ISSN: 0067-2904

A New Beta Chaotic Map with DNA Encoding for Color Image Encryption

Ibtisam A. Taqi, Sarab M. Hameed*,
Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Received: 3/9/2019 Accepted: 17/12/2019

Abstract
Images hold important information, especially in military and commercial surveillance as well as in industrial inspection and communication. Therefore, the protection of the image from abuse, unauthorized access, and damage became a significant demand. This paper introduces a new Beta chaotic map for encrypting and confusing the color image with Deoxyribonucleic Acid (DNA) sequence. First, the DNA addition operation is used for diffusing each component of the plain image. Then, a new Beta chaotic map is used for shuffling the DNA color image. In addition, two chaotic maps, namely the proposed new Beta and Sine chaotic maps, are used for key generation. Finally, the DNA XOR is applied concerning the produced key and shuffled DNA image to yield the cipher image. The experimental results prove that the proposed method surpassed the other methods in terms of Mean Square Error (MSE), Peak Signal-To-Noise Ratio ($PSNR$), entropy, and correlation coefficient.

Keywords: Beta chaotic map, DNA encoding, Image Encryption, Sine map, Confusion, Diffusion.

خريطة بيتا فوضية جديدة مع ترميز الحمض النووي لتشفير صورة ملونة

ابتسام عبدالله تقي، سراب مجيد حميد
قسم علوم الحاسوب ، كلية العلوم ، جامعة بغداد ، بغداد، العراق

الخلاصة
تحتوي الصور على معلومات مهمة خاصة في المجالات العسكرية والتجارية والمراقبة والتفتيش الصناعي والاتصالات. لذلك ، أصبحت حماية الصورة من سوء الاستخدام والوصول غير المصرح به والأضرار مطلبًا كبيرًا. يقدم هذا البحث خريطة بيتا فوضوية جديدة لتشفير وخلط الصورة الملونة مع سلسلة الحمض النووي. أولاً ، يتم استخدام عملية إضافة الحمض النووي لنشر كل مكون من مكونات الصورة العادية. ثم ، يتم استخدام خريطة بيتا فوضوية جديدة لخلط صورة الحمض النووي. بالإضافة إلى ذلك ، يتم استخدام خريطتين فوضويتين هما خرائط الفوضى الجديدة المقترحة من بيتا و **Sine** لإنشاء المفاتيح. أخيرًا ، يتم تطبيق **DNA XOR** بين المفتاح الذي تم إنشاؤه وصورة الحمض النووي المختلطة لإنتاج صورة التشفير. تثبت النتائج التجريبية أن الطريقة المقترحة افضل من الطرق الأخرى من حيث مربع متوسط الخطأ ، نسبة الإشارة إلى الضوضاء ، الانتروبي ومعامل الارتباط

1. Introduction

The evolution of new technologies in computer sciences led to the widespread growth of information, such as those of images, sounds, and videos stored in digital forms on hard disks or distributed over the internet. Furthermore, abuse and illegal access to private information have come to be a severe

*Email: sarab.m@sc.uobaghdad.edu.iq

challenge in the digital world. One of the effective methods for solving these concerns is encryption [1].

The conventional cryptographic techniques are based on a number of theoretic or algebraic concepts and hence they are inappropriate for multimedia data encryption because of their enormous sizes, high redundancy of pixels, interactive processes, complexity, and inadequacy for handling various data formats and demand of real-time responses. Recent researches suggest that the chaos-based image encryption schemes are highly efficient concerning speed and security for traditional cryptographic schemes [2].

Further, the properties of chaotic maps, such as being sensitive to the initial situation and system parameter, ergodicity, property of pseudorandom, and non-periodic and topological mixing, meet the cryptographic requirements. The idea of chaotic image encryption indicates the capability of chaotic maps of producing a pseudorandom number of sequences based on initial conditions and control parameters. Little variation in them provides an entirely different set of random numbers [2]. In addition, due to the recent advances in DNA technologies, DNA computing has entered the domain of cryptography, mainly in the field of image encryption [3].

This paper proposes an encryption method for a color image by combining DNA encoding and a new chaotic map that controls the encryption process, namely generating the key and shuffling the pixel position.

The paper is structured as follows: in section 2, related work is presented. Section 3 explains chaotic maps and DNA operations. In section 4, the proposed RGB image encryption and decryption are described in detail. Section 5 clarifies the evaluation of the results concerning the security analysis of the image. Finally, conclusions are given in section 6.

2. Related work

A considerable amount of literature has been published on gray and color image encryption. Xiaoling Huang, in 2012, suggested an image encryption algorithm that generates a key by utilizing Chebyshev chaotic map. The performance of the algorithm showed that the keyspace was large and a slight change in initial settings influenced the performance [4]. Wu *et al*., in 2012, proposed an image encryption method using two- dimensional logistic chaotic maps and permutation-substitution network structure. The results showed that the proposed method could produce a random cipher image and withstand several attacks including the statistical and the differential attacks [5]. Zhang *et al*., in 2014, proposed an enhanced algorithm for encrypting an image via DNA encoding, 2D logistic and wavelet chaotic map. The chaotic system was used to disturb the locations and the value of the pixel. Then, DNA encoding was carried out. The experimental results clarified that the algorithm increases image security by providing a large keyspace, along with its capability to counter attack statistical and exhaustive attacks [6]. Zhou *et al*., in 2015, suggested an image encryption algorithm via skew tent map and line map for shuffling. The proposed algorithm was implemented in parallel to obtain a high performance regarding speed. The results illustrated the robustness of the proposed algorithm against a chosen plaintext attack [7]. Kumar *et al*., in 2015, suggested a new procedure that used a multiple of chaotic maps for diffusion an image. The results illustrated that the suggested algorithm was appropriate for encrypting an image with high security [8]. Niyat *et al*., in 2015, used DNA sequence operation, a hyper-chaotic system, namely the 1D logistic map, and sine map for color image encryption, as well as the Chen hyper chaotic system for shuffling. The proposed algorithm results indicated that it could counter statistical analysis and exhaustive attacks [9]. Jain and Rajpal, in 2016, proposed an image encryption algorithm using DNA and 1D and 2D chaotic logistic maps. A 1D chaotic map was used for producing a mask matrix. Then, DNA addition operation and 2D chaotic map were applied to permute the image. The results clarified that the algorithm is robust against known plaintext attack, statistical attacks, and differential attacks [10]. Liu and Miao, in 2016, proposed an image encryption algorithm via logistic chaotic map using a varying parameter that was used for shuffling an image. After that, a dynamical algorithm was employed for encrypting the image. The results clarified that the algorithm provides high security and is competitive with several image encryption algorithms [11]. Rostami *et al*., in 2017, proposed a parallel image encryption algorithm by chaotic windows based on the 1D logistic map. The image was divided into 16 ×16 blocks. Then, the XOR operation between a chaotic window and these blocks was performed to produce an encrypted image. The results showed that the algorithm was able to withstand the statistical attacks, brute force

