Hameed et al. Iraqi Journal of Science, 2018, Vol. 59, No.1B, pp: 434-446
DOI:10.24996/ijs.2018.59.1B.24

Iraqi Journal of Science

ISSN: 0067-2904

Image Encryption Using DNA Encoding and RC4 Algorithm

Sarab M. Hameed*[1], Hiba A. Sa'adoon[1], Mayyadah Al-Ani[2]
[1]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq.
[2]Douglas College, British Columbia, Canada.

Abstract

Nowadays, the rapid development of multi-media technology and digital images transmission by the Internet leads the digital images to be exposed to several attacks in the transmission process. Therefore, protection of digital images become increasingly important.

To this end, an image encryption method that adopts Rivest Cipher (RC4) and Deoxyribonucleic Acid (DNA) encoding to increase the secrecy and randomness of the image without affecting its quality is proposed. The Means Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Coefficient Correlation (CC) and histogram analysis are used as an evaluation metrics to evaluate the performance of the proposed method. The results indicate that the proposed method is secure against statistical attacks and provides a good security without affecting the quality of the image.

Keywords: Image encryption, Symmetric encryption, RC4 algorithm, DNA encoding.

تشفيرالصورة باستخدام ترميز الحمض النووي وخوارزمية RC4

سراب مجيد حميد*[1]، هبة عبد الزهرة سعدون[1]، ميادة العاني[2]
[1]قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق.
[2]كلية دوغلاس، كولومبيا البريطانية، كندا.

الخلاصة

في الوقت الحاضر، التطور السريع في تكنولوجيا الوسائط المتعددة ونقل الصور الرقمية باستخدام الانترنت أدى الى تعرض الصور الرقمية لعدة هجمات اثناء عملية النقل. لذا أصبحت حماية الصور الرقمية ذات أهمية متزايدة.

ولتحقيق هذه الغاية، اقترحت طريقة تشفير الصورة التي تعتمد تشفير رافست (RC4) وترميز الحمض النووي (DNA) لزيادة سرية وعشوائية الصورة دون التاثير على جودتها. متوسط مربع الخطأ، ذروة الإشارة بالنسبة الى الضوضاء، معامل الارتباط وتحليل المخطط البياني استخدمت كمقاييس تقييم لتقييم أدآء الطريقة المقترحة. تشير النتائج الى ان الطريقة المقترحة آمنة ضد الهجمات الإحصائية وقادرة على توفير الأمن دون التاثير على جودة الصورة.

1. Introduction

In the recent years, the need for protecting valuable information from illegal access is increasing and the necessity raised to produce a secure communication for exchanging confidential information, the information can be audio, video, or image. One means to produce such secure communication is to

*Email: sarab_majeed@yahoo.com

modify the transmitted data shape via using encryption. In the process of the encryption, the data is encrypted by utilizing a secret key and an encryption method. Various encryption algorithms are used for image encryption in a wide area of application. Therefore, the image encryption becomes the common effective means to ensure transmit security of images [1, 2].

The Deoxyribonucleic Acid (DNA) cryptography represents a new and promising direction in cryptography research. DNA can be employed in cryptography for storing and carrying the information, in addition to computation. DNA is proved to be very powerful in cryptography, cryptanalysis and steganography problems. Hence, DNA can be utilized in cryptography to achieve an improvement in security and speed to the other cryptography methods. At a recent time, image encryption based on DNA becomes more and more popular [3]. In this paper, a new colored image encryption method that combines DNA operations and Rivest Cipher (RC4) algorithm for transmitting an image in a secure way is introduced.

The rest of this paper is organized as follows. The related work is presented in section 2. The RC4 and DNA encoding are briefly described in section 3. Section 4 presents the evaluation metrics that are used to evaluate the proposed image encryption. Section 5 introduces the proposed image encryption in detail. The results of the proposed encryption image method are then evaluated in section 6. Section 7 presents the comparison results with other methods. Finally, section 8 provides the conclusions and some hints for future work.

2. Related Works

DNA cryptography is a rapidly rising field of DNA computing research to afford a powerful cryptographic technique. The following points illustrate some works that exploit either RC4 or DNA encoding.

1. Liu et al. in 2012 [4] proposed an algorithm for Red Green Blue (RGB) image encryption using DNA encoding and chaotic map. The result clarifies that the proposed algorithm is appropriate for RGB image encryption. Due to it has a big secret keyspace and it can withstand brute force attack, statistical attack.

2. Ginting and Dillak in 2013 [5] proposed an algorithm for encrypting an image that utilizes RC4 stream cipher algorithm and chaotic logistics map. The results demonstrate that the ability of the proposed algorithm encrypt image without losing any information and eliminate the correlation between plain image and cipher image.

3. Huang and Ye in 2014 [6] proposed an image encryption algorithm using hyper-chaos and DNA sequence. To counter the known-plaintext and chosen-plaintext attacks, the secret keys are dependent on the plain image. The results show the efficiency of the proposed algorithm.

4. Kumar et al. in 2015 [7] proposed an RGB image encryption algorithm using diffusion method with a combination of chaotic maps. The results with two standard images show that the proposed algorithm offers high security and is suitable for practical image encryption.

5. Jain and Rajpal in 2016 [8] used DNA operations and chaotic maps for an image encryption algorithm. The results clarify that proposed algorithm was strong for known plaintext attack, statistical attacks and differential attacks.

6. Kumar et al. in 2016 [9] proposed an image encryption algorithm that adopts Elliptic Curve Cryptography (ECC) and DNA encoding. Standard test mages are used for evaluation the performance of the proposed algorithm. The results show that the proposed algorithm can resist brute force attack.

7. Zhen et al. in 2016 [10] proposed image encryption method that takes the benefit of DNA encoding, the chaotic system, and information entropy for a secure image. The experimental result shows that the proposed method is resisting different attacks, brute-force attack, statistical attack, differential attack, and chosen-plaintext attack.

8. Wang and Liu in 2017 [11] proposed an image encryption algorithm by combing chaos and DNA encoding rules. Piecewise Linear Chaotic Map (PWLCM) and Logistic Map are utilized to produce all parameters the algorithm needs and DNA encoding. The results show that the ability of the proposed algorithm to withstanding typical attacks.

9. Chai et al. in 2017 [12] presented an image encryption method based on DNA sequence operations, chaotic system and Secure Hash Algorithm 256 (SHA 256). First, a plain image is encoded into a DNA matrix. Then, wave-based permutation and row-by-row diffusion operations performed on it.

The results demonstrate that the proposed method has a good encryption effect, larger secure keyspace, and a high sensitivity to the secret key and to the plain image.

3. Preliminaries

3.1 RC4 Algorithm Description

RC4 is referred to as “ARCFOUR” or “ARC4” and represents as one of the common state-of-the-art software stream ciphers used by wide industrial applications. RC4 is utilized in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards. It is also used in the Wired Equivalent Privacy (WEP) protocol and the newer WiFi Protected Access (WPA) protocol that is part of the Institute of Electrical and Electronics Engineers 802.11 (IEEE 802.11) wireless Local Area Network (LAN) standard. RC4 involves two integer indices and a one-dimensional integer array. The RC4 cipher has two components, namely, the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA) [13].

