# Encryption Quality Analysis of the RCBC Block Cipher Compared with RC6 and RC5 Algorithms

**Abdul Hamid M. Ragab, Osama S. Farag Alla, Amin Y. Noaman**
Ahm_ragab@yahoo.com, osam_sal@yahoo.com, anoaman@kau.edu.sa.

***Abstract- in this paper, we investigate the encryption quality of the robust chaotic block cipher (RCBC) algorithm; which is based on chaotic map. In addition to visual inspection of images encryption testing, five analytical metrics are developed for analyzing the encryption quality. These metrics are used to evaluate several encrypted images factors include: maximum deviation, irregular deviation, information entropy, correlation coefficients, and avalanche effect. Comparison of the encryption quality for RCBC, RC6 and RC5 implantations to digital images are performed. In the experimental results, we have made our tests using color images Lena, Cman, and Peppers, each of size 512x512 pixels, as the original images (plain-images). Results show better quality of the RCBC.***

***Key Words: Block ciphers encryption, Encryption evaluation metrics, and Images encryption quality.***

## 1 INTRODUCTION

Encryption has been used for achieving security of data in many applications in different fields, among which are telecommunication, storage of text, and multimedia data including images, audio and video [1, 2]. Many types of block cipher algorithms have been used for encryption of digital images, among these are RC5 [3], RC6 [4], and Rijndael [5]. Recently, however many new block ciphers have been proposed using chaotic maps [6, 7], since they achieve better security and performance.

In this paper, we evaluate the encryption quality of the robust chaotic block cipher presented in [8,26,27]. With the application of an encryption algorithm to an image, its pixels values change when compared with the original image. A good encryption algorithm must make these changes in an irregular manner and also maximize the difference in pixels values between the original and the encrypted images. One of the important metrics in examining an encrypted image is the visual inspection [9, 10], where the more the hidden features of the image are, the better the encryption algorithm. However, depending on the visual inspection only is not enough in judging the complete hiding of the contents of the image. So, other evaluation metrics are considered to evaluate the degree of encryption, quantitatively Diffusion [11-14] is an important parameter that must be measured to judge the encryption algorithm randomization. If an algorithm has a good diffusion characteristic, the relation between the encrypted image and the original image is too complex and it cannot be predicted, easily. To measure the diffusion of any algorithm, a bit is changed in the plain image, and the difference between the encrypted image obtained from the original plain image and the encrypted image obtained from the modified one is obtained.

In this paper, we study, in detail, two families of encryption metrics; the first family evaluates the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image. In this family, three metrics, which are the histogram deviation in section (5.1), the correlation coefficient in section (5.3) and the irregular deviation in section (5.4) are studied. The second family evaluates the diffusion characteristics of the encryption algorithm. In this family, three metrics, which are the Avalanche effect in section (5.5), NPCR and UACI in section (5.6), are studied. We apply these metrics for evaluating the encryption quality of RCBC, RC6 and RC6 block ciphers algorithms in next sections.

## 2 RELATED WORKS

Most previous studies on image encryption were based on the visual inspection to judge the effectiveness of the encryption technique used in hiding features. This visual inspection is insufficient in evaluating the amount of information hidden [15]. So, we use mathematical measure to evaluate the degree of encryption quantity. Image encryption quality has been studied in several articles [17-20]. In [16], an image encryption scheme was proposed based on combination of pixel shuffling and new modified version of simplified AES, where Chaos is used to expand diffusion and confusion in the image. They tested encryption quality using visual test and histogram analysis. In [18], Different types of bitmap images encryption quality was estimated for RC6, MRC6, and Rijndael block cipher algorithms. They used both visual inspection and analytical measurements, like entropy and correlation for analyzing encryption quality. The work in [19] compared the generated results of the algorithms AES, RC6 and BFS on the basis of two parameters entropy and correlation.
In our work in this paper, we compare the encryption quality between the three well known block ciphers: RCBC, RC6 and RC5.

