Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images

Hossam El-din H. Ahmed[1], Hamdy M. Kalash[2], and Osama S. Farag Allah[2]

[1]Department of Electronics & Communication Eng., Faculty of Electronic Engineering, Menouf-32952,Egypt

[2]Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf-32952,Egypt

***Abstract*—This paper investigates the encryption efficiency of RC6 block cipher application to digital images, introducing a mathematical measure for encryption efficiency, which we will call the encryption quality instead of visual inspection, The encryption quality of RC6 block cipher is investigated among its several design parameters such as word size, number of rounds, and secret key length and the optimal choices for the best values of such design parameters are given. Also, the security analysis of RC6 block cipher for digital images is investigated from strict cryptographic viewpoint. The security estimations of RC6 block cipher for digital images against brute-force, statistical, and differential attacks are explored. Experiments are made to test the security of RC6 block cipher for digital images against all aforementioned types of attacks. Experiments and results verify and prove that RC6 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 RC6 block cipher algorithm. So, RC6 block cipher can be considered to be a real-time secure symmetric encryption for digital images.**

***Index Terms*—Block cipher, Image encryption, Encryption quality, and Security analysis.**

I. Introduction

In digital world nowadays, the security of digital images becomes more and more important since the communications of digital products over open network occur more and more frequently. Also, applications of digital imaging are prevalent and still continuously and rapidly increasing today, and yet the main obstacle in 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 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 communication systems.

In order to fulfill such a task, many different image encryption methods have been proposed such as DES (Data Encryption Standard) [1], IDEA (International Data Encryption Algorithm) [2] and RSA [3]. However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as bulk 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 [4], RC6 block cipher was proposed, which makes essential heavy use of data-dependent rotations. Its salient features include the use of four working registers instead of two as in RC5 [5], and the inclusion of integer multiplication as an additional primitive operation. The use of multiplication with four working registers greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increased throughput. It is also capable to handle 128-bits plaintext and ciphertext block sizes and suitable to be implemented simply using hardware or software. RC6 has a variable word size, a variable number of rounds, and a variable-length secret key.

The paper explores the encryption efficiency of RC6 block cipher along with its detailed security analysis regarding brute-force, statistical, and differential attacks. The rest of the paper is organized as follows: In Section II, we firstly give a brief description for the structural features and characteristics of RC6 block cipher. Test, verification and efficiency of RC6 application to digital images are given in Section III. Encryption efficiency, measurement of encryption quality, and encryption quality analysis of RC6 block cipher for digital images are explored in Section IV. Section V discusses the detailed security analysis of RC6 block cipher that includes key space analysis, statistical analysis, and differential analysis. Experimental results are also included in Sections III-IV, and the last section concludes this paper.

II. Structural Features and Characteristics of RC6 Block Cipher

RC6 has a simple structure and description relative to the other proposed block ciphers. In the following we refer to [6-8] for further descriptions and notation. RC6 was one of five

Manuscript received January 28, 2007. This work was supported by the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menouf-32952, Egypt

finalists for the Advanced Encryption Standard [9]. It consists of two Feistel networks whose data are mixed via data dependent rotations. The operations in one round of RC6 are the following: two applications of the squaring function f (x) = x (2x + 1) mod 2^{32}, two fixed 32-bit rotations, two data-dependent 32-bit rotations, two exclusive-ors and two additions modulo 2^{32}. A version of the RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a non-negative number of rounds r, and b denotes the length of the encryption key in bytes. RC6 is an evolutionary extension of the block cipher RC5, which receives much attention because of its design which is even simpler than that of RC6. where RC5 works on two 32-bit words, RC6 is extended to operations on four 32-bit words. The relative simple structure of RC5 has allowed for some easy analysis and yet it seems that 16 rounds of RC5 still resists all known attacks well. The design of RC6 is more complex than that of RC5, and consequently an analysis of the cipher gets more involved. The security of RC6 relies on the strength of data-dependent rotations, the mixed use of exclusive-or operations and modular additions, and on the squaring function f together with the fixed rotation. Table I summarizes a comparison between RC5 and RC6 different design parameters such as word size, block size, number of rounds, and secret key size.