1. The KSA uses the key (K) to shuffle the elements of S. The KSA uses the symmetric key to permute an array S that contains 256 entries. S array is initialized with identity permutation ranging from 0 to 255. Then, a loop of 256 iterations is used to generate a random permutation of the array S, where the entries of the S array are continually swapped using the key value.

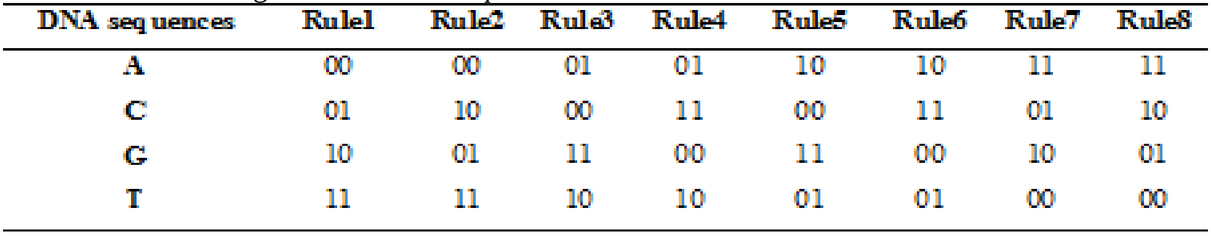
2. The PRGA uses this scrambled permutation to generate pseudo-random key stream bytes. In the PRGA, two indices i, j are initialized to zero. In each iteration, i is recomputed as $(\mathrm{i}+1) \bmod 256$ and j is recomputed as $(\mathrm{j}+\mathrm{S}[\mathrm{i}]) \bmod 256$, and then a swap operation is conducted between $\mathrm{S}[\mathrm{i}]$ and $\mathrm{S}[\mathrm{j}]$. The keystream that is XORed with plaintext is generated as $\mathrm{S}[(\mathrm{S}[\mathrm{i}]+\ \mathrm{S}[\mathrm{j}]) \bmod 256]$.

3.2DNA Encoding

DNA cryptography is a technology of bioscience to encrypt the large message and in a compressed size. DNA is a class of organic macromolecule and is composed of nucleotides that hold a separate base. Four kinds of bases have existed: Adenine (A) and Thymine (T) or Cytosine (C) and Guanine (G) [14].

DNA bases join with each other. This means ‘A’ constantly joins with ‘T’, and ‘C’ constantly joins with ‘G’. That is, ‘A’ and ‘T’, and ‘C’ and ‘G’ are corresponding pairs, respectively. The binary system is used to process and store the information in computers, wherever ‘0’ and ‘1’ are complementary. Accordingly, it can be concluded that ‘00’ and ‘11’ are complementary, and ‘01’ and ‘10’ are also complementary. Twenty four kinds of coding schemes can be deduced when the binary numbers ‘00’, ‘01’, ‘10’ and ‘11’ are applied to describe four bases ‘A’, ‘C’, ‘G’ and ‘T’ respectively, but only eight kinds satisfy the complementary rule of Watson-Crick [15]. Table-1 clarifies the eight encoding rules for DNA sequences.

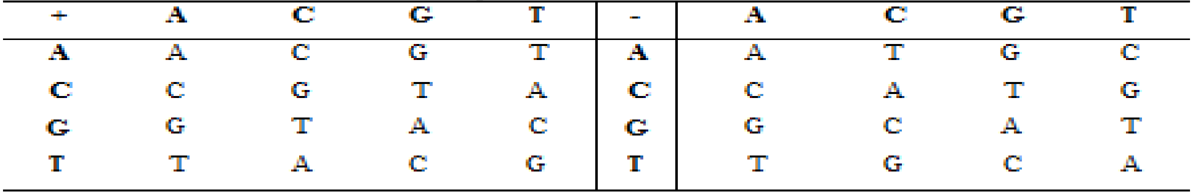
Table 1-The encoding rules for DNA sequences.



DNA sequences	Rule1	Rule2	Rule3	Rule4	Rule5	Rule6	Rule7	Rule8
A	00	00	01	01	10	10	11	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

Several biological and algebraic operations for the DNA sequences are propose by the researchers. These operations are addition and subtraction. The subtraction is the inverse operation of addition; however, the structure is not double helix. Table-2 reports the addition and subtraction rules [16].

Table 2-DNA addition and subtraction operations.



+	A	C	G	T	-	A	C	G	T
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

4. Evaluation Metrics

The Means Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Coefficient Correlation (CC) and histogram analysis metrics are used to evaluate the performance of the proposed encryption method.

1. The MSE is a quantitative measure that clarifies the difference between original image and encrypted image. The MSE between the original image and the corresponding encrypted image is calculated as in Equation 1 [17].

$$MSE = \frac{1}{M\times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[(f^{\sim}(x,y) - f(x,y)]^2 \tag{1}$$

Where $M \times N$ size of image, (x, y) is the position of the pixels, $f(x, y)$ is the original image and $f^{\sim}(x, y)$ is the encrypted image.

2. PSNR is used to evaluate the image quality as formulated in Equation 2 [18].

$$PSNR = 20\log_{10}\left(L/\sqrt{MSE}\right) \tag{2}$$

Where MSE is mean square error.
L is the maximum possible pixel value of the image.

3. Coefficient correlation is used to analyze the relationship between two neighboring pixels. It is

$$r_{x,y} = \frac{cov(x,y)}{\sqrt{D_x}\sqrt{D_y}} \tag{3}$$

$$cov(x,y) = E\big[\big(x - E(x)\big)\big(y - E(y)\big)\big] \tag{4}$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \tag{5}$$

$$D_x = \frac{1}{L}\sum_{i=1}^{L}\big(x_i - E(x)\big)^2 \tag{6}$$

Where x and y are the value of the adjacent pixels, and L is the number of samples taken.

5. The Proposed Image Encryption Method

Vvcvbb The proposed image encryption method is based on the combination of RC4 algorithm and DNA coding. The proposed method consists of two layers. In the first layer, RC4 is utilized to encrypt an image. In the second layer, the encrypted image is transformed into DNA sequences.

5.1 Image Encryption via RC4 and DNA

An RGB image is disintegrated into three components $R, G,$ and B. Then, each component is encrypted independently using RC4 with a secret key to produce three encrypted components R_{En}, G_{En} and B_{En} . Next, R_{En}, G_{En} and B_{En} components are converted separately to binary numbers. After that, the binary numbers of each component are converted to DNA sequence depending on Rule 1 in Table-1 to obtain three DNA matrices RD_E, GD_E and BD_E that are expressed in four nucleic acid bases Next, DNA addition operation was applied on RD_E, GD_E and BD_E using equation 7, 8 and 9 to get three DNA encoded matrices RC_E, GC_E and BC_E.

$$RC_E(x,y) = RD_E(x,y) + GD_E(x,y) \tag{7}$$

$$GC_E(x,y) = GD_E(x,y) + BD_E(x,y) \tag{8}$$

$$BC_E(x,y) = BD_E(x,y) + GC_E(x,y) \tag{9}$$

Where RD_E, GD_E and GD_E are image components and x, y are the coordinate of the pixel.

Finally, the DNA matrices RC_E, GC_E and BC_E are decoded and convert to an RGB image that represents the encrypted image. Algorithm 1 clarifies the steps of the proposed image encryption method.

5.2 Image Decryption via RC4 and DNA

The process of image decryption is similar to the encryption process but the steps are taken by the reverse order. This means the image should be decoded using DNA encoding then decrypted using RC4 and a secret key.

An encrypted image RGB image is disintegrated into three components R, G, and B. Then, each component is converted to binary numbers. Next, each component is transformed to DNA sequence. After that, the DNA subtraction operation using the following equation.

$$BD_E\,(x,y) = BC_E(x,y) - GC_E(x,y) \tag{10}$$

$$GD_E(x,y) = GC_E(x,y) - BD_E(x,y) \tag{11}$$

$$RD_E(x,y) = RC_E(x,y) - GD_E(x,y) \tag{12}$$

Where BC_E, GC_E and RC_E are image components. And x, y are the coordinate of the pixel.

Finally, each component is decrypted separately using RC4 and a secret key that is identical to the encryption key to get the decrypted image similar to the original image.

Algorithm 1: The Proposed Image Encryption

Input:
$\boldsymbol{I}$: Original RGB Image
$\boldsymbol{K}$: Secret key.

Output:
I' **:** Encrypted Image.

```
1:  Permute $S$ depending on $K$
    $set\ \ n = 256$
    $set\ \ l = |K|$
    $set\ \ j = 0$
    $\boldsymbol{for}\ i = 0\ to\ n-1\ \boldsymbol{do}$
      $set\ \ S_i = i$
    $\boldsymbol{for}\ i = 0\ to\ n-1\ \boldsymbol{do}$
        $j = (j + S_i{+}k_{i\ mod\ l})\ mod\ n$
       $swap\ (\ S_i\ , S_j)$
     $\boldsymbol{End}$
2:  Decompose image $\boldsymbol{I}$ of size $\boldsymbol{MXN}$ into three components $\boldsymbol{R}, \boldsymbol{B}, \boldsymbol{G}$
3:  $set\ \ i$ =0
    $set\ \ j = 0$
    $\boldsymbol{for}\ k = 0\ to\ M-1$
    $\boldsymbol{for}\ h = 0\ to\ N-1$
    $i\ \leftarrow (i+1)\ mod\ N$
    $j \leftarrow (j + S_i)\ \ mod\ N$
    $swap\ (\ S_i\ , S_j)$
    $set\ t\ \leftarrow (S_i + S_j)\ mod\ N$
    $R_{En}(k,h) = S_t \oplus R$
    $G_{En}(k,h) = S_t \oplus G$
    $B_{En}(k,h) = S_t \oplus B$
    $\boldsymbol{End}$
    $\boldsymbol{End}$
4:  Encoding $\boldsymbol{R_{En}}$, $\boldsymbol{G_{En}}$ and $\boldsymbol{B_{En}}$DNA Sequence
    $\boldsymbol{for}\ k = 0\ to\ M-1$
    j=0
    $\boldsymbol{for}\ h = 0\ to\ N-1$
    Find 8-bit binary representation of $R_{En}(k,h), G_{En}(k,h)$ and $B_{En}(k,h)$
    Represent 8-bit binary representation of $R_{En}(k,h), G_{En}(k,h)$ and $B_{En}(k,h)$ in a DNA
    sequence by four DNA bases.
    Store DNA bases in
                    $RD_E(i,j), RD_E(i,j+1), RD_E(i,j+2), RD_E(i,j+3)$
                    $GD_E(i,j), GD_E(i,j+1), GD_E(i,j+2), GD_E(i,j+3)$
                    $BD_E(i,j), BD_E(i,j+1), BD_E(i,j+2), BD_E(i,j+3)$
    $j\ =\ (j\ +\ 4)\ mod\ 4N$
    $\boldsymbol{End}$
    $\boldsymbol{End}$
```

```
5:  Perform the DNA Addition Operation
    $\boldsymbol{for}\ k = 0\ to\ M-1$
    $\boldsymbol{for}\ h = 0\ to\ 4N-1$
    $RC_E(k,h) = RD_E(k,h) + GD_E(k,h)$
    $GC_E(k,h) = GD_E(k,h) + BD_E(k,h)$
    $BC_E(k,h) = BD_E(k,h) + GC_E(k,h)$
    $\boldsymbol{End}$
    $\boldsymbol{End}$
```

```
6:  Recombine
    $\boldsymbol{for}\ k = 0\ to\ M-1$
    j=0
    $\boldsymbol{for}\ h = 0\ to\ N-1$
    Find a DNA sequence representation of $RC_E(k,h), GC_E(k,h)$ and $BC_E(k,h)$
    Represent four DNA bases of $RC_E(k,h), GC_E(k,h)$ and $BC_E(k,h)$ in 8-bit binary representation.
    Store binary representation in
        $RR_d(i,j), RR_d(i,j+1), RR_d(i,j+2), RR_d(i,j+3), RR_d(i,j+4), RR_d(i,j+5), RR_d(i,j+6), RR_d(i,j+7)$
        $RG_d(i,j), RG_d(i,j+1), RG_d(i,j+2), RG_d(i,j+3), RG_d(i,j+4), RG_d(i,j+5), RG_d(i,j+6), RG_d(i,j+7)$
        $RB_d(i,j), RB_d(i,j+1), RB_d(i,j+2), RB_d(i,j+3), RB_d(i,j+4), RB_d(i,j+5), RB_d(i,j+6), RB_d(i,j+7)$
    $j = (j+7)\ mod\ 7N$
    $\boldsymbol{End}$
    $\boldsymbol{End}$
    $I'$ = Compose ($RR_d, RG_d, RB_d$)
```

6. Results

The proposed method is coded in vb.net and the experiments are conducted on an HP ProBook 450 G3 laptop with Intel(R) Core (TM) i7-6500U, CPU@ 2.50 GHz and a Memory of 8.00 GB RAM and 64-bit system type. The performance of the proposed method is evaluated using the image dataset of Signal and Image Processing Institute (SIPI) maintained by University of South California (USC) [19] an evaluation data. The original and cipher images are displayed in Figure-1. The results show that all cipher images are wholly distorted which means that the proposed method has a good encryption result.

