Security of Digital Images Using Cryptographic Algorithms

Yi Yi Aung, Tin Mar Kyi, Myo Thidar Win

Faculty of Computer System and Technology, Myanmar Institute of Information Technology (MIIT), Mandalay, Myanmar

Abstract: - **Today, the world is going to be digitalized in all the ways. Every business units, government and private sectors, research units are using the digital image as transferring mode for every critical data. These images over the internet which will not be secure. Therefore, there is a need of image security. Currently, there exists various image security techniqueslike encryption, watermarking, steganography, etc.In this paper, we compared image encryption algorithms.Implementations of these algorithms have been realized for experimental purpose. The results of analysis are given in this paper.**

Keywords: **Cryptographic Algorithms, Image Encryption, Encryption procecss, Histogram**

I. INTRODUCTION

Nowadays internet is used for faster transmission of large volume of important and valuable data, since internet has many points of attack, so this information need to be protected from unauthorized access.To protect data from unauthorized access there are many Data Protection techniques like Masking Data, Watermarking, Encryption, etc are implemented.

Furthermore special and reliable security in storage transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications and confidential video conferencing, etc.

In this regard, strong security technology is required to protect users' sensitive digital data. Encryption is the most trusted practical security technique for digital data in computer and communicationsystems. In order to fulfill such a task, many different image encryption methods have been proposed such as DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) and RSA. However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as data capacity and high redundancy, which are troublesome for traditional encryption. Moreover, these encryption schemes require extra operations on compressed image data thereby demanding long computational time and high computing power.

In this paper, different Bitmap images are encrypted with RC6 and MARS. The qualities of the encrypted images are tested with visual inspection and different quality of encryption algorithms.

The paper is organized as follows: Section 2 will briefly discuss the two encryption algorithms: RC6 and MARS. Section 3 will discuss the process of encrypting images with the two encryption algorithms. The method of the quality of encryption is discussed in Section 4.The results of the paper appear in Section 5.The paper is concluded in Section 6.

II. BACKGROUND

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [1].

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attention recently, and many different image encryption methodshave beenproposed to enhance the security of these images [2].

Image encryption techniques try to convert an image to another one that is hard to understand [2]. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

Most of the algorithms specially designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms RC6 and MARS.

A. Overview of the system

This section will give a brief overview on the construction of each encryption algorithm and encryption quality of these two algorithms. Each of the following algorithms is a symmetric block cipher algorithm. Symmetric means the key used for encryption and decryption is the same, while block means the data (information)to be encrypted is divided into block of equal length [3].

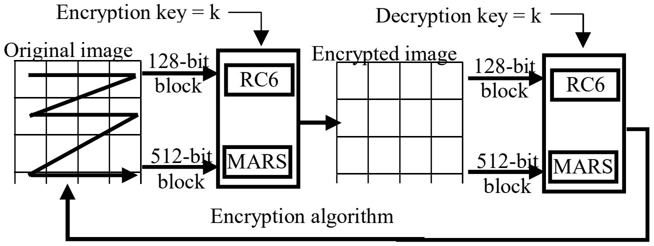

Fig. 1 The image encryption/decryption process with RC6 or MARS

B. Why Images Are Encrypted

Images are encrypted for many reasons, including identifying the creator of an image, protecting copyright information, deterring piracy, and blocking images from being viewed by users who shouldn't have access to them. By encrypting images, you can send them through email or over the internet without worrying about your images are being viewed by people that you don't want to see them.

Encrypting images on your home computer will also give you a measure of security in case a hacker gains access to your hard drive, and encrypting the images on your laptop or smartphone will likewise make your images safer if your computer or laptop are lost or stolen.

C. Encryption Process

A picture can be encrypted in the same way that text is encrypted by software. By running a sequence of mathematical operations, called an algorithm, on the binary data that comprises an image, encryption software changes the values of the numbers in a predictable way. A software key is necessary to unlock the encryption code, and it's created by the same software that scrambles the picture.

The encrypted image and the key are sent to the recipient separately to minimize the chance that a hacker could intercept both. The software key, which is usually a type of password, is typed into decryption software to decipher the encoded image. The security of the encryption depends on how difficult the encrypted data are to unencrypt.

D. RC6 block cipher algorithm

This algorithm depends mainly on the use of four working registers, each of size 32 bits. So, it handles 128 bits input/output blocks. Its parameterized family is: (w) word size in bits, (r) non-negative number of rounds, and (b) the length of encryption/ decryption key in bytes. RC6 has six primitive operations, which are $(+, -, <<<, >>>, *, \oplus)$. The use of multiplication greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increases throughput. RC6 uses an expanded key table, s [0, …,t–1], consisting of key t = 2r + 4 w-bit words. All details of RC6 are described in [4].

