Encryption Quality Evaluation of Robust Chaotic Block Cipher for Digital Imaging

Abdul Hamid M. Ragab, Osama S. Farag Allah, Amin Y. Noaman, Khalid W. Magld

***Abstract:** The visual inspection is an important factor in examining encrypted images, where the highly disappeared features of the image, the better the encryption algorithm used. However, depending on the visual inspection only is not enough in judging the quality of complete hiding of the content of the data image. In this paper, we estimate the degree of image encryption quality not only practically using visual inspection, but also quantitatively using quality evaluation metrics.*

The efficient robust chaotic block cipher (RCBC) encryption quality algorithm for digital imaging is investigated. Comparative analysis regarding encryption quality (EQ) of the RCBC with algorithms such as RC6, and RC5 is performed. Ciphers design parameters are analyzed for their optimal values, as function of different ciphers operation modes, including ECB, CBC, CFB, and OFB. Thorough experimental tests are carried out with detailed analysis demonstrating the better performance of the RCBC block cipher.

***Index Terms**: Symmetric block ciphers, images encryption quality, and encryption algorithms analysis.*

I. INTRODUCTION

The field of encryption is very important for realizing information security which plays an important issue in telecommunication, storage of text, and multimedia data including images, audio and video. In this regard, a variety of encryption schemes have been proposed to mask the multimedia data streams, such as DES (Data Encryption Standard) [1, 2] optical encryption [3, 4] IDEA (International Data Encryption Algorithm) [5, 6] and RSA [7]. However, these encryption schemes appear not to be ideal for such multimedia applications, due to some intrinsic features of multimedia such as bulk data capacity and high redundancy, which are troublesome for traditional encryption [8, 9]. Moreover these encryption schemes require extra operations on compressed multimedia data thereby demanding long computational time and high computing power. In real-time communications, due to their low encryption and decryption speeds, they may introduce significant latency [10, 11].

So that, the characteristics of the chaotic maps have attracted the attention of cryptographers since it has many fundamental properties such as ergodicity, sensitivity to initial condition and system parameter, and mixing property [12,13].

In this regard, this paper investigates the encryption quality that can be realized for digital images using the Robust Chaotic Block Cipher (RCBC) explained in details in [14], which is based on symmetric encryption. The encryption quality of the RCBC is investigated with respect to its design parameters including: word size, number of rounds, and secret key length and compared with RC5 and RC6 at the several ciphers operation modes (ECB, CBC, CFB, and OFB). The optimal choices for the best values of these parameters are taken into account for the best trade-off between encryption quality and computational efficiency. In section II, literature review, section II, encryption quality visual testing, section IV describes several ciphers operation modes, ciphers design parameters and their effects on encryption quality, section V is the conclusion.

II. LITERATURE REVIEW

Encryption has several applications, for examples, in Internet communication, multimedia systems, medical imaging, telemedicine, military communication, pay-TV, and confidential video conferencing [15]. 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 [16]. So, we develop a mathematical measure to evaluate the degree of encryption quantity. Image encryption quality has been studied in several articles [17-20]. In [15], 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 at several ciphers operation modes, and as functions of ciphers design parameters achieving their optimal values.

Since, block ciphers such as the 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).

Revised Manuscript Received on 30 January 2014.
* Correspondence Author

Prof. Abdul Hamid M. Ragab*, Department of Information System, King Abdulaziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia.

Dr. Osama Salah Farag Alla, Computer Science and Engineering, Menoufaia University, Faculty of Electronic Engineering, Menouf, Egypt,.

Dr. Amin Yousef Noaman, Department of Computer Science, Abdulaziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia.

Dr. Khalid Waheb. Magld, Department of Information Technology, Abdulaziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia.

So, there will be different versions of RC6-w/r/b.

In this paper we use a develop mathematical model for the measurement of the amount of encryption quantity to determine the optimal version of block cipher-w/r/b that gives better encryption quality for RCBC, RC6 and RC5 block ciphers. So, the effect of block cipher design parameters must be taken into account by evaluating the 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 the 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 on the encryption quality for digital images. In all experiments, we use the grey-scale two images-- Lena of size 512 x 512, grey-scale (0-255) as the original images (plainimages).

