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

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

Abstract—This paper investigates the encryption efficiency of RC6 block cipher application to digital images, providing a new 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.

Keywords—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 am 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 2, 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 3. Encryption efficiency, measurement of encryption quality, and encryption quality analysis of RC6 block cipher for digital images are explored in Section 4. Section 5 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 3-5, 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-
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, rounds, and secret key size.

### TABLE I

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Algorithm type</th>
</tr>
</thead>
<tbody>
<tr>
<td>w (word size in bits)</td>
<td>16, 32, 64, 16, 32, 64</td>
</tr>
<tr>
<td>r (No. of rounds)</td>
<td>0, 1, 2, 255, 0, 1, 2, 255</td>
</tr>
<tr>
<td>b (Key length)</td>
<td>0, 1, 2, 255, 0, 1, 2, 255</td>
</tr>
<tr>
<td>Block size in words</td>
<td>2w</td>
</tr>
<tr>
<td>Block size in bits</td>
<td>32, 64, 128</td>
</tr>
<tr>
<td>Max. block size in bits</td>
<td>128, 256</td>
</tr>
<tr>
<td>No. of keys derived from key schedule</td>
<td>2r + 2, 2r + 4</td>
</tr>
<tr>
<td>Transformation function f(x)</td>
<td>Does not exist, x(2x+1) mod 2^w</td>
</tr>
<tr>
<td>Used Operation</td>
<td>⊕, -, B, &lt;&lt;&lt;, &gt;&gt;&gt;</td>
</tr>
</tbody>
</table>

### 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. 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.

### 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.

Since, RC6 block cipher is a fully parameterized family of encryption algorithms. A version of the RC6 block cipher is more accurately specified as RC6-w/r/b. So, there are several different choices for the values of RC6 design parameters such as word size w, number of rounds r, and secret key length b. So, there will be different versions of RC6-w/r/b.

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 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 r 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,
Encryption Quality = \[ \sum_{L=0}^{255} \left| H_L(F') - H_L(F) \right| \]  
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 \( M \times N \) pixels with \( L \) grey levels. \( F(x, y), F'(x, y) \in [0, \ldots, L - 1] \) are the grey levels of the images \( F, F' \) at position \( (x, y) \), \( 0 \leq x \leq M - 1, 0 \leq y \leq N - 1 \). 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 number of changes to each grey level \( L \) and it can be expressed mathematically as in [13]:

\[ \text{Encryption Quality} = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)|}{256} \]  

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 2.

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 results 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 3 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 3. From these results, we suggest the use of secret key length (b) to be 16 as this value gives 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.

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 4 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.

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

<table>
<thead>
<tr>
<th>Encryption Quality (E.Q) of RC5 and RC6</th>
<th>Image Name</th>
<th>Algorithm type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ø</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ø</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ø</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ø</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ø</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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:

B. 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 plaintext-image-ciphertext image 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 $k$-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 $2^{2000}$ operations to successfully determine the key, which is practically infeasible.

C. 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.

D. 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.

D.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).

D.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:

$$\text{cov}(x, y) = E((x - E(x))(y - E(y)))$$
where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \]  

(4)

\[ D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \]  

(5)

\[ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \]  

(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 5.

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

<table>
<thead>
<tr>
<th>Direction of Adjacent pixels</th>
<th>Plainimage</th>
<th>Cipherimage</th>
<th>Algorithm type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RC5</td>
<td>RC6</td>
<td>RC5</td>
</tr>
<tr>
<td>Horizontal</td>
<td>0.9910</td>
<td>0.9921</td>
<td>0.0054</td>
</tr>
<tr>
<td>Vertical</td>
<td>0.9830</td>
<td>0.9852</td>
<td>0.0038</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.9696</td>
<td>0.9768</td>
<td>0.0031</td>
</tr>
</tbody>
</table>

E. 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

\[ \text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \]  

(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

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

(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 6.
With respect to NPCR estimation versus ciphering rounds, the experimental results in Table 6 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 6 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

<table>
<thead>
<tr>
<th>ciphering rounds (r)</th>
<th>NPCR UACI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Algorithm type</td>
</tr>
<tr>
<td></td>
<td>RC5</td>
</tr>
<tr>
<td>1</td>
<td>0.0034%</td>
</tr>
<tr>
<td>2</td>
<td>0.005%</td>
</tr>
<tr>
<td>3</td>
<td>0.053%</td>
</tr>
<tr>
<td>4</td>
<td>0.053%</td>
</tr>
<tr>
<td>8</td>
<td>0.053%</td>
</tr>
<tr>
<td>12</td>
<td>0.053%</td>
</tr>
<tr>
<td>16</td>
<td>0.053%</td>
</tr>
<tr>
<td>20</td>
<td>0.053%</td>
</tr>
<tr>
<td>24</td>
<td>0.053%</td>
</tr>
<tr>
<td>30</td>
<td>0.053%</td>
</tr>
</tbody>
</table>

### VI. CONCLUSION

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

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.

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


---

International Scholarly and Scientific Research & Innovation 1(2) 2007 389 scholar.waset.org/1999.1/15813