TABLE 1
COMPARISON BETWEEN RC5 AND RC6 BLOCK CIPHER AT DIFFERENT DESIGN PARAMETERS

Parameters	Algorithm type	
	RC5	RC6
w (word size in bits)	16, 32, 64	16, 32, 64
r (No. of rounds)	0, 1, 2.., 255	0, 1, 2.., 255
b (Key length) in bytes	0, 1, 2.., 255	0, 1, 2.., 255
Block size in words	2w	4w
Block size in bits	32,64,128	64,128,256
Max. block size in bits	128	256
No. of keys derived from key schedule	2r + 2	2r + 4
Transformation Function f(x)	Does not exist	x(2x+1) mod 2w
Used Operation	+, -, ⊕, <<<, >>>	+, -, *, ⊕, <<<, >>>

III. TEST, VERIFICATION AND EFFICIENCY OF APPLICATION OF RC6 FOR DIGITAL IMAGES

In this section, to evaluate the efficiency of RC6 block cipher for application to digital images, some experiments' results are given to prove the efficiency of RC6 block cipher application for digital images. So, RC6 block cipher is applied to several digital images. Before encryption/decryption, we must firstly extract the image header for the image to be encrypted/decrypted. So, we must study the file format for image to determine all parts of the file header and to determine the beginning of the data stream to be encrypted [10,11]. Then, the RC6 block cipher is applied to the image.

We use the grey-scale images--Lena and Cman, each of size 256 x 256, grey-scale (0-255) as the original images (plainimages) and we use RC6-32/20/16. Figs. (1-2) show the results of RC6 block cipher for Lena and Cman images in both encryption/decryption. The visual inspection of Figs. (1-2) shows the possibility of applying RC6 block cipher to digital images successfully in both encryption/decryption. Also, it reveals its effectiveness in hiding the information contained in them.

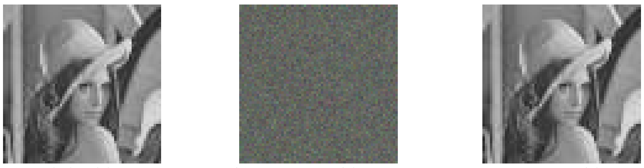

a) Original image b) Encrypted image c) Decrypted image

Fig. 1. Application of RC6 block cipher to Lena Plainimage/Cipherimage

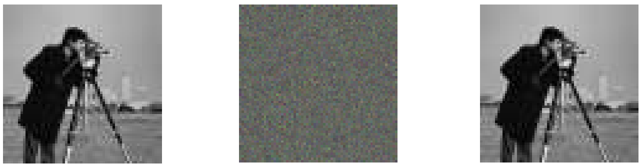

a) Original image b) Encrypted image c) Decrypted image

Fig. 2. Application of RC6 block cipher to Cman Plainimage/Cipherimage

IV. ENCRYPTION QUALITY ANALYSIS OF RC6 BLOCK CIPHER

All previous studies on image encryption were based on the visual inspection to judge the effectiveness of the encryption technique used in hiding features. Visual inspection is insufficient in evaluating the amount of information hidden [12]. So, we need to develop a mathematical measure to evaluate the degree of encryption quantity, which we will call the encryption quality.

The main goal here is to develop a mathematical model for the measurement of the amount of encryption quantity (Encryption quality) and to determine the optimal version of RC6-w/r/b that gives the most better encryption quality for RC6 block cipher. So, the effect of RC6 block cipher design parameters such as word size w, secret key length b, and the number of rounds b must be taken into account by evaluating the RC6 block cipher encryption quality as a function of its design parameters w, r, and b. Such estimations will help in determining the optimal choices for the values of such design parameters that will give better encryption quality for RC6 block cipher.

