Efficiency and Security of Some Image Encryption Algorithms

Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry

Abstract— **This paper describes the results of efficient measuring methods whereby the encryption capability of four algorithms are evaluated. Specifically this work focuses on measuring the encryption quality, the memory requirement and the execution time of the encryption as an indicator to the usage of the software and the hardware. Also, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. A number of requirements are therefore identified upon which the algorithms are evaluated. The results of the efficient measuring methods show that each algorithm has its own strengths and weaknesses and no single encryption mechanism is able to get the maximum security with minimum execution time. The paper proposes that it may be possible to develop new algorithms providing adequate means of efficiency with acceptable security.**

***Index Terms*— Efficiency, Encryption, Image, Security.**

I. Introduction

A digital image is defined as a two dimensional rectangle array. The elements of this array are denoted as pixels. Each pixel has an intensity value (digital number) and a location address (row, column). Many image data security solutions have been proposed in recent years. Encryption is one of these important common tools. Traditional encryption technique such as Data Encryption Standard (DES) treats the image data as the traditional text data, while image encryption uses special image data structure which leads to get efficiency of encryption with minimum requirement of encryption time [1], [2].

Encryption process transforms plain-image data into cipher-image through involving an algorithm for combining the original image with one or more keys. Techniques that use the same secret key for encryption and decryption are grouped under private key techniques [3], [4]. While, asymmetric key techniques use two different keys; public key for encryption and private key for decryption [5].

With wide usage of images in various applications, it is important to protect the confidential image using encryption techniques. Many works on image encryption techniques have been published as an attempt to develop more efficient performance and for enhancing security of cryptosystem. Considering that it is not significant to achieve secure cryptosystem with performance consuming. So, it will not be accepted by both practitioners and cryptanalysts.

From the cryptographical point of view, a strong cryptosystem should be secure enough against all kinds of attacks that try to break the system such as known-plaintext attack, ciphertext-only attack, brute-force attack, statistical attack, and differential attack [6]. This paper explores the security analysis which has been performed on the proposed image encryption schemes (statistical and differential attacks), that demonstrates how much scheme is a satisfactory security. Also, evaluates efficiency by measuring the encryption quality, the memory requirement, and the execution time of the encryption.

The rest of this paper is organized as follows. Section II provides a description of the selected image encryption algorithms. The efficient measuring methods and security analysis are presented in section III. This is followed by the experimental results in section IV. Finally, the concluding notes are introduced in section V.

II. Encryption Techniques

Image encryption algorithms can become an integral part of the image delivery process if they aim towards efficiency and at the same time preserve the highest security level. The following subsections describe briefly four symmetric image encryption algorithms. These algorithms can be classified into three techniques: transposition, substitution, and transposition - substitution techniques.

A. *Transposition Techniques (Position Permutation)*

Transposition means rearranging elements in the plain-image. Mitra *et al.* (2006) have used a random combinational of bit, pixel, and block permutations [3]. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8 (as the number of bits in each pixel). The number of permutations is = 8! = 40320 and the number of keys are 121. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. The block size is (8 × 8) then it is difficult to decrypt. To extract the image, a combinational sequence of permutations and the permutation keys using pseudo random index generators should be known. In this investigation the combination of

Manuscript received March 18, 2008.

Marwa Abd El-Wahed is a supervisor of quality control department in the International Group for Legal Consultation (IGLC) and Master of Science student in the Institute of Graduate Studies and Research, Department of Information Technology, Alexandria University, Egypt (e-mail: marwa2004_mm@yahoo.com).

Saleh Mesbah is an Assistant Professor in the Department of Information Technology, Alexandria University, Egypt (e-mail: saleh.mesbah@gmail.com).

Amin Shoukry is a Professor of Computer and Systems Engineering in the Faculty of Engineering, Alexandria University, Egypt (e-mail: amin.shoukry@gmail.com).

block, bit, and pixel permutation are used respectively.