attack, differential attack, chosen-plaintext attack, and chosen-ciphertext attack [12]. Zahmoul *et al*., in 2017, suggested a Beta chaotic map to generate chaotic sequences that were intended for the encryption. Different pseudo-random sequences were generated to shuffle the image pixels position and unclear the relationship between the encrypted and the original image. The proposed algorithm was qualified for thwarting many attack [13].Niyat *et al*., in 2017, suggested color image encryption algorithm using hyper-chaotic system and cellular automata. Security analysis showed that the proposed method has a considerable keyspace and is able to withstand against noise and attacks. Adjacent pixels correlation in the encrypted image was decreased, and the quantity of entropy was equal to 7.9991 [1]. Chai *et al*., in 2017, suggested a chaos-based image encryption algorithm with DNA operations. First, a new wave-based permutation was applied to the plain image after converting it to DNA. Then, a 2D Logistic chaotic was used for the column circular permutation and row circular permutation of the DNA matrix. The security analysis proved that the algorithm provided a larger secure keyspace and high sensitivity to the secret. Experimental results showed that the algorithm is capable of resisting differential, noise entropy, known-plaintext, occlusion, and chosen-plaintext attacks [14]. Wu *et al*., in 2018, presented a new lossless and robust color image encryption algorithm employing DNA operation and one-way coupled-map lattices. Firstly, the DNA encoding rules were applied to the three components of the plain image to get three DNA matrices. After that, XOR operation was applied to the DNA matrices for two times. Finally, the cipher image was obtained by a diffusion process. The results proved the robustness of the proposed algorithm against histogram equalization, noise adding, JPEG compression, contrast adjustment and cropping [15]. Elamrawy *et al*., in 2018, suggested an image encryption algorithm employing DNA encoding followed by a 2D logistic chaotic map. The plain image was encoded to DNA coding and the 2D logistic map was used to permute the DNA coded image. The encrypted image was diffused by the 2D logistic map. The results demonstrated that the algorithm provided high entropy and a small correlation coefficient [16]. Girdhar and Kumar, in 2018, introduced a robust color image encryption by combining Lorenz-Rossler chaotic map and DNA encoding. Lorenz and Rossler chaotic map was employed to produce the arbitrary sequence, whereas the rules of DNA were used to encode the plain image. Moreover, cross-channel operation was applied to the plain image. The results revealed that the proposed algorithm provided superior correlation coefficient than the existing algorithms; the key sensitivity was high and the keyspace was large to resist exhaustive attacks [17].

3. DNA sequence operations and chaotic maps

This section presents the basic background related to DNA sequence operations and chaotic maps that are utilized in the proposed image encryption.

3.1 DNA rules and operations

DNA is a form of natural macromolecule which consists of nucleotides that hold a separate base. Four essential nucleic acids are employed to make the DNA sequence. These are Adenine (A), Cytosine(C), Guanine (G) and Thymine (T). A is constantly associates with T, while C regularly associates with G. The total numbers of potential combinations are twenty-four, while just eight characterize the complementary rule, as shown in Table-1. DNA encoding includes describing each nucleotide with a binary number that follows the complementary rule [2].

Table 1-The encoding rules for DNA sequences.

	Rule							
DNA Sequence	1	2	3	4	5	6	7	8
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

The subtraction and addition of DNA are achieved over modulo 4. Table-2 reports the addition and subtraction operations of DNA when rule one is utilized [3]. Table-3 shows the DNA-XOR operation [3].

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

Table 3-DNA XOR operation

⊕	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

3.2 Chaotic maps

Sine chaotic map and Beta chaotic map are utilized in this paper. Sine map is described by Equation 1 [9]:

$$y_{n+1} = rSin(\pi y_n) \tag{1}$$

Where

$r \in (0,4], y_n \in (0,1), n = 0,1,2,..$

Equation 2 defines the beta chaotic map which is used in numerous applications, such as image compression and image object detection [15]

$$\text{Beta}(x, x_1, x_2, x_c, p, q) = \begin{cases} \left(\frac{x-x_1}{x_c-x_1}\right)^p \left(\frac{x_2-x}{x_2-x_c}\right)^q & \text{if } x \in [x_1, x_2] \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Where

$$x_c = \frac{(px_2+qx_1)}{(p+q)} \tag{3}$$

$$p = b_1 + c_1 \times a \tag{4}$$

$$q = b_2 + c_2 \times a \tag{5}$$

4. The proposed image encryption

In this section, the components of the proposed image encryption method that integrates DNA sequence and chaotic maps are illustrated.

4.1 Key sequence generation

An essential process for the proposed encryption method is the key sequence generation via chaotic maps. A chaotic map is used for generating the key sequence because it is sensitive to initial state and control parameters. The initial values of the chaotic maps are generated by using a secret key of 128-bit $K = \{k_1, k_2, \ldots k_{32}\}$, where k_i represents a 4-bit hexadecimal digit.