III. ENCRYPTION VISUAL TESTING OF RCBC, RC6 AND RC5 TO DIGITAL IMAGING

In this section, we investigate visual Inspection of encryption algorithms of RCBC, RC6 and RC5 for several ciphers operation modes and the effect of ciphers design parameters on encryption quality.

A. Ciphers Operation Modes of RCBC, RC6 and RC5

Block ciphers, such as RCBC, RC6, and RC5 can operate in one of several modes of operation, which are investigated in this paper; the following are the most important:

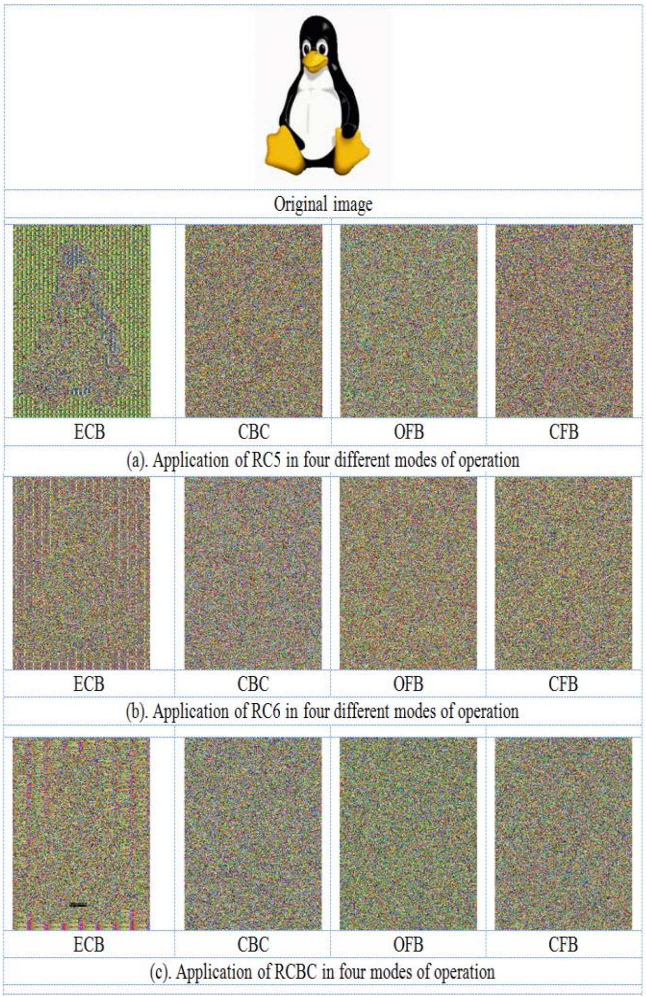
1- ***Electronic Codebook (ECB) mode*** is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a cipher-text block. Two identical plaintext blocks, then, will always generate the same cipher-text block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.

2- ***Cipher Block Chaining (CBC) mode*** adds a feedback mechanism to the encryption scheme. The plaintext is exclusively-ORed (XORed) with the previous cipher text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.

3- ***Cipher Feedback (CFB) mode*** is a block cipher implementation as a self-synchronizing stream cipher. It allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register of the same size as the block, encrypted, and the block is transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e. everything above and beyond the one byte) are discarded.

4- ***Output Feedback (OFB) mode*** is a block cipher implementation conceptually similar to a synchronous stream cipher. It prevents the same plaintext block from generating the same cipher-text block by using an internal feedback mechanism which is independent of both the plaintext and the ciphertext bit streams.

To demonstrate the effects of different ciphers modes of operation, we use the gray-scale image Tux of size 256 x 256 pixels that containing large areas of the same color or repeated patterns. Fig. 1 shows the results of applying RC5, RC6 and RCBC for Tux image in both encryption and decryption.


