Analyzing Encryption Quality of RC5 and RC6 Block Ciphers for Grey Image Encryption Algorithm

Nwe Thazin
Computer University, Pinlong
nwethazin87 @gmail.com

Abstract

With the fast progression of information exchange in electronic way, security is becoming more important in information transmission as well as in storage. To protect the confidential data from unauthorized access, several encryption methods have been used. In this paper, we present an image encryption system based on RC5 and RC6 block ciphers. Then we analyze image encryption qualities of RC5 and RC6 as functions of their design parameters: word size w, number of rounds r, and secret key length b. From this analysis, optimal values for w, r and b are suggested to get maximum encryption quality of RC5 and RC6. This system is implemented by Java programming.

1. Introduction

The requirements of information security within an organization have undergone tremendous changes. Before the widespread use of data processing equipment, the security of sensitive documents depends on filing cabinets with a combination lock for storing paper-based files or documents. However the scenario has change with the introduction of computer in handling businesses in organizations. At the same time, advances in networking and communication technology bring the business organizations worldwide working together as one entity [4].

As the rapid progress of technology in the real world, the security of digital images and videos has become more and more important. How to protect the security of images is a serious problem. To meet the challenges arising from different applications, good encryption of digital images is necessary. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. Currently there are several approaches available for protecting digital images [6].

In this paper, encryption qualities of RC5 and RC6 are analyzed using several digital images. This paper is organized as follows: Section 2 briefs related works. Section 3 presents system architecture and the characteristics of RC5 and RC6 block ciphers. Encryption quality analysis is described in section 4 and the results obtained are shown in section 5. Conclusion, limitation and further extension are presented in section 6.

2. Related works

Encryption is the process of transforming the information to insure its security. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. In order to fulfill such a task, many different image encryption methods have been proposed.

In [2], 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. In [3], successful efficient implementation of RC6 block cipher for digital image is proposed. The results of their security analysis show that RC6 block cipher algorithm as a candidate for image encryption is very promising for real-time secure image.

3. System architecture

In this system, there are two main parts: encryption of RC5 and RC6 block cipher and encryption quality analysis of RC5 and RC6 block cipher for digital images. Detailed structure of proposed system design is described in figure 1.

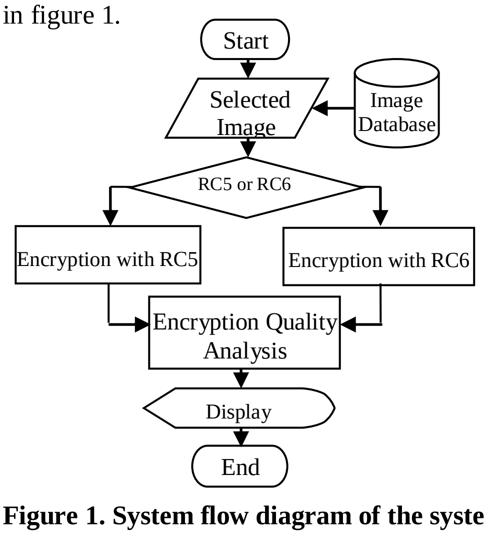


Figure 1. System flow diagram of the system

3.1 Characteristics of RC5

The RC5 encryption algorithm is a block cipher that converts plaintext data a blocks of 16, 32, and 64 bits into ciphertext blocks of the same length. 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) . 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 bitwise 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-2w 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 [1]

3.2 Characteristics of RC6

RC6 has a simple structure and description relative to the other proposed block ciphers. RC6 was one of five finalists for the Advanced Encryption Standard. 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 232, two fixed 32-bit rotations, two data-dependent 32-bit rotations, two exclusive-ORs and two additions modulo 232. 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 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 resist 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 1 summarizes a comparison between RC5 and RC6 different design parameters such as word size, block size, number of rounds, and secret key size [2] [7] [5].

Table 1. Comparison between RC5 and RC6 block cipher at different design parameter

Parameter	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	+, -, ⊕, <<<, >>>	+, -, ⊕,*, <<<, >>>

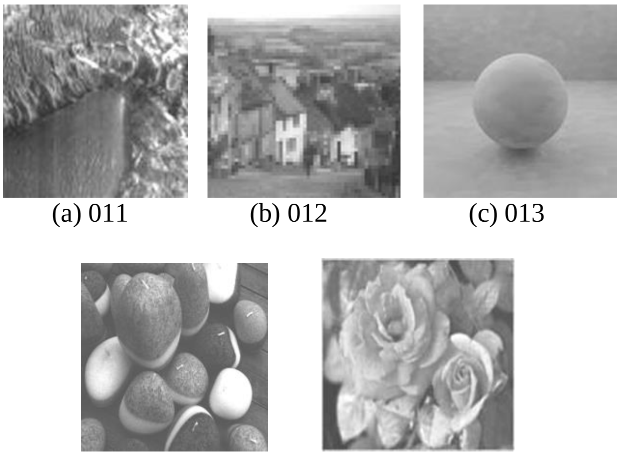
4. Encryption quality analysis

With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently this means that the higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption. So, the quality of encryption may be determined as follows [4]:

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) ∈ {0,…., L – 1} are the grey levels of the images F, F´ at position (x, y), $0 \le x \le M-1,0 \le y \le N-1$. Let $H_L(F)$ denote the number of occurrences of each grey level L in the original image (plainimage) F. Similarly, $H_L(F')$ denotes the number of occurrences of each grey level L in the encrypted image (cipherimage) F´. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as

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

For all tests we have used five images shown in figure 3. All of the images are 512×512 pixel, grey scale (0-255).


(a) 011 (b) 012 (c) 013

(d) 014 (e) 015

Figure 2.Testing images for encryption quality analysis

In encryption quality analysis, the effects of the design parameters of RC5 and RC6 on encryption qualities are examined. And then, compare the results such as; the effect of number of rounds on the encryption quality for RC5 and RC6, the effect of secret key length on the encryption quality for RC5 and RC6, the effect of the block size on the encryption quality for RC5 and

RC6. Figure 2 show the encryption quality analysis of this system.

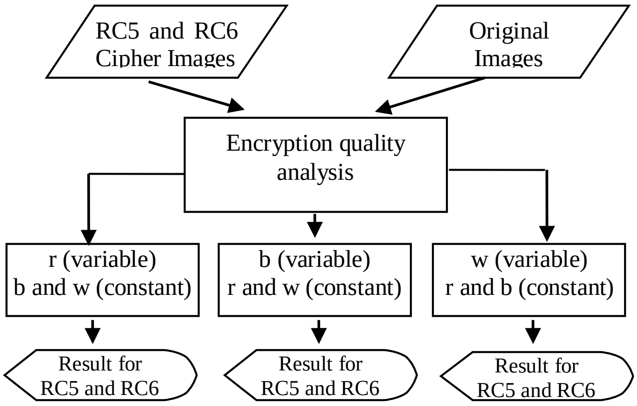

RC5 and RC6 Cipher Images
Original Images
Encryption quality analysis
r (variable) b and w (constant)
b (variable) r and w (constant)
w (variable) r and b (constant)
Result for RC5 and RC6
Result for RC5 and RC6
Result for RC5 and RC6

Figure 3. System flow diagram of encryption quality analysis

4.1 Effect of number of rounds on the encryption quality of RC5 and RC6

The effect of number of rounds r on the encryption quality of RC5 and RC6 is investigated while 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 and 3, respectively.

Table 2. Encryption quality of RC5 as a function of number of rounds at w = 32, b = 16

Encryption Quality (E.Q) of RC5					
No. of round r	Image Name				
	011	012	013	014	015
4	897.719	762.335	721.133	858.312	897.351
8	903.148	764.312	721.791	867.585	901.018
12	903.369	765.875	724.838	884.250	903.371
16	903.371	765.919	726.719	886.191	905.148
20	903.356	765.884	725.916	886.190	903.289
24	903.371	765.768	725.916	886.191	904.116
30	903.371	765.912	724.113	886.191	905.120

Table 3. Encryption quality of RC6 as a function of number of rounds at w = 32, b = 16

Encryption Quality (E.Q) of RC6					
No. of round r	Image Name				
	011	012	013	014	015
4	915.734	763.718	719.977	872.625	902.008
8	916.988	765.093	723.234	881.476	904.192
12	918.651	765.894	726.312	887.923	904.266
16	918.672	766.375	726.117	890.101	905.585
20	918.734	766.859	726.633	890.125	905.719
24	918.726	766.859	725.523	890.123	905.711
30	918.731	766.859	725.828	890.125	905.711

4.2 Effect of secret key length on the encryption quality of RC5 and RC6

The effect of secret key length on the encryption quality of both RC5 and RC6 is investigated for fixed with 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.

Table 4. Encryption quality of RC5 as a function of number of key length at w = 32, r = 20

Encryption Quality (E.Q) of RC5					
Secret key length b	Image Name				
	011	012	013	014	015
8	896.991	752.375	724.703	853.884	898.046
16	903.369	765.875	724.838	884.250	903.371
32	901.919	762.008	725.609	859.617	903.281
48	903.842	761.918	720.008	868.046	902.962
64	903.373	757.391	722.820	864.562	903.428

Table 5. Encryption quality of RC6 as a function of number of key length at w = 32, r = 20

Encryption Quality (E.Q) of RC6					
Secret key length b	Image Name				
	011	012	013	014	015
8	916.121	752.456	723.719	867.664	900.328
16	918.651	765.894	726.312	887.923	904.266
32	918.528	759.412	721.727	884.812	903.281
48	918.562	762.808	722.469	881.265	902.962
64	918.412	762.141	722.891	884.273	903.428

4.2 Effect of block size on the encryption quality of RC5 and RC6

The effect of block size on the encryption quality of both RC5 and RC6 is investigated with fixed number of rounds and secret key length, at r=16, and b=16. The results are shown in Table 4. 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.