Some analysis is to be examined for the measurement of encryption quality and to provide the effect of RC6 block cipher design parameters such as block size, secret key length, and number of rounds on the encryption quality of RC6 block cipher for digital images.

In all experiments, we use the grey-scale two images--Lena, and Cman, each of size 512 x 512, grey-scale (0-255) as the original images (plainimages).

A. Measurement of Encryption Quality

With the application of encryption to an image a change takes place in pixels values as compared to those values before encryption. Such change may be irregular. This means that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality.

So the encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one. A measure for encryption quality may be expressed as the deviation between the original and encrypted image. The quality of image encryption may be determined as follows:

Let F , F' denote the original image (plainimage) and the encrypted image (cipherimage) respectively, each of size M*N pixels with L grey levels. $F(x,y), F'(x,y) \in \{0,..,L-1\}$ are the grey levels of the images F , F' at position (x,y), $0 \le x \le M-1, 0 \le y \le N-1$. We will define $H_L(F)$ as the number of occurrence for each grey level L in the original image (plainimage), and $H_L(F')$ as the number of occurrence for each grey level L in the encrypted image (cipherimage). The encryption quality represents the average

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} \mid H_L(F') - H_L(F) \mid}{256} \qquad (1)$$

number of changes to each grey level L and it can be expressed mathematically as in [13]:

B. *Effect of Number of Rounds on the Encryption Quality of RC5 and RC6*

The effect of number of rounds r on the encryption quality for RC5 and RC6 is investigated. The block size and secret key length are both constant, w = 32 and b = 16. The encryption quality (E.Q) of RC5 and RC6 is computed as a function of number of rounds (r) as shown in Table II.

TABLE II
ENCRYPTION QUALITY OF RC5 AND RC6 AS A FUNCTION OF NUMBER OF ROUNDS AT W = 32, B = 16 FOR LENA AND CMAN IMAGES

Encryption Quality (E.Q) of RC5 and RC6				
No. of Rounds r	Image Name			
	Lena		Cman	
	Algorithm type			
	RC5	RC6	RC5	RC6
4	726.133	719.977	991.727	992.172
8	725.791	723.234	991.727	990.219
12	724.838	726.133	988.961	991.719
16	721.719	725.523	999.742	992.672
20	721.711	725.609	999.742	993.234
24	721.711	723.117	999.742	990.266
30	721.719	723.828	999.742	990.117

The obtained results show that the RC6 block cipher achieves the maximum encryption quality after 20 rounds at r = 20. Also, RC5 has a maximum encryption quality at r = 16 rounds. Any increment for the number of rounds beyond these values for both RC5 and RC6 does not contribute to increase the encryption quality. So we suggest the use of number of rounds (r) to be 20 for RC6 and 16 for RC5 as standard values, which will result in a maximum value for encryption quality.

C. *The Effect of Secret Key Length on the Encryption Quality of RC5 and RC6*

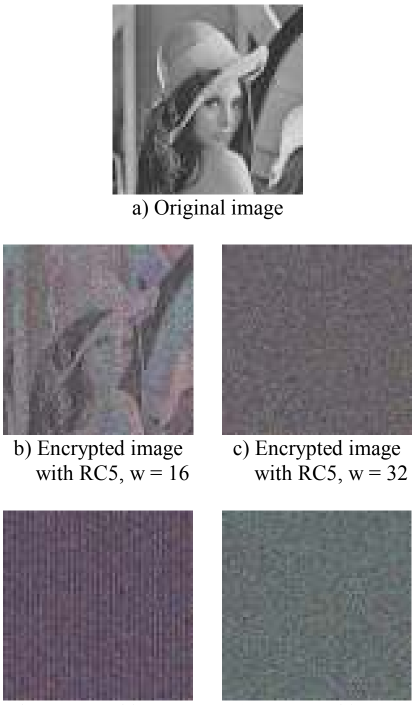
The effect of secret key length on the encryption quality for both RC5 and RC6 is investigated for fixed block size and number of rounds, at w = 32 and r = 20. Table III shows the computed results. These results show that the secret key length has a non-continuous effect on the encryption quality of RC5 and RC6 and the amount of variation to encryption quality (by increasing or decreasing) is small relative to large change in secret key length. In some cases, increasing secret key length may contribute to increase or decrease the encryption quality and vice versa as shown in Table III. From these results, we suggest the use of secret key length (b) to be 16 as this value give a moderate value of encryption quality for both RC5 and RC6. Secret key length contributes to increase the security of RC5 and RC6, which means increasing the security of block cipher by increasing its value.