### 2.1 Image Encryption and Decryption

There are two inputs to the encryption function, which are the plain-image to be encrypted and the expanded secret key. For RCBC image encryption, all parts of the file header are determined so as to know the start of the image pixels data array and the image header is excluded on which the encryption is performed [21-23].
The image data bit stream (not including the image header) is divided into blocks of 256-bit length. The first 256-bit block of image is entered as the plain-image to the encryption function of RCBC. The second input to the RCBC encryption algorithm is the expanded secret key that is derived from the user-supplied secret key by means of the key schedule. The key schedule is an important component of a block cipher; since it computes the round keys from the user-supplied secret key. Then, the next 256-bit plain-image block follows it, and so on as shown in Fig. 1. In the decryption process, the encrypted image (or cipher-image) is also divided into 256-bit blocks. The 256-bit cipher-image is entered to RCBC decryption algorithm and the same expanded secret key is used to decrypt the cipher-image but the expanded secret key is applied in a reverse manner. Then the next 256-bit cipher-image block follows it, and so on with the same scan path.

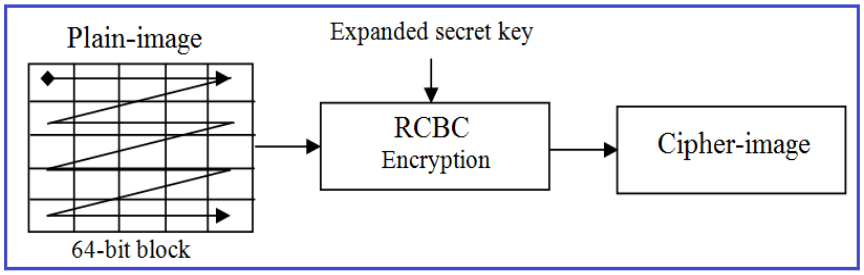


***Fig. 1: RCBC image encryption process.***

### 2.2 Block Ciphers Design Parameters

Since, the block ciphers RCBC, RC6 and RC5 are a fully parameterized family of encryption algorithms. An RC6 block cipher, for example can be specified more accurately as RC6-w/r/b. So, there are several different choices for the values of block cipher 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. Table 1 shows a comparison of the RCBC design parameters with RC5, and RC6 block ciphers [3, 4]. It seen from Table 1 that RCBC uses more cryptographic parameter (logistic maps). Hence it can be more robust than both RC5 and RC6. Its security analysis was student in [8], and its encryption quality evaluation detained analysis is explained in next sections.

Table 1 Comparison of the RCBC design parameters with RC5, and RC6.

| Parameter | RC5 | RC6 | RCBC |
|---|---|---|---|
| w : word size in bits | 16, 32, 64 | 16, 32, 64 | 16, 32, 64 |
| b: block size in bits | 32,64,128 | 64,128,256 | 128,256,512 |
| r : No. of rounds | 0, 1, 2.., 255 | 0, 1, 2.., 255 | 0, 1, 2.., 255 |
| Key length in bytes | 0, 1, 2.., 255 | 0, 1, 2.., 255 | 0, 1, 2.., 255 |
| Block size in words | 2w | 4w | 8w |
| Max. block size in bits | 128 | 256 | 512 |
| No. of keys derived from key schedule | 2r + 2 | 2r + 4 | 4r + 8 |
| Transformation Function | not exist | $x(2x+1) \bmod 2^w$ | F1(W,X,Y,Z) F2(W,X,Y,Z) |
| Logistic map | not exist | not exist | exist |

## 3 ENCRYPTION QUALITY EVALUATION OF RCBC ALGORITHM TO DIGITAL IMAGES

The visual inspection is one of the most important factors in examining the encrypted image where the highly disappeared features of the image, the better the encryption algorithm. But depending on the visual inspection only is not enough in judging the efficiency of complete hiding of the content of the data image. So, other evaluation metrics are considered to estimate the degree of encryption quantitatively.