Table 6. Encryption Quality of RC5 as a function of number of word size at b= 16, r = 16

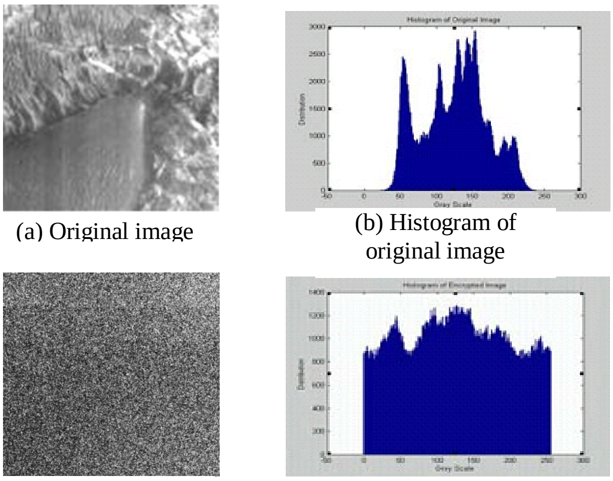
Encryption Quality (E.Q) of RC5					
Word size w	Image Name				
	011	012	013	014	015
8	898.305	698.192	608.192	766.476	712.811
16	902.270	762.441	698.441	801.428	849.562
32	903.369	765.875	724.838	884.250	903.371

Table 7. Encryption Quality of RC6 as a function of number of word size at b= 16, r = 16

Encryption Quality (E.Q) of RC6					
Word size w	Image Name				
	011	012	013	014	015
8	903.371	712.859	672.375	770.476	763.648
16	913.008	760.281	718.812	820.818	882.892
32	918.651	765.894	726.312	887.923	904.266

5. Experimental Result

According to the results obtained, RC5-32/16/16 and RC6-32/20/16 were suggested as optimal versions to use in encryption. To verify this, a digital image was applied to the system, which used optimal versions of RC5 and RC6. Firstly, the original image Cave (Fig.4(a)) is encrypted by using RC5 and RC6. Then we have evaluated the encryption qualities. The system offers encryption qualities of (903.371) with RC5 and (918.734) with RC6.

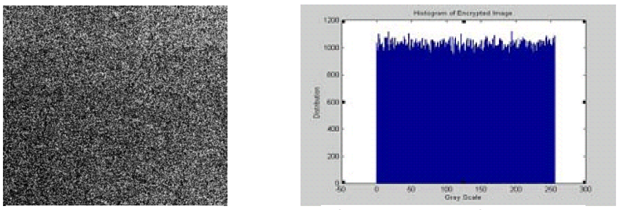


(a) Original image

(b) Histogram of original image

(c) Encrypted image using RC5

(d) Histogram of encrypted image using RC5



(e) Encrypted image using RC6

(f) Histogram of encrypted image using RC6

Figure 4. Original image and encrypted images

Figure 4.(b) refers histogram of the original image. Figure 4.(c) shows encrypted image with RC5 and its histogram can be seen in Figure 4.(d). Figure 4.(e) shows encrypted image with RC6 and its histogram can be seen in Figure 4.(f).

6. Conclusion

This paper presents image encryption based on symmetric key cryptography, using RC5 and RC6 block ciphers. When comparing image encryption quality of RC5 and RC6 block cipher algorithms, most of the results pointed out that RC6 block cipher algorithm can give better encryption quality. This system can only be used for digital images of 512 × 512 pixels, grey-scale (0-255) as the original images. But, it can further be extended to become a system that is enabling to accept colour images as the input to the system.

7. References

[1]. 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”, International Journal of Computer, Information, and Systems Science, and Engineering 1;1 © www.waset.org Winter 2007.

[2]. Hossam El.din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, “Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Image”, International Journal of Information Technology Volume 3 Number 4.

[3]. Mazieena Salleh, Subariah Ibrahim & Ismail Fauzi Isnin, “Image Encryption Algorithm Based On Chaotic Mapping”, Jurnal Teknologi, 39(D) Dis.2003: 1-12.

[4]. Mohammad Ali Bani Youned and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS-35-1-03.

[5]. Ronald L.Rivest, “RC5 Encryption Algorithm”, Dr Doobs Journal, vol.226, PP 146-148, Jan. 1995.

[6]. Ronald L. Rivest1, M.J.B. Robshaw2, R. Sidney2, and Y.L. Yin2, “The RC6 Block Cipher”, Version 1.1 - August 20, 1998.

[7]. Ronald L.Rivest, M.J.B Robshaw, and Yiqun Lisa Yin, “The security of the RC6^{TM} Block Cipher”, Version 1.0- August 20, 1998.