Original image

(a). Application of RC5 in four different modes of operation

(b). Application of RC6 in four different modes of operation

(c). Application of RCBC in four modes of operation

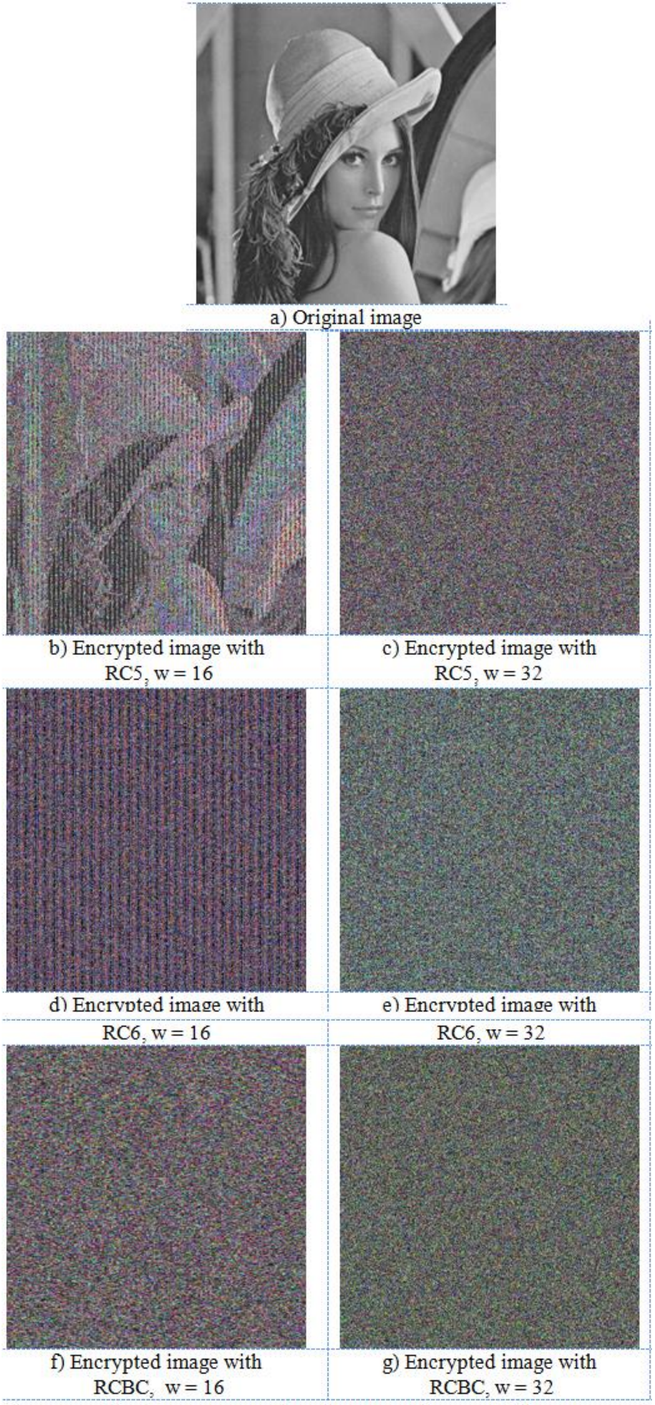
Fig. 1: Encryption of Tux original image by RC5, RC6, and RCBC with four modes of operation in (a) RC5, (b) RC6, and (c) RCBC

B. Effect of Ciphers Design Parameters on Visual Inspection

In this section, some simulation experiments; using MATLAB and simulation; are carried out to check the efficiency of RCBC, RC6 and RC5 for application to digital images. We must firstly extract the image header for the image to be encrypted /decrypted before application. 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 cipher is applied to the image. We use the gray-scale images for Lena of size 256 x 256 pixels, gray-scale (0-255) as the original images (plainimages). Fig. 2 shows the encryption and decryption results of RCBC, RC6 and RC5 for Lena, at fixed secret key length (b) =16, and number of rounds (r) =20, and word size (w) =16 and 32 bits, respectively. By comparing the original and the encrypted images in Fig.2 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 shows the possibility of applying RCBC, RC6 and RC5 to digital images successfully in both encryption and decryption.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

Encryption quality analysis and evaluation as functions of ciphers design parameters are investigated in details in the following sections.



a) Original image

b) Encrypted image with RC5, w = 16

c) Encrypted image with RC5, w = 32

d) Encrypted image with RC6, w = 16

e) Encrypted image with RC6, w = 32

f) Encrypted image with RCBC, w = 16

g) Encrypted image with RCBC, w = 32

Fig. 2: Results of RC5, RC6, and RCBC to Lena image with b = 16, r = 20

IV. ENCRYPTION QUALITY ANALYSIS AND EVALUATION

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. The main goal here is to utilize a mathematical model for the measurement of encryption quantity amount (Encryption quality) and to determine the optimal version of cipher -w/r/b that gives the better encryption quality for RCBC, RC6 and RC5. The optimality is defined as the choice of the most suitable and reasonable values for the cipher design parameters that give better encryption quality taking into account the best trade-off between encryption quality and computational efficiency.