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 expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one. In addition to the visual inspection, five encryption evaluation metrics are used to evaluate and compare encryption quality of the RCBC implantation to digital images. In our experimental results, we have made our tests using color images Lena, Cman, and Peppers, each of size 512x512 pixels, as the original images (plainimages) and apply the RCBC block cipher algorithm with the parameters w = 32, r=16 round and b=16.

## 4 VISUAL TESTING OF THE RCBC TO DIGITAL IMAGES

We have conducted some experiments to test check the encryption quality of the RCBC for application to digital images. As stated previously, we must firstly extract the image header for the image to be encrypted/decrypted before applying the RCBC. Then, we can apply the RCBC algorithm to the image.

We have made our tests using color images Lena and Peppers, each of size 512x512 pixels, as the original images (plainimages) and apply RCBC algorithm. Figs. 2 and 3 show the result of applying the RCBC to Lena and Peppers images in both encryption and decryption. Based on the results shown in Figs. 2 and 3, there is no visual information observed in the encrypted image, and the encrypted images are visual indistinguishable even with a big difference with respect to the original images. So, the visual inspection of Figs. 2 and 3 show the possibility of applying RCBC algorithm successfully to digital images.

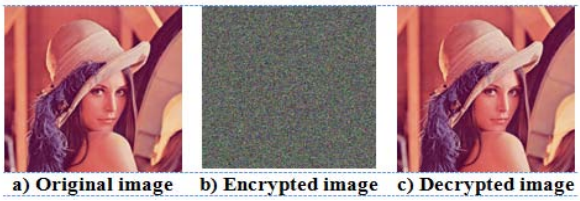


Fig. 2: Application of the RCBC to Lena image

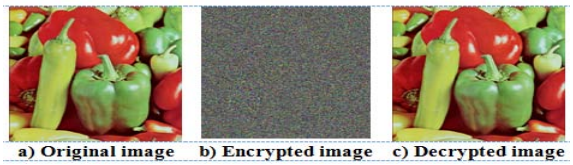


Fig. 3: Application of the RCBC Peppers image

## 5 THE ENCRYPTION EVALUATION METRICS

### 5.1 Histogram

The histogram of the cipherimage is plotted to see whether it is sufficiently uniform. A good image encryption scheme should always generate a cipherimage of uniform histogram for any plainimages. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig. 4.

The original-image with the size 256x256 is shown in Fig.4 (a) and the histogram of the original-image is shown in Fig.4 (b). Fig.4 (c) is the encrypted image and Fig.4 (d) is the histogram of the encrypted image.
It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

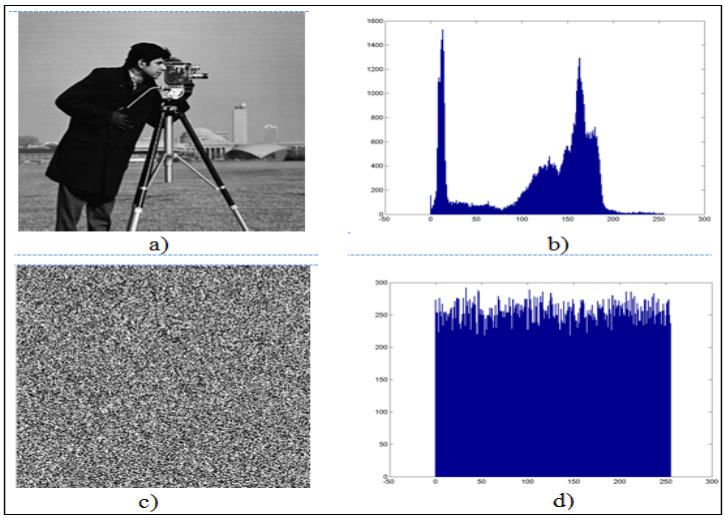


Fig.4. The original-image , the encrypted image , and the histogram for each one:

(a) The original-image; (b) the histogram of the original-image;
(c) The encrypted image; (d) the histogram of the encrypted image.