The Beta map with some modification is suggested to formulate a new Beta chaotic map, as shown in Equation 6. The suggested equations in 7, 8 and 9 are used to initialize the parameters of new Beta chaotic maps. Each equation is divided by 2^{23} for normalization purposes.

$$\forall n, n \in \{0,1,2,\ldots\}, \text{newBeta}(x_n, x_s, x_e, x_c, p, q) = k \times \left(\left(\frac{x_n-x_s}{x_c-x_s}\right)^p \left(\frac{x_e-x_n}{x_e-x_c}\right)^q\right) mod\ 1 \tag{6}$$

$$x_0 = \frac{k_1 k_{2\ldots} k_{10}}{2^{23}}\ mod\ 1 \tag{7}$$

$$x_s = \frac{k_{11} k_{12\ldots} k_{20}}{2^{23}}\ mod\ 1 \tag{8}$$

$$x_e = \frac{k_{21} k_{22..} k_{32}}{2^{23}}\ mod\ 1 \tag{9}$$

In addition, the initial values (y_0 and r) for sine chaotic map are obtained from the suggested equations in 10 and 11.

$$y_0 = (x_0 + x_s + x_e)\ mod\ 1 \tag{10}$$

$$r = 3.9 + \frac{(x_s+x_e)\ mod 1}{10} \tag{11}$$

The mixture of Sine chaotic map in Equation 1 and new Beta chaotic map in Equation 6 are proposed to generate a sequence, z_n , as formulated in Equation 12

$$\forall n, \mathrm{n} \in \{0,1,2,\dots\}, z_n = (x_n + y_n)\ mod\ 1 \quad (12)$$

Three chaotic sequences, $S_x = \{x_1, x_2, \dots x_{M\times N}\}$, $S_y = \{y_1, y_2, \dots y_{M\times N}\}$ and $S_z = \{z_1, z_2, \dots z_{M\times N}\}$, are generated using Equations 13, 14 and 15, respectively.

$\forall i, 1 \le i \le M \times N$

$$x_i = \lfloor (x_i \times 10^{14})\ mod\ 256 \rfloor \quad (13)$$

$$y_i = \lfloor (y_i \times 10^{14})\ mod\ 256 \rfloor \quad (14)$$

$$z_i = \lfloor (z_i \times 10^{14})\ mod\ 256 \rfloor \quad (15)$$

M is the length of the image.

N is the width of the image.

After that, Rule 1 in Table-1 is used to transform the three sequences S_x, S_y and S_z to DNA sequence. Then, three DNA encoded matrices, S_{xe} , S_{ye} and S_{ze}, are obtained by performing DNA XOR operation, as follows:

$$\left.\begin{aligned} S_{xe} &= S_{xc} \oplus S_{yc} \\ S_{ye} &= S_{yc} \oplus S_{zc} \\ S_{ze} &= S_{zc} \oplus S_{ye} \end{aligned}\right\} \quad (16)$$

4.2 Image encryption via DNA sequence and chaotic map

Confusion and diffusion are two important properties that should be satisfied by the proposed method. These properties are achieved by changing each pixel value of the plain image $\boldsymbol{I}$ by DNA operation and shuffling image pixels using a new Beta chaotic map.

The first level of DNA confusion that is satisfied by DNA addition operation is clarified as follows:

Step1: the plain image $\boldsymbol{I}$ is decomposed into three components $\boldsymbol{R}(\boldsymbol{M},\boldsymbol{N})$, $\boldsymbol{G}(\boldsymbol{M},\boldsymbol{N})$ and $\boldsymbol{B}$ $(\boldsymbol{M},\boldsymbol{N})$.

Step2: the contents of $\boldsymbol{R}$, $\boldsymbol{G}$ and $\boldsymbol{B}$ matrices that hold numbers in [0,255] are transformed to binary.

Step3: rule 1 in Table-1 is applied for yielding 3 DNA coding matrices $\boldsymbol{R_c}$, $\boldsymbol{G_c}$ and $\boldsymbol{B_c}$

Step4: DNA addition operation is applied for producing 3 DNA encoding matrices $\boldsymbol{R_e}$, $\boldsymbol{G_e}$ and $\boldsymbol{B_e}$, as follows:

$$\left.\begin{aligned} R_e &= R_c + G_c \\ G_e &= G_c + B_c \\ B_e &= B_c + G_e \end{aligned}\right\} \quad (17)$$

After performing the first level of confusion, the DNA matrices R_e, G_e and B_e are shuffled (diffusion level) to exclude the correlation among the neighboring by using a new Beta chaotic map. In the new Beta chaotic map, a sequence x of a size $4MN$ is generated, where M is image width and N is image height. Then, the inverse of the decimal part is conserved and the integer part is eliminated for shuffling each value of R_e, G_e and B_e matrices. Next, the sequence x is arranged in an ascending order to confirm that all indexes are generated.

$$[x_{new}, ind] = sort(x) \quad (18)$$

Where

x_{new} is the sorted sequence and ind is the index of the element.

Finally, R_e, G_e and B_e are shuffled as follows

$\forall i, 1 \le i \le M$ and $\forall j, 1 \le j \le 4N$ and

$$R_S(i,j) = R_e(ind(i), x_{new}(j)) \quad (19)$$

$$G_S(i,j) = G_e(x_{new}(i), ind(j)) \quad (20)$$

$$B_S(i,j) = B_e(ind(i), ind(j)) \quad (21)$$

The operation of DNA XOR between the produced sequences S_{xe}, S_{ye} and S_{ze} and R_s, G_s, B_s is applied to produce an encrypted image C, as follows

$$\left.\begin{aligned} C_R &= R_s \oplus S_{xe} \\ C_G &= G_s \oplus S_{ye} \\ C_B &= B_s \oplus S_{ze} \end{aligned}\right\} \quad (22)$$

The decryption process for an image is like the encryption process; however, the stages are handled in the reverse order.

