

Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms

Nawal El-Fishawy¹ and Osama M. Abu Zaid²

(Corresponding author: Nawal El-Fishawy)

Department of Electronics & Electrical Communication Eng, Faculty of Electronic Eng., Menouf, Egypt¹

(Email: nelfishawy@hotmail.com)

B. Sc. Math. & Computer Science, Faculty of Science, Shebin Elkom, Egypt²

(Received Oct. 16, 2005; revised and accepted Nov. 23, 2005 & Aug. 22, 2006)

Abstract

RC6, MRC6, and Rijndael are three block cipher algorithms. Different types of Bitmap images are encrypted with each of the three encryption algorithms. Visual inspection is not enough on judging the quality of encrypted images. So, other measuring factors are considered based on: measuring the maximum deviation between the original and the encrypted images, measuring the correlation coefficient between the encrypted and the original images, the difference between the pixel value of the original image and its corresponding pixel value of the encrypted one, the encryption time and the throughput. These measuring factors are applied on the three encryption algorithms to evaluate images containing many high frequency components and others containing very large areas of single colors as an example of binary images. The results of the nominal electronic code book are not enthusiastic, so the Cipher Block Chaining and the output feed back modes are implemented and the results are compared.

Keywords: Image encryption, quality measurements, MRC6, RC6, Rijndael

1 Introduction

Now we are living the age of communications revolution which necessitates multimedia transmission in a secure manner. Visual encryption is important in transferring image through the communication networks to protect it against reading, alteration of its content, adding false information, or deleting part of its content.

The block cipher algorithm RC6 appeared in 1997 [9] is an evolutionary improvement of RC5, designed to meet the requirements of the Advanced Encryption Standard (AES). MRC6 [3] is an improvement on RC6 where it achieved less encryption/decryption time and higher throughput than RC6. In October 2000, Rijndael was

chosen as the AES algorithm [1, 4]. It is a very strong block cipher for its simplicity, efficient structure, and its strength against linear and differential cryptanalysis.

In this paper, different Bitmap images are encrypted with RC6, MRC6, and Rijndael. The quality of the encrypted images are tested with visual inspection and evaluated with different quality of measuring algorithms.

The paper is organized as follows: Section 2 will briefly discuss the three encryption algorithms: RC6, MRC6, and Rijndael. Section 3 will discuss the process of encrypting the images with the three encryption algorithms on considering three modes of operations, the electronic code book and the Cipher Block Chaining (CBC) mode and the Output Feed Back (OFB) mode. The methods of evaluating the quality of encryption is discussed in Section 4. The results of the paper appear in Section 5. The paper is concluded in Section 6.

2 Overview on the Encryption Algorithms

This section will give a brief overview on the construction of each encrypting algorithm and the admissible values of each building factor. Each of the following encryption algorithms is a symmetric block cipher algorithm. Symmetric means the key used for encryption and decryption is the same, while block means the data (information) to be encrypted is divided into blocks of equal length.

2.1 RC6 Block Cipher Algorithm

This algorithm depends mainly on the use of four working registers, each of size 32 bits. So, it handles 128 bits input/output blocks. Its parameterized family is: (w) word size in bits, (r) non-negative number of rounds, and (b) the length of encryption/decryption key in bytes. RC6

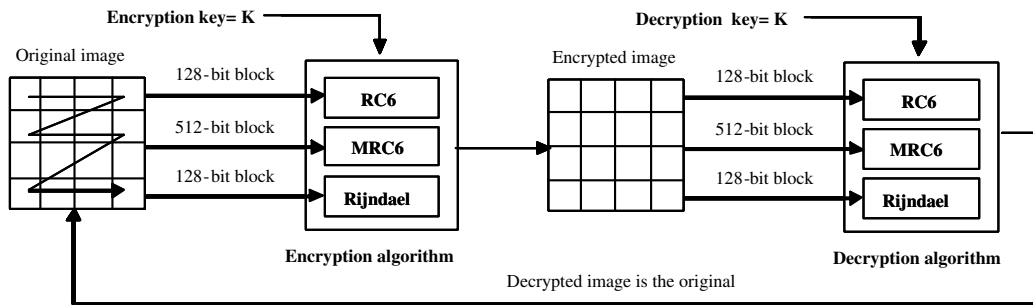


Figure 1: The bitmap image encryption/decryption process with RC6, MRC6 and Rijndael

has six primitive operations, which are $(+, -, \ll, \gg, *, \oplus)$. The use of multiplication greatly increases the diffusion achieved per round, allowing for greater security, fewer rounds, and increases throughput. RC6 uses an expanded key table, $S[0, \dots, t-1]$, consisting of key $t = 2r + 4$ w-bit words. All details of RC6 are described in [9].

2.2 MRC6 Block Cipher Algorithm

MRC6 is our modification on RC6. MRC6 [3] block cipher algorithm was based on the use of 16 working register each of 32 bits, instead of 4 as in RC6. So, MRC6 is capable of handling 512 bits input/output block. It uses the same parameterized family (w , r , and b), and the same primitive operations of RC6. MRC6 uses an expanded key table, $S[0, \dots, t-1]$, consisting of key $t = 8r + 16$ w-bit words. All details of MRC6 block cipher algorithm are described in [3].