TABLE III
ENCRYPTION QUALITY OF RC5 AND RC6 AS A FUNCTION OF SECRET KEY LENGTH AT W = 32, R = 20 FOR LENA AND CMAN IMAGES

Encryption Quality (E.Q) of RC5 and RC6				
Secret key length (b)	Image Name			
	Lena		Cman	
	Algorithm type			
	RC5	RC6	RC5	RC6
8	724.703	721.719	991.836	989.484
16	722.039	725.523	995.938	993.234
32	725.609	721.727	988.156	987.773
48	720.008	722.469	994.398	994.352
64	722.820	722.891	993.328	988.359
80	723.578	726.320	993.984	991.742
96	726.391	723.625	989.914	993.008
112	722.281	724.375	991.719	994.125
128	724.469	722.141	994.969	991.969
160	721.172	725.445	996.977	991.969
192	728.242	723.969	990.320	990.469
255	724.703	723.883	989.227	991.258

D. *The effect of block size on the encryption quality of RC5 and RC6*

The effect of block size on the encryption quality for both RC5 and RC6 is investigated for fixed number of rounds and secret key length, at r = 16, and b = 16. The theoretical calculated results and the practical results are shown respectively in Table IV and Figs. 3-4 for Lena and Cman images. These results clearly show that the encryption quality of RC6 block cipher increases with increasing block size and vice versa, so increasing the block size contributes to increase the encryption quality of RC5 and RC6. So we will suggest the use of w = 32 for both RC5 and RC6 which will result in a block size of 2w (64-bit block size) for RC5 and 4w (128-bit block size) for RC6 as an optimal choice for word length as it contributes to achieve a maximum value of encryption quality for both RC5 and RC6. Also, the agreement or compatibility between the theoretical and practical results proves the correctness of the proposed derived formula for the encryption quality.



