2011 8th International Multi-Conference on Systems, Signals & Devices

IMPLEMENTATION OF RC5 AND RC6 BLOCK CIPHERS ON DIGITAL IMAGES

Asma Belhaj Mohamed[1], *Ghada Zaibi*[1], *Abdennaceur Kachouri*[2]

[1] Sfax University, National Engineering School of Sfax, LETI Laboratory,
[2] Gabes University ISSIG Higher Institute Of Industrial Systems Gabes CP 6011 TUNISIA.

ABSTRACT

With the fast evolution of the networks technology, the security becomes an important research axis. Many types of communication require the transmission of digital images. This transmission must be safe especially in applications that require a fairly high level of security such as military applications, spying, radars, and biometrics applications. Mechanisms for authentication, confidentiality, and integrity must be implemented within their community. For this reason, several cryptographic algorithms have been developed to ensure the safety and reliability of this transmission. In this paper, we investigate the encryption efficiency of RC5 and RC6 block cipher applied to digital images by including a statistical and differential analysis then, and also we investigate those two block ciphers against errors in ambient noise. The security analysis shows that RC6 algorithm is more secure than RC5. However, using RC6 to encrypt images in rough environment (low signal to noise ratio) leads to more errors (almost double of RC5) and may increase energy consumption by retransmitting erroneous packets. A compromise security/energy must be taken into account for the good choice of encryption algorithm.

Index Terms— RC5, RC6, Block cipher, Digital Image encryption, symmetric encryption

1. INTRODUCTION

Historically developed to ensure secrecy in the mail, encryption of information today is used more broadly to prohibit access to or modification of sensitive data and ensure confidentiality in computer applications, so cryptology is the science that studies the scientific aspects of these techniques (cryptography and cryptanalysis) and it is essentially based on arithmetic [1]. Encryption techniques have evolved since their inception: modern encryption uses the power of modern computers. Since the data processed by computers are only as digital (bit), the methods of substitutions and transpositions are still used but now only on two primary elements (0 and 1). Thus, encryption has adapted to the progress of our times by abandoning the old methods for modern methods.

Encryption of digital images is increasingly used following the evolution of communication technology in the digital world, and that requires the secure transmission like medical imaging systems, pay TV, confidential video conferencing, etc [2].

Many cryptographic algorithms appeared to ensure the encoding of that information such as DES, RSA etc.

However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as data capacity and high redundancy, which are troublesome for traditional encryption [3]. Moreover, these encryption schemes require extra operations on compressed image data thereby demanding long computational time and high computing power.

RC5 and RC6 block Cipher was proposed to encrypt information by using simple arithmetic operators and data-dependent rotations. Both of the two block ciphers were designed by Ronald Rivest for RSA Security (RC5 in 1995 and RC6 in 1998) [4], [5]. The acronym "RC" stands for "Ron's Code" or "Rivest's Cipher." It has the advantage of having a data block “w”, a number of rounds “r” and key lengths “b” variables (which are illustrate in table 1).

Arithmetic and logic operations used in RC5 and RC6 block ciphers are:

a + b: integer addition modulo 2w.

a – b: integer subtraction modulo 2w.

a $\oplus$ b: bitwise exclusive-or of w-bit words.

a × b: integer multiplication modulo 2w (only in RC6 block cipher).

a << b: rotate the w-bit word into the left by the amount given by the least significant log $_w$ bits of b.

a >> b: rotate the w-bit word into the right by the amount given by the least significant log$_w$ bits of b.

In this work, we study encryption efficiency of RC5 and RC6 applied to digital images using Matlab. In section 2 we present the Feistel function of the two algorithms. Security and statistical analysis as well as a comparison of both algorithms, are done in section 3.

In the last section, we investigate the robustness of RC5 and RC6 against errors in ambient noise.

978-1-4577-0411-6/11/$26.00 ©2011 IEEE

2. STRUCTURAL FEATURES OF RC5 AND RC6 BLOCK CIPHER

Both RC5 and RC6 block ciphers, have a simple structure. The RC5 algorithm uses an input of 2 WORDS of w bits (A and B). Arithmetic and logic operations are applied on those blocks as depicted in figure1.

