Measurement of Encryption Quality of Bitmap Images with RC6, and two modified version Block Cipher

Ashwaq T. Hashim* **Baedaa H. Helal***

Received on: 17 /1 / 2010
Accepted on: 3 / 6 /2010

Abstract

With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. In this paper, RC6 with two modified version 512 bit RC6 and 640 bit RC6-Cascade encryption algorithms will be analyzed to investigate the encryption efficiency for them to digital images and providing a new mathematical measure for encryption efficiency. Detailed results in terms of security analysis and implementation are given. Comparative study with three versions of RC6 encryption algorithms is shown the superiority of the modified algorithms. Three measuring quality factors will be considered to evaluate and compare between the three encryption algorithms RC6, 512 RC6, and 640 RC6-Cascaded. These measuring factors are the maximum deviation, the correlation coefficient and irregular deviation.

Keywords: RC6, Bitmap, Quality, Encryption.

التشفير الكتلي RC6 و اثنين من النسخ المعدلة

الخلاصة

مع التطور السريع لتبادل البيانات الرقمية، أمن المعلومات أصبح من المهم جدا في خزن البيانات ونقلها. ونتيجة لزيادة استخدام الصور في العملية الصناعية، فإنه من الضروري حماية البيانات السرية للصورة من الوصول غير المصرح به. في هذا البحث، تم تحليل RC6 مع اثنين من خوارزميات التشفير المعدلة وهي 512 bit RC6 و 640 bit RC6-Cascade للتحقق من كفاءة التشفير بالنسبة لهم الصور الرقمية وتوفير قياس رياضي جديد لتحقيق كفاءة التشفير.أعطيت النتائج التفصيلية من حيث التحليل الأمني والتنفيذ. دراسة المقارنة مع ثلاثة إصدارات RC6 من خوارزميات التشفير لإظهار تفوق الخوارزميات المعدلة. واعتمدت ثلاثة عوامل قياس الجودة لتقييم ومقارنة خوارزميات التشفير الثلاثة RC6، 512 bit RC6 ، و- 640 bit RC6 Cascade . هذه العوامل هي قياس الانحراف الأقصى، معامل الارتباط، وعدم انتظام الانحراف.

1. Introduction

In digital world nowadays, the security of digital images becomes more and more important since the communications of digital products over open network occur more and

* Control and Systems Department, University of Technology / Baghdad

https://doi.org/10.30684/etj.28.17.16
2412-0758/University of Technology-Iraq, Baghdad, Iraq

more frequently. Also, applications of digital imaging are prevalent and still continuously and rapidly increasing today, and yet the main obstacle in the widespread deployment of digital image services has been enforcing security and ensuring authorized access to sensitive data. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image communications and confidential video conferencing, etc.

In this regard, strong security technology is required to protect users' sensitive digital data. Encryption is the most trusted practical security technique for digital data in computer and communication systems [1].

In this paper some of related work will be presented. In [2] investigate the implementation and application of the RC5 block cipher algorithm for digital images and provide testing, verification, and encryption efficiency of the RC5 block cipher for digital images. In [3] a block-based transformation algorithm is proposed for image security using a combination of image transformation and encryption techniques. This algorithm will be used as a pre-encryption transform to confuse the relationship between the original images and the generated$ ones. The generated images are then fed to the Blowfish encryption algorithm. Correlation, histogram, and entropy have been used to measure the security level of the images. While in [4] encryption quality for bitmap images encrypted with rijndael and KAMKAR block ciphers will be measured.

In this paper, different Bitmap images are encrypted with RC6, 512 RC6 and 640 RC6-Cascade. The quality of the encrypted images are tested with visual inspection and evaluated with different quality of measuring algorithms.

2. 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 has six primitive operations, which are (+,−,<<<,>>>,×,⊕). 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, . . . , t − 1], consisting of key t = 2r + 4 w-bit words figure (1) shows the encryption with RC6. All details of RC6 are described in [5].