### *5.2* The Maximum Deviation

This measurement technique measures the quality of encryption based on the deviation between the plaintext and ciphertext. The more the ciphertext is deviated from the plaintext, the better is the encryption algorithm. It measures the encryption quality in terms of how it maximizes the deviation between the original and the encrypted images [10]. The steps of this measure are done as follows:

1. Count the number of pixels of each grayscale value in the range from 0 to 255 and present the results graphically (in the form of curves) for both original and encrypted images (i.e.; get their histogram distributions).
2. Compute the absolute difference or deviation between the two curves and present it graphically.
3. Count the area under the absolute difference curve, which is the sum of deviations (D) and this represents the encryption quality. D is given by the following equation:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad 1$$

Where $h_i$ is the amplitude of the absolute difference curve at value i. Of course, the higher the value of D, the more the encrypted image is deviated from the original image [10]. With the measure of D the greater is the better to obtain high encryption quality.

Table 2: Encryption quality Comparison of the RCBC, RC5, and RC6 for Lena, Cman and Barbra images using maximum deviation

| Image name | Cipher name | | |
|---|---|---|---|
| | RCBC | RC5 | RC6 |
| Lena | 15694 | 15428 | 15523 |
| Cman | 14817 | 14565.5 | 14729 |
| Barbra | 17324 | 17010 | 17263 |

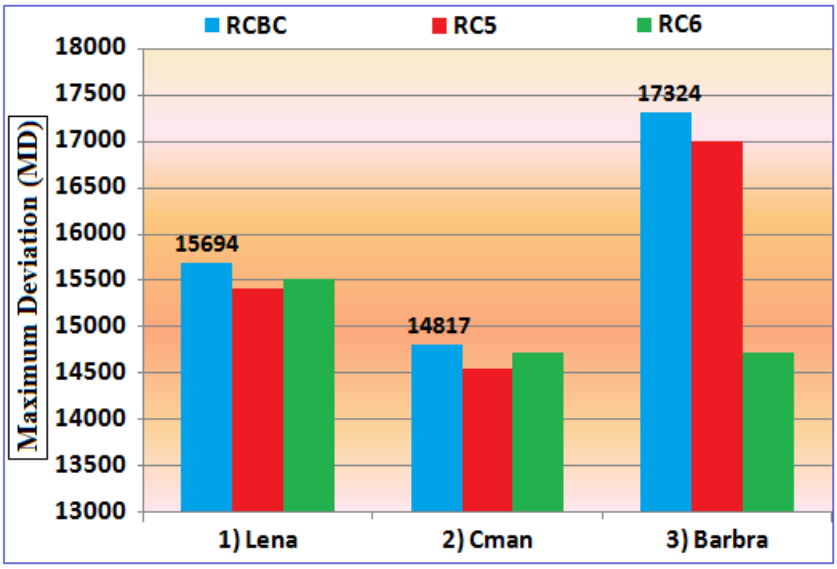


Fig. 5: Encryption quality Comparison of the RCBC, RC5, and RC6 for Lena, Cman and Barbra images using maximum deviation (MD).

The encryption quality for the RCBC, RC5 and RC6 is estimated using maximum deviation with Lena, Cman, and Barbra images as shown in Table-2 and Fig.5. From these results, we can conclude that the RCBC block cipher algorithm gives better encryption quality compared with RC5 and RC6, since its MD is the maximum.