a) Original image

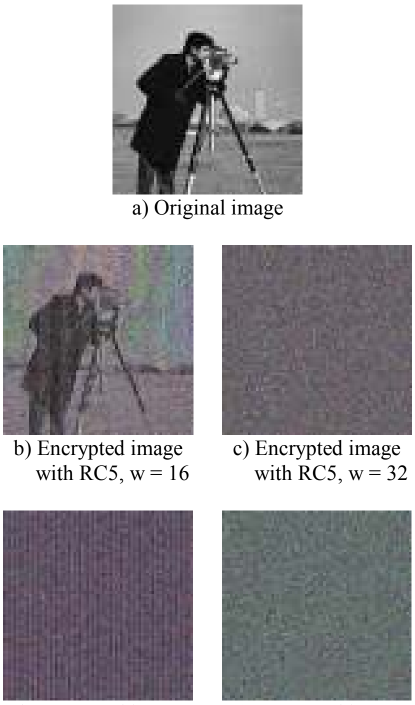
b) Encrypted image with RC5, w = 16

c) Encrypted image with RC5, w = 32

d) Encrypted image with RC6, w = 16

e) Encrypted image with RC6, w = 32

Fig. 3. Results of RC5 and RC6 to Lena image with b = 16, r = 16



a) Original image

b) Encrypted image with RC5, w = 16

c) Encrypted image with RC5, w = 32

d) Encrypted image with RC6, w = 16

e) Encrypted image with RC6, w = 32

Fig. 4. Results of RC5 and RC6 to Cman image with b = 16, r = 16

TABLE IV ENCRYPTION QUALITY OF RC5 AND RC6 AS A FUNCTION OF WORD SIZE AT B = 16, R = 16 FOR LENA AND CMAN IMAGES

Encryption Quality (E.Q) of RC5 and RC6				
Word size w (bits)	Image Name			
	Lena		Cman	
	Algorithm type			
	RC5	RC6	RC5	RC6
16	362.867	713.258	499.742	983.844
32	722.039	914.620	995.938	1100

V. SECURITY ANALYSIS AND TEST RESULTS

A good cipher should have strong ability to withstand all kinds of cryptanalysis and attacks that try to break the system such as the known-plaintext attack, ciphertext only attack, various brute-force attacks, statistical attacks, and differential attacks [14-17].

To a certain extent, the resistance against attacks is a good measure of the performance of a cryptosystem. So, it is often used to evaluate cryptosystems.

The security of RC6 block cipher is estimated for digital images, even under brute-force attack, statistical and differential attacks. It is shown that RC6 block cipher is secure from the strongly cryptographic viewpoint. The results show the satisfactory security of the RC6 block cipher, as demonstrated in the following subsections. Here, some security analysis results on the scheme are described, including the most important ones like key space analysis, statistical analysis, and differential analysis. The evaluation consisted of theoretical derivations and practical experimentation.

A. Key space Analysis

A good block cipher should be sensitive to the cipher keys, and key space should be large enough to make brute-force attacks infeasible. For RC6, the key space analysis and testing have been carefully carried out, with results summarized as follows:

A.1 Exhaustive key search

The RC6 block cipher algorithm is a 128-bit encryption scheme whose key space size is in the range (0-2040) bit. An exhaustive key search will take 2^k operations to succeed, where k is the key size in bits. This attack needs a few known plainimage-cipherimage pairs. An attacker simply tries all keys, one by one, and checks whether the given plainimage encrypts to the given cipherimage. For a block cipher with a k-bit key and n-bit blocks, the number of pairs of images needed to determine the key uniquely is approximately [k/n] as shown in [18]. The key space size should be large enough to prevent such exhaustive searching. Therefore, an opponent may try to bypass guessing the key and directly guesses all the possible combinations will need about 2^{2040} operations to successfully determine the key, which is practically infeasible.

A.2 Key sensitivity test

Assume that a 16-character ciphering key is used. This means that the key consists of 128 bits. A typical key sensitivity test has been performed, according to the following steps:

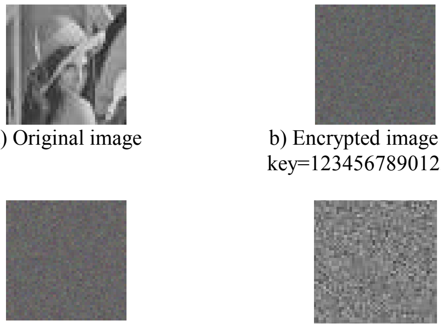
1-First, a 512x512 image is encrypted by using the test key "1234567890123456".

2-Then, the least significant bit of the key is changed, so that the original key becomes, say "1234567890123457" in this example, which is used to encrypt the same image.

3-Finally, the above two ciphered images, encrypted by the two slightly different keys, are compared.

The result is that the image encrypted by the key "1234567890123456" has 99.63% 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. 5 shows the test result. Moreover, when a 16-character key is used to encrypt an image while another trivially modified key is used to decrypt the ciphered image, the decryption also completely fails.

Fig. 6 has verified this and clearly shows that the image encrypted by the key "1234567890123456" is not correctly decrypted by using the key "1234567890123457", which has also only one bit difference between the two keys.