5. Experimental results

The Signal and Image Processing Institute ($SIPI$) data set, maintained by the University of South California (USC), is used as an evaluation data to evaluate the performance of the proposed method [18]. The results of encryption and decryption of Lena (512×512), Baboon (256×256), and Peppers (256×256) are depicted in Figure-1. The figure clarifies that any information cannot be retrieved from the cipher images. In other words, the proposed method provides good encryption. All the results are obtained by setting the new Beta parameters as follows
$b1 = 3,\ b2 = 5,\ c1 = 1,\ c2 = -1,\ a = 0.7$ and $k = 0.99$

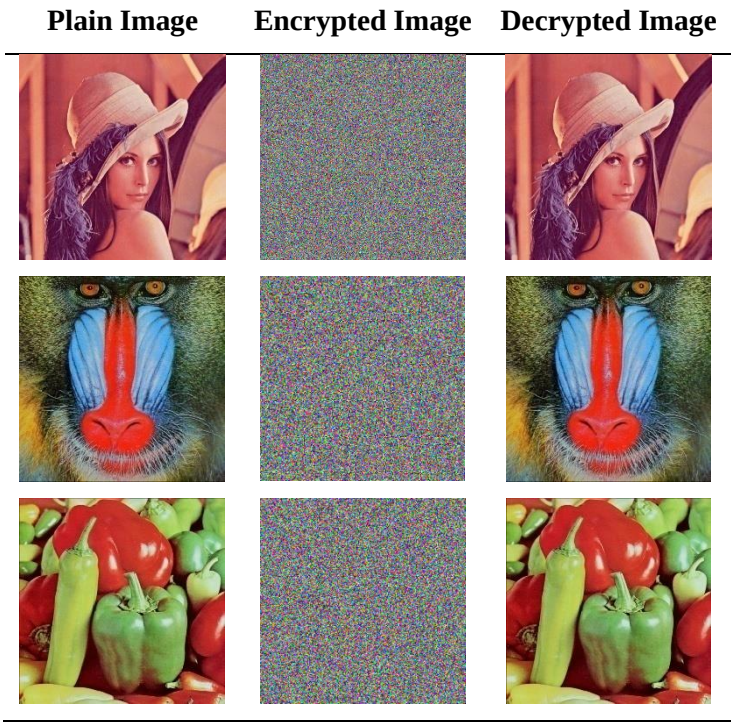

Figure 1-Encryption and decryption of images by the proposed method.

5.1 Evaluation concerning MSE and PSNR

Mean Square Error (MSE) and Peak Signal-To-Noise Ratio ($PSNR$) metrics are used to assess the performance of the proposed encryption method. MSE measures the distinction between plain image and cipher image, as in Equation 23 [15].

$$MSE = \frac{1}{MN}\sum_{i=0,j=0}^{M,N}(I(i,j) - C(i,j))^2 \quad (23)$$

Where
$I(i,j)$ is plain image pixel value, $C\ (i,j)$ is cipher image pixel value, M and N are the dimensions of the image.
The mathematical demonstration of $PSNR$ is as in Equation 24 [3].

$$PSNR = 20\ \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad (24)$$

The MSE and $PSNR$ values of cipher images and their corresponding decrypted images are reported in Tables- (4 and 5). The results reveal that the cipher image and the plain image are different, as explained by the large value of MSE and small value of $PSNR$.

Table 4-MSE value of the proposed method

Image	MSE			
	Component of Image			
	R	G	B	Average
Lena	10642.4271	9067.8538	7109.7853	8940.0221
Baboon	8614.0818	7863.5261	9578.9543	8685.5207
Peppers	8020.5557	11224.0195	11136.6674	10127.0809

Table 5-PNSR value of the proposed method

Image	PSNR (dB)			
	Component of Image			
	R	G	B	Average
Lena	7.8604	8.5558	9.6122	8.6761
Baboon	8.7787	9.1746	8.3176	8.7570
Peppers	9.0888	7.6293	7.6633	8.1271

5.2 Evaluation concerning keyspace

The keyspace size illustrates the strength of the proposed method to stand against the brute-force attack. The parameters x_0, x_s, x_e, k of the new beta map and r and y_0 of sine map are represented in a secret key. In the proposed method, the secret key consists of the sine map and $newBeta$ parameters. Hence, the keyspace of the proposed method is $(10^{14*3} \approx 2^{140}) \times 2^{24} \times 2^{128} = 2^{292}$ that seems to be sufficient for countering the brute force attack.

5.3 Evaluation concerning statistical attack

The suggested method for encryption is assessed in terms of histogram analysis, entropy (H) and correlation coefficient for demonstrating the ability of the suggested method for determining the statistical attack.

$$H(m) = -\sum_{i=0}^{L} p(m_i) log_2 p(m_i) \quad (25)$$

Where

$L = 255$, m_i is the i^{th} pixel value of an image, and $p(m_i)$ is the m_i probability.

Correlation coefficient (CC) is calculated as in Equation 26, which measures the relationship of adjacent pixels [1].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (26)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x_i)\big)^2$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x_i)\big)\big(y_i - E(y_i)\big)$$

Where

x and y are two neighboring pixels values in the image,

$D(x)$ is the variance, and N is the number of the chosen neighboring pixels of the image.

The histograms of red, green and blue components of encrypted Lena image are depicted in Figure-2. The results demonstrate that the cipher image histogram does not provide any information and is very flat.

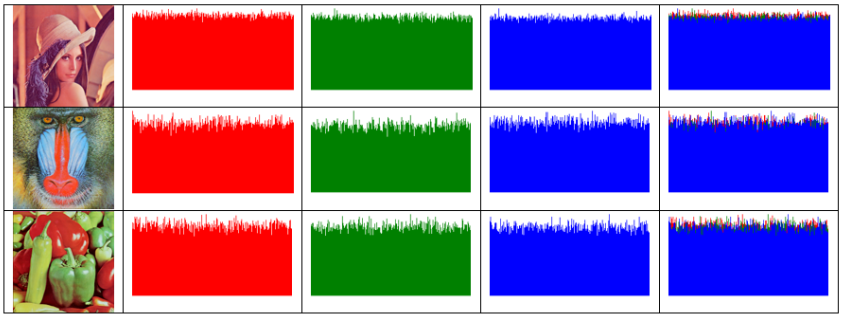

Figure 2-Red, green and blue components histogram of cipher images

The cipher image entropy of the proposed method is nearer to 8 and somewhat better than that shown by previous works [1, 8, 15 and 17], as reported in Table-6. This points out that the proposed method provides high randomness, while the probability of inferring any information is too slight, which indicates that the proposed method can resist the statistical attack.