### 5.3 The Correlation Coefficient

Correlation is a measure of the relationship between two variables. If the two variables are the plainimage and cipherimage, then they are in perfect correlation if they are highly dependent. In this case the cipherimage is the same as the plainimage and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the plainimage and its cipherimage are totally different. If the correlation coefficient equals -1, this means the cipherimage is the negative of the plainimage. So, success of the encryption process means smaller values of the correlation coefficient. The correlation coefficient is measured by the following equation [11-13]:

$$\text{The Correlation Coefficient} = \frac{\text{cov}(x, y)}{\sigma_x \sigma_y} \qquad 2$$

$$= \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^{N} x_i - E(x))^2)}\sqrt{(\sum_{i=1}^{N} y_i - E(y))^2)}}$$

Where ( $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ ) and x and y are gray-scale pixel values of the plainimage and cipherimage.

The procedure to test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in plainimage/cipherimage is as follows. First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient. The encryption quality for the RCBC-32/16/16 block cipher algorithm is estimated using the correlation coefficient of two horizontally, two vertically and two diagonally adjacent pixels in the plainimage/cipherimage with Lena, Cman, and Barbra images as shown in Table 3.

Table 3: Encryption quality Comparison of the RCBC, RC5 and RC6 for Lena, Cman and Barbra images using correlation coefficients

| Image name | Direction of Adjacent pixels | Plainimage | Cipher name | | |
|---|---|---|---|---|---|
| | | | RCBC | RC5 | RC6 |
| Lana | Horizontal | 0.9915 | 0.0035 | 0.0041 | 0.0038 |
| | Vertical | 0.9836 | 0.0029 | 0.0034 | 0.0032 |
| | Diagonal | 0.9698 | 0.0025 | 0.0028 | 0.0027 |
| Cman | Horizontal | 0.9812 | 0.0077 | 0.0084 | 0.0081 |
| | Vertical | 0.9797 | 0.0069 | 0.0084 | 0.0072 |
| | Diagonal | 0.9794 | 0.0036 | 0.0043 | 0.0038 |
| Barbra | Horizontal | 0.9946 | 0.0059 | 0.0063 | 0.0061 |
| | Vertical | 0.9888 | 0.0078 | 0.0084 | 0.0081 |
| | Diagonal | 0.9791 | 0.0053 | 0.0059 | 0.0056 |

From the obtained results, we can conclude that the RCBC algorithm obtained minimum correlation coefficient and maximum encryption quality and with respect to RC5 and RC6.

### 5.4 The Irregular Deviation Measuring Factor

This quality measuring factor is based on how much the deviation caused by encryption on the cipherimage is irregular [14]. It gives an attention to each individual pixel value and the deviation caused at every location of the plainimage before getting the histogram as described in [10] which does not preserve any information about the location of the pixels. This method can be summarized in the following steps:

1. Calculate the 'D' matrix which represents the absolute values of the difference between each pixel values before and after encryption. So, D can be represented as:
   D =| I - J | 3
   Where I is the input image, and J is the encrypted image.
2. Construct the histogram distribution 'H' of the absolute deviation between the input image and the encrypted image. So, H = histogram (D).

3. Get the average value of how many pixels are deviated at every deviation value (i.e., the number of pixels at the histogram if the statistical distribution of the deviation matrix is a uniform distribution).This average (DC) value can be calculated as:

$$DC = \frac{1}{256}\sum_{i=0}^{255} h_i \qquad 4$$

Where hi is the amplitude of the absolute difference histogram at the value i.

4. Subtract this average from the deviation histogram, and then take the absolute value of the result.

$$AC(i) = \left| H(i) - DC \right| \qquad 5$$

5. Count the area under the absolute AC value curve, which is the sum of variations of the deviation histogram from the uniformly distributed histogram.

$$ID = \sum_{i=0}^{255} AC(i) \qquad 6$$

The lower the ID value, the better the encryption algorithm [14].

The encryption quality for the RCBC, RC5 and RC6 is estimated using the irregular deviation with Lena, Cman, and Barbra images as shown in Table 4, and Fig.6. From the obtained results, we can conclude that the RCBC obtained minimum irregular deviation and so maximum encryption quality with respect to RC5 and RC6.