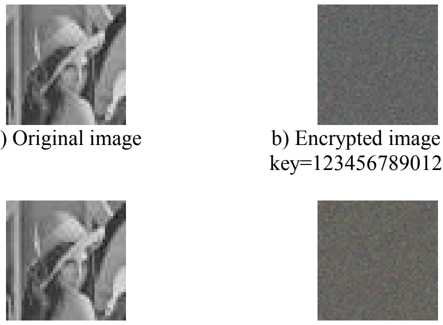
a) Original image

b) Encrypted image with key=1234567890123456

c) Encrypted image with key=1234567890123457

d) Difference image

Fig. 5. Key sensitive test result 1 with RC6-32/20/16



a) Original image

b) Encrypted image with key=1234567890123456

c) Decrypted image with key=1234567890123456

d) Decrypted image with key=1234567890123457

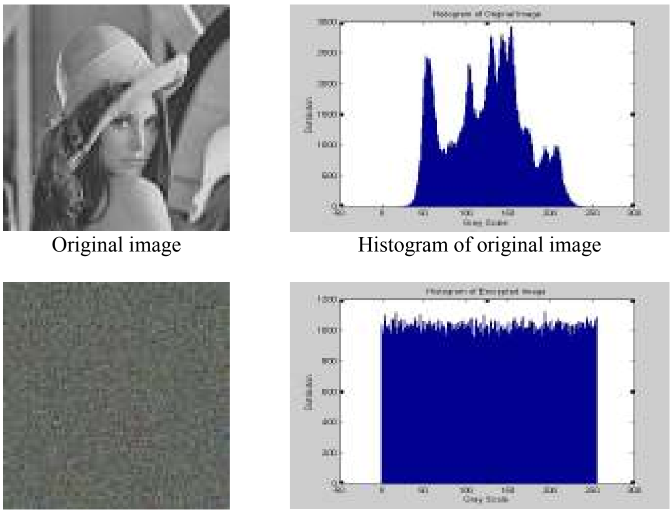
Fig. 6. Results of RC5 block cipher to Lena image with b = 16, r = 16

B. Statistical Analysis

In his masterpiece [19], Shannon said, "It is possible to solve many kinds of ciphers by statistical analysis," and, therefore, he suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis. Statistical analysis has been performed on the RC6 block cipher algorithm, demonstrating its superior confusion and diffusion properties, which strongly resist statistical attacks. This is shown by a test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

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. 7. 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. 7. Histograms of the Plainimage and the cipherimage

C.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:

$$\operatorname{cov}(x,y) = E(x - E(x))(y - E(y)), \tag{2}$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{3}$$

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

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

$$D(x) = \tfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{5}$$

$$\operatorname{cov}(x,y) = \tfrac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{6}$$

Fig. 8 shows the correlation distribution of two horizontally adjacent pixels in the plainimage/cipherimage for RC6 block cipher. The correlation coefficients are 0.9921 and 0.0077 respectively for RC6, which are far apart. Similar results for diagonal and vertical directions were obtained, and summary of results for both RC5 and RC6 is shown in Table V.

TABLE V
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN TWO IMAGES FOR RC5 AND RC6

Direction of Adjacent pixels	Plainimage		Cipherimage	
	Algorithm type			
	RC5	RC6	RC5	RC6
Horizontal	0.9910	0.9921	0.0054	0.0077
Vertical	0.9830	0.9852	0.0038	0.0015
Diagonal	0.9696	0.9768	0.0031	0.0064

