World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:8, 2007

Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems

Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah

Abstract**—**This paper examines the implementation of RC5 block cipher for digital images along with its detailed security analysis. A complete specification for the method of application of the RC5 block cipher to digital images is given. The security analysis of RC5 block cipher for digital images against entropy attack, brute-force, statistical, and differential attacks is explored from strict cryptographic viewpoint. Experiments and results verify and prove that RC5 block cipher is highly secure for real-time image encryption from cryptographic viewpoint. Thorough experimental tests are carried out with detailed analysis, demonstrating the high security of RC5 block cipher algorithm.

Keywords**—**Image encryption, Security analysis.

I. Introduction

THE security of digital images becomes more and more important since the communications of digital products over open network occur more and more frequently, and the widespread deployment of digital image services has been enforcing security and ensuring authorized access to sensitive data. Furthermore, special and reliable security in storage and 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 order to fulfill such a task, many image encryption methods have been proposed [1,6] to protect the contents of digital images, but some of them [1-3] have been known to be insecure [3,4-6].

In [7], R. Rivest proposes RC5 block cipher, which is a value transformation cipher. The RC5 encryption algorithm is a fast symmetric block cipher suitable for hardware or software implementation. A noval feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a variable-length secret key. The encryption and decryption algorithms are exceptionally simple. The paper presents security analysis of RC5 block cipher with respect to brute-force, statistical, and differential attacks. Also, it shows some other measurements regarding encryption/decryption speeds. Generally speaking, RC5 is secure from strongly cryptographic viewpoint and can be used in any strict applications. The rest of the paper is organized as follows: In Section II, we firstly give a brief description for the architecture and specification of RC5 block cipher. Image encryption/decryption with RC5 block cipher is explored in section III. The detailed security analysis of RC5 block cipher including information entropy analysis, key space analysis, statistical analysis, and differential analysis is made in Section IV. Experimental results are also included in Section IV and the last section concludes this paper.

II. Architecture and Specification of RC5 Block Cipher

The RC5 encryption algorithm is a block cipher that converts plaintext data blocks of 16, 32, and 64 bits into ciphertext blocks of the same length [8-10]. It uses a key of selectable length b (0, 1, 2, ..., 255) byte. The algorithm is organized as a set of iterations called rounds r that takes values in the range (0, 1, 2, ..., 255) as illustrated in Fig. 1.

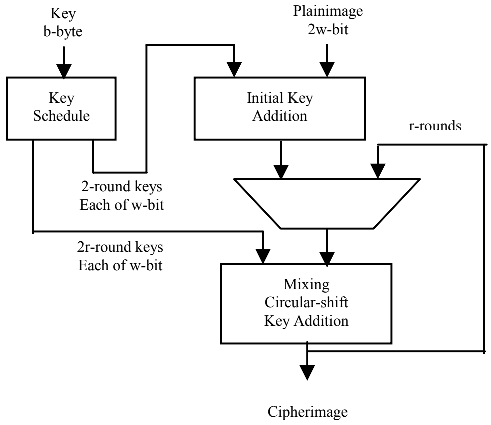


Fig. 1 RC5 Encryption Algorithm

An expanded key array is created out from the original key by means of a key schedule. The expanded key array is used with both encryption/decryption routines and its length is dependent on the number of rounds.

The operations performed on the data blocks include bit-wise exclusive-OR of words, data-dependent rotations by means of circular left and right rotations and Two's complement addition/subtraction of words, which is modulo-2^w addition/subtraction, where w is the word size in bits. They always affect a complete 16, 32 or 64-bit data block at a time.

This work was supported by the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt.

Hossam El-din H. Ahmed is the dean of the Faculty of Electronic Engineering, Menouf-32952, Egypt, (e-mail: hossameldin_hussien@yahoo.com).

Hamdy M. Kalash is the head of the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt, (e-mail: hamdy_kalash@yahoo.com).

Osama S. Farag Allah is with the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt, (contact author e-mail: osam_sal@yahoo.com, Tel: 202-048-3660716, Fax: 202-048-3660716).