Table 4: Encryption Quality Evaluation of the RCBC, RC5, and RC6 for Lena, Cman and Barbra images using the irregular deviation

| Image name | Cipher name | | |
|---|---|---|---|
| | RCBC | RC5 | RC6 |
| Lena | 17855 | 18024 | 17996 |
| Cman | 27135 | 27986 | 27564 |
| Barbra | 31180 | 32145 | 31523 |

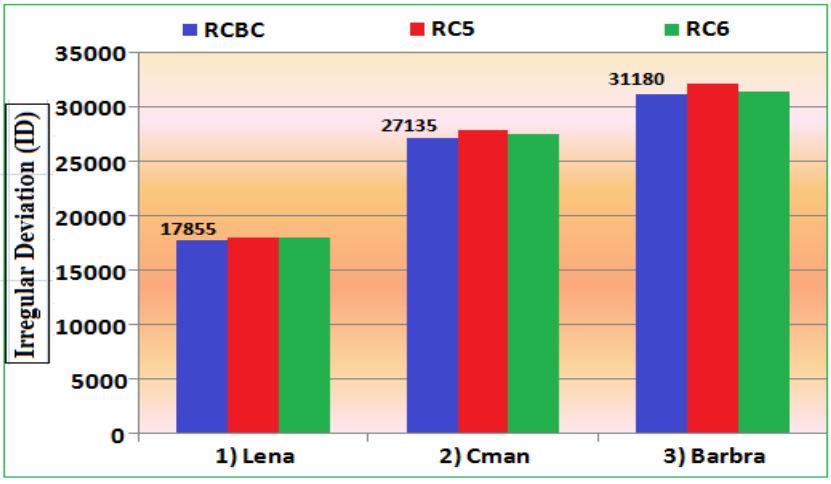


Fig.6: Encryption Quality Evaluation of the RCBC, RC5, and RC6 for Lena, Cman and Barbra images using the irregular deviation (ID).

### 5.5 The avalanche effect Measuring Factor

Diffusion is an important parameter that must be measured to judge the encryption algorithm randomization. A desirable property for the RCBC block cipher algorithm is that it is highly sensitive to small change in the plainimage (single bit change in plainimage) [15-16]. In general, the opponent may make a slight change such as modifying only one pixel of the original image, and then observes the change of the result. In this way, we may find out a meaningful relationship between the plainimage and the cipherimage. As one minor change in the plainimage can cause a significant change in the cipherimage, this differential attack would become very inefficient and practically useless.

If an algorithm has a good diffusion characteristic, the relation between the encrypted image and the original image is too complex and it cannot be predicted, easily. To measure the diffusion of any algorithm, a bit is changed in the plainimage, and the difference between the encrypted image obtained from the original plainimage and the encrypted image obtained from the modified one is obtained [17].

To test the influence of one-pixel change on the whole image, encrypted by the RCBC algorithm, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [12]. 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 respectively the width and height of C1 or C2. 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. The higher the values of NPCR and UACI, the better diffused the encryption. One performed test is on the one-pixel change influence on Lena, Cman and Barbra images of size 512×512. The test results are shown in Table 5.

999

Table 5: Encryption quality evaluation of the RCBC, RC5 and RC6 for Lena, Cman and Barbra images using NPCR and UACI estimations

| Image name | Cipher name | | | | | |
|---|---|---|---|---|---|---|
| | RCBC | | RC5 | | RC6 | |
| | NPCR | UACI | NPCR | UACI | NPCR | UACI |
| Lena | 78.4% | 31.2% | 52.4% | 28.6% | 62.3% | 25.6% |

| | | | | | | |
|---|---|---|---|---|---|---|
| Cman | 80.5% | 31.8% | 57.6% | 29.1% | 63.5% | 26.4% |
| Barbra | 83.3% | 30.7% | 55.7% | 27.8% | 61.4% | 25.7% |

With respect to NPCR and UACI estimations, the experimental results in Table 5 and Fig.7 show that with the RCBC, RC5 and RC6 modes of operation, the effect of one-pixel change has great influence especially in RCBC and results in good diffusion.