3. 512 Bit RC6 Block Cipher

This algorithm differs from the RC6 of 128 bits which could be used to encrypt and decrypt 512 bits block size. The structure of 512 bit RC6 is a Feistel network. It consists of splitting the plaintext into two 256 bit halves as shown in figure (2). Feistel ciphers are a special class of iterated block ciphers, where the ciphertext is calculated from the plaintext by repeated application of the same transformation or round function. The round function is applied to one half using a subkey and the output of F function is XORed with the other half. The two halves are then swapped. Each round follows the same pattern except for the last round where there is no swapping.

Each half of Feistel network is 256 bits. RC6 applied as round

function of Feistel network where the word is doubled to 64 bit instead of 32 bits in the 128 bit RC6 previous algorithm. All the operation of 512 RC6 is on 64 bits as shown in [6].

4. RC6-Cascade Block cipher

RC6-Cascade is 640-bit RC6-like block cipher. The plaintext is 640 bit which is divided into five parts p1, p2, p3, p4 and p5 each of which is 128 bit. The F-function in RC6-Cascade will be used cascaded design instead of rounds as it is shown in Figure (3). The output is 640 bit c1, c2, c3, c4, and c5 where each of is128 bit [7].

4.1 The F-function

The F-function of RC6-Cascaded uses two rounds of pervious RC6 algorithm in a Feistel network. The input of each function is two plaintexts of 128 bits and four subkey Si,Si+1,Si+2,Si+3 as shown in figure (4). The Feistel network consists of dividing the input into two halves, and applying a non-linear function only to the right half. The result is added into the left half and subsequently left and right half are swapped. Ciphers following this approach are called Feistel ciphers. The output of one nonlinear function is input directly to the next one, which increases the propagation of local changes. The non-linear function of RC6-Cascaded is the pervious RC6 algorithm [7].

5.1 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. The steps of this measure will be done as follows: 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).
- Compute the absolute difference or deviation between the two curves and present it graphically.
- 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:

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

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.

5.2 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, 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:

$$\text{Correlation Coefficient} = \frac{\text{cov}(x,y)}{s_x s_y}$$

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

5.3 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. It gives an attention to each individual pixel value and the deviation caused at every location of the input image before getting the histogram. This method can be summarized in the following steps:

- 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:

$$D = |I - J| \quad \ldots\ldots\ldots\ldots(4)$$

Where *I* is the input image, and *J* is the encrypted image.

- Construct the histogram distribution 'H' of the absolute deviation between the input image and the encrypted image. So, H = histogram (D).
- 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:

$$DC = \frac{1}{256}\sum_{i=0}^{255} h_i \quad \ldots\ldots\ldots(5)$$

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

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

$$AC(i) = |H(i) - DC| \quad \ldots\ldots\ldots(6)$$

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

$$ID = \sum_{i=-}^{255} AC(i) \quad \ldots\ldots\ldots(7)$$

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

x and y are gray-scale pixel values of the original and encrypted images.

6. Results and Discussion

In this paper, three different BMP images are evaluated. These images are 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,

Lena.bmp (Figure 6) as it is the reference image used in image processing research (it does not contain many high frequency components), and peppers.bmp (Figure 7) as an example of an image containing many high frequency components.

The three images are encrypted using RC6, 512 RC6, and 640 RC6-Cascaded. The results of the three measuring factors are given in table (1), where (D) indicates the Maximum Deviation measure, (C.C.) indicates the Correlation Coefficient measure, and (ID) indicates the Irregular Deviation measure. With the measure of the Maximum Deviation (D) the greater is the better; with the Correlation Coefficient (C.C) the closer to zero is the better, while with the Irregular Deviation (ID) the smaller is the better. Based on the figures (1),(2) and (3),which show the histograms for images and each encryption method, we see that the Irregular Deviation (ID) 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 the Irregular Deviation (ID) agrees with other measuring factor, it will be good judging, otherwise the final decision on measuring the quality of the encryption algorithms will be based on the Irregular Deviation (ID) which is based on each pixel value.

Nike.bmp image with The Correlation Coefficient (C.C), 512 RC6 gives a greater result than the other ciphers, and 640 RC6-cascaded gives the smallest result. But by visual inspection of the histograms for encrypted images in Figures (1), (2), and (3), the best hiding of all the features is achieved with 640 RC6-cascaded, 512 RC6, and RC6 respectively. So, the Maximum Deviation (D) is not accurate in some cases. With the Correlation Coefficient (C.C), 640 RC6-cascaded is closer to zero than the others. With the Irregular Deviation (ID), 640 RC6-cascaded is smaller than theothers and 512 RC6 gives result greater than RC6. The Correlation Coefficient (C.C) measurement 640 RC6-cascaded is the best one.

Lena.bmp image with The Correlation Coefficient (C.C), 512 RC6 gives a result that is greater than the other ciphers and RC6 gives the smallest result. With the Correlation Coefficient (C.C), 640 RC6- Cascaded is the closest to zero and 512 RC6 is closer to zero than RC6. With the Irregular Deviation (ID), RC6 gives the smallest result and 640 RC6-Cascaded gives result higher than 512 RC6. So, 640 RC6-Cascaded is the best one.

Peppers.bmp image with the Maximum Deviation (D), RC6 gives greater than 512 RC6 and 640 RC6-cascaded is better than 512RC6. With the Correlation Coefficient (C.C), 640 RC6-cascaded is closer to zero than the others. With the Irregular Deviation (ID), RC6 gives the smallest result and 512 RC6 is smaller than 640 RC6-cascaded. So, the best result with 640 RC6-cascaded will be achieved table (1) will be showed these results.

Note that:

1) All programs which applied 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 D, C.C, and ID are designed by MATLAB 7.6 on the same machine.

Conclusions

This paper inspected three encryption algorithms RC6, 512 bit

RC6, and 640 bit RC6-Cascade on encrypting images of different constructions. Three evaluating measuring factors are considered, in addition to visual inspection. With most of the measuring factors, RC6-Cascade achieved the best result on images of binary data.

References

[1] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah," Encryption

Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", International Journal of Computer, Information, and Systems Science, and Engineering vol.1,pp.33-39, Winter 2007.

[2] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah," Encryption quality analysis of the RC5 block cipher algorithm for digital images", Opt. Eng., Vol. 45, 107003 (2006); doi:10.1117/1.2358991.

[3] Mohammed A. Younes, "AN APPROACH TO ENHANCE IMAGE ENCRYPTION USING BLOCK BASED TRANSFORMATION ALGORITHM", Thesis, University Sains Malaysia, 2009.

[**4]** Elkamchouchi, H.M.; Makar, M.A.,"Measuring encryption quality for bitmap images encrypted with rijndael and KAMKAR block ciphers**",** Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National, Volume, Issue , March 15-17, 2005 Page(s): 277 – 284

[5] R. L. Rivest, M. J. B. Robshaw, R. Sidney,and Y. L. Yin, " The RC6TM Block Cipher" , 1998. http://www.rsasecurity.com/rsalabs/rc6/

[6] Ashwaq T. Hashim , Janan A. Mahdi and Salma H. Abdullah," The Proposal 512-bits RC6 Encryption Algorithm", accepted at IJCCCE, Univ. of Technology ,2009.

[7] Ashwaq T. Hashim and Yossra H. Ali, "Proposed Cascaded Design of 640-bit RC6 Block Cipher", First Conferences of Computer Science Dept., Univ. of Technology, 2-3 Feb., 2010.

[8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based Algorithm for Image Encryption", PROCEEDINGS of World Academy of Science, Engineering And Technology Volume 21 May 2007 Issn 1307-6884

Table (1) Quality measures for RC6, 512 RC6, and RC6_ Cascade encrypted images

Cipher	RC6			512 RC6			640 RC6-Cascade		
	D	C.C	ID	D	C.C	ID	D	C.C	ID
Nike	50358	0.0330	28570	50362	-0.0528	29686	50256	0.0113	31285
Lena	12686	0.0024	38482	12916	0.0144	38247	12658	0.000355	38582
Peppers	46915	-.00074863	50613	46783	-0.0087	50652	46927	-0.0177	50655

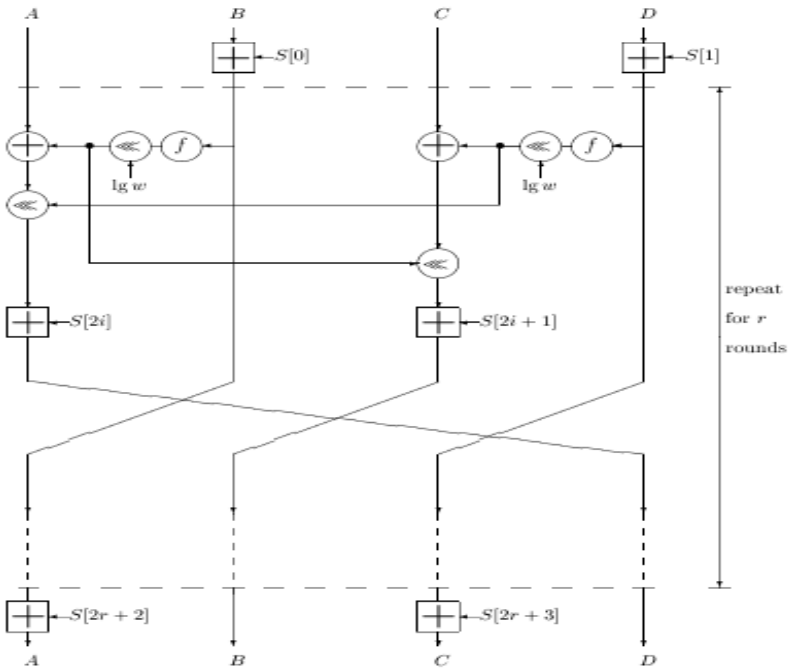

Figure 1: Encryption with RC6 –*w/r/b*. Here *f(x) =x (2x+1)*.

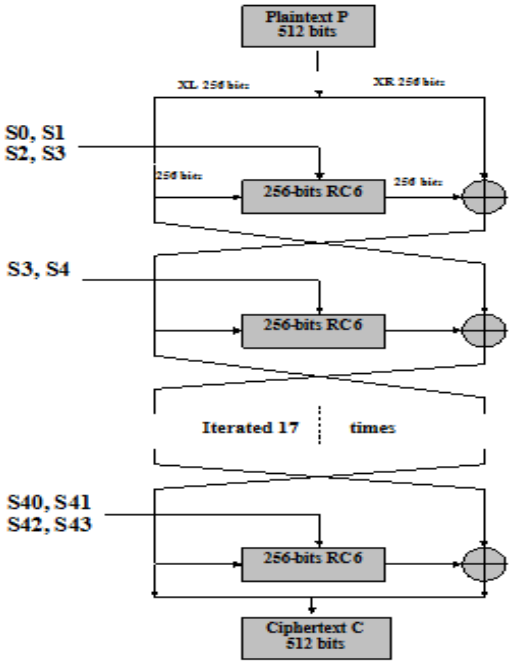

Figure 2: The Encryption with 512 bit RC6 where w=64

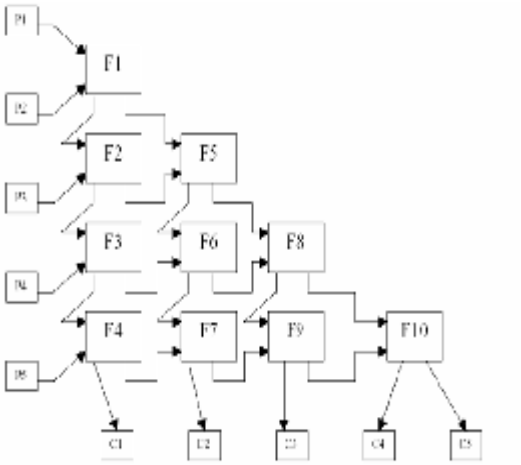

Figure 3: The Encryption with 640 bit RC6-Cascade

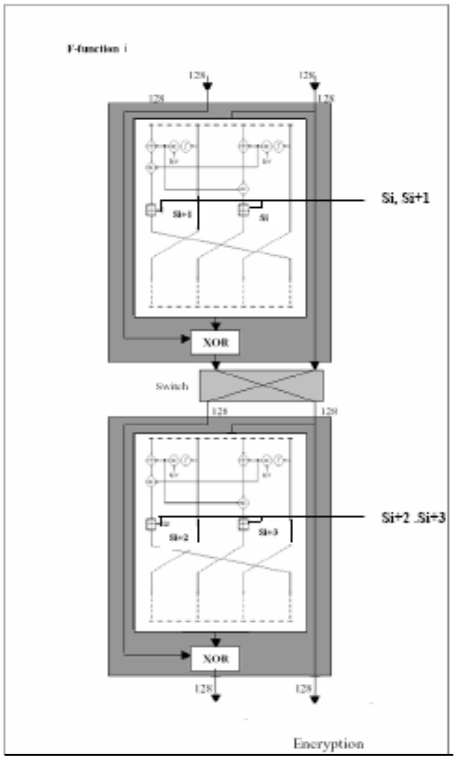

Figure 4: The F-function of RC6-Cascaded

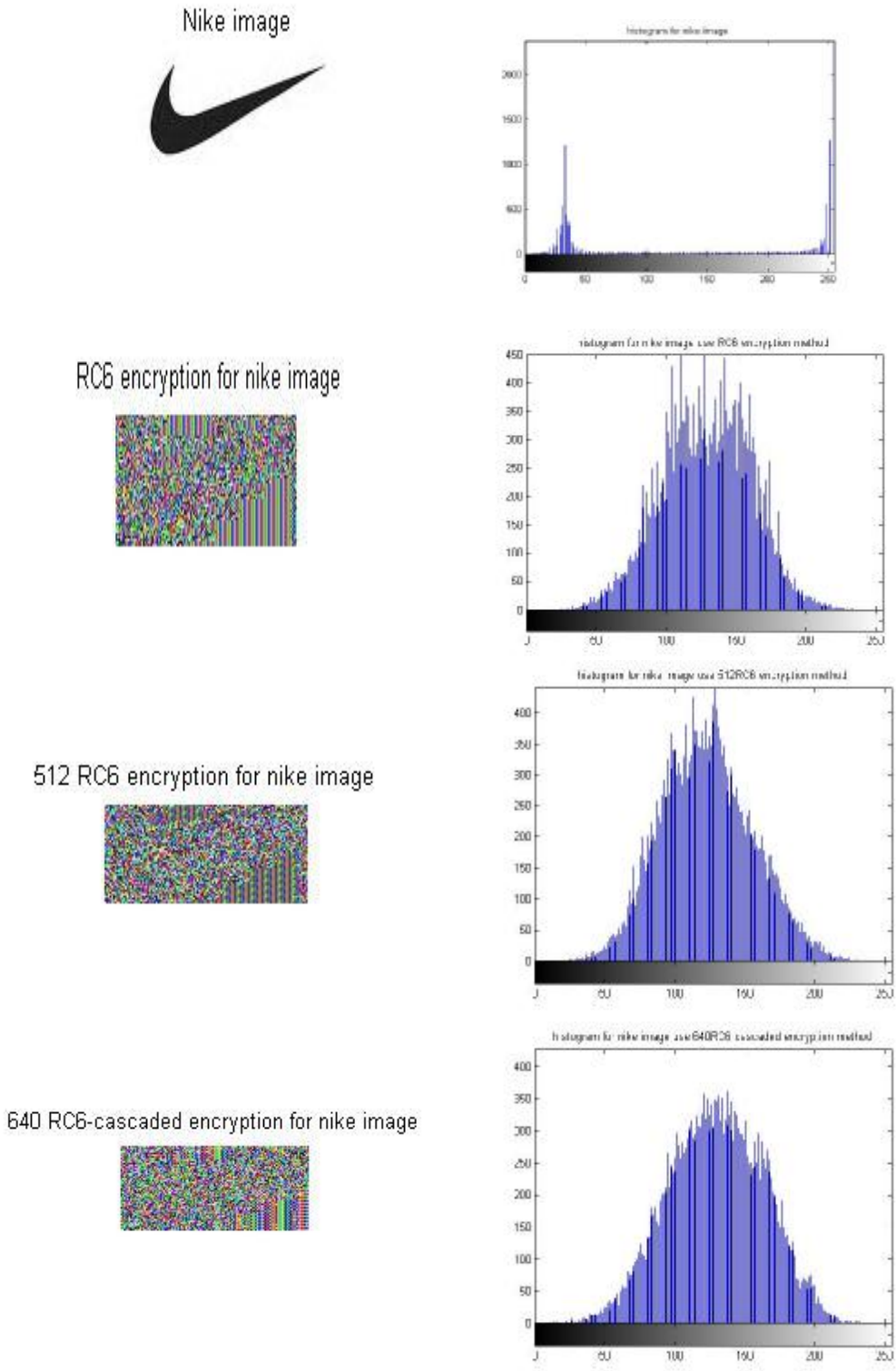

Figure 5: Encryption of Nike.bmp by RC6, 512 bit RC6, and 640 bit RC6-Cascade

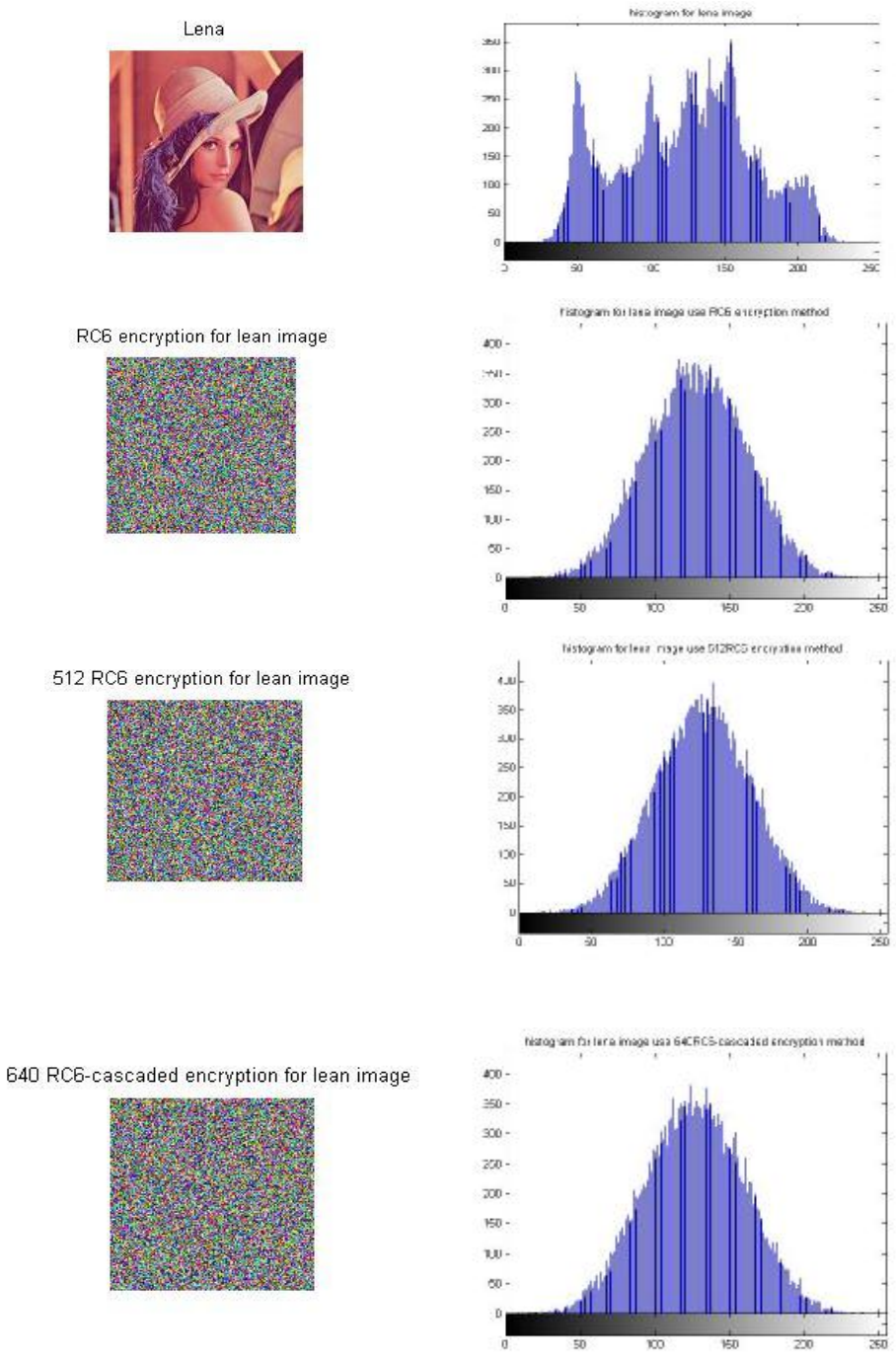

Figure 6: Encryption of Lena.bmp by RC6, 512 bit RC6, and 640 bit RC6-Cascade

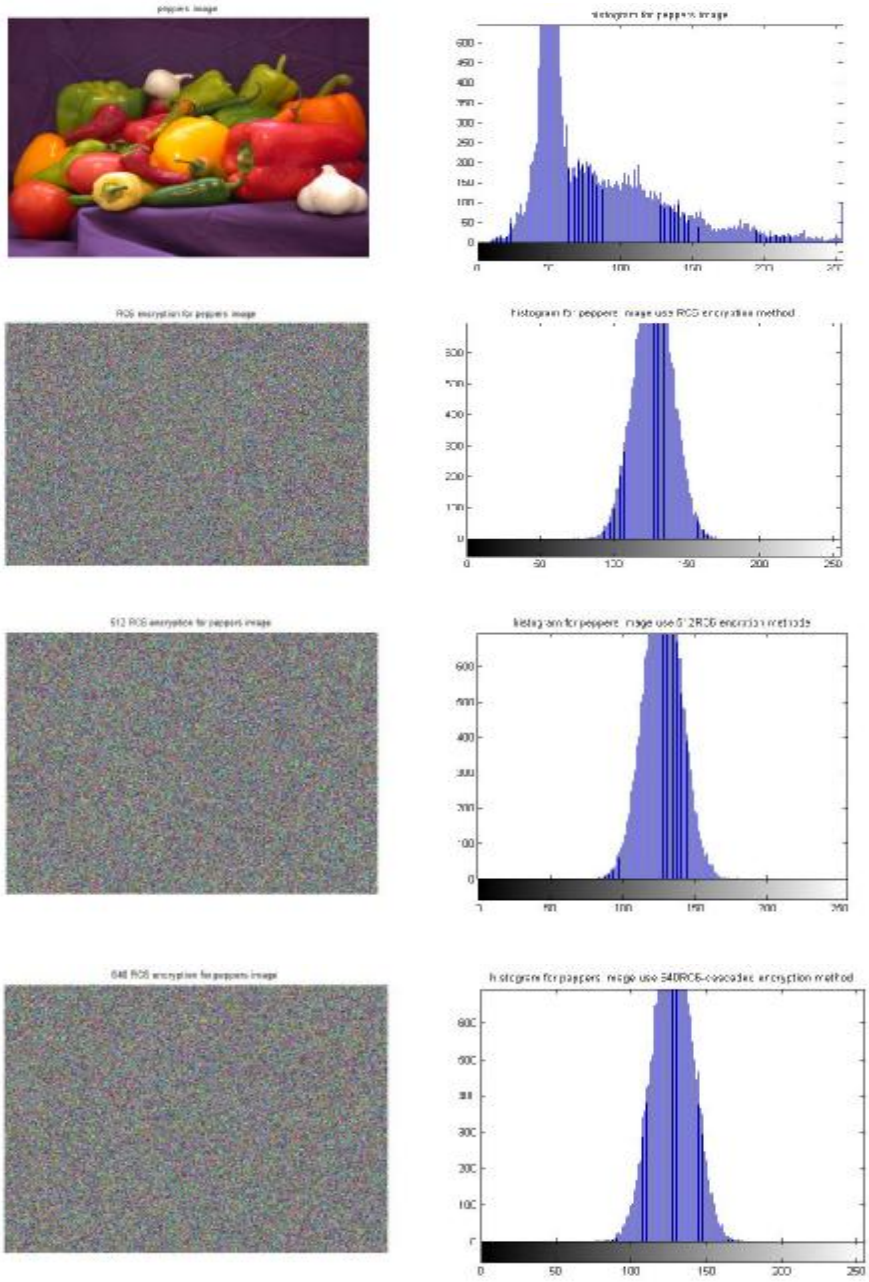

Figure 7: Encryption of Peppers.bmp by RC6, 512 bit RC6, and 640 bit RC6-Cascade