III. Image Encryption & Decryption with RC5 Algorithm

There are two inputs to the encryption function, which are the plainimage to be encrypted and the expanded secret key. For RC5 image encryption, the image header is extracted from the image to be encrypted and the image data stream is divided into blocks of 64-bit length [11]. The first 64-bit block of image is entered as the plainimage to the encryption function of RC5. The second input the RC5 encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by the key schedule. Then, the next 64-bit plainimage block follows it, and so on with the scan path shown in Fig. 2 until the end of the image data bit stream.

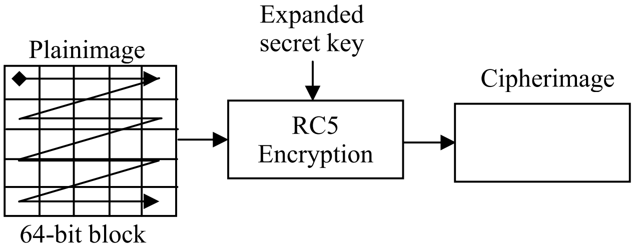


Fig. 2 RC5 Image Encryption Process

In the decryption process, the encrypted image (cipherimage) is also divided into 64-bit blocks. The 64-bit cipherimage is entered to RC5 decryption algorithm and the same expanded secret key is used to decrypt the cipherimage but the expanded secret key is applied in a reverse manner. Then the next 64-bit cipherimage block follows it, and so on with the same scan path as shown in Fig. 3.

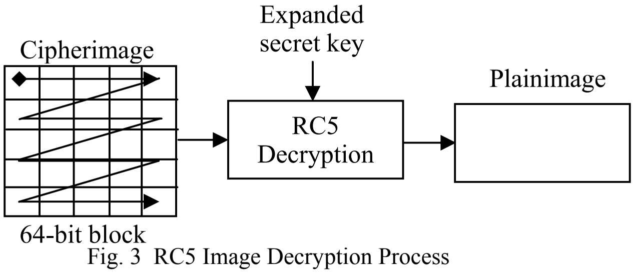


Fig. 3 RC5 Image Decryption Process

IV. Security Analysis and Test Results

A good encryption scheme should resist all kinds of known attacks, such as known-plaintext attack, ciphertext-only attack, statistical attack, differential attack, and various brute-force attacks [12-15].

The security of RC5 block cipher is estimated for digital images, even under brute-force attack, statistical and differential attacks. It is shown that RC5 block cipher is secure from the strongly cryptographic viewpoint. The results show the satisfactory security of the RC5 block cipher as demonstrated in the following subsections. Here, some security analysis results are described, including the most important ones like key space analysis, statistical analysis, and differential analysis. The evaluation consists of theoretical derivations and practical experimentation.

A. Information Entropy Analysis

Information theory is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [16]. Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics.

To calculate the entropy $H(m)$ of a source m, we have:

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} \quad bits, \tag{1}$$

where $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m=\{m_1, m_2,..., m_{2^8}\}$. After evaluating Eq. (1), we obtain its entropy $H(m)=8$, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

Let us consider the ciphertext of image encryption using the RC5, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. The entropy is as follows:

$$\begin{aligned} H(m) &= \sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} \\ &= \sum_{i=0}^{255} p(m_i)\log_2 \frac{1}{p(m_i)} = 7.9963 \approx 8 \end{aligned} \tag{2}$$

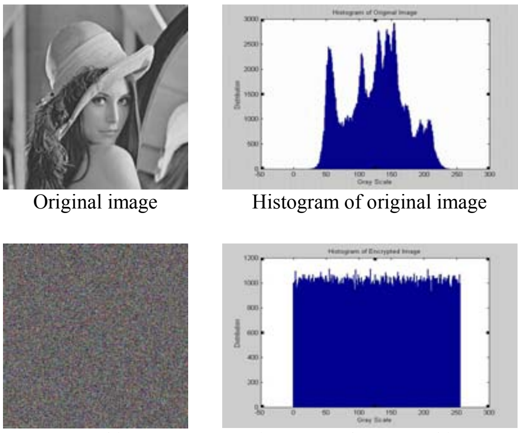
The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

B. Statistical Analysis

In [16], Shannon said, "It is possible to solve many kinds of ciphers by statistical analysis". Statistical analysis has been performed on the RC5 block cipher, demonstrating its superior confusion and diffusion properties, which strongly resist statistical attacks. This is shown by a test on the histograms of the encrypted images and on the correlations of adjacent pixels in the cipherimage.