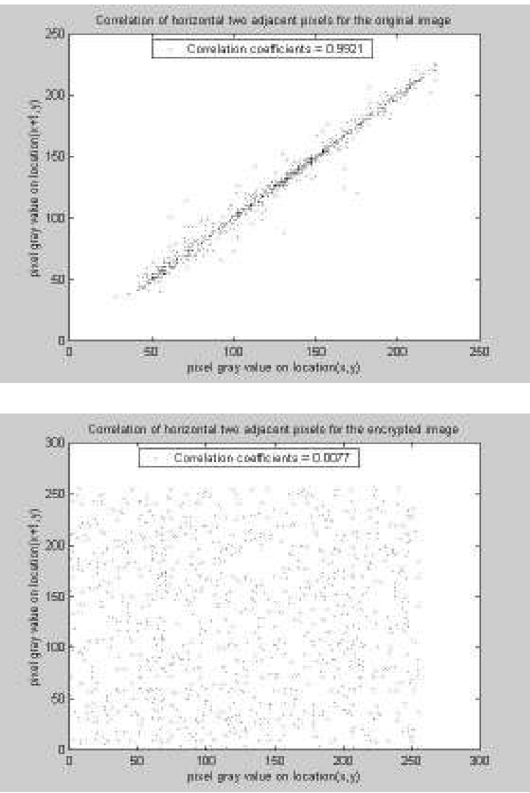


Fig. 8. Correlations of two horizontally adjacent pixels in plainimage/cipherimage.

C. Differential Analysis

In general, the opponent may make a slight change such as modifying only one pixel of the encrypted 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, with respect to diffusion and confusion, 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 RC6 or RC5, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). 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

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad (7)$$

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

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%, \qquad (8)$$

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 VI.

With respect to NPCR estimation versus ciphering rounds, the experimental results in Table VI for both RC5 and RC6 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 VI for both RC5 and RC6 show that with the increasing of ciphering rounds, the influence of one-pixel change is increased. But the rate influence due to one pixel change is very small. Generally, these obtained results for NPCR and UACI may put both RC6 and RC5 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.

TABLE VI
NPCR AND UACI ESTIMATION VERSUS R WITH RC5 AND RC6 AT W = 32, B = 16.

ciphering rounds (r)	NPCR		UACI	
	Algorithm type			
	RC5	RC6	RC5	RC6
1	0.0034%	0.0034%	0.02%	0.28%
2	0.005%	0.0057%	0.34%	0.48%
3	0.053%	0.0061%	0.46%	0.57%
4	0.053%	0.0061%	0.49%	0.64%
8	0.053%	0.0061%	0.56%	0.52%
12	0.053%	0.0061%	0.42%	0.41%
16	0.053%	0.0061%	0.29%	0.79%
20	0.053%	0.0061%	0.29%	0.64%
24	0.053%	0.0061%	0.29%	0.61%
30	0.053%	0.0061%	0.34%	0.54%

VI. CONCLUSION

This paper introduces a successfully efficient implementation of RC6 block cipher for digital images; provide its testing, verification, encryption efficiency analysis, and security evaluation.

A mathematical measure for encryption efficiency, that is called encryption quality was introduced, and may be considered to compare the effectiveness of different encryption techniques to digital images instead of visual inspection.

Comparative analysis and 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 RC6 block cipher achieved the most better encryption quality for the choices of word size w = 32, number of rounds = 20, and secret key length b = 16. Based on such results, the optimal version of RC6-w/r/b block cipher algorithm that gives maximum encryption quality is estimated to be RC6-32/20/16.

From an engineer's perspective, the use of RC6 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] National Bureau of standards. "Data Encryption Standard," Federal Information processing standards Publication 46, US Government Printing Office, Washington, D.C., 1977.

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

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

[4] R.L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "The RC6TM Block cipher," v.1.1, August 20, 1998. Available at ww.rsa.com/rsalabs/aes/.

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

[6] RSA Security. "The RC6 Block cipher," Cryptographic Technique Specifications.

[7] RSA Security. "The RC6 Block cipher," Self Evaluation Report.

[8] Osama S. Farag Allah, Abdul Hamid M. Ragib, and Nabil A. Ismali, "Enhancements and Implementation of RC6 Block Cipher for Data Security". IEEE Catalog Number: 01CH37239, Published 2001.