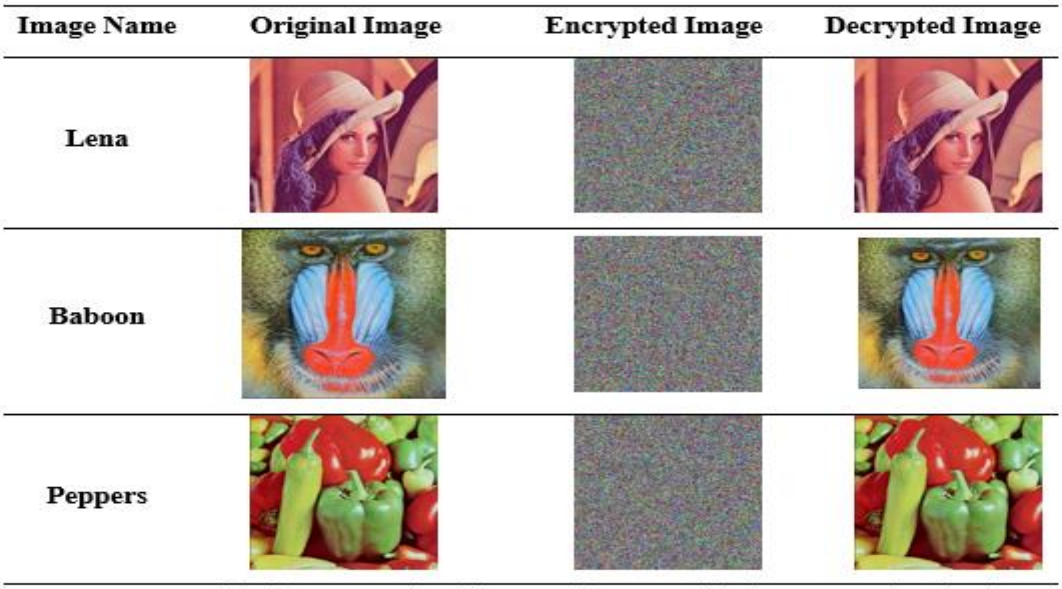


Figure 1: Original, encrypted and decrypted images with the proposed method.

6.1 Image Quality

MSE and $PSNR$ are used to evaluate the quality of an image when the proposed encryption and decryption methods are applied. Tables-(3, 4) report the MSE value and $PSNR$ value of encrypted images and decrypted images using the proposed method and RC4 algorithm. The results point out that MSE value between the encrypted image and the original image is large. Furthermore, the MSE value between the decrypted image and the original image is zero. This means that the proposed encryption is lossless image encryption (i.e. the original image and decrypted image are identical). In addition, the results show that $PSNR$ values between the original and encrypted images using the proposed method are smaller than using the RC4 encryption algorithm only. This means that the proposed encryption has better security effect than RC4. In addition, $PSNR$ value is infinite between the decrypted image and the original image. This indicates that the decrypted image is like to the original image.

Table 3: MSE and PSNR values of encrypted image using the proposed method and RC4 algorithm.

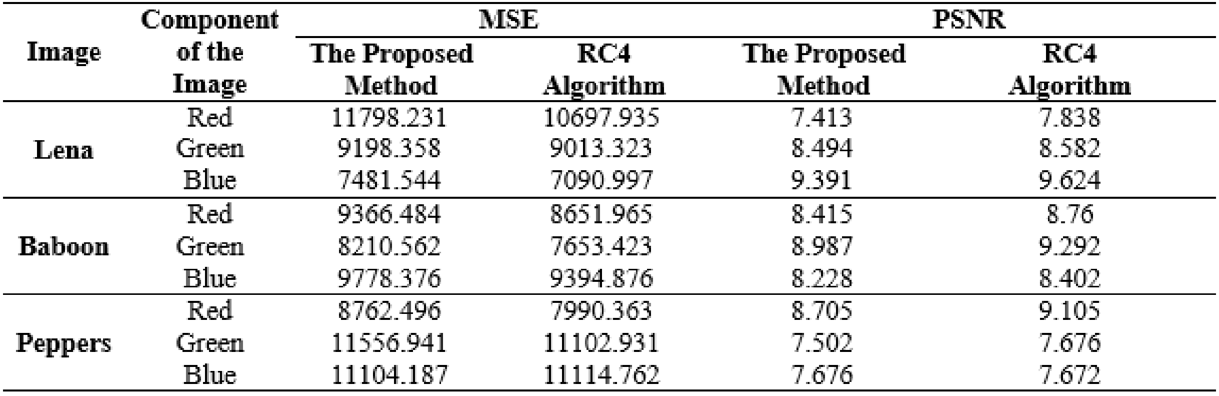


Image	Component of the Image	MSE		PSNR	
		The Proposed Method	RC4 Algorithm	The Proposed Method	RC4 Algorithm
Lena	Red	11798.231	10697.935	7.413	7.838
	Green	9198.358	9013.323	8.494	8.582
	Blue	7481.544	7090.997	9.391	9.624
Baboon	Red	9366.484	8651.965	8.415	8.76
	Green	8210.562	7653.423	8.987	9.292
	Blue	9778.376	9394.876	8.228	8.402
Peppers	Red	8762.496	7990.363	8.705	9.105
	Green	11556.941	11102.931	7.502	7.676
	Blue	11104.187	11114.762	7.676	7.672

Table 4: MSE and PSNR values of decrypted image using the proposed method and RC4 algorithm.

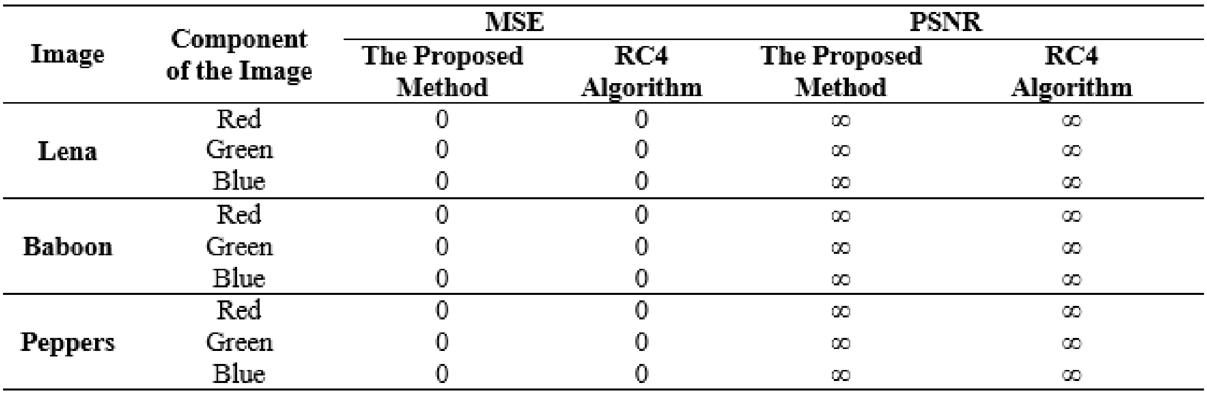


Image	Component of the Image	MSE		PSNR	
		The Proposed Method	RC4 Algorithm	The Proposed Method	RC4 Algorithm
Lena	Red	0	0	∞	∞
	Green	0	0	∞	∞
	Blue	0	0	∞	∞
Baboon	Red	0	0	∞	∞
	Green	0	0	∞	∞
	Blue	0	0	∞	∞
Peppers	Red	0	0	∞	∞
	Green	0	0	∞	∞
	Blue	0	0	∞	∞

6.2 Security Analysis

Coefficient correlation and histogram analysis are used to show the ability of the proposed encryption method to resist the statistical attacks.