B.1 Histograms of encrypted images

Select several 256 grey-level images with size of 512 x 512 that have different contents, and calculate their histograms. One typical example among them is shown in Fig. 4. From the figure, one can see that the histogram of the encrypted image (cipherimage) is fairly uniform and is significantly different from that of the original image (plainimage).



Original image   Histogram of original image

Encrypted image   Histogram of encrypted image

Fig. 4 Histograms of the plainimage and the cipherimage

B.2 Correlation of two adjacent pixels

To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plainimage/cipherimage, respectively, the procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$\operatorname{cov}(x,y) = E(x-E(x))(y-E(y)), \qquad (3)$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad (4)$$

Where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \tfrac{1}{N}\sum_{i=1}^{N} x_i \qquad (5)$$

$$D(x) = \tfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \qquad (6)$$

$$\operatorname{cov}(x,y) = \tfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \qquad (7)$$

Fig. 5 shows the correlation distribution of two horizontally adjacent pixels in the plainimage/cipherimage. The correlation coefficients are 0.9910 and 0.0054, respectively, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear from the Fig. 5 and Table 1 that there is negligible correlation between the two adjacent pixels in the cipherimage. However, the two adjacent pixels in the plainimage are highly correlated.

TABLE I
CORRELATION COEFFICIENTS IN PLAINIMAGE/CIPHERIMAGE

Direction of Adjacent pixels	Plainimage	Cipherimage
Horizontal	0.9910	0.0054
Vertical	0.9830	0.0038
Diagonal	0.9696	0.0031

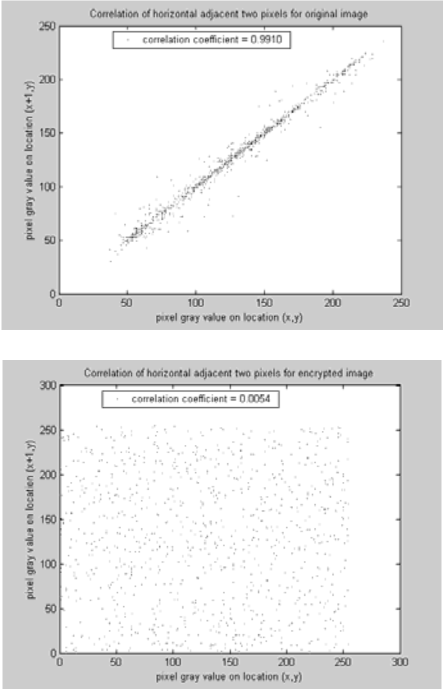


Fig. 5 Correlations of two horizontally adjacent pixels in plainimage/cipherimage

C. Key space Analysis

A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible. For the RC5 block cipher, the key space analysis and testing have been carefully performed and completely carried out, with results summarized as follows:

C.1 Exhaustive key search

For a secure image cryptosystem, the key space should be large enough to make the brute force attack infeasible. The RC5 block cipher is a 64-bit encryption scheme whose key space size is ranged from (0-2040) bit. An exhaustive key search will take 2^k operations to succeed, where k is the key size in bits. An attacker simply tries all keys, one by one, and checks whether the given plainimage encrypts to the given cipherimage.