Table 6-The proposed method entropy compared vs. that of previously reported works [1, 8, 15 and 17]

		Entropy			
Method	**Name of Image**	**Component of Image**			
		R	**G**	**B**	**Average**
Proposed Method	**Lena (512×512)**	7.9993	7.9992	7.9993	7.9993
	Lena (256×256)	7.9972	7.9971	7.9972	7.9972
	Baboon	7.9972	7.9971	7.9972	7.9972
	Peppers	7.9973	7.9975	7.9976	7.9975
[1]	**Baboon**	7.9972	7.9972	7.9972	7.9972
	Peppers	7.9971	7.9975	7.9974	7.9973
[8]	**Baboon**	7.9973	7.9968	7.9976	7.9972
[15]	**Lena (256×256)**	7.9895	7.9894	7.9894	7.9894
	Baboon	7.9899	7.9896	7.9888	7.9894
	Peppers	7.9898	7.9886	7.9894	7.9893
[17]	**Lena (256×256)**	7.9974	7.9969	7.9979	7.9974
	Baboon	7.9970	7.9972	7.9973	7.9972
	Peppers	7.9974	7.9973	7.9969	7.9972

The correlation coefficient results that are obtained by randomly selecting 1000 pairs of neighboring pixels in three directions from the original image and the corresponding cipher image are reported in Tables- (7-9). The results show that the proposed method is capable of fighting the statistical attacks better than the other previously reported works [1, 8, 9, 15 and 17].

Table 7-Vertical correlation coefficient of the proposed method vs. that of previously reported works [1, 8, 9, 15 and 17]

		Vertical Correlation Coefficient			
Method	**Name of Image**	**Component of Image**			
		R	**G**	**B**	**Average**
Proposed Method	**Lena (512×512)**	-0.0742	0.0009	0.0738	0.0002
	Baboon	0.0278	-0.0363	0.0090	0.0002
	Peppers	-0.0041	0.0102	-0.0065	-0.0001
[1]	**Baboon**	–	–	–	–
	Peppers	0.0031	0.0001	0.0022	0.0018
[8]	**Lena**	-0.0099	0.0126	0.0063	0.0030
[9]	**Baboon**	0.0744	0.0788	0.0748	0.0760
[15]	**Lena (256×256)**	-0.0026	0.0199	0.0120	0.0098
[17]	**Lena (256×256)**	0. 0026	0.0009	-0.0030	0.0009
	Baboon	-0.0007	0.0039	0.0061	0.0050
	Peppers	0.0023	0.0053	0.0005	0.0027

Table 8-Horizontal correlation coefficient of proposed method vs. that of previously reported works [1, 8, 9, 15 and 17]

		Horizontal Correlation Coefficient			
Method	**Name of Image**	**Component of Image**			
		R	**G**	**B**	**Average**

Proposed Method	**Lena** (512×512)	-0.0114	0.0042	0.0069	-0.0001
	Baboon	0.0160	-0.0238	0.0067	-0.0004
	Peppers	0.0261	-0.0069	-0.0188	0.0001
[1]	**Baboon**	–	–	–	-0.0008
	Peppers	0.0049	0.0054	0.0053	0.0052
[8]	**Lena**	0.0181	-0.0067	0.0154	0.0089
[9]	**Baboon**	0.0761	0.0827	0.0757	0.0782
[15]	**Lena** (256×256)	-0.0112	0.0050	-0.0179	-0.0080
[17]	**Lena** (256×256)	-0.0001	-0.0011	-0.0010	-0.0001
	Baboon	-0.0017	0.0028	0.0041	0.0035
	Peppers	-0.0016	-0.0043	0.0013	0.0013

Table 9-Diagonal correlation coefficient of proposed method vs. that of previously reported works [1, 8, 9, 15 and 17]

Method	**Name of Image**	**Diagonal Correlation Coefficient**			
		Component of Image			
		R	**G**	**B**	**Average**
Proposed Method	**Lena** (512×512)	-0.0063	-0.0152	0.0211	-0.0001
	Baboon	-0.0198	0.0276	-0.0068	0.0003
	Peppers	0.0624	-0.0084	-0.0537	0.0001
[1]	**Baboon**	–	–	–	-0.0006
	Peppers	0.0007	0.0017	0.0007	0.0010
[8]	**Lena**	0.0085	0.0127	-0.0155	0.0019
[9]	**Baboon**	0.0733	0.0687	0.0701	0.0707
[15]	**Lena** (256×256)	0.0052	-0.0064	-0.0161	-0.0058
[17]	**Lena** (256×256)	-0.0053	0.0026	-0.0051	0.0026
	Baboon	0.0015	0.0015	0.0025	0.0018
	Peppers	0.0004	-0.0008	0.0008	0.0006

5.4 Evaluation concerning the differential attack

Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) that are calculated in Equation 27 and 28, respectively, are used to show the effect of changing one pixel in the plain image on the cipher image [1].

$$UACI(C1, C2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C1(i,j) - C2(i,j)|/255}{M \times N} \times 100 \quad (27)$$

Where

M and N are image width and height, respectively.

and

$C1$ and $C2$ are encrypted images of the plain image and the modified one.

$$NCPR(C1, C2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100 \quad (28)$$

Where

$$D(i,j) = \begin{cases} 0, & if\ C1(i,j) = C2(i,j) \\ 1, & if\ C1(i,j) \neq C2(i,j) \end{cases}$$

A comparison between the proposed method in this study and the methods presented previously [1, 8, 15 and 17] based on NPCR and UACI is reported in Tables- (10 and 11). Table-10 shows that the NPCR of our proposed methods is close to 100% and UACI is more close to 33.58 than the values of the previously reported methods. This indicates that the sensitivity of the suggested method for the alteration of the plain image is high. In addition, the competence of resisting the differential attack and plaintext attack of the suggested method is more amenable than that reported by the previously reported methods.

