Research Paper Computer Science

An Approach To Enhance Image Encryption Using Blockbased Cryptography Algorithm

*Pratik A Vanjara ** Dr. Kishor Atkotiya

* Department Of Computer Science & I.T.,Shree. M & N Virani Science College ,Rajkot

** Head,Department of Computer Science,J. H. Bhalodia Women's College,Rajkot

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 paper, a block-based cryptography 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

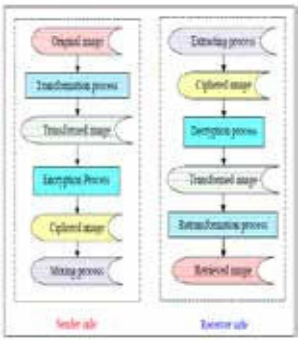
Keywords : Information and communication technologies, diaspora, migration.

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

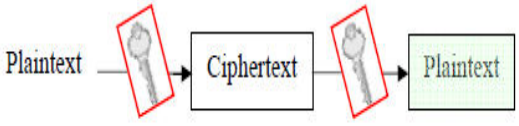
Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data. There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types

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 due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable. 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 image elements using certain transformation techniques. A general block diagram of the transformation and encryption techniques is shown in Figure



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. 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



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 hence, this algorithm will be used mainly in this research as part of the new combination encryption technique.

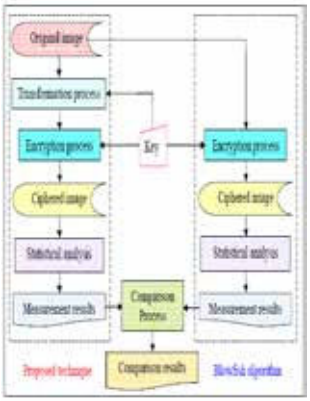
Image Encryption Using Block-Based Transformation Algorithm

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



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. 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

In this Paper, 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

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

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

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 = 2b ……quation 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, this given illustrates the image color space.

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, 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 × BR ……..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:

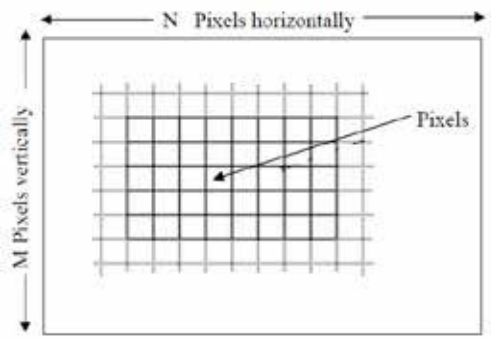
IMGSS = W × H × BR = 640 × 480 × 24 bits = (7372800/1024/8)= 900 KB.

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



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

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

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

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

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.

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

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

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

Conclusion
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.

REFERENCES

1.Whitfield Diffie and Martin E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory | | 2 (Password) Authenticated Key Establishment: From 2-Party To Group Michel Abdalla1, Jens-Matthias Bohli2, Mar´ıa Isabel Gonz´alez Vasco3, | and Rainer Steinwandt4 | | 3 Threshold Cryptography Based on Asmuth-Bloom Secret Sharing? Kamer Kaya?? , Ali Ayd_n Sel_cuk, Zahir Tezcan | | 4 An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm Joyshree Nath A.K.Chaudhuri School of I.T | | 5 new randomized data hiding algorithm with encrypted secret message using modified generalized Vernam Cipher Method: RAN-SEC algorithm Rishav Ray, Jeeyan Sanyal2, Tripti Das3, Kaushik Goswami4, Sankar Das5, Asoke Nath6