B. *Substitution Techniques (Value Transformation)*

Substitution maps each element in the plain-image into another element. Yen and Guo (2000) have proposed a chaotic key based algorithm (CKBA) to change the pixel values of the plain-image [7]. This algorithm relies on a one-dimensional chaotic map for generating a pseudo-random key sequence. The encryption procedure of CKBA is applied by selecting two bytes key1 and key2 (8 bits) and the initial condition of a one-dimensional chaotic system as the secret keys of the encryption system.

C. *Transposition - Substitution Techniques*

Transposition - substitution techniques mean the schemes, which are composed of two basic parts: position permutation and diffusion of pixel value. Maniccama and Bourbakisa (2004) have proposed a method that is based on permutation of pixels and substitution of the pixel values [8]. The permutation is done by encryption keys that are generated by the SCAN methodology. The pixel values are replaced using a simple substitution rule, which adds confusion (hide relationship between key and cipher-image) and diffusion (hide relationship between plain-image and cipher-image) properties to the encryption method. The permutation and substitution operations are applied in intertwined manner and iteratively. The encryption algorithm uses four scan keys to increase the complexity of pixel rearrangement. The user specifies two of them as part of encryption key and the other two keys are fixed as part of encryption algorithm.

Socek *et al.* (2005) enhance the CKBA algorithm (ECKBA) by replacing the one-dimensional chaotic Logistic map to a piecewise linear chaotic map to improve properties of the secret bits generated by the chaotic map, increase the key size to 128 bits, and add two more cryptographic primitives and extend the scheme to operate on multiple rounds [4]. A pseudo-random permutation generator of the bits within each pixel value based on the new chaotic map is introduced as an additional component in the encryption and decryption processes to create a permutation box, and add a much needed diffusion to the system.

III. Comparison Criteria

In this investigation, the set of criteria for comparing the selected algorithms; encryption quality, memory requirement, execution time, and security analysis (statistical and differential attacks) are presented. Each of these metrics is described in the following subsections.

A. *Encryption Quality*

With the implementation of an image encryption algorithm, a change takes place in pixel values on the encrypted image as compared to the values before encryption. A measure for encryption quality may be expressed as how much the deviation (changes) caused in pixel values at every location of the plain-image. The measure will be done by calculating the 'X' matrix which represents the absolute values of the deviation between each pixel values before and after encryption. Next, present the results graphically (histogram distributions). After that, compute the average value of how many pixels are deviated at every deviation value 'D'. This is followed by computing the absolute value of subtracting this average from the deviation histogram 'S'. Finally, count the area 'AS' under the absolute curve 'S' (sum of variations of the deviations histogram from the uniformly distributed histogram.) [9].

The followed steps summarize this measure:

1. $X = | I - E |$
2. H = histogram (X)
3.

$$D = \frac{1}{256}\sum_{i=0}^{255} h_i, \tag{1}$$

4. $S(i) = | H(i) - D |$
5.

$$AS = \sum_{i=0}^{255} D(i), \tag{2}$$

I: the plain-image.
E is the encrypted image.
H: histogram distribution.
h_i: the amplitude of the absolute difference histogram at the value i.

B. *Correlation Coefficient*

Statistical analysis such as correlation coefficient factor is used to measure the relationship between two variables; the image and its encryption. This factor demonstrates to what extent the proposed encryption algorithm strongly resists statistical attacks. Therefore, encrypted image must be completely different from the original one [10].

The correlation coefficient is measured by the following equation:

$$C.C = \frac{\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(x))^2}\sqrt{\sum_{i=1}^{N} (y_i - E(y))^2}}, \tag{3}$$

C.C: correlation coefficient

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{4}$$

x and y: gray-scale pixel values of the original and encrypted images.

C. *Differential Attack*

Attacker tries to find out a relationship between the plain-image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Trying to make a slight change such as modifying one pixel of the encrypted image, attacker observes the change of the plain-image.

To test the influence of one pixel change on the whole encrypted image by the proposed algorithm, two common measures are used [11]:

1) Number of Pixels Change Rate (NPCR)

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{5}$$

2) Unified Average Changing Intensity (UACI)

$$\text{UACI} = \frac{1}{\text{W} \times \text{H}} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%, \tag{6}$$

C_1 and C_2: two ciphered images, whose corresponding original images have only one-pixel difference. C_1 and C_2 have the same size.

$C_1(i, j)$ and $C_2(i, j)$: grey-scale values of the pixels at grid (i,j).

D(i, j): determined by $C_1(i, j)$ and $C_2(i, j)$, if $C_1(i, j) = C_2(i, j)$, then, D(i, j) = 1; otherwise, D(i, j) = 0.

Wand H: columns and rows of the image.

D. *Memory Requirement*

To evaluate cryptosystem, the cost associated with the implementation and execution of the cipher should be studied. Therefore, computational efficiency like memory requirements in software implementations has to be considered.

E. *Execution Time*

Another important tool to evaluate the efficiency of algorithms is measuring the amount of time required to encrypt an image. In this investigation, actual time in CPU cycles will be used as a measure of execution time.

IV. Experimental Results

To encrypt an image, all the data except header will be encrypted from top to bottom. Performance of an algorithm can be measured by computational efficiency "encryption speed" and "memory requirements", which can be affected by many factors. Some factors are associated with algorithm structure, algorithm implementations and others are associated with executing environment; such as CPU structure, the memory size, the OS platform and the developing language. Thus, it is meaningless to compare the encryption algorithms without using the same developing environments and optimization methods.

In this work, all programs applied in simulating the encryption algorithms, the security analysis, and the efficient measuring methods used to produce the values of comparison criteria are designed by Borland Delphi 5.0 and MATLAB 7.0 under Microsoft Windows XP Professional Version 2002 Service Pack 2 on, Intel(R) Pentium(R) 4 CPU 2.66 GHz, 512 MB of RAM, and 80 GB hard-disk capacity (Laptop computer). The test is applied on two selected bitmap grayscale images (Lena and Goldhill); each image is 512 × 512 pixels in size and 8 bits per pixel (bpp), or 256 intensity levels.

A. *Encryption Quality*

The lower value of area 'AS' under the absolute curve 'S', that means the more effective of image encryption and hence the encryption quality. The results of this experiment are shown in Table 1.

TABLE 1.
ENCRYPTION QUALITY

Proposal Algorithm	Lena	Goldhill
Combinational permutation	2064	2489
CKBA	3917	4814
Encryption using SCAN patterns	1539	1619
ECKBA	1679	1985

B. *Correlation Coefficient*

If the correlation coefficient equals one, that means the original image and its encryption is identical. If the correlation coefficient equals zero, that means the encrypted image is completely different from the original (i.e. good encryption). If the correlation coefficient equals minus one that means the encrypted image is the negative of the original image. The results of this experiment are shown in Table 2.

TABLE 2.
CORRELATION COEFFICIENT FACTOR

Proposal Algorithm	Lena	Goldhill
Combinational permutation	0.0073	0.0106
CKBA	0.0044	0.0098
Encryption using SCAN patterns	$1.72e^{-4}$	$1.93e^{-4}$
ECKBA	$2.07e^{-4}$	$2.18e^{-4}$

C. *Differential Attack*

The goal of this experiment is to determine the performance of each algorithm due to the differential attack. Differential attack would become inefficient, if one minor change in the plain-image can cause a significant change in the cipher-image. The results of this experiment are shown in Table 3 and Table 4.

TABLE 3.
NPCR (%)

Proposal Algorithm	Lena	Goldhill
Combinational permutation	0.33	0.53
CKBA	0.53	0.77
Encryption using SCAN patterns	0.87	0.92
ECKBA	0.67	0.79

TABLE 4.
UACI (%)

Proposal Algorithm	Lena	Goldhill
Combinational permutation	0.28	0.33
CKBA	0.39	0.56
Encryption using SCAN patterns	0.61	0.75
ECKBA	0.52	0.64

D. *Memory Requirement*

Table 5 shows the reading of memory usage in software implementations.

TABLE 5.
MEMORY REQUIREMENT (Bytes)

Proposal Algorithm	Lena	Goldhill
Combinational permutation	1036529	2049780
CKBA	1182523	2596305
Encryption using SCAN patterns	3457636	4893782
ECKBA	2547844	3448896

E. *Execution Time*

Designer should attempt to optimize a cryptosystem to make the execution time as lower as possible. The results of this test are shown in Table 6.

TABLE 6.
TIME OF IMAGE ENCRYPTION ALGORITHMS (In Second)

Proposal Algorithm	Lena	Goldhill
Combinational permutation	0.33	0.98
CKBA	1.05	2.27
Encryption using SCAN patterns	2.54	4.77
ECKBA	1.84	2.96

V. Conclusion

In this paper, four image encryption algorithms have been studied by means of measuring the encryption quality, the memory requirement, and the execution time of the encryption. In addition, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. The results are compared, focusing on those portions where each scheme is performed differently.

Based on the experimental results, it can be concluded that:

1) Permutation techniques achieve efficient schemes (minimum encryption time and memory requirement) compared with substitution techniques.
2) Permutation techniques are attractive due to their efficiency. But the drawbacks of these techniques are evident in terms of generated key and security.
3) Techniques that based on SCAN methodology achieve the highest security.
4) The chaos-based encryption scheme still need further study to achieve a reasonable degree of security and acceptable efficiency.
5) A security defect exists in the schemes that generated key based on random number sequence compared with these techniques that based on scan methodology. If a solution requires random numbers it is important to evaluate the efficiency and implicating the security will be considered.
6) When permutation technique combined with substitution technique in intertwined manner and iteratively, it leads to design complex, but secure and efficient techniques when variable key size and key number is used (according to plain-image size).
7) The schemes implementation using the computational approach for selecting random permutations performs slower time.
8) If the key used to encrypt plaint-image is random and the length of the key exceeds the amount of plaint-image to be encrypted, then the cipher-image is unbreakable.

From these results, it appears that there are three main criteria should be considered at the same level of importance to evaluate new cryptosystems: how much it eases implementation, level of security, and efficiency. To identify an optimal security level, it is necessary to compare carefully the cost of the multimedia information to be protected and the cost of the protection itself.

References

[1] I. Öztürk and I. Sogukpınar, "Analysis and comparison of image encryption algorithms", Transactions on Engineering, Computing and Technology, vol. 3, pp. 1305-5313, 2004.

[2] V. Potdar and E. Chang, "Disguising text cryptography using image cryptography", International Network Conference in Plymouth, UK, 6 - 9 July, 2004.

[3] A. Mitra, Y. V. Subba Rao, and S. R. M. Prasanna, "A new image encryption approach using combinational permutation techniques", International Journal of Computer Science, vol. 1, no. 2 , pp. 1306-4428, 2006.

[4] D. Socek, S. Li, S. S. Magliveras, and B. Furht, "Enhanced 1-D chaotic key-based algorithm for image encryption", IEEE/CreateNet SecureComm, Athens, Greece, pp. 406-408, September 5-9, 2005.

[5] H. Shuihua and Y. Shuangyuan, "An asymmetric image encryption based on matrix transformation", ECTI Transactions on Computer and Information Technology, vol. 1, no. 2, November 2005.

[6] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps", International Journal Bifurcation and Chaos, June 2003.

[7] J.-C. Yen and J.-I. Guo, "A new chaotic key-based design for image encryption and decryption", IEEE International Conference Circuits and Systems, vol. 4, pp. 49–52, 2000.

[8] S.S. Maniccama and N.G. Bourbakisa, "Image and video encryption using SCAN patterns", Pattern Recognition 37, pp. 725 – 737, 2004.

[9] H. Elkamchouchi and M. A. Makar, "Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR block ciphers", Twenty Second National Radio Science Conference (NRSC 2005), pp. C11, Cairo, Egypt, March 15-17, 2005.

[10] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, vol. 21, pp. 749-761, 2004.

[11] G. Chen and T. Ueta, "Yet another chaotic attractor", International Journal Bifurcation and Chaos 9, pp. 1465-1466, 1999.