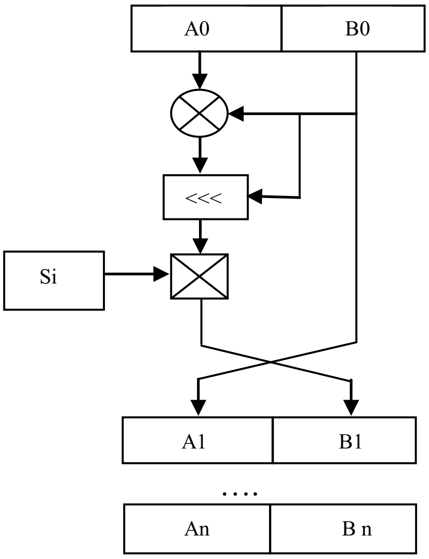


Figure 1. RC5 block cipher.

RC6 uses an input of 4 words of w bits (A, B, C and D). The same arithmetic and logic operations are applied on these blocks with an extra multiplication and a transformation function (figure 2).

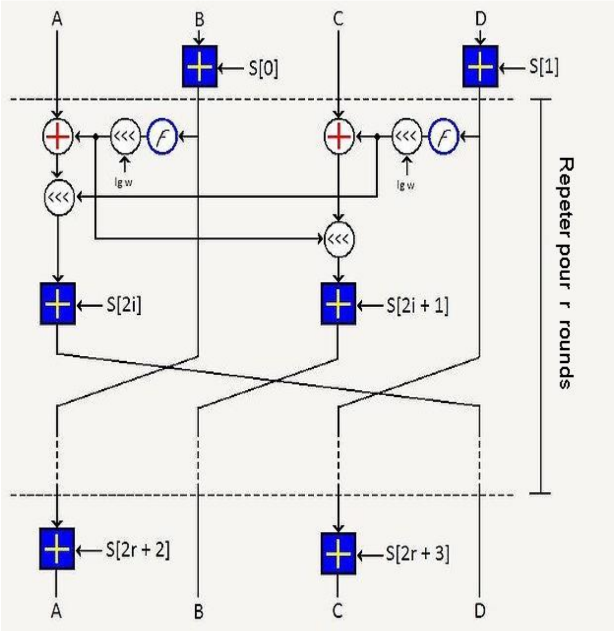
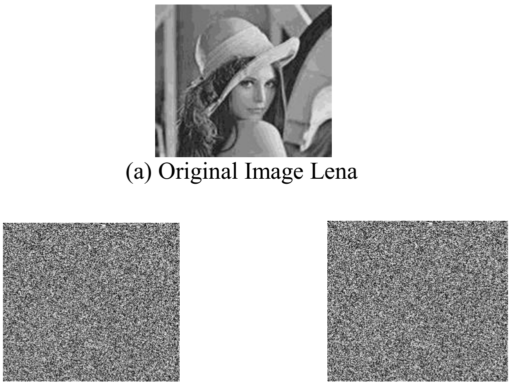


Figure 2. RC6 block cipher.

3. APPLICATION ON DIGITAL IMAGES

In this section, we will analyze and test RC5 end RC6 on digital images. The safety estimates of these two algorithms against brute force, statistics and differential attacks are explored. Using Matlab, we applied RC5 and RC6 block Ciphers on the digital image "Lena" using an arbitrarily chosen key K = 78 33 48 E7 5A EB 0F 2F D7 69 B1 BB8D 67 87 C1 and the following parameters considered as optimal values [6]:
For RC5: r = 16 rounds, b = 16 bytes, w =32 bits.
For RC6: r = 20 rounds, b = 16 bytes, w = 32 bits.
The results of encryption and decryption are shown in Figure 3:



(a) Original Image Lena

(b) Image Encrypted with RC5

(c) Image encrypted with RC6

Figure 3. Application of RC5 and RC6 block cipher On digital image Lena.

A simple visual inspection of the results above shows the effectiveness of hiding the information contained in each image and thus the possibility of applying RC5 and RC6 on digital images successfully.

3.1 Security analysis

A good encryption algorithm should have a strong resilience against attacks that attempt to break the system such as brute force attacks, static and differential attacks that we are going to discuss later. Resistance against attacks is a good measure of the performance of a cryptography system, so it is often used to evaluate these systems. In this section we make some safety tests such as analysis of the space key, static analysis and differential analysis.