A. *Measurement of Encryption Quality*

We suggest using the following strategy to approximate encryption quality measurement. With the application of encryption to an image, a change takes place in pixels values as compared to those values before encryption. 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 can 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 can be determined as follows [21-24]:

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

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

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

The effect of number of rounds (r) on the encryption quality for RC5, RC6 and RCBC is investigated for different modes of operation such as ECB, CBC, CFB and OFB. The block size and secret key length are both constant, w = 32 and b = 16. The encryption quality (EQ) is computed as a function of number of rounds (r). Figs.3-6. show encryption quality results using Lena image. From these results we find out the following:

(a) Results shown in Fig.3 for ECB mode show that:
1. RC5 achieves the max. EQ at r = 4,
2. RC6 achieves the Max EQ at r= 12 and 16,
3. RCBC achieves the Max EQ at r = 8, 20, 24, and 30.

(b) Results shown in Fig.4 for CBC mode show that:
1. RC5 achieves the max EQ at r= 4 and 8.
2. RC6 achieves the min. EQ at all rounds (r).
3. RCBC achieves the Max EQ at r = 12, 16, 20, 24 and 30.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

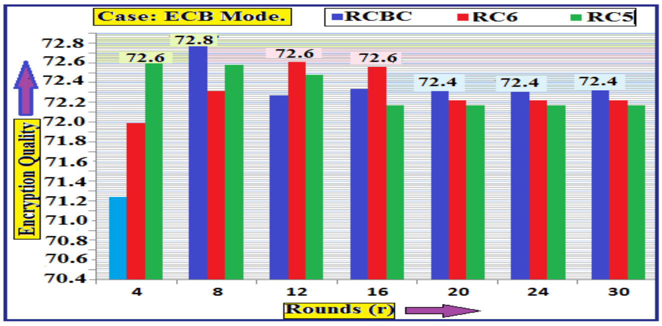


Fig.3 the EQ as a function of number of rounds (r), Case: ECB Mode.

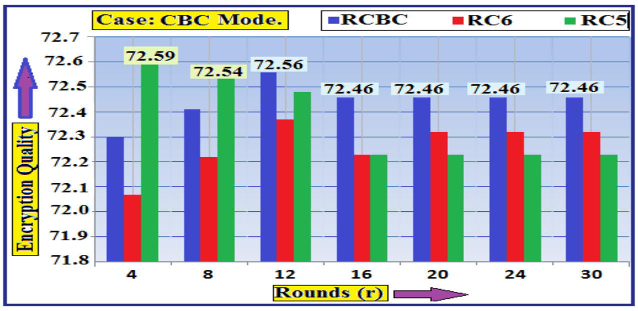


Fig.4 the EQ as a function of number of rounds (r), Case: CBC Mode.

(c) Results shown in Fig.5 for CFB mode show that:

1. RC5 achieves the max EQ at r= 4 only.
2. RC6 achieves the max EQ at r=8, 12 and 16.
3. RCBC achieves the max EQ at r = 20, 24, and 30.

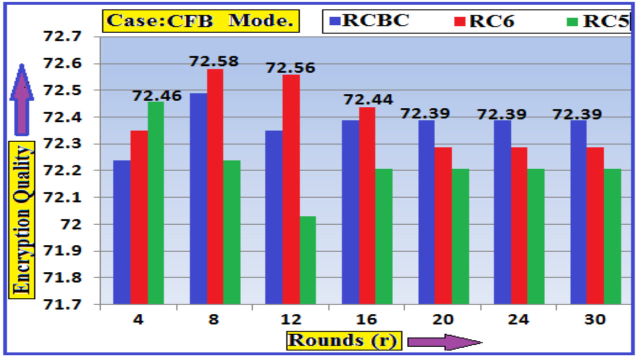


Fig.5 the EQ as a function of number of rounds (r), Case: CFB Mode.

(d) Results shown in Fig.6 for OFB mode show that:

1. RC5 achieves the max EQ at r= 12 only.
2. RC6 achieves the min EQ at all rounds (r).
3. RCBC achieves the max EQ at r = 20, 24, and 30.