2.3 The Rijndael Block Cipher Algorithm

The Rijndael [1, 4] is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits. The intermediate cipher result is called “state” which is a rectangular array of four rows and number of columns equal to the block length divided by 32. The cipher key is similarly a rectangular array with four rows and number of columns equal to the key length divided by 32. The number of rounds is related to the key size, so for key sizes of 128, 192 and 256 the number of rounds are 10, 12 and 14 respectively. Each round consists of fixed sequence of transformations, except the first and the last round. These transformations are:

- 1) The SubByte: It is a non linear byte substitution, operating on each of the state bytes independently. The substitution table (S-box) is a multiplicative inverse in the $GF(2^8)$ followed by applying by an affine over $GF(2)$. The inverse process is true with the decryption process, which is obtained by the inverse of the

affine mapping followed by taking the multiplicative inverse in the $GF(2^8)$.

- 2) The Shift Row: In Shift Row, the rows of the state are cyclically shifted over different offsets, which depend on the block length.
- 3) The MixColumn: In MixColumn, the columns of the state are considered as polynomials over $GF(2^8)$ and multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = '03'x^3 + '01'x^2 + '01'x + '02'$.
- 4) Add Round Key: In this operation, the round key is applied to the state by a simple bitwise XOR.

In our study, we selected the case of Rijndael which is chosen as AES such that the block length is 128 bits and the key length is 128 bits also.

3 Bitmap Image Encryption

Bitmap (BMP) image is a type of uncompressed image format which preserves all information about the image data. The encryption process has two inputs, the plaintext (data image) and the encryption key. To encrypt an image, its header is excluded and the start of the bitmap's pixels or array begins right after the header of the file. The bytes of the array are stored in row order from left to right with each row representing one scan line of the image. The rows of the image are encrypted from top to bottom.

As shown in Figure 1, the block length of RC6, MRC6, and Rijndael are 128, 512, and 128 respectively. The key length for the three algorithms is 16 bytes (128 bits). In the decryption process, the encrypted image is divided into the same block length of each algorithm from top to bottom. The first block is entered to the decryption function of each algorithm and the same encryption key is used to decrypt the image but the application of sub-keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom.

In this paper the bitmap image encryption will be done with three modes of operation, the Electronic Code Book (ECB) mode, the Cipher Block Chaining (CBC) mode,

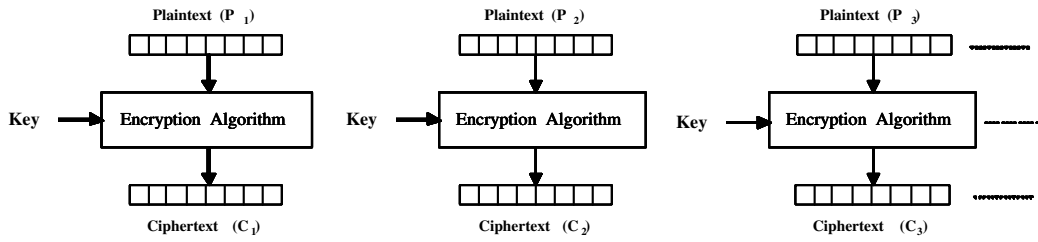


Figure 2: The construction of the electronic code book encryption algorithm

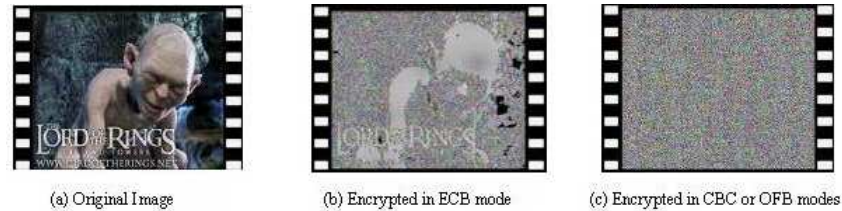


Figure 3: An image with large areas of a single color encrypted in ECB mode and CBC or OFB: (a) Original Image, (b), Encrypted in ECB mode, and (c) Encrypted in CBC or OFB modes

and the Output Feed Back (OFB) mode [5, 6, 7, 8]. The three modes are used to decide which one of them will increase hiding the data of the image.

The ECB is the simplest mode of operation, where the message (file) is divided into blocks of equal length and each block is encrypted separately with the same encryption key, See Figure 2. The plaintext is divided into blocks (P_1, P_2, P_3, \dots) of size n bits which are encrypted to ciphertext blocks (C_1, C_2, C_3, \dots). The encryption algorithm is $C_j = E_K(P_j)$, and the decryption algorithm is $P_j = D_K(C_j)$ such that $j = 1, 2, 3, \dots$, and E_K is encryption map with the key (K), and D_K is decryption map with the same key (K). The disadvantage of this method is that identical plaintext blocks are encrypted to identical ciphertext blocks; it does not hide data patterns. Thus, in some senses it doesn't provide message confidentiality at all, and is not recommended for cryptographic protocols [5]. The advantage is that error propagation is limited to a single block. The disadvantage of ECB mode appears well in image encryption if we have an image with large areas of the same color or repeated patterns so that there are many blocks of the same plaintext [2]. This disadvantage appear in Figures 3 and 5 such that, ECB cannot hide all features of the original images. This disadvantage is treated in CBC mode or OFB mode. So, both of them with that kind of images are better than ECB.

The CBC is the second mode of operation for encryption ciphers. In the CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to that point [5]. CBC mode uses what is known as an initialization vector (IV) of a certain length. In decryption, the same XOR operation is

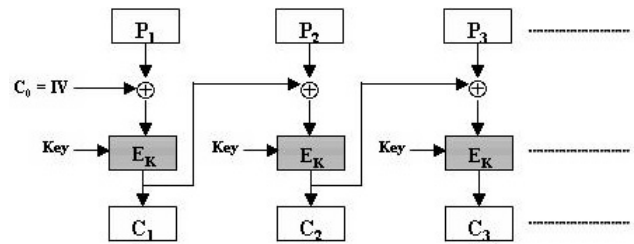


Figure 4: The construction of the CBC mode

repeated so that its effect is cancelled. This mechanism is shown in Figure 4. The main disadvantage of CBC mode is that an error in (or attack upon) one ciphertext block impacts two plaintext blocks upon decryption [2].

In the CBC mode, the encryption algorithm is $C_j = E_K(C_{j-1} \oplus P_j)$, and the decryption algorithm is $P_j = D_K(C_j) \oplus C_{j-1}$, such that $j = 1, 2, 3, \dots$ and $C_0 = IV$.

The third mode of operation considered in this paper is the OFB mode. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext [5]. The XOR value of each plaintext block is created independently of both the plaintext and ciphertext [6]. The advantage of OFB mode is relevant to applications for which error propagation must be avoided [8]. Like CBC, OFB uses what is known as an initialization vector (IV). OFB generates the next keystream block by encrypting the last one. And the first keystream block is generated by encrypting the IV . Figure 6 shows the technique of the OFB mode. The encryption algorithm is $C_j = P_j \oplus I_j$, and the decryption algorithm is $P_j = C_j \oplus I_j$, and $I_j = E_K(I_{j-1})$, such that $j = 1, 2, 3, \dots$,

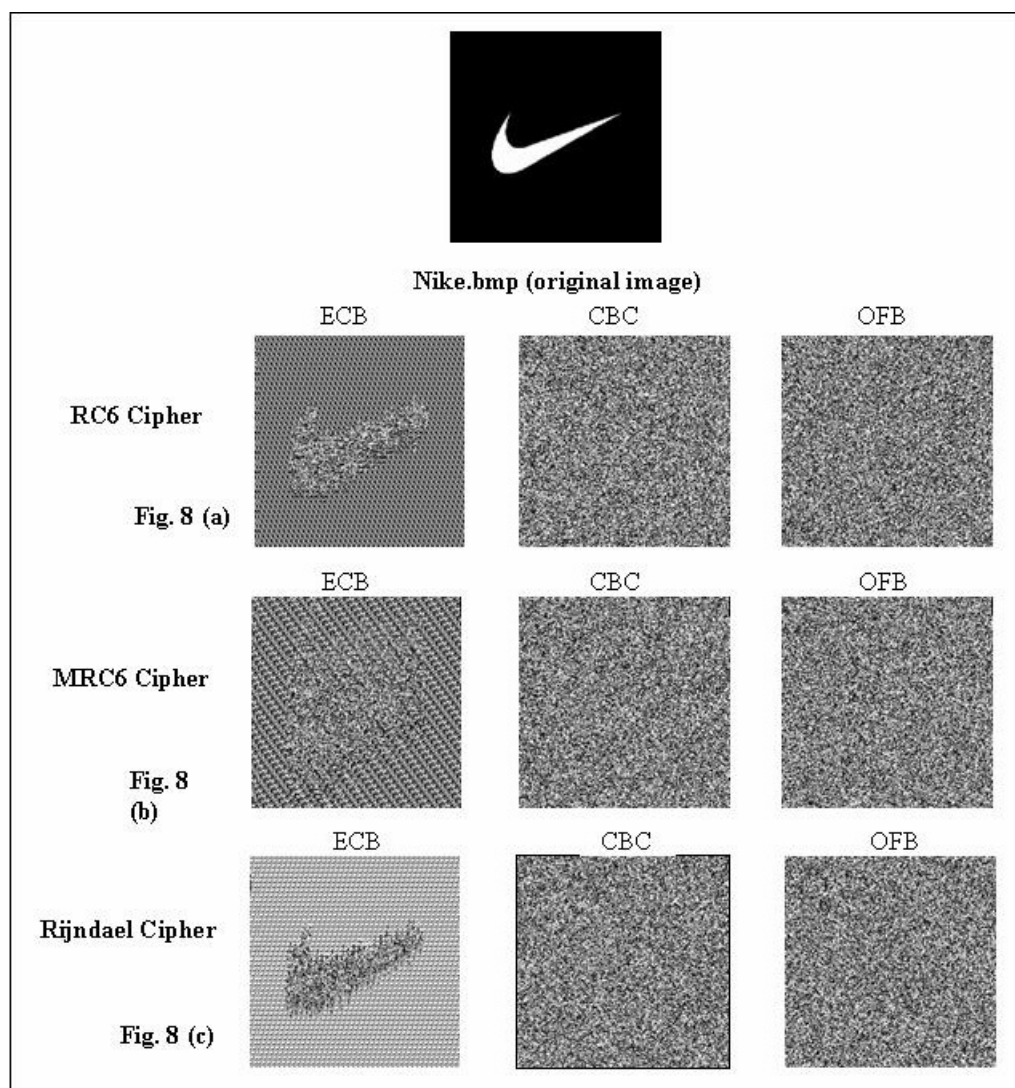


Figure 5: Encryption of Nike.bmp by RC6, MRC6, and Rijndael with the three modes used (a) RC6, (b) MRC6, and (c) Rijndael

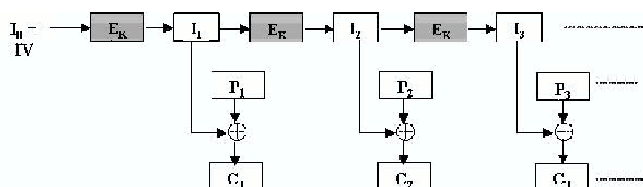


Figure 6: The construction of the OFB mode

and $I_0 = IV$.

4 Quality of Encryption Measuring Factors

One of the important factors in examining the encrypted image is the visual inspection 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 complete hiding of the content of the data image. So, other measuring techniques are considered to evaluate 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 [10].

In addition to the visual inspection, three measuring quality factors will be considered to evaluate and compare between the three encryption algorithms RC6, MRC6, and Rijndael. These factors are, the maximum deviation, the correlation coefficient and irregular deviation [2]. Also another factor is measured which is the encryption time, and the throughput.

4.1 The Maximum Deviation Measuring Factor

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [10]. The steps of this measure will be 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:

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

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.

4.2 The Correlation Coefficient Measuring Factor

Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, then they are in perfect correlation (i.e; the correlation coefficient equals one) if they are highly dependent (identical). In this case the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different, i.e., the encrypted image has no features and highly independent on the original image. If the correlation coefficient (C.C) equals -1, this means the encrypted image is the negative of the original image. So, success of the encryption process means smaller values of the C.C. The C.C is measured by the following equation:

$$\begin{aligned} \text{The_Correlation_Coefficient} &= \frac{\text{cov}(x, y)}{\sigma_x \sigma_y} \\ &= \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N (x_i - E(x))^2} \sqrt{\sum_{i=1}^N (y_i - E(y))^2}}, \end{aligned}$$

where $E(x) = \frac{1}{N} \sum_{i=1}^N x_i$, and x and y are gray-scale pixel values of the original and encrypted images. Measuring the C.C is done through running the C.C built in function in the used MATLAB 6.0 software (**Corr2**).

4.3 The Irregular Deviation Measuring Factor

This quality measuring factor is based on how much the deviation caused by encryption (on the encrypted image) is irregular [2]. It gives an attention to each individual pixel value and the deviation caused at every location of the input image 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:

$$D = |I - J|$$

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

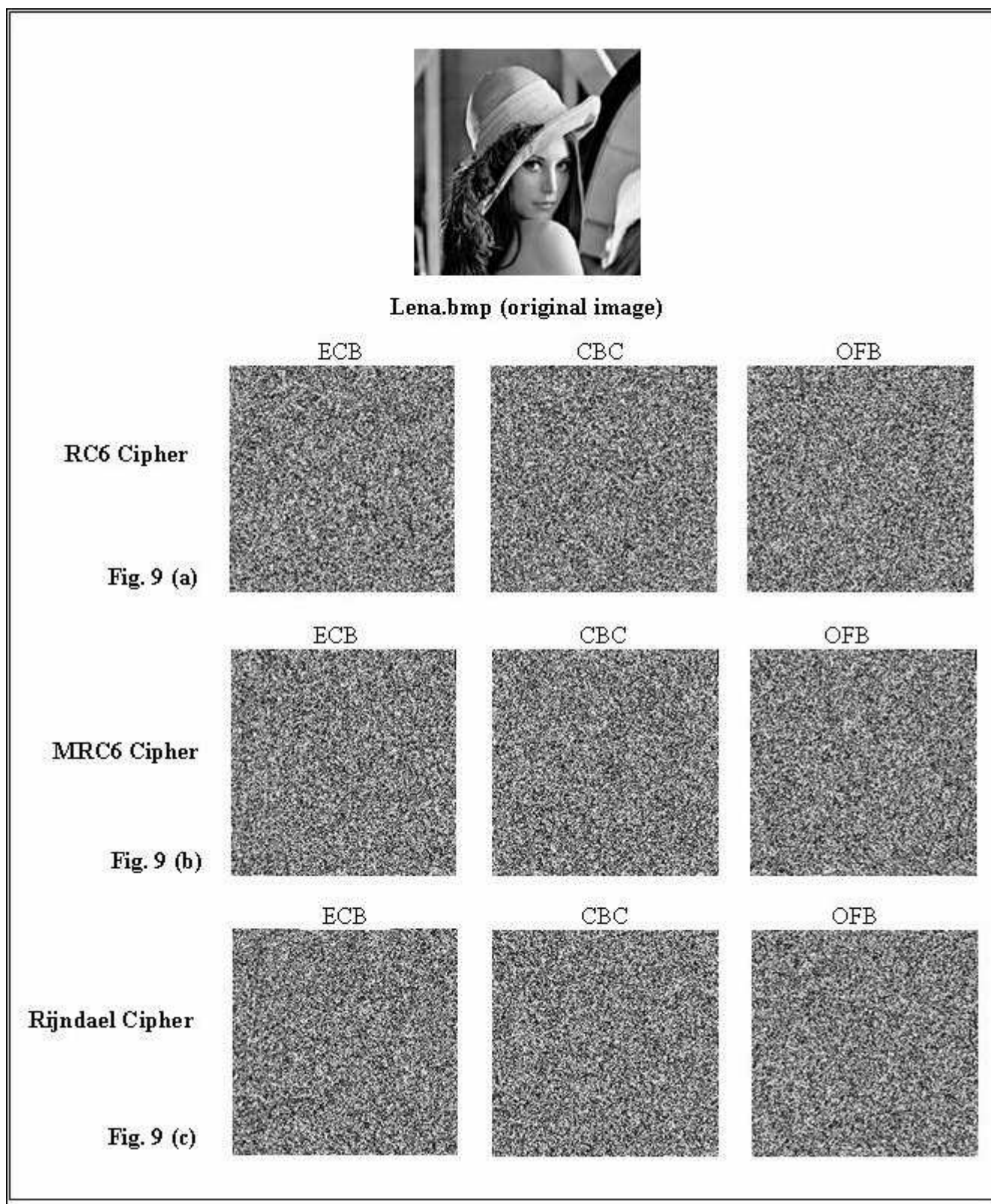


Figure 7: Encryption of Lena.bmp by RC6, MRC6, and Rijndael with the three modes used (a) RC6, (b) MRC6, and (c) Rijndael

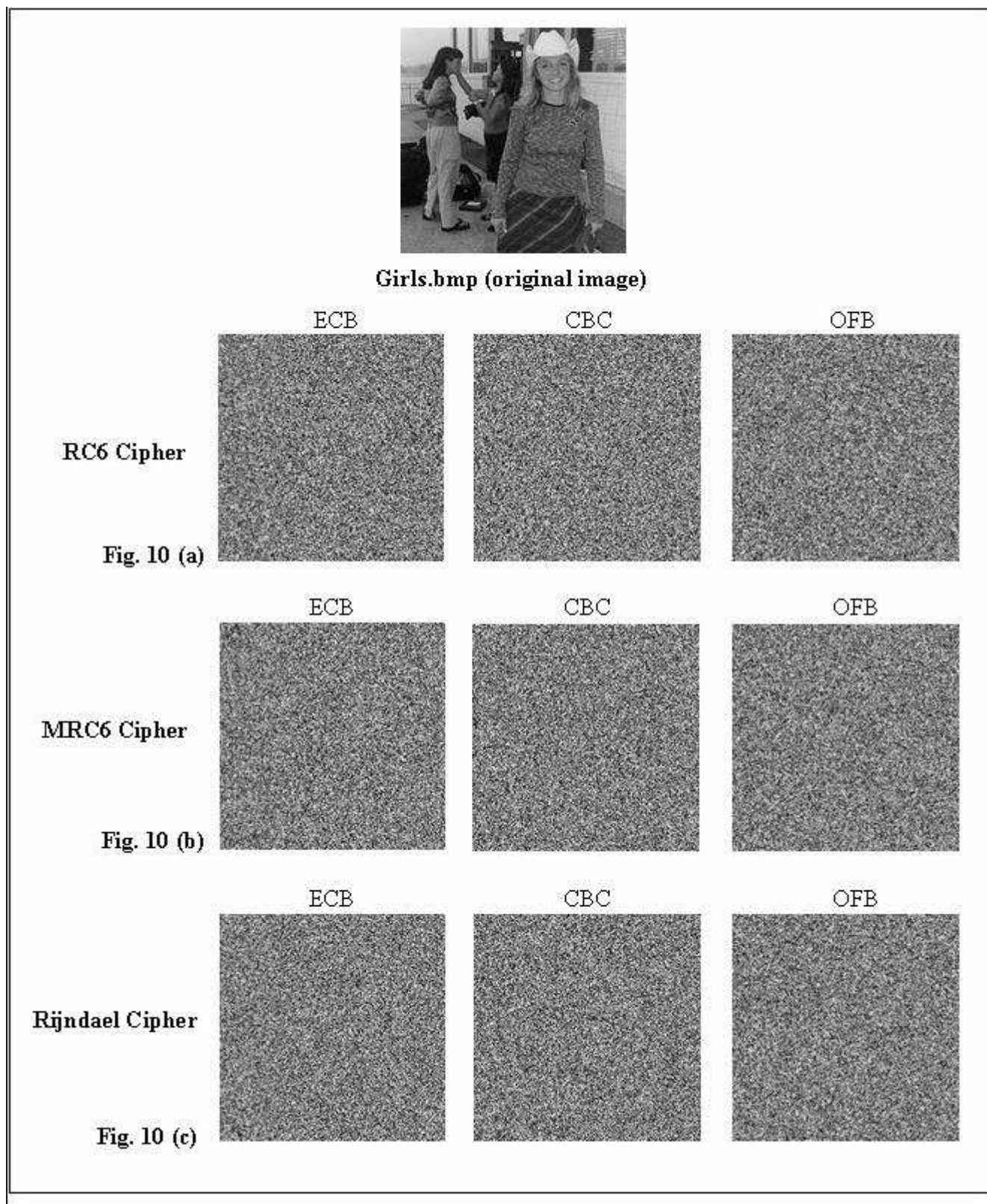


Figure 8: Encryption of Girls.bmp by RC6, MRC6, and Rijndael with the three modes used (a) RC6, (b) MRC6, and (c) Rijndael

Table 1: Quality measures for RC6, MRC6, and Rijndael encrypted images using the ECB mode

cipher	RC6			MRC6			Rijndael		
	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3
Nike	43638	0.0355	48066	42988.5	0.0163	31970	43321	-0.1273	48226
Lena	12368	$1.079e^{-4}$	16172	12622.5	0.0085	16260	12496.5	-0.0057	16142
Girls	33946.5	$6.641e^{-4}$	39438	34829.5	$-6.093e^{-4}$	39036	34833.5	-0.0050	39070

Table 2: Quality measures for RC6, MRC6, and Rijndael encrypted images using the CBC mode

cipher	RC6			MRC6			Rijndael		
	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3
Nike	42416.5	0.0170	2374	42472	$1.749e^{-4}$	2164	42504	-0.0057	2232
Lena	12693.5	0.0056	16188	12628	-0.0033	16140	12401	-0.0026	16172
Girls	34324	0.0014	39180	34313	0.0044	39394	34217.5	-0.0021	39172

Table 3: Quality measures for RC6, MRC6, and Rijndael encrypted images using the OFB mode

cipher	RC6			MRC6			Rijndael		
	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3	DEV-1	DEV-2	DEV-3
Nike	42565.5	$6.223e^{-4}$	2354	42431.5	0.0038	2098	42442	-0.0049	2380
Lena	12628	0.0073	16192	12737	-0.0034	16062	12438	-0.0049	16016
Girls	34009.5	$8.417e^{-4}$	39144	34022.5	-0.0028	39308	34423	-0.0023	39060

of the deviation matrix is a uniform distribution). This average (DC) value can be calculated as:

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

where h_i is the amplitude of the absolute difference histogram at the value i .

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

$$AC(i) = |H(i) - DC|.$$

- 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.

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

The lower the ID value, the better the encryption algorithm.

5 Results and Discussion

In our simulation programs three different BMP images are evaluated. These images are Lena.bmp (Figure 7) as

it is the reference image used in image processing research (it does not contain many high frequency components), Nike.bmp (Figure 5) as an example of an image containing very large areas of a single color and it is an example of a binary image, and Girls.bmp (Figure 8) as an example of an image containing many high frequency components.

The three images are encrypted using RC6_{w/r/b}, MRC6_{w/r/b}, and Rijndael. The number of rounds for Rijndael at the case of AES is (Nr=10), so this number of rounds is kept the same for RC6 and MRC6. For all encryption algorithms, the key length is kept the same at 16 bytes such that this key = (41424361 62636465 61656661 65616563)₁₆. The initialization vector is ($IV = (000000 \dots)_{16}$) which is used for all ciphers with CBC and OFB modes.

The results of the three measuring factors are given in the following tables where DEV-1 indicates the maximum deviation measure, DEV-2 indicates the correlation coefficient measure, and DEV-3 indicates the irregular deviation measure. Tables 1, 2, and 3 illustrate the results with ECB, CBC, and OFB modes, respectively. With the measure of DEV-1 the greater is the better, with DEV-2 the closer to zero is the better, while with DEV-3 the smaller is the better.

To measure the encryption time and the throughput, the Girls.bmp image is taken as a case study. The encryption time of Girls.bmp image when applying the three encryption algorithms with the three modes of operation is shown in Table 4 and Figure 9. Girls.bmp is 256*256 pix-

els and equals to 65 KBytes size. It is clear that MRC6 with OFB mode achieves the smallest encryption time. The throughput is defined as the amount of encrypted data per unit time (Kbps). Table 5 and Figure 10 indicate the throughput values of the three algorithms with the three modes. It is clear that MRC6 with OFB mode has the highest throughput while Rijndael with CBC has the smallest throughput value.

Table 4: Time of encryption of Girls.bmp by all ciphers with the three modes

Time (Sec) of encryption of Girls.bmp with the three modes			
	ECB	CBC	OFB
RC6	0.1909 sec	0.2300 sec	0.1899 sec
MRC6	0.1800 sec	0.2000 sec	0.1800 sec
Rijndael	0.2399 sec	0.2509 sec	0.1909 sec

Table 5: Throughput of encryption of Girls.bmp by all ciphers with the three modes

Time (Sec) of encryption of Girls.bmp with the three modes			
	ECB	CBC	OFB
RC6	2723.936	2260.872	2738.28
MRC6	2888.888	2600	2888.888
Rijndael	2167.568	2072.536	2723.936

Note that:

- 1) all programs which applied in simulating the encryption algorithms are designed by Borland C++ Builder 6.0 with processor of Pentium III (800 MHz) and 128-MB RAM on windows XP.
- 2) the programs which are used to produce the values of DEV-1, DEV-2, and DEV-3 are designed by MATLAB 6.0 on the same machine.
- 3) Figures 3 and 5 illustrate that CBC and OFB modes are better than ECB mode in hiding all features of the image specially the image which contains large areas of single color.
- 4) Based on the discussion presented in [2], DEV-3 did not give any misleading results and it can be used alone to test the quality of encryption in the field of image encryption. So, if DEV-3 agrees with other measuring factor, it will be good judging, otherwise the final decision on measuring the quality of the three encryption algorithms will be based on DEV-3 which is based on the irregular deviation on each pixel value.

Now here is a detailed discussion of the previous results.

- 1) Testing the results of the images with the **ECB** mode (see Table 1).

- **Nike.bmp** image with DEV-1, RC6 gives a greater result than the other ciphers, and MRC6 gives the smallest result. But by visual inspection of the encrypted images in Figures 5(a, b, c), the best hiding of all the features is achieved with MRC6, RC6, and Rijndael respectively. So, DEV-1 is not accurate in some cases. With DEV-2, MRC6 is closer to zero than the others. With DEV-3, MRC6 is more smaller than the others and Rijndael gives result greater than RC6. So, with DEV-2 and DEV-3 MRC6 is the best one.

- **Lena.bmp** image with DEV-1, MRC6 gives a result that is greater than the other ciphers and RC6 gives the smallest result. With DEV-2, all ciphers give results below 0.01. RC6 is the closest to zero and Rijndael is closer to zero than MRC6. With DEV-3, Rijndael gives the smallest result and MRC6 gives result higher than RC6. So, Rijndael is the best one.

- **Girls.bmp** image with DEV-1, MRC6 gives result near to Rijndael but Rijndael is greater than MRC6 and both of them are better than RC6. With DEV-2, MRC6 is closer to zero than the others and RC6 is closer to zero than Rijndael. With DEV-3, MRC6 gives the smallest result and Rijndael is smaller than RC6. So, with DEV-2 and DEV-3 MRC6 achieves the best result.

- 2) Testing the results of the images with the **CBC** mode (see Table 2).

- **Nike.bmp** image with DEV-1, MRC6 achieves result near to Rijndael and both of them are greater than RC6. With DEV-2, MRC6 is closer to zero than others, and with DEV-3 MRC6 gives the smallest result. So, with DEV-2 and DEV-3 MRC6 is the best one.

- **Lena.bmp** image with DEV-1, MRC6 gives results near to RC6 and both are greater than Rijndael, with DEV-2 all ciphers are below .01, and with DEV-3 MRC6 is more smaller than the others. So, DEV-1 and DEV-3 agree on MRC6 is the best.

- **Girls.bmp** with DEV-1, MRC6 gives result near to RC6 and both of them are greater than Rijndael, with DEV-2 Rijndael and RC6 are closer to zero than MRC6, and with DEV-3 Rijndael gives results smaller than the other ciphers. So, DEV-2 and DEV-3 agree on Rijndael is the best.

- 3) Testing the results of the images with the **OFB** mode (see Table 3).

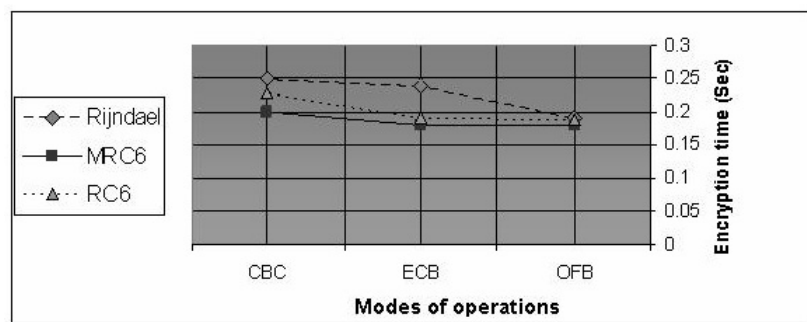


Figure 9: The time (in Sec.) of encryption of Girls.bmp by all ciphers with the three modes

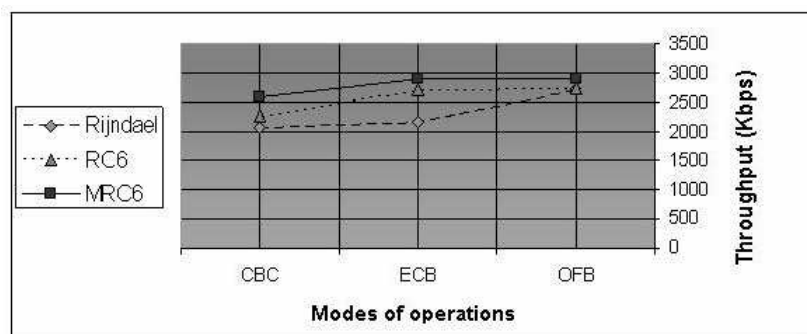


Figure 10: The throughput of encryption of Girls.bmp by all ciphers with the three modes

- The result agrees with the previous results of ECB and CBC that MRC6 is better with Nike.bmp.
 - The result agrees with the previous result of ECB that Rijndael is better with Lena.bmp.
 - The result agrees with the previous result of CBC that Rijndael is better with Girls.bmp.
- 4) Comparing the results of Nike.bmp to the other two images in ECB mode, we see that although its quality of encryption is very poor, it gives the highest result in the three images when the maximum deviation quality measure is used. This is a drawback with the maximum deviation quality measure.
- 5) As a general result:
- MRC6 cipher gives very good results in the kind of images (Nike.bmp) with all modes of operations compared to RC6 and Rijndael and causes better deviation on output pixel values.
 - MRC6 cipher gives good results in the kind of image (Lena.bmp) with CBC mode compared to RC6 and Rijndael. With the others modes (ECB and OFB), Rijndael gives good results for the same image (Lena.bmp) compared to RC6 and MRC6.
 - MRC6 cipher gives good results in the kind of image (Girls.bmp) with ECB mode compared to RC6 and Rijndael. With the others modes (CBC and OFB), Rijndael gives good results for the same image (Girls.bmp) compared to RC6 and MRC6.
- 6) MRC6 cipher achieves minimum time and maximum throughput with every modes.

6 Conclusion

This paper inspected three encryption algorithms RC6, MRC6, and Rijndael on encrypting images of different constructions with three modes of operations. Four evaluating measuring factors are considered, in addition to visual inspection. The ECB mode of operation failed in hiding the details of a binary image and CBC had the highest encryption time. MRC6 encryption algorithm with OFB mode achieved the minimum encryption time and the highest throughput. With most of the measuring factors, MRC6 achieved the best result on images of binary data with all modes of operation, little high frequency components with CBC mode, and more high frequency components with ECB mode. Rijndael is better than MRC6 on images of little high frequency components and more high frequency components with the others modes.

References

- [1] J. Daeman, and V. Rijmen, *AES Proposal: Rijndael*, <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndael.docV2.zip>, 1999.
- [2] H. Elkamchouchi and M. A. Makar, "Measuring encryption quality of Bitmap images encrypted with Rijndael and KAMKAR block ciphers," in *Proceedings Twenty second National Radio Science Conference (NRSC 2005)*, pp. C11, Cairo, Egypt, Mar. 15-17, 2005.
- [3] N. E. Fishawy, T. E. Danaf, and O. A. zaid, "A Modification of RC6 Block Cipher Algorithm for Data Security (MRC6)," in *Proceedings The International Conference on Electrical, Electronic and Computer Engineering (ICEEC'04)*, pp. C8, Cairo, Egypt, Sep. 2004.
- [4] B. Gladman, *A Specification for Rijndael, the AES Algorithm*, May 2003, http://fp.gladman.plus.com/cryptography_technology/rijndael/aes.Spec.311.pdf.
- [5] Encyclopedia article about Block cipher modes of operation-Electronic codebook (ECB), pp. 1-4, <http://encyclopedia.thefreedictionary.com/Block%20cipher%20modes%20of%20operation>.
- [6] Swiss encryption technology, MediaCrypt, Modes of operation, pp. 1-4, http://www.mediacypt.com/_pdf/MC_modes_1204.pdf.
- [7] Clifford Bergman, Encryption modes, Lecture 16, Feb. 2005, pp. 1-18, http://orion.math.iastate.edu/cbergman/crypto/ps_files/4up/chaining.pdf.
- [8] Elementray cryptography, Modes of operation, pp. 29-33, http://magma.maths.usyd.edu.au/~kohel/teaching/MATH3024/Lectures/lectures_05.pdf.
- [9] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, *The RC6TM Block Cipher*, 1998. <http://www.rsasecurity.com/rsalabs/rc6/>
- [10] I. Ziedan, M. Fouad, and D. H. Salem, "Application of Data encryption standard to bitmap and JPEG images," in *Proceedings Twentieth National Radio Science Conference (NRSC 2003)*, pp. C16, Egypt, Mar. 2003.



Nawal El-Fishawy received the Ph.D degree in mobile communications from the faculty of Electronic Eng., Menoufia university, Menouf, Egypt, in collaboration with Southampton university in 1991.

Now she is a Professor in the department of Electronics and Electrical Communication Eng., Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modelling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms.

She has served as a reviewer for many national and international journals and conferences. Also she participated in many technical program committees of major international conferences in wireless communications.



Osama M. Abu Zaid was graduated from the faculty of science, Menoufia University, Egypt in 2001. He is an assistant lecturer. He is working as a network manager in Menoufia University. He is working for his Ph.D. He is interested in security over wired and wireless networks.