3.*1.1 Key Space Analysis*

A good block cipher must be sensitive to key stream: key space should be big enough to inhabit brut attack.

a) Exhaustive key research

The objective is testing the relation between the key and the encrypted information. As it's known, RC5 and RC6 are 128 bits cryptographic algorithms. So, an attempt of research of the key must take 2^k operations to success with "k" is the key size in bits. Besides, those attacks need an acknowledgement of some pairs of the original image and the encrypted one. So a hacker must guess all the possibility of the key and do almost 2^{128}=3.4028×10^{38} operations to find the key, which is actually hard to do [6].

To do that test we first encrypted the original image Lena with 16 bytes key (K= 78 33 48 E7 5A EB 0F 2F D7 B1 69 BB 8D C1 67 87), then, we changed the last bit of the key and we encrypt the image again with the new key K' (K'= 78 33 48 E7 5A EB 0F 2F D7 B1 69 BB 8D C1 67 86). We calculated the difference of gray levels between the two images for each algorithm. The results of this comparison are illustrated in Figure 4.

Table 1. Comparison between RC5 and RC6 Block ciphers 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	156
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	+, -, ⊕, <<<, >>>	+, -, *, ⊕, <<<, >>>

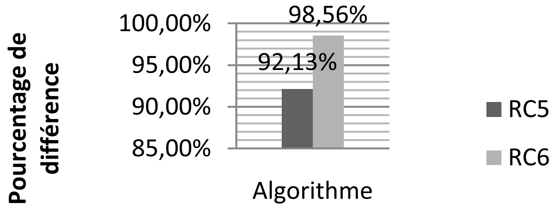


Figure 4. Comparison of the key sensitivity test results of RC5 and RC6.

As shows the illustration, the two algorithms present a large percentage of difference between the image encrypted by the key K and the key K' although one only bit of the key has been changed. The biggest difference value is when using the RC6 algorithm (98.56%).

3.1.2 Statistical Analysis

Static analysis was performed on RC5 and RC6 while demonstrating the superiority of its confusion and diffusion properties that provide high resistance to statistics attack. This analysis is shown by testing the histograms of encrypted image and the correlation between its adjacent pixels.

a) Images Histogram

We calculated the histograms of the image "Lena" before and after each encryption algorithm. In Order to calculate the histogram and analyze the amount of gray levels contained in the image, which means analyzing the transformation of information during encryption.
The histograms are shown in Figures 5, 6 and 7.

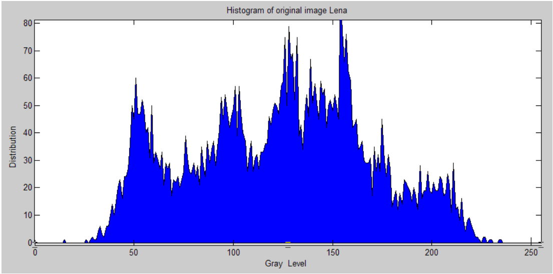


Figure 5. Histogram of the original image

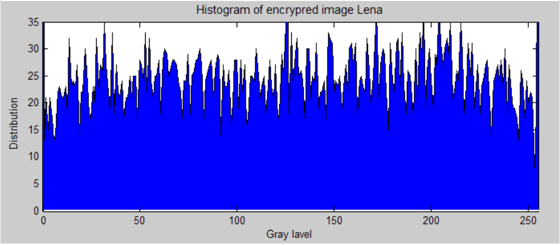


Figure 6. Histogram of the image encrypted with RC5

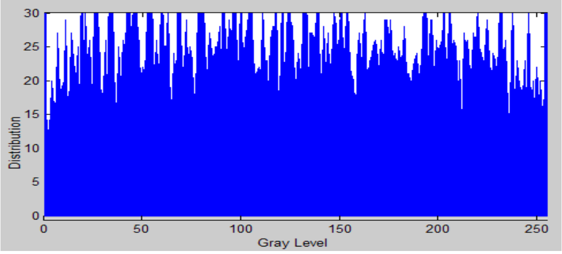


Figure 7. Histogram of the image encrypted with RC6

After application of RC5 and RC6, the values of gray levels of information become too close, especially for RC6. The information undergoes a highly ambiguity.

b) Correlation of adjacent pixels

When encrypting, the information is completely changed. To test the link between it, we chose to do experiments on the same image "Lena" as follows [7]: After application of each algorithm, we randomly selected 1000 pairs of adjacent pixels in the image encrypted and calculate the correlation coefficient between them while taking into account the horizontal, vertical and diagonal adjacency using the following formulas:

$$\mathrm{cov}(x,y) = E(x - E(x))(y - E(y)) \quad (1)$$

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \quad (2)$$

With:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i). \quad (3)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (4)$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \qquad (5)$$

Table 2. Coefficients of correlation of adjacent pixels

Direction of adjacent pixels	**Horizontal**	**Vertical**	**Diagonal**
Original Image	**0.8631**	**0.9364**	**0.8048**
Image Encrypted with RC5	0.0055	0.0082	0.0098
Image Encrypted with RC6	-0.0120	-0.0098	0.0032

From the table 2, the values of correlations found in the three senses, after application of RC5 and RC6 block cipher, are very low. This shows the non-association between the information contained in each image after encryption. RC5 values are more important than RC6 which means adjacent pixels of RC6 encrypted image are more decorrelated.

We take for example the case of horizontal adjacency: the correlation between pixels of the original image is illustrated in Figure 8, while the result of distribution of the correlation in the encrypted image is illustrated in Figures 9 and 10 for respectively RC5 and RC6 algorithms.

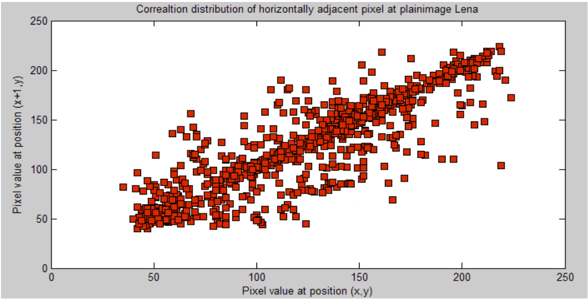


Figure 8. Correlation between adjacent pixels in the original image

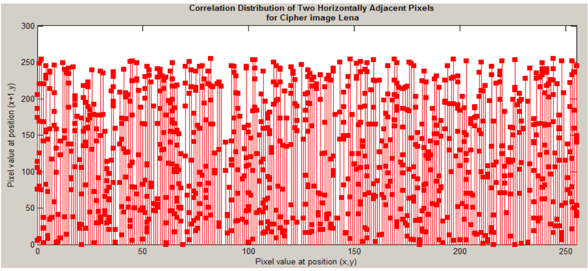


Figure 9. Correlation between adjacent pixels in the RC5 ciphered image

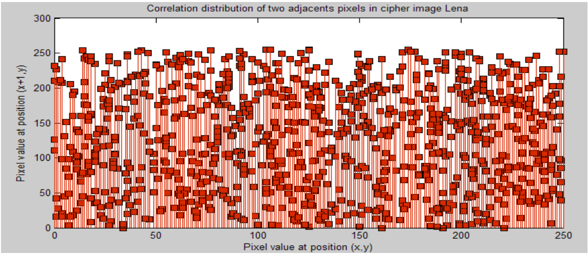
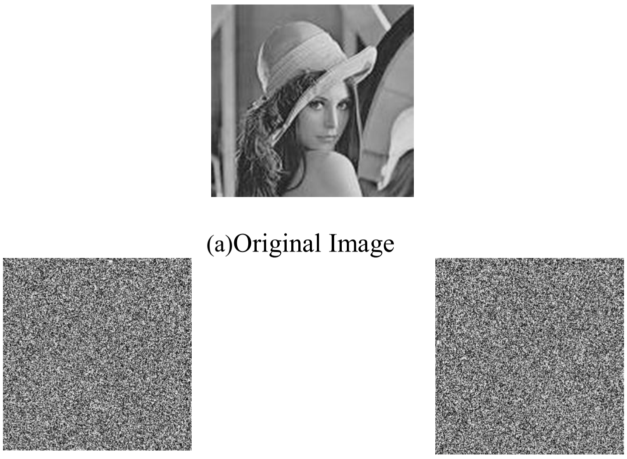


Figure 10. Correlation between adjacent pixels in the RC6 ciphered image

Figure 8 shows the linearity of the information contained in the original image, while figures 9 and 10 present result contradictory to the original one. The nonlinearity of the information contained encrypted, and therefore it is difficult for a striker is a relationship between this information.

3.1.3 Differential analysis

In general, for an attacker to recognize the key, it tries a little change on the encrypted image as a single pixel change and observes the result of this change [8]. So he can discover a wonderful relationship between the encrypted information and the unencrypted. If a minor change on the initial information may cause a big change on the encrypted information, observing the diffusion and confusion, so the differential attacks will be ineffective and unnecessary [9]. Then, to test the effect of changing a single pixel in an image encrypted by RC5 and RC6 two metrics of measurement can be used: the exchange rate of the number of pixels (Number of Pixels Exchange Rate) "NPCR "Average and unified changing intensity (Unified Average Changing Intensity)" UACI ".

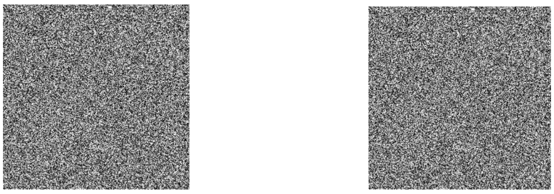


(a)Original Image

(b) Image C1 for RC5

(c) Image C2 for RC5

Figure 11. Result after application of differential analysis RC5



(d) Image C1 for RC6 (e) Image C2 for RC6

Figure 12. Result after application of differential analysis RC6

The experiments were made on image "Lena" encrypted with both algorithms, so that each time his original differs from a single pixel: that is to say that we changed the first pixel " Lena value 15, then we have encrypted by RC5 and we repeated the same procedure with RC6, we obtain an encrypted image C2 other than that before modification of the first pixel (see figures 11 and 12).

We denote by C1 (i, j) and C2 (i, j) the value of gray level of pixel (i, j) in the obtained images. We define a D-dimensional array of the same size as C1 and C2. D is determined by using the following expressions [3]:

$$D(i,j)=\begin{cases} 1 & si\ \ C1(i,j) = C2(i,j) \\ 0 & si\ \ C1(i,j) \neq C2(i,j) \end{cases} \qquad (6)$$

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

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C1(i,j) - C2(i,j)}{255}\right] \times 100\% \qquad (8)$$

W and H are the width and the height of C1 and C2.

NPCR measures the percentage difference in number of pixels of both images and UACI measures the average difference in intensity between two images. Test results are shown in Table 3.

Table 3. Values of NPCR and UACI

Algorithm	**RC5**	**RC6**
NPCR	0.049 %	0.058 %
UACI	0.29 %	0.64 %

The average difference in intensity between two images is greater for UACI RC6 as well as the percentage difference in number of pixel NPCR, although the results are close.

3.2 Image quality

When we study security algorithms we always think about security as the main issue of the good choice of the encryption algorithm. However, in rough and energy constrained environments like wireless sensor networks (WSN) we should pay attention to transmission errors. A classic error control scheme overcomes errors by retransmitting packets and leads to a waste of energy. If few errors occurred, few packets are retransmitted. In this section we compare the robustness against errors of conventional encryption algorithms like RC5 and RC6.

Encrypted images are modulated by a digital binary modulation (BPSK) and then transmitted via AWGN channel with snr =5dB as shows Figure 13.