E. MARS block cipher algorithm

MARS is a symmetric key block cipher a block size of 128 bits and a variable key size from 128 to 400 bits. MARS algorithm uses a big variable of different operations. Additions, subtractions and xors operations are used to mix data and key values together. Table look-up is similar to the S-boxes inMARS cipher a table look-up is used. It uses a single table of 512 32-bit words, simply called S-box. Fixed rotations, data-dependent rotations may lead to differential weaknesses. This problem is solved in MARS by combining these rotations with most modern computer architectures. MARS algorithm uses 16 multiplications per block.

F. Histogram

It can apply to enhances for the image type of 256 gray-scale and any resolution BMP image. The improvement over the original image is quite evident. The histogram equalization causes a histogram with a mountain grouped together to "spread out" into a flat or equalized histogram. The histogram equalization process also increases the dynamic range of gray levels and, consequently produces an increase in image contrast. Although this histogram equalization method can be quite useful, it does not lend itself to interactive image enhancement applications. The reason is that-this method is capable of generating only one result: an approximation to a uniform histogram.

III. BITMAP IMAGE ENCRYPTION

Bitmap (BMP) image is a type of uncompressed image format which preserves all information about the image data. The encryption process has two inputs, the plaintext (data image) and the encryption key. To encrypt an image, its header is excluded and the start of the bitmap's pixels or array begins right after the header of the file. The bytes of the array are stored in row order from left to right with each row representing one scan line of the image. The rows of the image are encrypted from top to bottom.

As show in Figure 1, the block RC6 and MARS are 128 and 512 respectively. The key length for the two algorithms is 16 bytes (128 bits). In the decryption process, the encrypted image is divided into the same block length of each algorithm from top to bottom. The first block is entered to the decryption function of each algorithm and the same encryption key is used to decrypt the image but the application of sub-keys is reversed.The process of decryption is continued with other blocks of the image from top to bottom [5].

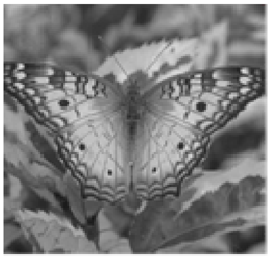

Fig.2a Original Image (butterfly.bmp)

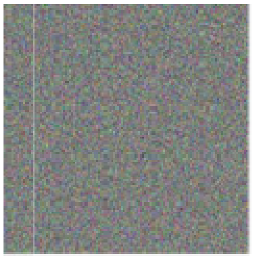

Fig.2b Encryption Image using RC6

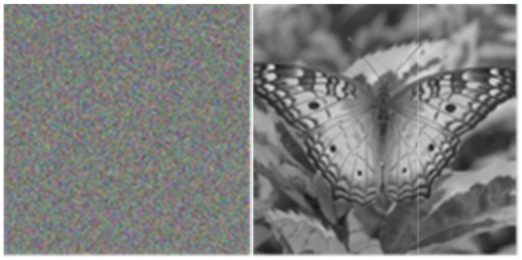

Fig.2c Encryption Image using MARS

Fig.2d The image after Decryption using RC6 and MARS

Fig.2 Image Encryption and Decryption with Cryptographic Algorithms

IV. COMPARISON OF ENCRYPTION QUALITY

To evaluate the quality of encryption, we have used the grey scale (0 – 255) bitmap image Butterfly as the original image (plainimage) of size 512 × 512. Figures 2A, 2B and 2C show the results of encryption and decryption for this image. In all experiments, we use the grey-scale bitmap image Butterfly.bmp, the size 512 × 512 with grey-scale value for each pixel ranging from 0 – 255 as the original images (plainimages).

Let F and F' denote the original image (plainimage) and the encrypted image (cipherimage) respectively each of size M*N pixels with L grey levels. F(x,y), F'(x,y) ,϶{0,.,L-1} are the grey levels of the images F and F' at position (x,y) (0≤ x≤ M–1, 0 ≤ y ≤ N – 1). Let H_L(F) denote the number of occurrences of each grey level L in the original image (plain image) F. Similarly,H_L(F') denotes the number of occurrences of each grey level L in the encrypted image (cipher image) F'. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as

$$\text{Encryption quality} = \frac{\sum_{L=0}^{255}\left|H_L(F')-H_L(F)\right|}{256}$$

The effect of number of rounds r on the encryption quality for RC6 and MARS is investigated. The block size and secret key length are both constants. The encryption quality (EQ) is computed as a function of number of rounds (r) and the results obtained for image mentioned above are shown in table.

Number of Rounds	Algorithm type	
	RC6	MARS
4	719.977	992.172
8	723.234	990.219
12	726.133	991.719
16	725.523	992.672
20	725.609	993.234
24	723.117	990.266
30	723.828	990.117

Table .Comparison of Encryption Qualities for the Image “butterfly.bmp” for different round

V. RESULT OF THE SYSTEM

With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently this meanthat the higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption. So, the quality of encryption may be expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one.

In addition to the visual inspection, two encryption qualities will be considered to evaluate and compare the two encryption algorithms RC6 and MARS.

1) Histogram of encrypted images:We have selected the 256 grey-level bitmap image Butterfly and its encrypted image and obtained theirhistograms. Figure 3 shows histograms, [6] for this image and corresponding encrypted image encrypted usingRC6 algorithm. From the figure, one can see that the histogram of the encrypted image (cipher image) is fairlyuniform and is significantly different from that of original image (plain image).

Similarly we have obtained histogram for the encrypted image of Butterfly. bmp encrypted using MARS algorithm. For the observation it is evident that the histogram of cipher image is also fairly uniform and different from that of the plain image and is shown in figure 4.Also see the percentage of number of pixels with certain grey scale values in the histogram of plain image.

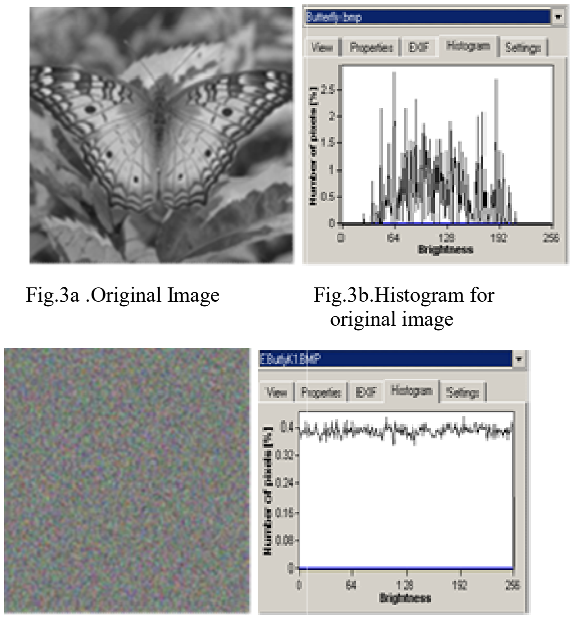

Fig.3a .Original Image

Fig.3b.Histogram for original image

Fig.3c. Encrypted image

Fig.3d.Histogram for Encrypted image

Fig.3. Results of Histogram for Plainimage and Cipherimage of RC6

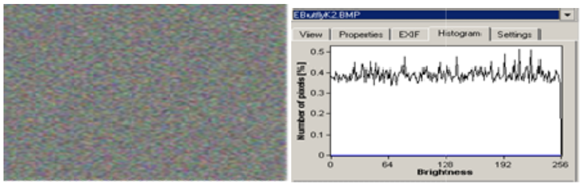

Fig.4a. Encrypted image

Fig.4b. Histogram of encryption image

Fig.4. Results of Histogram for Cipher image of MARS

VI. CONCLUSION

This paper introduces a successful efficient implementation of RC6 and MARS block ciphers for digital images. A mathematical modeling for encryption efficiency evaluation, that is called encryption quality was proposed, and may be considered to compare the effectiveness of different encryption techniques to digital images instead of visual inspection. The system is allow other extension of images (jpegs, gif, etc.) by changing the key length, number of rounds and block size.

Comparison of encryption quality evaluation criteria are achieved using simulation programs. Effect of number of rounds, secret key length, and data block size on encryption quality is evaluated and compared using several test values. Results obtained show that the MARS block cipher achieved the better encryption quality.

From an engineer's perspective, the use of MARS block cipher algorithm as a candidate for image encryption is very promising for real-time secure image and video communications in military, industrial, as well as commercial applications.

REFERENCES

[1]. H.El-din. H.Ahmed, H.M.Kalash, and O.S. Farag Allah, "Encryption quality anlaysis of the RC5 block Cipher algorithm for digital images".

[2]. Li. Shujun, x – Zheng- "Cryptanalysis of a chaotic image encryption method", Inst of Image Process.

[3]. R.L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, The RC6TM Block Chiper,1998. http://www.rsasecurity.com/rsalabs/rc6/

[4]. William Stallings, "Cryptography and Network Security", Third Edition, Pearson Education,2003.

[5]. I.Ziedan, M. Fouad, and D.H. Sulem, "Application of Data encryption standard to bitmap and JPEG images".

[6]. Hossam El-din H. Ahmed, Hamdy, M.Kalash. And OsamaS.Farang Allah,"Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images".