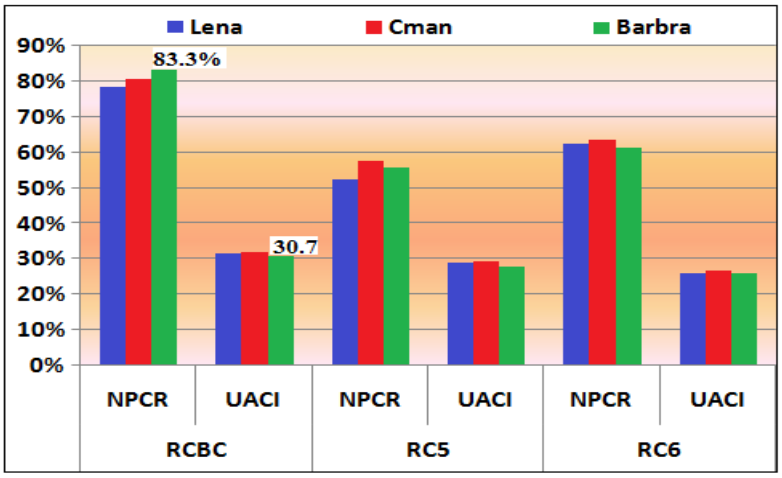


Fig.7: Encryption quality evaluation of the RCBC, RC5 and RC6 for Lena, Cman and Barbra images using NPCR and UACI estimations.

### 5.6 Information Entropy Analysis

Information theory is the mathematical theory of data communication and storage founded by Shannon [24]. To calculate the entropy $H(m)$ of a source $m$, we have:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad bits, \qquad 9$$

Where $p(m_i)$ represents the probability of symbol $m_i$ and the entropy is expressed in bits. Suppose that the source emits $2^8$ symbols with equal probability, i.e., $m = \{m_1, m_2, ..., m_{2^8}\}$. After evaluating Eq. 9, we obtain its entropy $H(m) = 8$, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Let us consider the ciphertext of image encryption using the RCBC, the number of occurrence of each ciphertext block is recorded and the probability of occurrence is computed. The information entropy obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against entropy attack. The cipherimage entropy for various values of $m$ is calculated using Eq. 9 and is listed in Table 6.

Table 6: Encryption quality evaluation of the RCBC-32/16/16 for Lena, Cman and Barbra images using information Entropy estimation

| Image name | The value of source $m$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2 | 4 | 8 | 16 | 32 | 64 | 256 |
| | Ideal value for entropy $H(m)$ | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| Lena | 0.749 | 1.413 | 2.679 | 3.820 | 4.893 | 5.913 | 7.926 |
| Cman | 0.908 | 1.952 | 2.968 | 3.883 | 4.938 | 5.964 | 7.969 |
| Barbra | 0.999 | 1.998 | 2.995 | 3.997 | 4.997 | 5.996 | 7.998 |

## 6 Conclusions

In this paper the quality of the encrypted images were tested with visual inspection and evaluated with different quality measures. In addition to this visual inspection tests, we present five encryption evaluation metrics for evaluating and comparing encryption quality of the symmetrical cryptography block ciphers included the robust chaotic block cipher (RCBC), RC6 and RC5 implantations to digital images. These metrics included: maximum deviation, irregular deviation, information entropy, correlation coefficients, and avalanche effect. The experimental results, made tests used color images Lena, Cman, and Peppers, each of size 512x512 pixels, as the original images (plainimages). Results proved that the RCBC achieved better encryption quality than both RC6 and RC5.

## References


[1] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater," Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Hindawi Publishing Corporation, EURASIP Journal on Information Security, Volume 2008.

[2] Rengarajan Amirtharajan, P. Archana and J.B.B. Rayappan," Why Image Encryption for Better Steganography", Research Journal of Information Technology, Volume: 5, Issue: 3,pp 341-351,2013.