Table 10-NPCR of the proposed method vs. that of previously reported works [1, 8, 15 and 17]

		NPCR			
Method	**Name of Image**	**Component of Image**			
		R	**G**	**B**	**Average**
Proposed Method	**Lena (512×512)**	99.6010	99.5998	99.6178	99.6062
	Lena (256×256)	99.6277	99.6078	99.6521	99.6292
	Baboon	99.6231	99.6368	99.6674	99.6424
	Peppers	99.6170	99.6323	99.6384	99.6292
[1]	**Baboon**	99.6536	99.6078	99.6520	99.6378
	Peppers	99.6357	99.6158	99.6247	99.6254
[8]	**Lena**	99.5659	99.5658	99.5959	99.5759
[15]	**Lena (256×256)**	99.6052	99.6060	99.6113	99.6075
	Baboon	99.6024	99.6252	99.6004	99.6093
	Peppers	99.6060	99.6286	99.5874	99.6073
[17]	**Lena (256×256)**	99.6230	99.6060	99.6520	99.6270
	Baboon	99.6140	99.5510	99.6060	99.5903
	Peppers	99.5890	99.5530	99.6310	99.5910

Table 11-UACI of the proposed method vs. that of previously reported works [1, 8, 15 and 17]

		UACI			
Method	**Name of Image**	**Component of Image**			
		R	**G**	**B**	**Average**
Proposed Method	**Lena (512×512)**	33.4670	33.4795	33.4730	33.4731
	Lena (256×256)	33.5791	33.5893	33.6369	33.6017
	Baboon	33.4026	33.5998	33.6296	33.5440
	Peppers	33.6158	33.5832	33.5471	33.5820
[1]	**Baboon**	33.4753	33.5090	33.4176	33.4673
	Peppers	33.4570	33.4705	33.4423	33.4566
[8]	**Lena**	33.2829	33.3459	33.327	33.3186
[15]	**Lena (256×256)**	33.4280	33.4966	33.3779	33.4342
	Baboon	33.4311	33.4500	33.4935	33.4582
	Peppers	33.4959	33.4874	33.4302	33.4712
[17]	**Lena (256×256)**	33.2450	33.3620	33.5210	33.3760
	Baboon	33.4000	33.4690	33.3840	33.4177
	Peppers	33.4680	33.5310	33.2420	33.4137

5.5 Evaluation concerning the noise attack

High secure cryptosystems must be resistant to all kinds of noise during transmissions, such as salt and pepper and Gaussian noise. The salt and pepper noise with five different densities d={0.05,0.10,0.15,0.20,0.50} and Gaussian noise with zero mean and five different variances { 0.00001,0.0001,0.001,0.01,0.1} are added to Lena cipher image. Table-12 clarifies quantitatively the MSE, PSNR and differences percentage between the Lena image and decrypted image, under salt and pepper noise and Gaussian noise, with different levels of noise for the proposed method.

Table 12-MSE, PSNR and differences between plain and decrypted images under salt and pepper noise and Gaussian noise with different levels of noise for proposed method

Noise Type	**Ratio**	**MSE**	**PSNR**	**Differences%**
Salt & pepper	**5%**	986.1228	18.1915	8.53
	10%	1912.9160	15.3138	16.52
	15%	2763.7078	13.7159	23.90
	20%	3517.5386	12.6684	30.46
	50%	6983.4256	9.6901	60.58

	0.00001	266.5197	23.8735	5.54
	0.0001	829.7865	18.9411	13.77
Gaussian	**0.001**	2309.3872	14.4958	29.51
	0.01	5483.4849	10.7402	53.86
	0.1	8404.7085	8.8856	73.80

Figure-3 depicts the Lena encrypted image, under salt and pepper noise with different five densities, and the corresponding decrypted image. Figure-4 shows the Lena encrypted image, under Gaussian noise with different four variances, and the corresponding decrypted image. From these figures, it can be noted that the decrypted Lena image can be recolonized

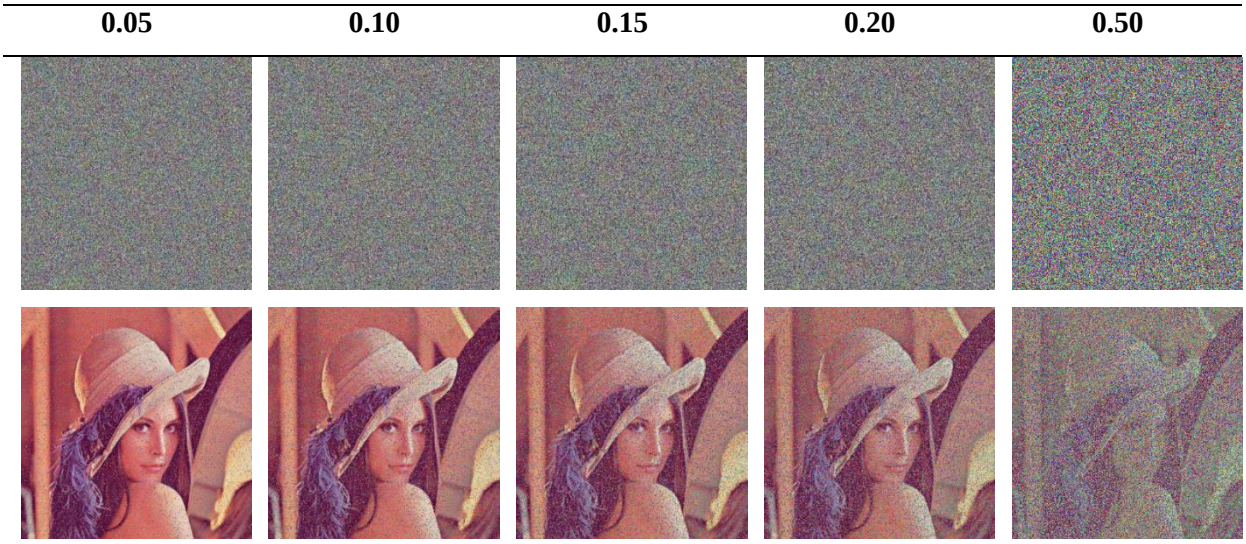

Figure 3-The decryption results of the proposed method under salt and pepper noise with different variances.