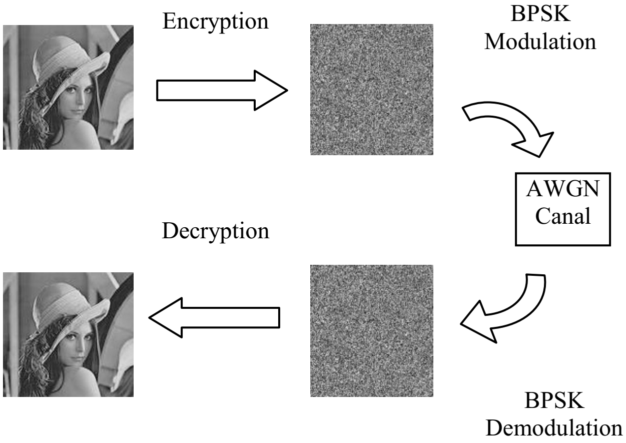


Figure13. Noise application when encrypting RC5 and RC6

We use the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) to compare the difference between the transmitted and the received image. MSE and PSNR are given by the following formulas:

$$MSE = \frac{1}{M * N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[P_S(x,y) - P_r(x,y)]^2 \qquad (9)$$

$$P_{SNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (10)$$

With: PS (x, y): the pixel value at the position (x, y) in the original image.

Pr (x, y): the pixel value at the position (x, y) in the received image.

M and N are the dimensions of the image.

Table 3 shows the numbers of errors occurred and bit error rate (BER) besides MSE and PSNR. We notice that RC5 have the fewer number of errors (650) and the lowest BER. MSE and PSNR values confirm this result, RC5 has the higher PSNR value so the lowest MSE. This would not have an effect only if we use a wireless sensor network or wireless personal area network to transmit images or signals from the studied field. So increasing security level by using RC6 algorithm may lead to a waste of energy. This consumption is caused by the added complexity and the vulnerability against noisy environment.

4. CONCLUSION

In this paper we studied the efficiency of two known block cipher algorithms RC5 and RC6 to encrypt images. The choice of these two algorithms is related to the simplicity of operations and functions and the suitability to be applied on digital image encryption.

We gathered the possible metrics to investigate and compare their efficiency to encrypt digital images. First, with the key space analysis we demonstrate that RC6 gives the largest difference between two encrypted images (98.56%) with slightly modified keys (1 bit).

The study of adjacent pixels correlation don't denied the previous conclusion, and RC5 encrypted image has the highly correlated adjacent pixels. Secondly, we used the exchange rate number of pixels (NPCR) and the unified changing intensity (UACI) to examine the vulnerability against differential attacks.

The average difference in intensity between two images is greater for RC6 UACI, as well as the percentage difference in number of pixel NPCR. In the last part, another metric is studied to have an idea about the sensitivity of the two encryption algorithms to noisy environment. We encrypted the images and sent it via an AWGN with a low SNR, and we measured the BER, PSNR and MSE. The use of a secure algorithm more sensitive to noise (which is the case of RC6) leads to retransmit defective packets with classic error control scheme.

In rough and energy constrained environments like wireless sensor networks (WSN), we should pay attention to transmission errors and so retransmission of packets.

This work is a preliminary study of our security algorithm implementation on real sensor network in order to transmit encrypted images.

5. REFERENCES

[1] Jacques Stern, La cryptologie: enjeux et perspective, Laboratoire d'informatique de l'ENS, CNRS/ENS, PariSTIC Nancy, 24 novembre 2006

[2] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "*Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems*", International Journal of Information Technology Volume 3 Number 2007

[3] 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 2007

[4] Ronald L. Rivest, The RC5 Encryption Algorithm, MIT Laboratory for Computer Science 545 Technology Square, Cambridge, Mass.02139 (Revised March 20, 1997)

[5] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, The RC6 TM Block Cipher , M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, Version 1.1 - August 20, 1998

[6] Krishnamurthy G N and Dr. V Ramaswamy Department , Performance Analysis of Blowfish and its Modified Version using Encryption quality, Key sensitivity, Histogram and Correlation coefficient analysis of Information , Science & Engineering, Bapuji Institute of Engineering & Technology, Davangere, Karnataka, India. International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[7] Helena Handschuh, « Cryptanalyse et Sécurité des Algorithmes à Clé Secrète », Thèse de doctorat, Ecole Nationale Supérieure des Télécommunications, Paris,France 24 Septembre 1999

[8] Ismail Amr Ismail, Mohammed Amin and Hossam Diab , A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps , Faculty of Computers and Informatics, Zagazig University, Egypt (Received Oct. 29, 2006; revised and accepted June 15, 2007 & May 14, 2008)

[9] Krishnamurthy G N, Dr. V Ramaswamy, Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images, International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009