[3] Ahmed, H.H., Kalash, H.M., & O.S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images", Journal of Optical Engineering, 2006.

[4] 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 and Information Engineering, 2007.

[5] Nawal El-Fishawy and Osama M. Abu Zaid," Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.
[6] Alireza Jolfaei, Abdolrasoul Mirghadri, "Image Encryption Using Chaos and Block Cipher" www.ccsenet.org/cis Computer and Information Science Vol. 4, No. 1; January 2011
[7] Bhavana Agrawal, Himani Agrawal, Monisha Mishra," Implementation of Various Cryptosystem Using Chaos", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 13, Issue 4, PP 77-84, Jul.-Aug. 2013.
[8] Abdul Hamid M. Ragab, Osama S. Farag Allah, Khalid W. Magld and Amin Y. Noaman," Security Evaluation of Robust Chaotic Block Cipher", International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-6, January 05, 2014.
[9] Ashwaq T. Hashim* & Baedaa H. Helal," Measurement of Encryption Quality of Bitmap Images with RC6, and two modified version Block Cipher", Eng. & Tech. Journal, Vol.28, No.17, 2010.
[10] Kevin Curran, Karen Bailey," An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Volume 2, Issue 2, 2003.
[11] Xuehu Yan, et al," A New Assessment Measure of Shadow Image Quality Based on Error Diffusion Techniques", Journal of Information Hiding and Multimedia Signal Processing, Volume 4, Number 2, April 2013.
[12] Jolfaei, A. & Mirghadri, A," A New Approach to Measure Quality of Image Encryption", *International* Journal of Computer and Network Security, 2(8), PP 38-44, 2010.
[13] G.A. Sathishkumar , K.Bhoopathy bagan. N.Sriraam," Image Encryption based on Diffusion and Multiple Chaotic Maps", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.
[14] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-we," A chaos-based digital image encryption scheme with an improved diffusion strategy", Optics Express, Vol. 20, No. 3 , Jan 2012.
[15] Rengarajan Amirtharajan, P. Archana and J.B.B. Rayappan," Why Image Encryption for Better Steganography", Research Journal of Information Technology, Volume: 5, Issue: 3,pp 341-351,2013.
[16]Alireza Jolfaei, Abdolrasoul Mirghadri," Image Encryption Using Chaos and Block Cipher", Computer and Information Science, Vol. 4, No. 1; January 2011.
[17] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater," Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Hindawi Publishing Corporation, EURASIP Journal on Information Security, Volume 2008.
[18] Nawal El-Fishawy and Osama M. Abu Zaid," Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.
[19] Umashankar Pandey, Manish Manoria, Jainendra Jain," A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation", *International Journal of Computer Applications, Volume 42– No.1, March 2012.*

[20 ] 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 and Information Engineering, 2007.
[21]Shiguo Lian, "A block cipher based on chaotic neural networks," Neurocomputing, doi:10.1016/j.neucom.2008.
[22] Shiguo Lian, "Efficient image or video encryption based on spatiotemporal chaos system," chaos, solitons and fractals, 2007.
[23] S. Behnia, A. Akhshani, A. Akhavan, H. Mahmodi, "Applications of tripled chaotic maps in cryptography," Chaos, Solutions and Fractals, 2007.
[24] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, No. 4, pp. 656-715, October 1949.
[25] Jawad Ahmad and Fawad Ahmed," Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04,2012.
[26] Abdul Hamid M. Ragab, Osama S. Farag Allah, Khalid W. Magld and Amin Y. Noaman," Security Evaluation of Robust Chaotic Block Cipher", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-6, January 05, 2014.
[27] Abdul Hamid M. Ragab, Osama S. Farag Allah, Amin Y. Noaman and Khalid W. Magld," Encryption Quality Evaluation of Robust Chaotic Block Cipher for Digital Imaging", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-6, January 30, 2014 .