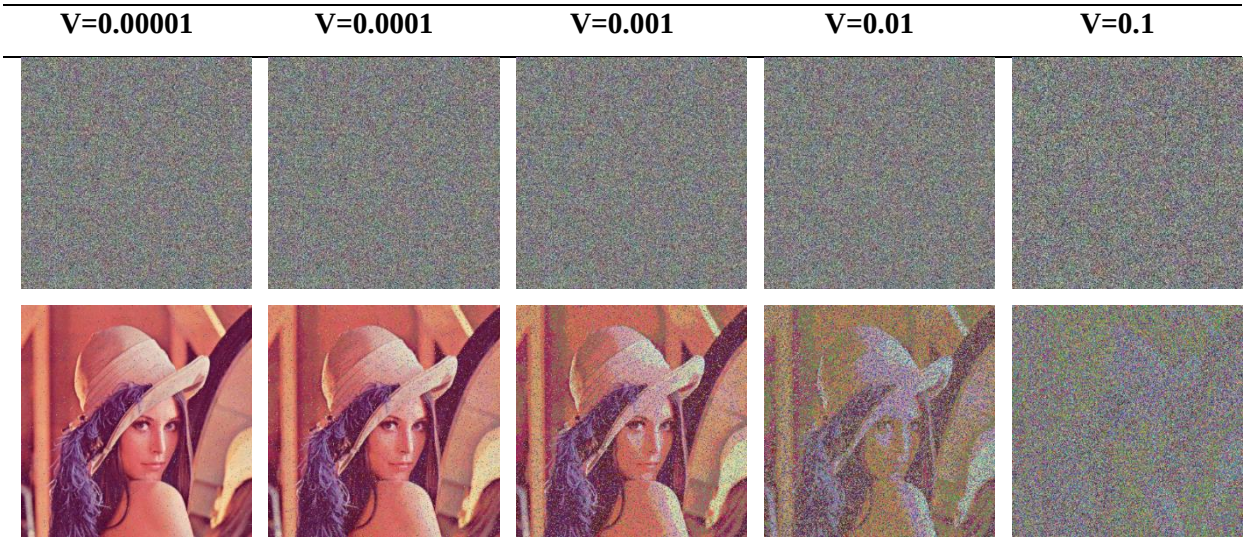

Figure 4-The decryption results of the proposed method under Gaussian noise with different variances.

5.6 Evaluation concerning the cropping attack

Image cropping is very popular and causes data loss. A robust system must resist this attack and preserve data during transmission. In Figure-5, different sizes of blocks (32×32, 64×64,

128×128, 256×256 *and* 256×512) are cropped from the Lena cipher image and the corresponding decrypted images. There is 50% of data lost but it is clear that the decrypted image is still recognizable and contains the most important visual information, which implies that the proposed method is robust against the cropping attacks.

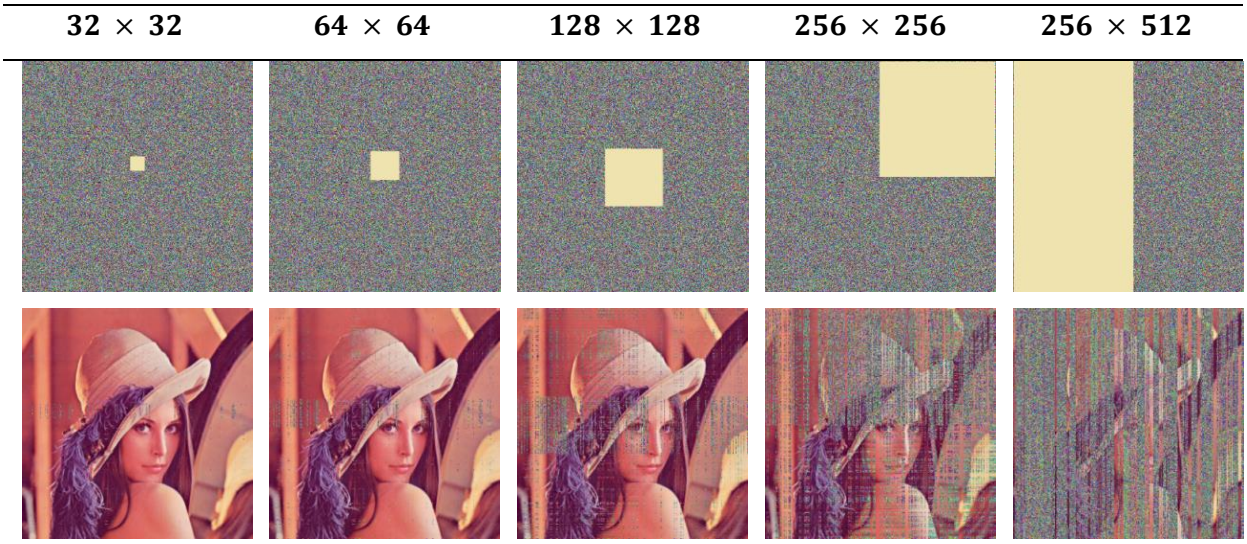

Figure 5-Cipher and decrypted images under cropping attack with different cropping window size (32×32, 64×64, 128×128, 256×256 and 256×512, respectively) for the proposed method.

5.7 Evaluation concerning the key sensitivity analysis

Good image encryption should be sensitive to a slight change in the secret key. Keys sensitivity can be observed in the proposed methods by modifying a single bit in the secret key and a minor alteration is performed for chaotic maps parameters. In this experiment, some of the secret keys are modified, where only one parameter is modified at each time.

Suppose the secret key K and the chaotic parameters $y = 0.0180513858795166$, $r = 3.97053072452545$ and $x_2 = 0.590390682220459$ are used to encrypt Lena image by the proposed method. Figure-6b qualitatively depicts the decryption of the encrypted Lena image when the secret key (K) is modified to K' while keeping the other keys, r, y and x_2 unchanged. Moreover, the parameter y is changed to $y' = 0.0180513858795167$ and the decryption process is depicted in Figure-6c. Also, the r parameter is changed to $r' = 3.97053072452544$ and the decryption of the encrypted image is shown in Figure-6d. Finally, the x_2 parameter is changed to $x'_2 = 0.590390682220458$ and the decryption process is shown in Figure-6e.