[9] R.L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin, "Some Comments on the First Round AES Evaluation of RC6," available at http:// csrc.nist.gov/encryption/aes/round1/pubcmnts.htm.

[10] Harley R. Myler and Arthur R. Weeks, "The Pocket Handbook of Image Processing Algorithms in C," Prentice-Hall, New Jersey, 1993.

[11] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, “Implementation of RC5 Block Cipher Algorithm for Digital Images”. Proceeding of The 5th Central European Conference on Cryptography (MoraviaCrypt 2005), 15-17 June, 2005, Brno, The Czech Republic.

[12] Ibrahim E. Ziedan, Mohammed M. Fouad, and Doaa H. Salem. "Application of data encryption standard to bitmap and JPEG images," in Proc. 12th National Radio Science Conference (NRSC2003), pp. C16/1-C16/8, 2003.

[13] 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

[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] 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.

[16] 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.

[17] 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.

[18] Business Software Alliance, Matt Blaze et al., "Minimum key length for symmetric ciphers to provide adequate commercial security," available at: http://www.bsa.org/bsa/cryptologists.html

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

Hossam El-din Hussein Ahmed was born in Sahka-kafer Elshekh Governorate- Egypt on 1946. He received a B.S. in Nuclear Engineering in June 1969 from Faculty of Engineering- Alexandria University. a M.Sc. in Microelectronic in April 1977 from Nuclear Department-Faculty of Engineering-Alexandria University, and a Ph.D. in June 1983 from High Institute of Electronic & optic-Paul Sabatier University-Toulouse, France. He appointed as Demonstrator in Faculty of Engineering and Technology-Menoufia University from January 1970 till August 1977. He became an assistant Lecturer in 1977 and a Lecturer in 1983. and promoted to an Associate Professor in 1988 and to a full Professor of Microelectronic and Computer Network in 1993 at the Dept. of Electronics & Communication Eng. He was the Vice dean for Education and Student in Faculty of Electronic Engineering, Menoufia University from July 1993 till July 1999 and the Director and Designer of Menoufia university WAN (21 LAN) from 1996 till now. He was appointed as the President of Dept. of Electronics & Communication Eng. From September 2001 till December 2001, and as the Dean of Faculty of Electronic Engineering in 9 December 2001. His research interests cover Microelectronics VLSI Design and Technology, Computer Networking, Communication systems, Computer Design, Microscopic: Electron Diffraction, Electrons Transmission and Backscatter, Transmission and scanning Microscope, Crystallography, Physical Metallurgy and Lithography, Cryptography, Multimedia Security, Image Encryption, Watermarking, Steganography.

Hamdy M. Kalash was born in Egypt in 1947. He received B.Sc., M.Sc., and Ph.D. degrees all in Computer Science & Engineering in 1971, 1978 and 1985, respectively. In 1972, he was appointed as an Instructor in the Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt. He became an assistant Lecturer in 1978. and a Lecturer in 1995, and promoted to an Associate Professor in 1991. His research interests cover Parallel Processing, Artificial Intelligence, Compiler Design, Cryptography, Internet Security, Multimedia Security, Image Encryption.

Osama S. Farag Allah was born in Menoufia, Egypt on August 29, 1974. He received a B.S. in Computer Science & Engineering (1997) from Menoufia University, Faculty of Electronic Engineering, Egypt in 1997, a M.Sc. in Computer Science & Engineering (2002) from Menoufia University, Faculty of Electronic Engineering, Egypt in 2002, and a Ph.D. in Computer Science & Engineering (2007) from Menoufia University, Faculty of Electronic Engineering, Egypt in 2007. He appointed as a demonstrator at the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, from 1997 to 2002. He became an assistant Lecturer in 2002 and promoted to a Lecturer in 2007. His research interests cover Computer Networks, Network Security, Cryptography, Internet Security, Multimedia Security, Image Encryption, Watermarking, Steganography, Data Hiding, Chaos Theory.