6.2.1 Coefficient Correlation

Generally, images have highly correlated with its neighboring pixel whether in horizontal, vertical and diagonal direction. For testing purpose, 5000 pairs of adjacent pixels in three directions from the original image and the corresponding cipher image are randomly selected. Table-5 through 7 report the correlated coefficient in horizontal, vertical and diagonal directions for the original image and the corresponding encrypted image. The results demonstrate that the correlation of the encrypted images is so small. This means that the proposed encryption method capable to resist the statistical attacks. The scatter plots of three directions horizontal, vertical and diagonal for Lena image and the corresponding encrypted image using the proposed method and RC4 are depicted in Figures-2 through 4.

Table 5: Correlation coefficients of two adjacent pixels in the original image and the corresponding cipher image in horizontal direction.

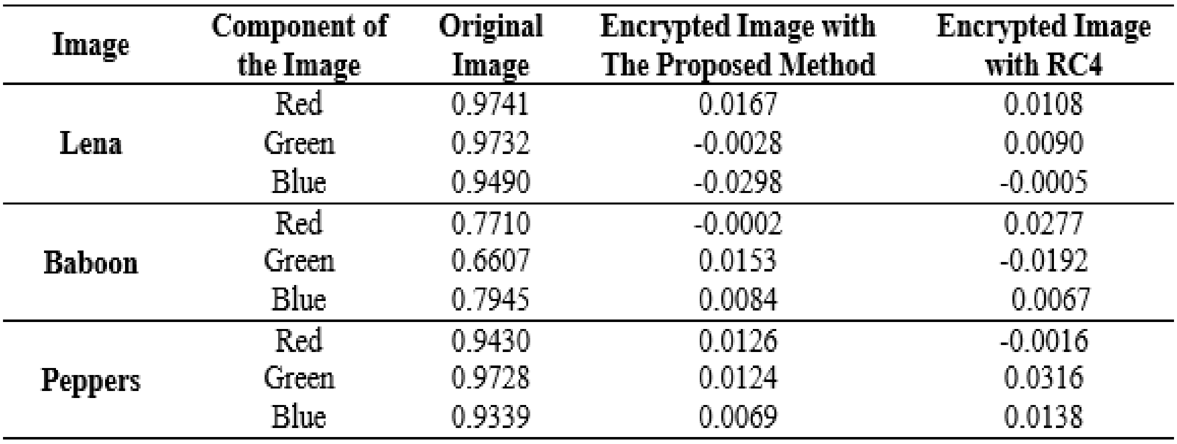


Image	Component of the Image	Original Image	Encrypted Image with The Proposed Method	Encrypted Image with RC4
Lena	Red	0.9741	0.0167	0.0108
	Green	0.9732	-0.0028	0.0090
	Blue	0.9490	-0.0298	-0.0005
Baboon	Red	0.7710	-0.0002	0.0277
	Green	0.6607	0.0153	-0.0192
	Blue	0.7945	0.0084	0.0067
Peppers	Red	0.9430	0.0126	-0.0016
	Green	0.9728	0.0124	0.0316
	Blue	0.9339	0.0069	0.0138

Table 6: Correlation coefficients of two adjacent pixels in the original image and the corresponding cipher image in vertical direction.

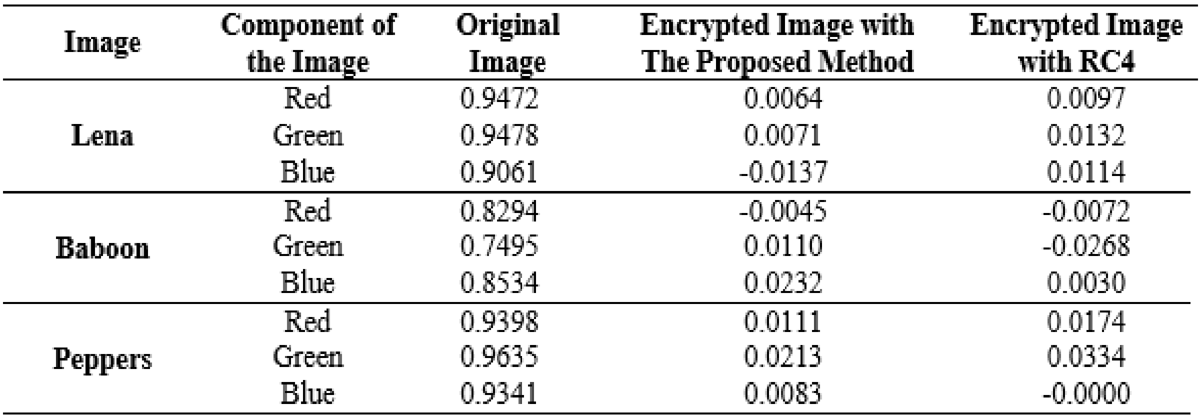


Image	Component of the Image	Original Image	Encrypted Image with The Proposed Method	Encrypted Image with RC4
Lena	Red	0.9472	0.0064	0.0097
	Green	0.9478	0.0071	0.0132
	Blue	0.9061	-0.0137	0.0114
Baboon	Red	0.8294	-0.0045	-0.0072
	Green	0.7495	0.0110	-0.0268
	Blue	0.8534	0.0232	0.0030
Peppers	Red	0.9398	0.0111	0.0174
	Green	0.9635	0.0213	0.0334
	Blue	0.9341	0.0083	-0.0000

Table 7: Correlation coefficients of two adjacent pixels in the original image and the corresponding cipher image in diagonal direction.

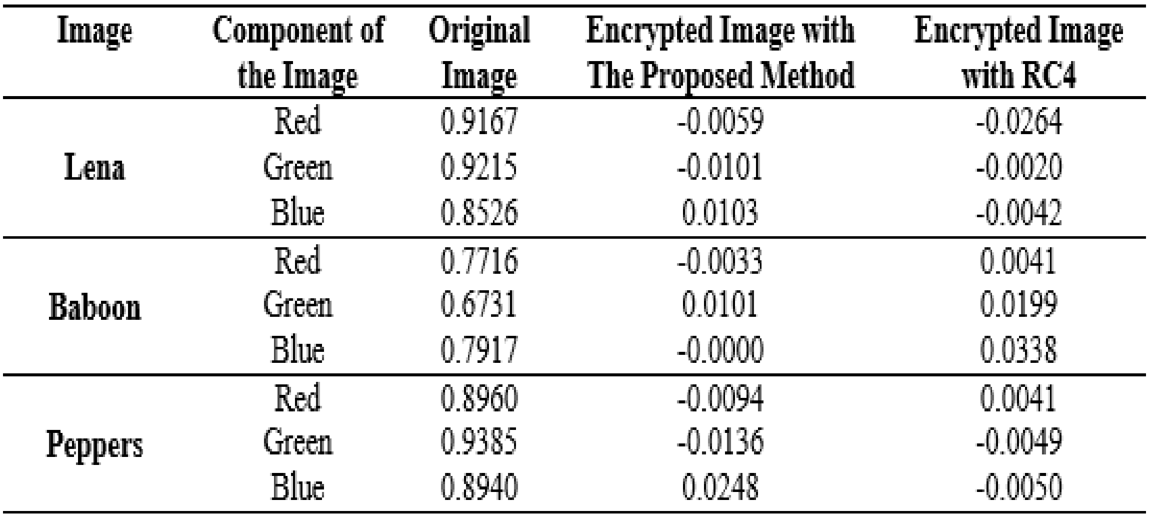
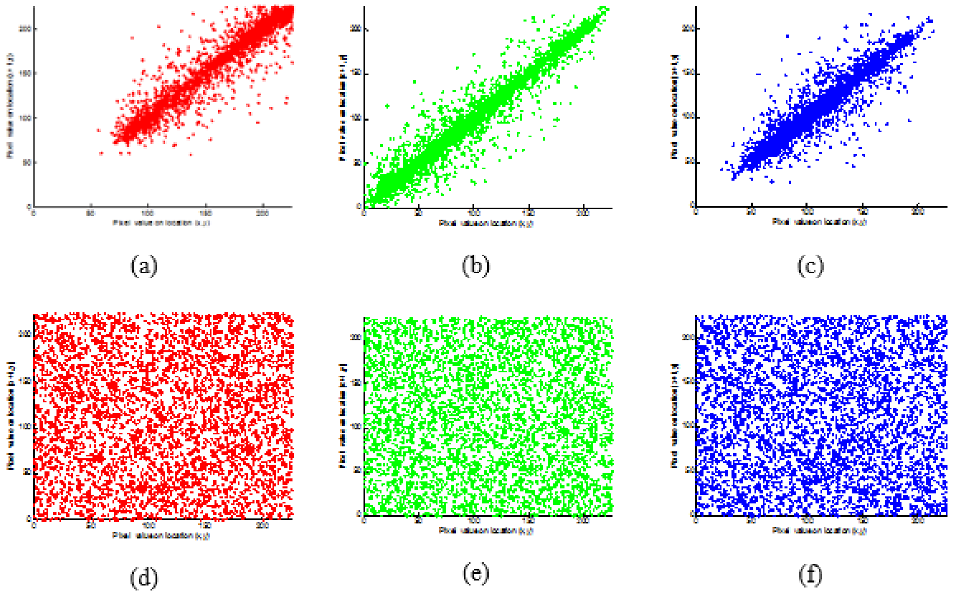


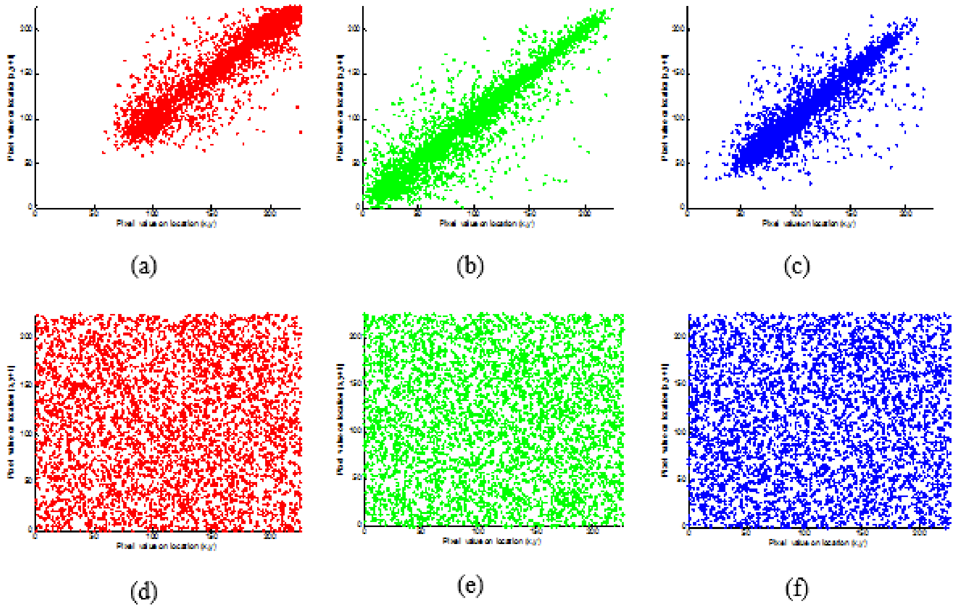
Image	Component of the Image	Original Image	Encrypted Image with The Proposed Method	Encrypted Image with RC4
Lena	Red	0.9167	-0.0059	-0.0264
	Green	0.9215	-0.0101	-0.0020
	Blue	0.8526	0.0103	-0.0042
Baboon	Red	0.7716	-0.0033	0.0041
	Green	0.6731	0.0101	0.0199
	Blue	0.7917	-0.0000	0.0338
Peppers	Red	0.8960	-0.0094	0.0041
	Green	0.9385	-0.0136	-0.0049
	Blue	0.8940	0.0248	-0.0050



(a) (b) (c)

(d) (e) (f)

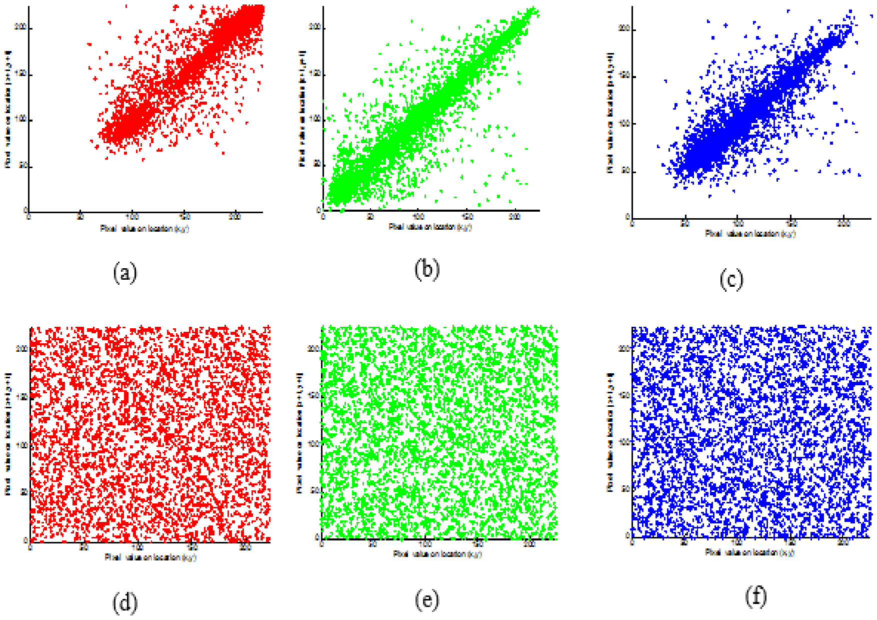
Figure 2: Horizontal correlation of the Lena image. (a), (b) and (c) are the RGB plots of the original image. (d), (e) and (f) are the RGB plots of the encrypted image using proposed method.



(a) (b) (c)

(d) (e) (f)

Figure 3: Vertical correlation of the Lena image. (a), (b) and (c) are the RGB plots of the original image. (d), (e) and (f) are the RGB plots of the encrypted image using proposed method.



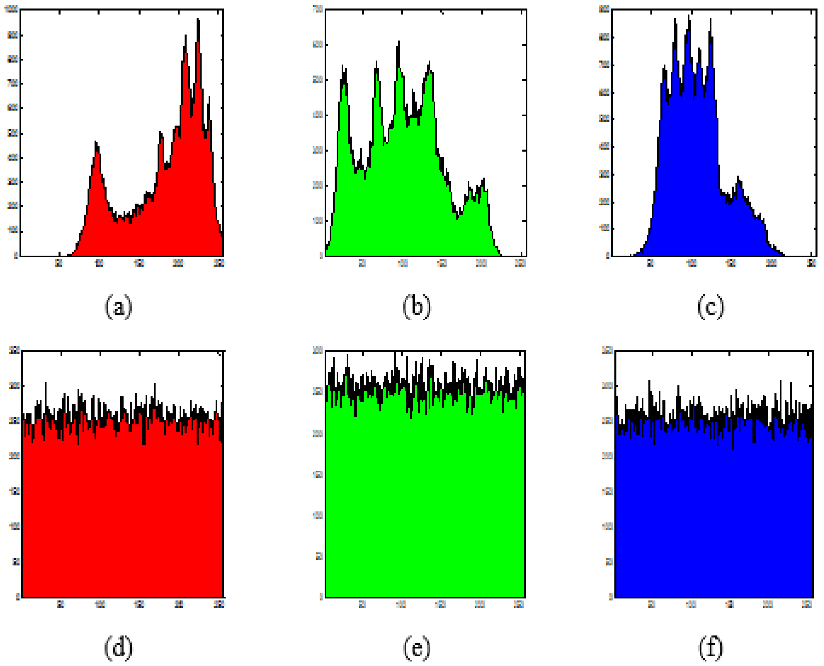
(a) (b) (c)

(d) (e) (f)

Figure 4: Diagonal correlation of the Lena image. (a), (b) and (c) are the RGB plots of the original image. (d), (e) and (f) are the RGB plots of the encrypted image using proposed method.

6.2.2 Histogram Analysis

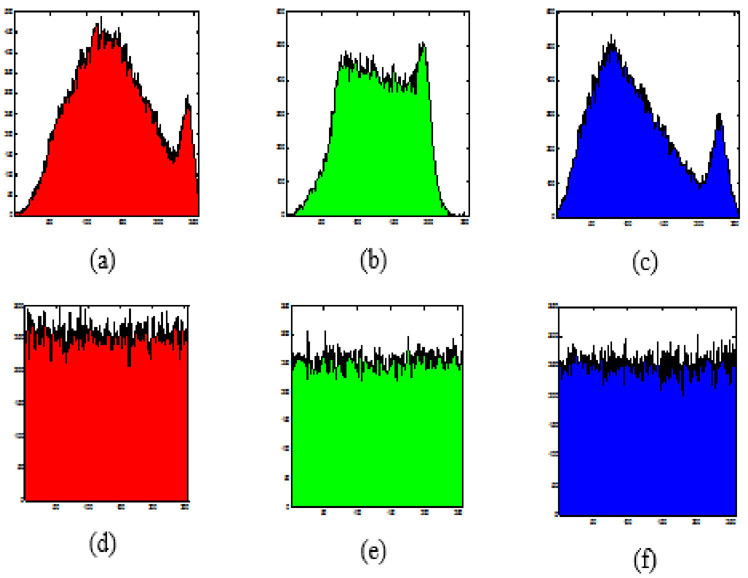
Figure-5 depicts the histograms of the Lena and the corresponding encrypted image. Figure-6 depicts the histograms of the Baboon and the corresponding encrypted. The results clarify that the histograms of the encrypted image have a uniform distribution and are considerably dissimilar from the original image histograms. This means that the proposed method can withstand histogram analysis attack.



(a) (b) (c)

(d) (e) (f)

Figure 5: Histograms analysis of the Lena image. (a), (b) and (c) are the RGB plots of the original image. (d), (e) and (f) are the RGB plots of the encrypted image using the proposed method.



(a) (b) (c)

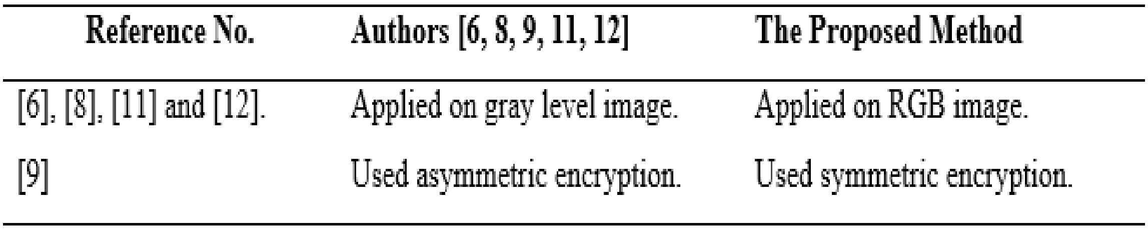
(d) (e) (f)

Figure 6: Histograms analysis of the Baboon image. (a), (b) and (c) are the RGB plots of the original image. (d), (e) and (f) are the RGB plots of the encrypted image using the proposed method.

7. Comparison with Other Methods

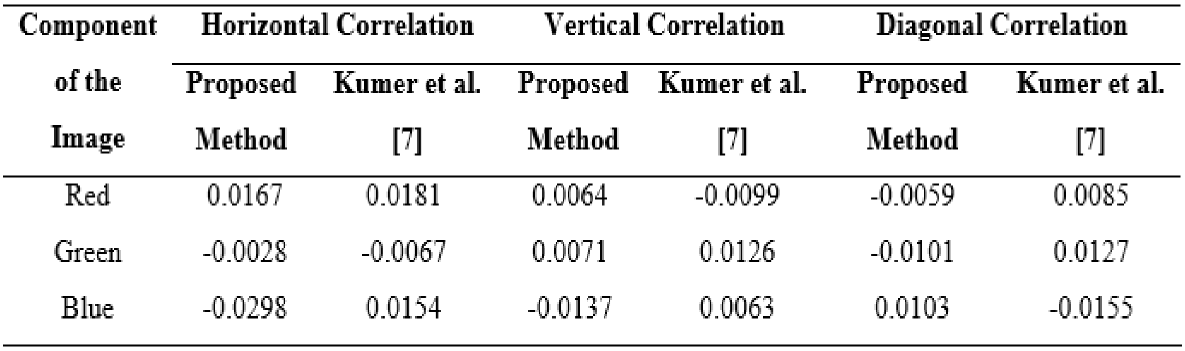
The proposed encryption method was compared with the related works [6], [8], [9], [11] and [12] as shown in Table-8. Table-9 clarifies that the proposed method more resists to statistical attack than Kumer et al. [7] due to the results of horizontal correlation, of vertical correlation and of diagonal correlation of the proposed method are better than the results of Kumer et al. [7]. Furthermore, Table-10 clarifies that the proposed method can decrypt the image without any loss as demonstrated by the values of MSE and PNSR while, in Kumer et al. [7] algorithm, some information was lost.

Table 8: Comparison of authors [6, 8, 9, 11 and 12] with the proposed method.



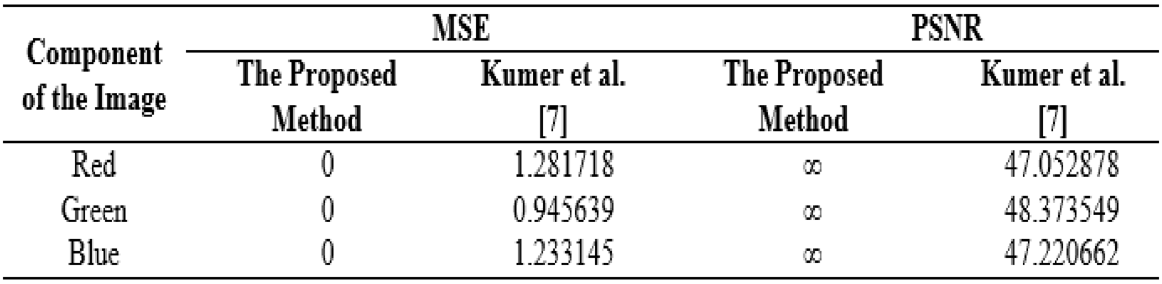
Reference No.	Authors [6, 8, 9, 11, 12]	The Proposed Method
[6], [8], [11] and [12].	Applied on gray level image.	Applied on RGB image.
[9]	Used asymmetric encryption.	Used symmetric encryption.

Table 9: Comparison of horizontal, vertical and diagonal correlation of encrypted Lena image with Kumer et al. [7].



Component of the Image	Horizontal Correlation		Vertical Correlation		Diagonal Correlation	
	Proposed Method	Kumer et al. [7]	Proposed Method	Kumer et al. [7]	Proposed Method	Kumer et al. [7]
Red	0.0167	0.0181	0.0064	-0.0099	-0.0059	0.0085
Green	-0.0028	-0.0067	0.0071	0.0126	-0.0101	0.0127
Blue	-0.0298	0.0154	-0.0137	0.0063	0.0103	-0.0155

Table 10: Comparison of MSE and PSNR values of decrypted image of Lena using the proposed method with Kumer et al [7].



Component of the Image	MSE		PSNR	
	The Proposed Method	Kumer et al. [7]	The Proposed Method	Kumer et al. [7]
Red	0	1.281718	∞	47.052878
Green	0	0.945639	∞	48.373549
Blue	0	1.233145	∞	47.220662

8. Conclusions

This paper proposes a secure image encryption method using RC4 algorithm and DNA encoding without affecting the quality of the image. The results show that utilizing DNA encoding in the proposed method improves the security level of RC4 algorithm. Moreover, the proposed method is lossless encryption and able to resist statistical attacks. In addition, it provides good security without affecting the quality of the image. Also, as a scope of further work, an additional quality could be used to investigate the ability of the proposed work to withstand known plaintext attack, chosen ciphertext attack and differential attack.

References

1. Paul, G. and Maitra, S. **2011**. *RC4 Stream Cipher and its Variants*. CRC press. Taylor & Francis Group.
2. Ismael, R. S., Yoail, R. S. and Wahhab, S. **2014**. Image encryption by using RC4 algorithm. *European Academic Research*, **2**(4): 5833-5839.
3. Ning, K. **2009**. A pseudo DNA cryptography method. *Computing Research Repository (CoRR)*, arXiv: abs/0903.2693.
4. Liu. L., Zhang, Q. and Wei, X. **2012**. A RGB image encryption algorithm based on DNA encoding and chaos map. *Computers and Electrical Engineering*, **38**(5): 1240-1248. Elsevier.
5. Ginting, R. U. and Dillak, R. Y. **2013**. Digital color image encryption using RC4 stream cipher and chaotic logistic map. *International Conference on Information Technology and Electrical Engineering (ICITEE)*, 101-105. IEEE.
6. Huang, X. and Ye, G. **2014**. An image encryption algorithm based on hyper-chaos and DNA sequence. *Multimedia tools and applications*, **72**(1): 57-70. Springer Science+Business Media New York.
7. Kumar, M., Powduri, P. and Reddy, A. **2015**. An RGB image encryption using diffusion process associated with chaotic map. *Journal of Information Security and Applications*, **21**: 20-30. Elsevier.
8. Jain, A. and Rajpal, N. **2016**. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools and Applications*, **75**(10): 5455-5472. Springer Science+Business Media New York.
9. Kumar, M., Iqbal, A. and Kumar, P. **2016**. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. *Signal Processing*, **125**: 187-202. Elsevier.
10. Zhen, P., Zhao, G., Min, L. and Jin, X. **2016**. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools and Applications,***75**(11): 6303-6319. Springer Science+Business Media New York.
11. Wang, X. and Liu, C. **2017**. A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications*, **76**(5): 6229-6245. Springer Science+Business Media New York.
12. Chai, X., Chen, Y. and Broyde, L. **2017**. A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, **88**: 197-213. Elsevier.

13. Stallings, W. **2017**. *Cryptography and Network Security : Principles and Practice*. 7th ed. Pearson.

14. Soni, R., Soni, V. and Mathariya, S. K. **2012**. Innovative field of cryptography: DNA cryptography. International Conference on Information Technology Convergence and Services. *Computer Science and Information Technology (CS&IT),*161-179.

15. Wu, X., Kurths, J. and Kan, H. **2017**. A robust and lossless DNA encryption scheme for color images. *Multimedia Tools and Applications,* 1-28. Springer Science+Business Media New York.

16. Soni, R., Johar, A. and Soni, V. **2013**. An encryption and decryption algorithm for image based on DNA. *International Conference on Communication Systems and Network Technologies (CSNT)*, 478-481. IEEE.

17. Wang, Z. and Bovik, A. C. **2009**. Mean squared error: Love it or leave it? A new look at signal fidelity measures. *IEEE Signal Processing Magazine,* **26**(1): 98-117. IEEE.

18. Hore, A. and Ziou, D. **2010**. Image quality metrics: PSNR vs. SSIM. *International Conference on Pattern Recognition (ICPR),* **20**: 2366-2369. IEEE.

19. Signal and Image Processing Insititute. University of South California.