For practical use of ECBFSC, assume that the secret key length is 128-bit Therefore, an opponent may try to bypass guessing the key and directly guesses all the possible combinations will need about 2^{128} operations to successfully determine the key. If an opponent employs a 1000 MIPS computer to guess the key by brute-force attack, the computational load is then:

$$\frac{2^{128}}{1000\ \mathrm{x}10^{6}\ \mathrm{x}\ 60\ \mathrm{x}60\ \mathrm{x}24\ \mathrm{x}365} > 10.7902831\ \ \mathrm{x}\ 10^{21}\ \ \text{years} \qquad (8)$$

This is a very long time. No image can be closed-door after such years which is practically infeasible.

C.2 Key sensitivity test

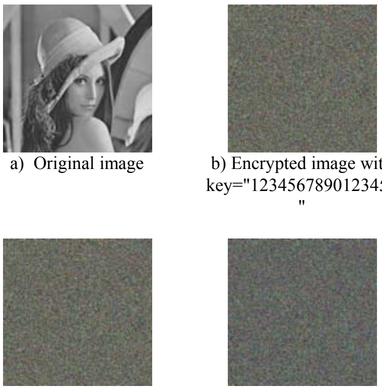
High key sensitivity is required by secure image cryptosystems, which means that the cipherimage cannot be decrypted correctly although there is only a slight difference between encryption or decryption keys. This guarantees the security of the RC5 against brute-force attacks to some extent. Assume that a 16-character ciphering key is used. This means that the key consists of 128 bits. For testing the key sensitivity of the RC5 encryption procedure, we have performed the following steps:

(a) An original image in Fig. 6(a) is encrypted by using the secret key “123457890123456” (in ASCII) and the resultant image is referred as encrypted image A as shown in Fig. 6(b).

(b) The same original image is encrypted by making the slight modification in the secret key i.e. “223457890123456” (in ASCII) (change is made in the most significant digit in the secret key) and the resultant image is referred as encrypted image B as shown in Fig. 6(c).

(c) Again, the same original image is encrypted by making the slight modification in the secret key i.e. secret key “123457890123457” (in ASCII) (change is made in the least significant digit in the secret key) and the resultant image is referred as encrypted image C as shown in Fig. 6(d).

(d) Finally, the three encrypted images A, B and C are compared.



a) Original image

b) Encrypted image with key="1234567890123456"

c) Encrypted image with key="2234567890123456"

d) Encrypted image with key="1234567890123457"

Fig. 6 Key sensitive test result 1 with RC5-32/16/16

TABLE II

CORRELATION COEFFICIENTS BETWEEN THE CORRESPONDING PIXELS OF THE THREE DIFFERENT ENCRYPTED IMAGES OBTAINED BY USING SLIGHTLY DIFFERENT SECRET KEY OF AN IMAGE SHOWN IN FIG. 6.

Image 1	Image 2	Correlation coefficient
Encrypted image A Fig. 6(b)	Encrypted image B Fig. 6(c)	0.0121
Encrypted image B Fig. 6(c)	Encrypted image C Fig. 6(d)	0.0172
Encrypted image C Fig. 6(d)	Encrypted image A Fig. 6(b)	0.0164

In Fig. 6, we have shown the original image as well as the three encrypted images produced in the aforesaid steps. It is not easy to compare the encrypted images by simply observing these images. So for comparison, we have calculated the correlation between the corresponding pixels of the three encrypted images. For this calculation, we have used the same formula as given in Eq. (4) except that in this case x and y are the values of corresponding pixels in the two encrypted images to be compared. In Table 2, we have given the results of the correlation coefficients between the corresponding pixels of the three encrypted images A, B and C. It is clear from the table that no correlation exists among three encrypted images even though these have been produced by using slightly different secret keys.

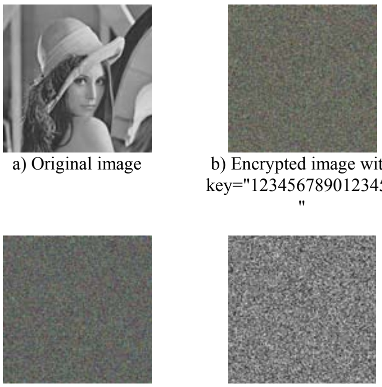
Another test for the key sensitivity of the RC5 is performed through the following steps:

1-First, a 512x512 image is encrypted by using the secret test key "123456789012346".