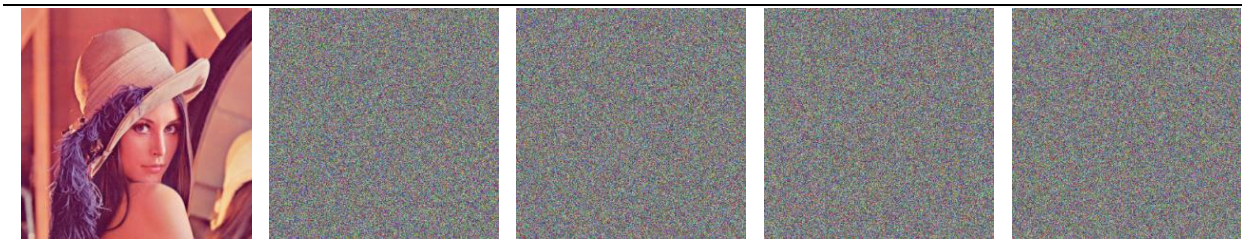

Figure 6-Key sensitivity results for the proposed method. a. Lena image. b. The decrypted image with $\boldsymbol{K'}$. c. The decrypted image with $\boldsymbol{y'}$. d. The decrypted image with $\boldsymbol{r'}$. e. The decrypted image with $\boldsymbol{x'_2}$

From Figure-6, it can be noted that, in all cases, the decryption process is not capable of recovering the original image when a slight change was performed to the secret key. This indicates that the proposed methods are extremely sensitive to the secret keys.

5.8 NIST test

The statistical tests suite provided by the National Institute of Standards and Technology (NIST) are used to evaluate the randomness of the proposed methods. The $p-value$ for statistical tests is compared with the significance level, α, that is set to 0.001. If the value of the test is greater than α then the method is passed the test. Otherwise, it fails to pass the test. Table-13 reports the $p-value$ of ten statistical tests for Lena, Baboon and Peppers of the proposed method. The results reveal that the proposed method achieves a high security level by successfully pass all statistical tests of the NIST test.

Table 13-The NIST Test of Lena, Baboon and Peppers of the proposed method.

Test Name	Lena	Baboon	Peppers	Pass
Frequency	0.911413	0.253551	0.602458	ok
Block Frequency	0.122325	0.911413	0.911413	ok
Cumulative Sums	0.949602	0.949602	0.148094	ok
Runs	0.739918	0.213309	0.213309	ok
Longest Run	0.671779	0.804337	0.804337	ok
Rank	0.253551	0.082177	0.213309	ok
FFT	0.739918	0.350485	0.468595	ok
Non Overlapping Template	0.991468	0.976060	0.976060	ok
Serial	0.468595	0.468595	0.602458	ok
Linear Complexity	0.534146	0.671779	0.911413	ok

6. Conclusions

This paper suggests a new encryption method for color image. Two chaotic maps including sine map and the proposed new Beta chaotic map are used to produce the key. Moreover, the diffusion and confusion properties are fulfilled by utilizing DNA operations and the proposed new Beta chaotic map, respectively. From the results presented, we can confirm the sensitivity of the proposed method to a slight change in the secret key and that it can counter several attacks, namely brute force attack, statistical attack, differential attack, plaintext attack, noise attack and cropping attack.

References

1. Abolfazl Yaghouti Niyat, Mohammad Hossein Moattar, Masood Niazi Torshiz, **2017**. "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*,**90**: 225–237.
2. Lili Liu, Qiang Zhang , Xiaopeng Wei, **2012**. "A RGB image encryption algorithm based on DNA encoding and chaos mapq," *Computers and Electrical Engineering*, **38**: 1240–1248.
3. Manish Kumar , Akhlad Iqbal , Pranjal Kumar,**2016**. "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Processing*,**125**: 187–202.
4. Huang, X. **2012**. "Image encryption algorithm using chaotic Chebyshev," *Nonlinear Dynamics*, **67**(4): 2411-2417.
5. Yue Wu, Joseph P. Noonan, Gelan Yang, Huixia Jin, **2012**. "Image encryption using the two-dimensional logistic chaotic map," vol. 21.
6. Qiang Zhang, Lili Liu, Xiaopeng Wei, **2014**. "Improved algorithm for image encryption based on DNA encodingand multi-chaotic maps," **68**: 186– 192.
7. Guomin Zhou, Daxing Zhang, Yanjian Liu, Ying Yuan, Qiang Liu, **2015**. "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, **169**: 150-157.
8. Manish Kumar,Pradeep Powduri ,Avinash Reddy, **2015**. "An RGB image encryption using diffusion process associated with chaotic map," *journal of Information Security and Applications*, **21**: 20-30.

9. Abolfazl Yaghouti Niyat,Reza Mohammad Hei Hei,Majid Vafaei Jahan, **2015**. "A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *International Congress on Technology,Communication and Knowledge (ICTCK)*.
10. Anchal Jain , Navin Rajpal, **2016**. "A robust image encryption algorithm resistant to attacks," **75**(10): 5455-5472.
11. Lingfeng Liu and Suoxia Miao, **2016**. "A new image encryption algorithm based on logistic chaotic map with varying parameter," *SpringerPlus*.
12. Mohamad Javad Rostami , Abbas Shahba , Saeid Saryazdi, Hossein Nezamabadi-pour, **2017**. "A novel parallel image encryption with chaotic windows based on logistic map," *Computers and Electrical Engineering,* **62**: 384-400, 2017.
13. Rim Zahmoul, Ridha Ejbali, Mourad Zaied, **2017**. "Image encryption based on new Beta chaotic maps," *Optics and Lasers in Engineering,***96**: 39–49, 2017.
14. Xiuli Chai ,YiranChen , LucieBroyde, **2017**. "A novel chaos-based image encryption algorithm using DNAsequence operations," *Optics and Lasers in Engineering,* **88**: 197–213, 2017.
15. Xiangjun Wu , Jürgen Kurths , Haibin Kan, **2018**. "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools and Applications,* **77**(10): 12349–12376, 2018.
16. Fayza Elamrawy, Maha Sharkas, Abdel Monem Nasser, **2018**. "An image encryption based on DNA coding and 2DLogistic chaotic map," *International Journal of Signal Processing,* **3**: 27-32.
17. Ashish Girdhar, Vijay Kumar, **2018**. "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools and Applications,* pp. 1-23.
18. Signal and Image Processing Insititute, [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc.