B) GIF Files

The Graphics Interchange Format (GIF) was originally developed by CompuServe in 1987. It is one of the most popular file formats for web graphics and exchanging graphics files between computers. The GIF format supports 8 bits of color information that is limited to 8 bits palette and 256 colors. Thus, only 256 different colors are available to represent the picture. It can be viewed by all common browsers. GIF also support animation, transparency and interlacing (Betcher and Gardner, 2006), (Robert Fry, 2006).

GIF images are automatically compressed when they are saved using a lossless compression method known as LZW (Lempel-Ziv-Welch) that does not degrade the image quality. GIF format provides four main features: interlacing, transparency, file compression, and primitive animation. The interlacing feature allows the browser to display portions of the image as it updates. The original image starts off with poor quality but gets better as more of the interlacing parts are updated. Interlaced GIF files allow users to view a portion of the image as the file is loading (Seeram and Radiography, 2006).

One of GIF's weaknesses is that GIF images are limited to a maximum of 256 colors. The quality of the image suffers if the color depth is reduced to less than the color depth of the original image. GIF files can store any of the 16.8 million colors but only a maximum 256 colors in each GIF file. Therefore, when converting an image to GIF, the program compresses the file by reducing the number of colors in the image from 24-bit (millions of colors) to 8-bit (256 colors). However, the GIF file format has the ability to store multiple images in a single file and play the images in a loop, thereby giving the appearance of animation (CIMC, 2006), (Sharon Wheeler, 2000).

c) JPEG Files

The Joint Photographic Experts Group, (JPEG) format, is one of the most popular formats for web graphics. It supports 24 bits of color information. The JPEG file format stores all of the color information in an RGB image, and then it compresses the file size to save storage space, or it saves only the color information that is essential to the image. Unlike GIF, JPEG does not support transparency.

The compression method used in JPEG is usually lossy compression, meaning that some visual quality is lost in the process. JPEGs can be saved in a variety of lossy compression levels. This means more or less compression can be applied to the image, depending upon which looks best. JPEG can be used by almost any browser. Since JPEG is an image compressor, it is best used for photographic quality images and detailed illustrations with many colors (Tom Lane, 2008).

The advantage of JPEG is that it is a highly compressed file format. Therefore, the image can be compressed while the quality is maintained. JPEG weakness is that lossy compression may result in low quality graphics. Another weakness noted in JPEG formats is that there is no support for pixel transparency. JPEGs lose quality every time they are opened, edited and saved. It is very important to minimize the number of editing sessions between the initial and final version of a JPEG image (Sharon Wheeler, 2000), (CIMC, 2006), (Graphics Academy, 1998).

d) PICT Files

The Picture File Format (PICT) is used primarily on the Macintosh platform. It is the default format for Macintosh image files as its standard metafile format. The PICT format is most commonly used for bitmap images, but can be used for vector images as well. The PICT is a lossless format. Since the PICT format supports only limited compression on Macintoshes with QuickTime installed, PICT files are usually large. PICT is used for images in video editing, animations, desktop computer presentations, and multimedia authoring (Chris Betcher and Margie Gardner, 2007).

e) EPS Files

The Encapsulated PostScript (EPS) file format is intended to make files usable as a graphics file format. The EPS file format is a metafile format. It can be used for vector images or bitmap images. It can also be used on a variety of platforms, including Macintosh and Windows. If an EPS image is placed into a document, we can scale it up or down without information loss (Chris Betcher and Margie Gardner, 2007).

f) PNG Files

The Portable Network Graphics (PNG) format is a bitmapped image format that employs lossless data compression. It will likely be the successor to the GIF file format. PNG is expected to become a mainstream format for web images and could replace GIF entirely. It is platform independent and should be used for single images only (not animations). Compared with GIF, PNG offers greater color support and better compression, gamma correction for brightness control across platforms, better support for transparency, and a better method for displaying progressive images (Sharon Wheeler, 2000), (Fulton, 2005).

g) TIFF Files

The Tag Interchange File Format (TIFF) is a tag-based international standard for storing and interchanging bitmaps between applications and hardware platforms. It is compatible with a wide range of software applications and can be used across platforms such as Macintosh, Windows, and UNIX. The TIFF format is complex, thus TIFF files are generally larger than GIF or JPEG files. TIFF supports lossless LZW compression. However, compressed TIFF takes longer to open. The format consists of items called tags which are defined by the standard. Each tag is followed by a tag dependent data structure (Graphics Academy, 1998).

The next section will explain the cryptographic system and image encryption.

2.3 Cryptographic Systems

Cryptography is the conversion of data into a secret code for transmission over a public network. Cryptography enables the sender to securely store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient (Harris Chen, 2001), (Gary Kessler, 2007).

Encryption of sensitive data is necessary. Cryptography is used to render the information unintelligible if transmission is intercepted by unauthorized individuals (Jae Shim, 2000). The intelligible form (original data) of information is called plaintext and the unintelligible form (protected data) is called ciphertext (Elbirt and Paar, 2005), (Stallings, 2003). The process of converting the plaintext into ciphertext is called encryption, while the reverse process of transforming ciphertext into the corresponding plaintext is called decryption.

In general, most cryptographic algorithms use a secret value called a key. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. The key is used for encryption and decryption and must be kept secret, thereby requiring the sender and receiver to agree on the same key before making any data transmissions. The key is independent of the plaintext. Therefore, the same plaintext encrypts to different ciphertext with different keys, and thus both processes are impossible without the use of the correct key (Weber and Fahrny, 2003), (Natasa, 2005), (Schneier, 1996).

Cryptography can be strong or weak. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is ciphertext that is very difficult to decipher without possession of the appropriate decoding tool. The sender and the recipient must keep the key secret because anyone who knows the key can use it to decrypt the plaintext. In addition, the strength of the algorithm is important. An unauthorized entity can take encrypted ciphertext and attempt to break the encryption by determining the key based on the ciphertext (Zhong et al, 2005).

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication, and therefore it is the process of recovering the plaintext or key, usually by using the ciphertext and knowledge of the algorithm (Albassal and Wahdan, 2004), (Bagnall et al, 1997), (Harris Chen, 2001). According to Kessler (2007), there are two types of algorithms: symmetric that uses a single key for both encryption and decryption, and asymmetric that uses one key for encryption and another for decryption (Kessler, 2007).

Cryptography can also be used to ensure the security of the communication path through the following: (a) data integrity which means ensuring that the data has not been modified by unauthorized entities. Thus, the message received by the recipient is the same as the message sent by the sender. (b) Non-repudiation ensures that the sender of any message cannot deny his/her actions. This can be achieved with digital signatures in conjunction with asymmetric key encryption. (c) Authentication is the process of proving the identity, and (d) privacy/confidentiality is the process to ensure that no one can read the message except the intended recipient (Alina Stan, 2007), (Solomon and Chapple, 2005).

The modern field of cryptography can be divided into several areas of study. In this section, two related categories for cryptography systems: public key cryptography and symmetric key cryptography will be discussed (Kaufman et al, 2002).

Public Key Cryptography (PKC) is also known as asymmetric cryptography. It uses one key for encryption and another for decryption. The encryption key known as public key is intelligible and can be distributed for all parities, while the decryption key known as private key is intelligible only to the recipient. Each user creates a pair of keys; if one is used for encryption then the other is used for decryption (Kaufman et al, 2002).

The public and private keys are mathematically related so that data encrypted with the public key can only be decrypted with the private key. This guarantees message privacy during transit. An important characteristic of public key encryption algorithms is that it should be computationally infeasible to determine the decryption key given only knowledge of the algorithm and the encryption key. Public key encryption can be used to exchange the secret key between the parties in a symmetric key cryptosystem (Stallings, 2003), (Baek, 2004). Figure 2.2, shows the main ingredients of public key cryptography system.

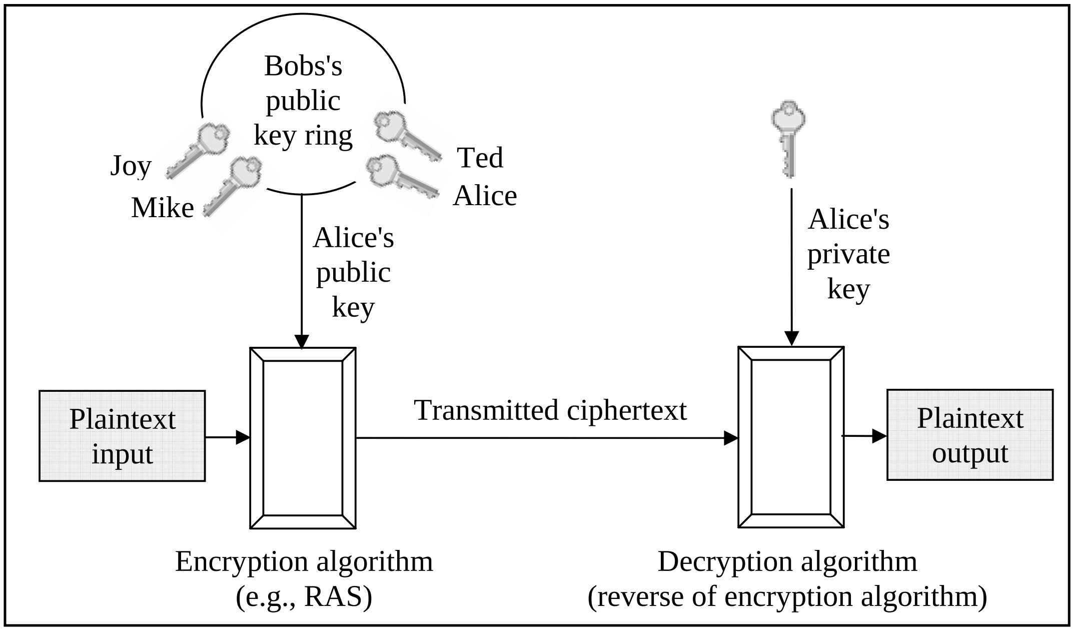

Figure 2.2 Public key encryption and decryption model (Stallings, 2003).

As illustrated in Figure 2.2, there are three basic steps to send a message by using public key encryption:

- Sender and receiver exchange the public keys, while the private key is kept secret by its owner.
- The sender uses the recipient's public key in encrypting a message for sending.
- The recipient's secret key is used to decrypt the received message.

In symmetric key cryptography, encryption and decryption are performed using the same secret key. The key can only be known by the sender and receiver to maintain integrity (Thomas Shinder, 2002). According to Whitman and Jason (2005), the primary disadvantage of symmetric key algorithms is that the key must remain secret at all times. For this reason, the key must be protected and secured requiring the sender to transmit the key to the recipient in a secure fashion (Jason Isom, 2005), (Whitman and Mattord HJ, 2005). Symmetric encryption is the most widely used algorithm. It has five ingredients as shown in Figure 2.3 (Stallings, 2006).