2-Then, changing the key least significant bit. The encrypting key will be "123456789012347".

3-Finally, compare the above two ciphered images.

The result is that the image encrypted by the key "1234567890123456" has 99.61% of difference from the image encrypted by the key "1234567890123457" in terms of pixel grey scale values, although there is only one bit difference in the two keys. Fig. 7 shows the test result.



a) Original image

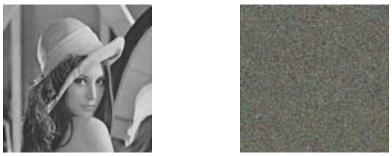
b) Encrypted image with key="1234567890123456"

c) Encrypted image with key="1234567890123457"

d) Difference image

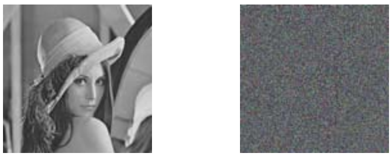
Fig. 7 Key sensitive test result 2 with RC5-32/16/16

Moreover, in Fig. 8, we have shown the results of some attempts to decrypt an encrypted image with slightly different secret keys than the one used for the encryption of the original image. Particularly, in Fig. 8(a) and Fig. 8(b) respectively, the original image and the encrypted image produced using the secret key “123457890123456” (in ASCII) are shown whereas in Fig. 8(c) and Fig. 8(d) respectively, the images after the decryption of the encrypted image (shown in Fig. 8(b)) with the secret keys “123457890123456” (in ASCII) and “123457890123457” (in ASCII). It is clear that the decryption with a slightly different key fails completely and hence the proposed image encryption procedure is highly key sensitive.



a) Original image

b) Encrypted image with key="1234567890123456"



c) Decrypted image with key="1234567890123456"   d) Decrypted image with key="1234567890123457"

Fig. 8 Key sensitive test result 3 with RC5-32/16/16

D. Differential Analysis

A desirable property for the RC5 is that it is highly sensitive to small change in the plainimage (single bit change in plainimage).

In general, the opponent may make a slight change such as modifying only one pixel of the original image, and then observes the change of the result. In this way, he may be able to find out a meaningful relationship between the plainimage and the cipherimage. If one minor change in the plainimage can cause a significant change in the cipherimage, then this differential attack would become very inefficient and practically useless.

To test the influence of one-pixel change on the whole image, encrypted by the RC5 block cipher, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [17-18]. Let two ciphered images, whose corresponding plainimages have only one pixel difference, be denoted by C1 and C2. Label the grey-scale values of the pixels at grid (i,j) in C1 and C2 by C1(i,j) and C2(i,j), respectively. Define a bipolar array, D, with the same size as images C1 and C2. Then, D(i,j) is determined by C1(i,j) and C2(i,j), namely, if C1(i,j) = C2(i,j) then D(i,j) = 1; otherwise, D(i,j) = 0.

The NPCR is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad (9)$$

where W and H are the width and height of C1 or C2. The NPCR measures the percentage of different pixel numbers between these two images.

The UACI is defined as

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%, \qquad (10)$$

which measures the average intensity of differences between the two images.

One performed test is on the one-pixel change influence on a 512 grey-scale image of size 512 x 512. The test results are shown in Table 3.

TABLE III

NPCR AND UACI ESTIMATION VERSUS R WITH RC5 AT W = 32, B = 16.

Ciphering rounds (r)	NPCR	UACI
1	0.0034%	0.02%
2	0.005%	0.34%
3	0.053%	0.46%
4	0.053%	0.49%
8	0.053%	0.56%
12	0.053%	0.42%
16	0.053%	0.29%
20	0.053%	0.29%
24	0.053%	0.29%
30	0.053%	0.34%

With respect to NPCR estimation versus ciphering rounds, the experimental results in Table 3 show that with the increasing of ciphering rounds, the influence of one-pixel change is negligible.

With respect to UACI estimation versus ciphering rounds, the experimental results in Table 3 show that with the increasing of ciphering rounds, the influence of one-pixel change is increased. But the rate of influence due to one pixel change is very small. Generally, these obtained results for NPCR and UACI may put the RC5 block cipher to some risks with respect to differential attacks. Hence, it is reasonable to increase the ciphering rounds in the test so as to achieve higher security; yet, this is at the expense of processing time.

V. Conclusion

The RC5 block cipher has proved to be an excellent alternative for the desire of having a simple and reliable image encryption scheme that has a high enough degree of security.

According to the results of our security analysis, we conclude that the RC5 is expected to be useful for real-time image encryption and transmission applications.

However, the RC5 block cipher may subjected to some risks with respect to differential attacks due to the obtained results for NPCR and UACI.

Security analysis experimental results show that, taking into account the trade-off between attack expense and information value as well as other issues such as operational speed, computational cost, and implementation simplicity this kind of image encryption schemes is very practical.

References

[1] Jui-Cheng Yen and Jiun-In Guo, "A new image encryption algorithm and its VLSI architecture," in Proc. IEEE Work-shop Signal Processing Systems, 1999, pp. 430–437.

[2] Jui-Cheng Yen and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," in Proc. IEEE Int. Conf. Circuits and Systems, 2000, vol. 4, pp. 49–52.

[3] C. Alexopoulos, Nikolaos G. Bourbakis, and N. Ioannou, "Image encrytion method using a class of fractals," J. Electronic Imaging, vol. 4, no. 3, pp. 251–259, 1995.

[4] Jinn-Ke Jan and Yuh-Min Tseng, "On the security of image encryption method," Information Processing Letters, vol. 60, pp. 261–265, 1996.

[5] Shujun Li and Xuan Zheng, "On the security of an image encryption method," in Proc. IEEE Int. Conference on Image Processing (ICIP'2002), volume 2, pages 925-928, 2002.

[6] Shujun Li and Xuan Zheng, "Cryptanalysis of a chaotic image encryption method," in Proc. IEEE Int. Symposium on Circuits and Systems (ISCAS'2002), volume II, pages 708-711, 2002.

[7] Ronald L. Rivest, "RC5 Encryption Algorithm," Dr Dobbs Journal, vol. 226, PP 146-148, Jan. 1995.

[8] W. Stallings, "Network and Internetwork Security: Principles and Practice," Prentice-Hall, New Jersey, 1995.

[9] Bruce Schneier, "Applied Cryptography – Protocols, algorithms, and source code in C," John Wiley & Sons, Inc., New York, second edition, 1996.

[10] W. Stallings, "Cryptography and Network Security: Principles and Practice," Prentice-Hall, New Jersey, 1999.

[11] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, “Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images.” Journal of Optical Engineering, vol. 45, 2006.

[12] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images". Submitted for publication in International Journal of Computer, Information, and Systems Science, and Engineering.

[13] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "An Efficient Chaos-Based Feedback Stream cipher (ECBFSC) for Image Encryption and Decryption”. Accepted for publication in An International Journal of Computing and Informatics, 2007.

[14] Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2004.

[15] Yaobin Mao and Guanrong Chen, "Chaos-based image encryption," in Eduardo Bayro-Corrochano, editor, Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics. Springer-Verlag, Heidelberg, April 2004.

[16] Shannon CE., "Communication theory of secrecy system," Bell Syst Tech J 1949;28:656-715.

[17] Yaobin Mao, Guanrong Chen, and Charles K. Chui, "A novel fast image encryption scheme based on 3D chaotic Baker maps," Int. J. Bifurcation and Chaos in June 2003.

[18] Yaobin Mao, Guanrong Chen, and Shiguo Lian, "A symmetric image encryption scheme based on 3D chaotic Cat maps," Chaos, Solitons and Fractals 21, pages 749-761, 2004.