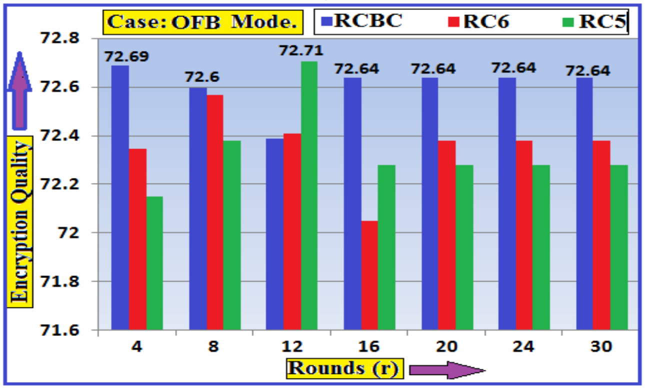


Fig.6 the EQ as a function of number of rounds (r), Case: OFB Mode.

C. Effect of Secret Key Length on the Encryption Quality of RC5, RC6 and RCBC

The effect of secret key length on the encryption quality for RCBC, RC5 and RC6 is investigated at fixed block size and number of rounds, w = 32 and r = 20 for different modes of operation such as ECB, CBC, OFB and CFB. Figs.7-10 show the computed results. These results show that the secret key length has a non-linear effect on the encryption quality of RCBC, 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. From Figs.7-10, we find out the following:

(a) Results shown in Fig.7 for ECB mode show that:

1- RC5 achieves the min EQ almost at all b.

2- RC6 achieves the max EQ at b=32.

3- RCBC achieves the max EQ at b = 16, 64,128, and 255.

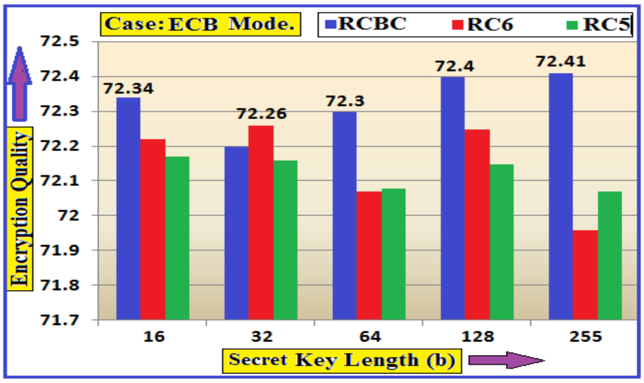


Fig.7 the EQ as a function of secret key length (b), Case: ECB Mode.

(b) Results shown in Fig.8 for CBC mode show that:

1- RC5 achieves the max EQ at b=128 and 255.

2- RC6 achieves the min. EQ at all secret key lengths.

3- RCBC achieves the max EQ at b = 16, 32, and 64.

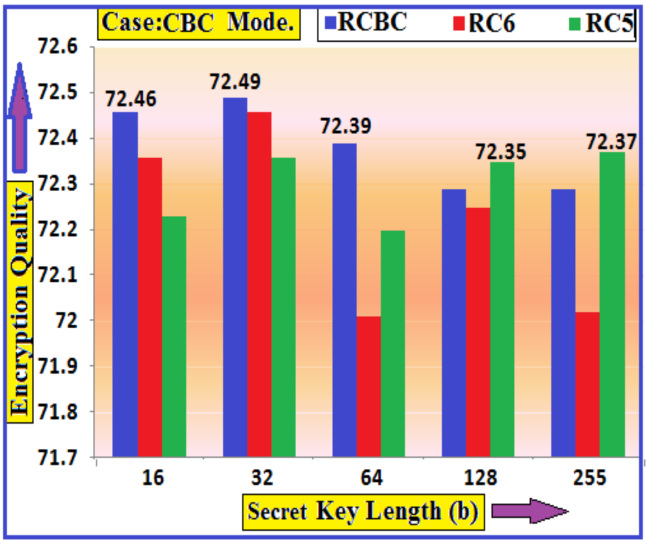


Fig.8 the EQ as a function of secret key length (b), Case: CBC Mode.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved

(c) Results shown in Fig.9 for CFB mode show that:
1- RC5 achieves the min EQ almost at secret key lengths.
2- RC6 achieves the max EQ at b = 32 and 128.
3- RCBC achieves the max EQ at b = 16, 64 and 255.

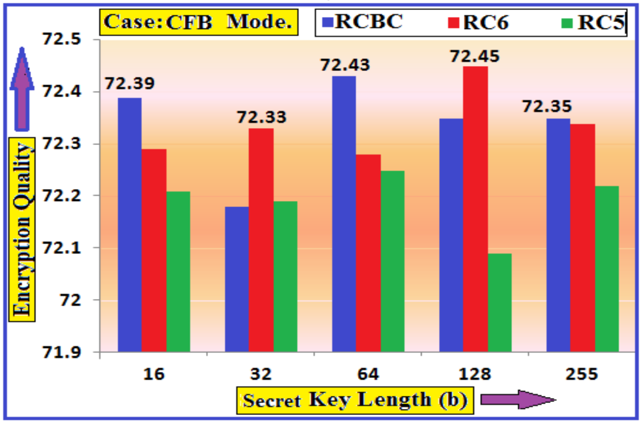


Fig.9 the EQ as a function of secret key length (b), Case: CFB Mode.

(d) Results shown in Fig.10 for OFB mode show that:
1- RC5 achieves the min EQ at all secret key lengths.
2- RC6 achieves the max EQ at b=64 only.
3- RCBC achieves the max EQ at b=16, 32,128 and 255.

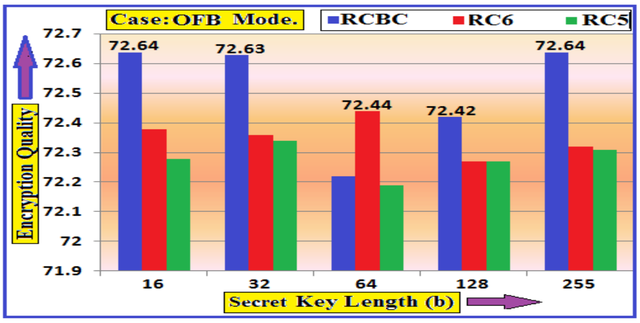


Fig.10 the EQ as a function of secret key length (b), Case: OFB Mode.

D. Effect of block Size on the Encryption Quality of RC5, RC6 and RCBC

The effect of block size on the encryption quality for RCBC, RC5 and RC6 is investigated at fixed number of rounds and secret key length, r = 20, and b = 16 for different modes of operation such as ECB, CBC, OFB and CFB. The theoretical calculated results and the practical results are shown respectively in Figs. 11-14.

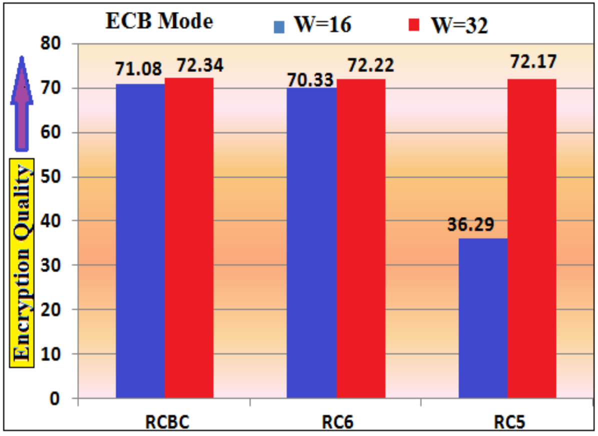


Fig.11 the EQ as a function of block size (w), Case: ECB Mode.

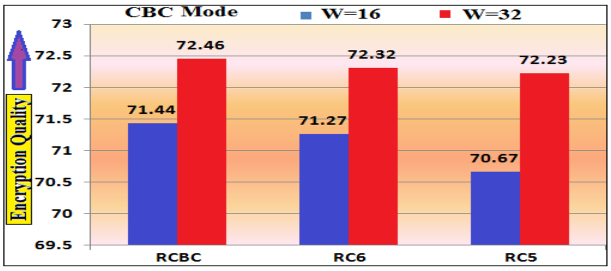


Fig.12 the EQ as a function of block size (w), Case: CBC Mode.

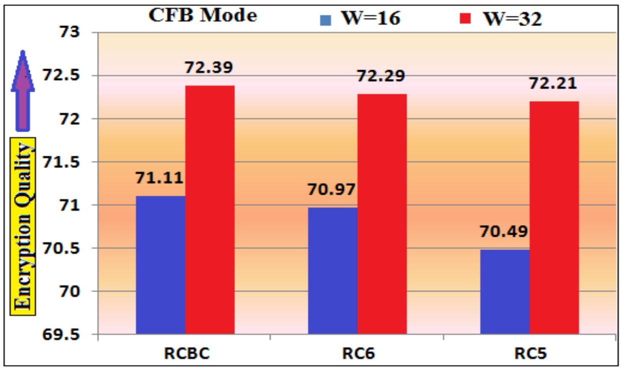


Fig.13 the EQ as a function of block size (w), Case: CFB Mode.

Results shown in Figs.11-14 clearly show that:

1. For different modes of operation, the RCBC has the largest encryption quality than both RC5 and RC6.
2. The encryption quality of RCBC, RC5 and RC6 block ciphers increases with increasing word size and vice versa, so increasing the word size contributes to increase the encryption quality of RCBC, RC5 and RC6.
3. So we will suggest the use of w = 32 for RCBC, RC5 and RC6 which will result in a block size of 8w (256-bit block size) for RCBC, 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 RCBC, RC5 and RC6.
4. The agreement and compatibility between the theoretical and practical results proves the correctness of the mathematical formula used for computing the encryption quality.

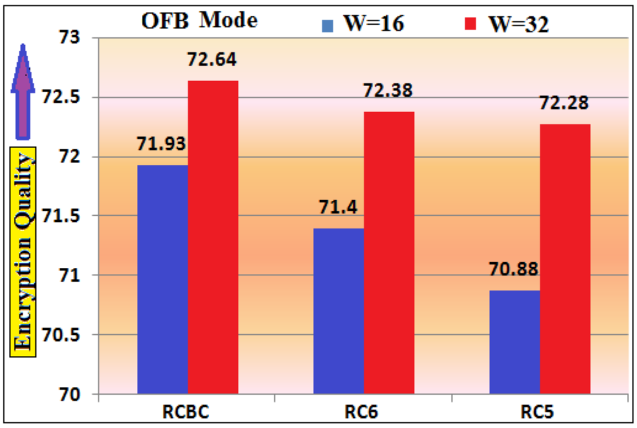


Fig.14 the EQ as a function of block size (w), Case: OFB Mode.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION

In this paper the efficient robust chaotic block cipher (RCBC) encryption quality algorithm for digital imaging was evaluated. Comparative analysis regarding encryption quality of the RCBC, RC6, and RC5 was performed. Their design parameters were analyzed as functions of different ciphers operation modes, including ECB, CBC, CFB, and OFB, to finding out the optimal values. Thorough experimental tests using analytical methods and simulation are carried out with detailed analysis demonstrating the better encryption quality of the RCBC block cipher. Results obtained show that the RCBC achieved better encryption quality for the choices of word size w = 32, number of rounds = 16, and secret key length b = 16. Based on these results, the optimal version of RCBC-w/r/b block cipher taking into account the best trade-off between encryption quality and computational efficiency is estimated to be RCBC-32/16/16. So, the RCBC can be considered as near to a real-time fast and secure symmetric encryption for digital imaging.

ACKNOWLEDGMENT

Authors would like to thank King Abdulaziz University in Jeddah, Saudi Arabia for offering the necessary facilities for accomplishing the related work in this research.

REFERENCES

1. The Data Encryption Standard (DES), Chapter2, www.facweb.iitkgp.ernet.in/ ~sourav/ DES.pdf.
2. Data Encryption Standard, http://en.wikipedia.org/wiki/ Data_Encryption_Standard.
3. Encryption at the Speed of Light? Towards a cryptanalysis of an optical CDMA encryption scheme, www.ipam.ucla.edu/publications/ scws4/scws4_6821.pdf.
4. Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, ”Security analysis of optical encryption”, Proc. of SPIE Vol. 5986 598603-1, 2005.
5. H.S. Chang, “IDEA International Data Encryption Algorithm”, https://users.cs.jmu.edu/.../IDEA-by-How-Shen-Chang-2004-FALL. doc.
6. S. Basu,” International Data Encryption Algorithm (IDEA) a Typical Illustration”, Journal of Global Research in Computer Science, Vol. 2, No. 7, July 2011.
7. RSA Cryptology and security, http://en.wikipedia.org/wiki/RSA.
8. T. Morkel, J.H.P. Eloff ,” Encryption Techniques: a Timeline Approach”, Information and Computer Security Architecture (ICSA) Research Group, www.icsa.cs.up.ac.za/issa/ 2004/ Proceedings/ Research/062.pdf
9. A. K. Wright, John A. Kinast, and Joe McCarty,” Low-Latency Cryptographic Protection for SCADA Communications”, Proc. Applied Cryptography and Network Security, 2004.
10. A. Canteaut,” Similarities Between Encryption and Decryption: how far can we go?” ,SAC 2013, www.sac2013.irmacs.sfu.ca/slides/s20.pdf.
11. J. Borgho, et al,” PRINCE A Low-Latency Block Cipher for Pervasive Computing Applications”, www. eprint.iacr.org/2012/529.pdf.
12. B. Agrawal, H. Agrawal,” Implementation of AES and RSA Using Chaos System”, International Journal of Scientific & Engineering Research, Vol.4, Issue 5, May-2013.
13. B. Agrawal, H. Agrawal, M. Mishra,” Implementation of Various Cryptosystem Using Chaos”, IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 13, Issue 4, PP 77-84, Jul.-Aug. 2013.
14. A. H. 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), Vol.3, Issue-6, January 05, 2014.
15. A. Jolfaei, A. Mirghadri,” Image Encryption Using Chaos and Block Cipher”, Computer and Information Science, Vol. 4, No. 1; January 2011.
16. R. Amirtharajan, P. Archana and J.B. Rayappan,” Why Image Encryption for Better Steganography”, Research Journal of Information Technology, Vol. 5, Issue: 3, pp 341-351,2013.
17. A. Massoudi, F. Lefebvre, C. D. Vleeschouwer, B. Macq, and J. Quisquater, “Overview on Selective Encryption of Image and Video: Challenges and Perspectives”, Hindawi Publishing Corporation, EURASIP Journal on Information Security, Vol. 2008.
18. N. El-Fishawy and O. M. AbuZaid,” 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. U. Pandey, M. Manoria, J. 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, Vol. 42, No.1, March 2012.
20. H. E. Ahmed, H. M. Kalash, and O. 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. H. E. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, “Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images”, Journal of Optical Engineering, vol. 45, 2006.
22. G. N. Krishnamurthy, 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.
23. A. Jolfaei, A. Mirghadri,” A New Approach to Measure Quality of Image Encryption”, International Journal of Computer and Network Security, Vol.2, No.8, PP 38-44, 2010.
24. A. Jolfaei, A. Mirghadri, “Image Encryption Using Chaos and Block Cipher”, www.ccsenet.org/cis Computer and Information Science Vol. 4, No. 1, January 2011.

AUTHOR PROFILE

Prof: Abdul Hamid M. Ragab He got his PhD from Essex University, UK, in 1985 in e Systems. He is Prof. since 1995, Academic Staff Member & Consultants & Chairman of Computer Science and Eng. Referee for scientific Journals and Conferences. Supervised hundreds of PhD and Msc thesis. He has several highly cited Articles in IEEE Journals His research interests include: Multilevel Network Security, e-systems Applications, Adaptive E-Learning Systems, and Developed DSS. His eMail: ahm_ragab@yahoo.com

Assoc. Prof: Osama S. Farag Allah He is Associate Prof in Computer Science & Engineering. He got his Ph.D. in Computer Science & Engineering in 2007 from Menoufia University. His research interests cover Computer networks, Network security, Cryptography, Internet Multimedia security, Image encryption, Watermarking, Steganographic, Data hiding, Chaos theory. He published several papers in these fields, and supervised many Msc and PhD Thesis. His eMail:osam_sal@yahoo.com

Assoc. Prof: Amin Y. Noaman His Ph.D. in computer science from University of Manitoba, Canada, in 1999.He published many papers in the field, and supervised many Msc and PhD thesis. Currently he is associate professor in the computer science dept., faculty of computing and information technology, King Abdulaziz University. His current research focuses on data warehousing, bioinformatics, distributed database systems, DSS, mobile database and E-Learning. His eMail: anoaman @kau.edu.sa.

Assist. Prof: Khalid W. Magld In 2007 he got his PhD in Computer Science University of Bradform, UK. Field of specialty: “Networking, and Information Systems Analysis and Applications”. He has several published work in this fields. His Research Interests: Unicast and multicast in mobile ad-hoc networks. Neural networks analysis and applications. Web-based simulation, training and education, E-Learning and applications. E- Government, e-Management Systems. His eMail: kmagld@kau.edu.sa

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved