Multimed Tools Appl (2016) 75:1–23
DOI 10.1007/s11042-014-2221-x

An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules

Ayesha Kulsoom · Di Xiao · Aqeel-ur-Rehman · Syed Ali Abbas

Received: 1 February 2014 / Revised: 2 July 2014 / Accepted: 28 July 2014 /
Published online: 5 November 2014

Abstract A novel image encryption algorithm in streaming mode is proposed which exhaustively employs an entire set of DNA complementary rules alongwith one dimensional chaotic maps. The proposed algorithm is highly efficient due to encrypting the subset of digital image which contains 92.125 % of information. DNA addition operation is carried out on this MSB part. The core idea of the proposed scheme is to scramble the whole image by means of piecewise linear chaotic map (PWLCM) followed by decomposition of image into most significant bits (MSB) and least significant bits (LSB). The logistic sequence is XORed with the decoded MSB and LSB parts separately and finally these two parts are combined to get the ciphered image. The parameters for PWLCM, logistic map and selection of different DNA rules for encoding and decoding of both parts of an image are derived from 128-bit MD5 hash of the plain image. Simulated experimental results in terms of quantitative and qualitative ways prove the encryption quality. Efficiency and robustness against different noises make the proposed cipher a good candidate for real time applications.

Keywords Stream cipher · Logistic · PWLCM · MD5 · DNA

1 Introduction

With the ripening in the field of communication system, the multimedia data has also gained more importance over textual data. It is almost impossible to completely avoid the eavesdropping in broadcasted data over internet and satellite communication. Hence, data needs to be secure especially multimedia data which originated from sensitive organizations like military, medical etc. For images, the encryption in digital domain is a straight forward

A. Kulsoom (✉) · D. Xiao · Aqeel-ur-Rehman · S. A. Abbas
College of Computer Science and Engineering, Chongqing University, Chongqing, People's Republic of China
e-mail: ayeshakhattak1@yahoo.com

Ayesha Kulsoom
e-mail: ayeshacqu@gmail.com

technique to convert into noise [39]. The standard ciphers are built for one dimensional binary bit stream which extracts a plain image bit by bit for encryption. Such types of techniques include AES [13], DES [14], Twofish [32] and BlowFish [1]. In the case of digital image, adjacent pixels often have similar gray-scale values and strong correlations, or image blocks have similar patterns, while for video data, consecutive frames are similar and most likely only few pixels would differ from frame to frame. Such an extremely high data redundancy of multimedia makes the conventional ciphers fail to obscure all visible information [18].

Commonly, two ways of image encryption are found: optical and digital encryption. The former adopts optical instrument to build physical systems for image encryption [22, 8, 43, 9, 33] which commonly relies on optics to randomize the frequency components in an image. The later one commonly takes advantage of a digital image and encrypts it either by an encryption algorithm in the form of software or a physical electronic device in the form of hardware. Most commonly employed encryption and security schemes are digital in nature since present communication systems are becoming entirely digital [2]. Thus among various digital image encryption techniques, the chaos-based image encryption method is believed to be good candidate for encryption purposes as chaotic systems are characterized by ergodicity, sensitive dependent on initial conditions and random like behaviors [6, 40, 11].

Recently, the characteristics of DNA computing such as massive parallelism, huge storage and ultra-low power consumption have been found [21]. Most of the researchers turned to use complementary rules of DNA to encrypt the data. DNA-based image encryption [36, 27, 42, 41] is one of the latest and most successful image encryption method. The fundamental idea of all DNA-based image encryption is categorized in two phases: first, using DNA theory to encode plain image pixels to a DNA sequence and using those rules to generate the key image. In the second phase, the encoded plain image pixels generated a key image based on DNA operation rules and form the cipher image [12].

Combining the benefits of both chaotic maps and DNA computing, many image encryption algorithms have been proposed by researcher which has some significant drawbacks such as A. Rehman [31] scheme lacks robustness against noise and have low efficiency due to calculation of new key for each block. Zhang et al. [41] is also not efficient and has no robustness against noise as encoded image is divided into blocks for addition with each other to achieve diffusion. In the same way, Liu et al. [27] transformed each nucleotide into its base pair for random time (s), which is pseudo random sequence by chebyshev map and is also less efficient.

In this paper, an image encryption algorithm is proposed which utilizes subset of an image to achieve diffusion in streaming mode under DNA addition operation. The selection of DNA complimentary rules for encoding and decoding both MSB and LSB parts and initial conditions and control parameter for PWLCM and logistic map are calculated from 128-bit hash of a plain image alongwith the use of common keys. The floating point Logistic sequence is converted into integer between 0 and 15 and then XORed with LSB and MSB separately. The usage of 1-D chaotic maps, streaming mode of encryption, simple mathematical operations like addition, XOR and MOD, selective data encryption alongwith MD5 hash are combined to achieve soaring efficiency. It also has the capability of encompassing the noisy factor that arises more often. The paramount advantage of this scheme is that it is capable to decrypt into original image despite the accumulation of noise due to noisy channel during transmission.

The rest of the paper is organized as follows: In Section 2, a brief description of the DNA rules and algebraic operation is provided. Section 3 is devoted to introduce the proposed method. In Section 4, discussion is made on the experimental results of the proposed cipher to demonstrate the validity. Concluding remarks of the paper are summarized in the final section.

2 Preliminaries

2.1 DNA rules for encoding and decoding of images

Knowledge of Deoxyribonucleic acid (DNA) sequences has become indispensable for basic biological research, and in numerous applied fields such as diagnostic, biotechnology, forensics, and biological systematics [20]. A single DNA sequence is comprised of four nucleic acid bases: A (Adenine), C (Cytosine), G (Guanine), and T (Thymine), where A and T, C and G are complementary pairs [20]. In the theory of binary system, 0 and 1 are complementary pair so 0 (00) and 3 (11) are complementary pair, 1 (01) and 2 (10) are also complementary pair. Four bases i.e., A, T, G, and C can be used to encode 01, 10, 00 and 11, respectively. In the total, the number of coding combination is 4!=24. Because of the complementary relation between DNA bases, there are only eight kinds of coding combinations that can meet the Watson-Crick complement rule out of 24 kinds of coding combinations [35] shown in Table 1. In this paper, we use DNA code to encode the grayscale image. Each 8-bit pixel value of the grayscale image can be encoded into a nucleotide string whose length is 4 [34], for example if the first pixel value of the grayscale image is 167, its binary stream is [10100111]. By employing the DNA first encoding rule to encode the stream, the corresponding DNA sequence [CCGT] is attained. Whereas by decoding the above DNA sequence with the DNA encoding rule 1, we can get the original binary stream [10100111]. But the resultant binary sequence will be different if any other DNA encoding rule is used to decode the same DNA sequence as for instance, according to the sixth decoding rule, we get another binary sequence [00001101]. This is simple DNA encoding which is used to encode the least significant part of an image in our algorithm.

2.2 Addition and subtraction algebraic operations for DNA sequences

With the rapid progression in DNA computing, some biological and algebraic operations on DNA sequence are reported by researchers such as addition and subtraction operations [24]. These algebraic operations for DNA sequences are performed according to traditional addition and subtraction in the binary. Eight kinds of DNA addition rules and eight kinds of DNA subtraction rules exist in correspondence to eight kinds of DNA encoding combinations. The addition operation is performed to encrypt the DNA coding sequence and subtraction operation is used to decrypt it. For example, on two dataset of DNA sequences [TTGT] and [CGTA], one rule of addition operation is performed as shown in Table 2 in order to add them. Resultantly, a sequence [GAAT] is obtained. Likewise, the sequence [TTGT] can also be

Table 1 Eight kinds of encoding and decoding mapping rule of DNA sequence

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

obtained by subtracting the sequence [GAAT] from [CGTA] under the subtraction operation. From Table 2, we can see that the base in each row or column is unique. This means that the results of addition and subtraction operation are unique. The algorithm of this paper uses these addition rules to substitute the most significant part of an image.

3 The proposed image encryption scheme

3.1 Generation of initial conditions

MD5 is a widely used cryptographic hash function that produces a 128-bit digest and it can expressed as a 32 digits hexadecimal number [26]. Even if there is only one bit difference between two images, their MD5 results will be completely different [27]. Presume that for each specific grayscale image: x_0, p_x are the initial condition and control parameter for PWLCM, and y_0 is the initial condition for logistic map respectively, calculated by using 128-bit hash alongwith the common input keys. Furthermore, four numeric values are required for the selection of encoding and decoding rules for both most significant and least significant parts, calculated directly from MD5 hash. For this, first 24 hexadecimal values of hash are divided into three groups, h_1, h_2, h_3 and each h_j is composed of 8 hexadecimal numbers where j=1,2,3. For each group, we convert it into a floating decimal number d_j (0,0.0156) by Eq. (3.1):

$$d_j = hex2dec(h_j)/2^{38}. \tag{3.1}$$

The PWLCM system has attained peerless attraction in chaos research recently due to its simplicity in representation, good dynamical behavior as well as efficiency in implementation [27]. Among the lower dimensional maps, PWLCM has high invariant natural density [38] and its trajectory visits entire interval for every value of control parameter, hence more suitable for permutation process to accomplish it in less time. An image is permuted using PWLCM as is described in Eq. (3.2)

$$x_{i+1} = \begin{cases} x_i / p_x & 0 \le x_i < p_x \\ (x_i - p_x)/(0.5 - p_x) & p_x \le x_i < 0.5 \\ 1 - x_i & x_i \ge 0.5 \end{cases} \tag{3.2}$$

Suppose the common initial condition and control parameter for PWLCM are x_0 and p_x the new numerical values can be generated by Eq. (3.3):

$$\begin{cases} x_0' = x_0 + d_1 \\ p_x' = p_x + d_2 \end{cases} \tag{3.3}$$

Table 2 Addition and subtraction operation for DNA sequence

+	A	G	C	T	−	A	G	C	T
A	A	G	C	T	A	A	T	C	G
G	G	C	T	A	G	G	A	T	C
C	C	T	A	G	C	C	G	A	T
T	T	A	G	C	T	T	C	G	A

The Logistic map shown in Eq. (3.4) is in chaotic state for the control parameter 3.57 to 4.0 but the distribution density of the chaotic sequence is not uniform over the interval 0 to 1. To overcome this drawback, the logistic sequence described in [23] is transformed to get uniform distribution in the entire interval by applying Eq. (3.5) but this works only for the control parameter 3.99. Another numerical value is required for logistic map shown in Eq. (3.4), which can be calculated by using Eq. (3.6),

$$y_{i+1} = \mu y_i(1-y_i) \quad y_i \ (0,1) \tag{3.4}$$

$$y_i^{'} = \frac{2}{\pi}\arcsin\left(\sqrt{y_i}\right) \tag{3.5}$$

$$y_0^{'} = y_0 + d_3 \tag{3.6}$$

$$s_j = \left(q_{j1}q_{j2}q_{j3}q_{j4}\right) mod\ 8. \tag{3.7}$$

The proposed cipher requires four more numerical values in the range of 0 to 7 for the selection of DNA rules as shown in Table 3 in order to encode and decode LSB and MSB parts of an image. For this purpose, the last 32-bits or 8 hexadecimal values of MD5 are divided into four groups as $q_{j1}q_{j2}q_{j3}q_{j4}$ where j=1,2,3,4.

3.2 Image encryption

In 1998, Fredrich proposed an architecture [17] for chaos based image encryption algorithm, since then most of the image encryption algorithms followed it. This architecture consists of two phases; confusion and diffusion. In the former phase, the sequence of information is changed and in later phase each piece of data is replaced by another symbol. The proposed image encryption algorithm also follows the same architecture by employing two chaotic sequences X and Y generated by PWLCM and logistic map respectively. In this paper, sequence X is used in position scrambling and Y is used to XOR with MSB and LSB parts after carrying out DNA addition operation on MSB part. Both confusion and diffusion phases are described in detail in the subsequent section as follows:

Table 3 Selection of DNA rules before and after diffusion operation

s_j	DNA rule
0	AGCT
2	ACGT
4	GATC
6	CATG
1	GTAC
3	TGCA
5	CTGA
7	TCGA

3.2.1 Confusion phase: using PWLCM system to generate confusion arrays

Step 1 Set the initial condition $x_0^{'}$ and control parameter $p_x^{'}$, iterate the above Eq. (3.2) $t+HW$ times, discard the former t values to avoid the transient effects to get sequence $X=\{x_1,x_2,....,x_{HW}\}$ where H and W are the height and width of an image.

Step 2 Sort X as

$$[lx\ ly] = sort(X),$$

where lx is the index values of sorted values ly in X

Step 3 Transform the 2-D image into 1-D array and rearrange the elements of I according to lx to get permuted image as shown in following Eq. (3.8),

$$I'(i) = I(lx(i)) \tag{3.8}$$

3.2.2 Substitution phase for most significant part

It is well known fact that each bit at different position of a gray image carries a different amount of information that can be calculated using the formula given in Eq. (3.9) which shows that the higher four bits contains 92.125% of information and the lower four contains only 5.875% [7]. In Fig. 1, the underlying theme of the above stated fact is depicted visually in which each image is carrying zero information simultaneously at two bit planes or at four bit planes. It can be perceived visually that by keeping value of two bits as zero simultaneously at different positions, the loss in information will be at large scale at higher position as shown in Fig. 1a to d while 1e and 1f depict results of four bit planes of an image from least significant to most significant.

$$p(i) = \frac{2^i}{\sum_{i=0}^{7} 2^i}. \tag{3.9}$$

In the proposed algorithm, the selective diffusion operation is applied on most significant part of an image under DNA addition operation after encoding. So, the higher bit planes of an image are selected for substitution by adding with lower bit planes after encoding into DNA sequence under the DNA algebraic operation. For the diffusion process, first the permuted image I' is converted into binary image as I'' of size $H\times 8W$ and then split into two parts representing LSB and MSB of sizes $H\times 4W$ each and then encoded into DNA sequence according to Table 3 using the numerical value of s_1 and s_2 respectively, thereafter transformed into 1-D sequence of size $H\times 2W$ as,

$$\begin{aligned} L &= \{l_1, l_2, \ldots, l_{2HW}\}, \\ M &= \{m_1, m_2, \ldots, m_{2HW}\}, \end{aligned} \tag{3.10}$$

The DNA addition is performed on L and R as,

$$R(i) = L(i) + M(i) \tag{3.11}$$

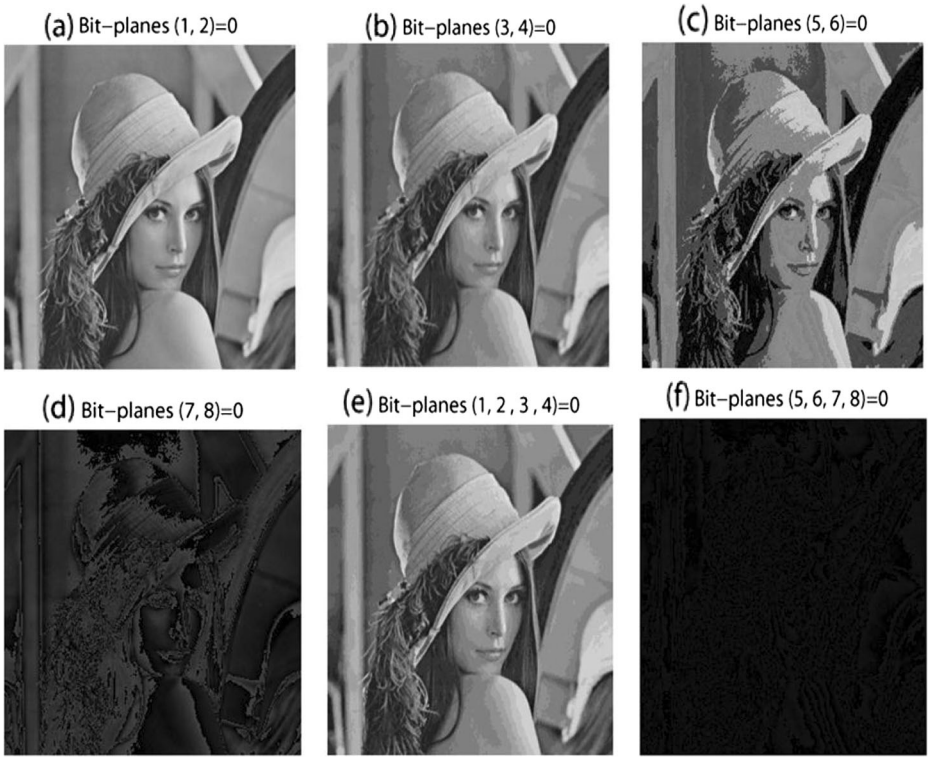


Fig. 1 Information fading effect at different bits of gray image Lena

After this, these parts L and R are decoded according to Table 3 using s_3 and s_4, we get,

$$\begin{aligned} R' &= s_3(R) \\ L' &= s_4(L) \end{aligned} \tag{3.12}$$

Equation (3.4) is used to iterate ($H\times 4W$) times with the initial condition $y_0^{'}$ and control parameter μ=3.99. To make the distribution of logistic sequence uniform, Eq. (3.5) is applied on Y and then converted it into integer numbers in the range of 0 to 15 as follows

$$y_i^{'} = \left(y_i \times 10^{-16}\right) mod 16. \tag{3.13}$$

Y' is divided into two groups as, $Y_{1'}=\{y_1,y_2,\ldots,y_{2HW}\}$ and $Y_{2'}=\{y_{2HW+1},y_{2HW+2},\ldots, y_{4HW}\}$ of size $2HW$. At final stage, $Y_{1'}$ is XORed with MSB and $Y_{2'}$ with LSB.

$$\begin{aligned} E_{MSB} &= R' \oplus Y_{1'} \\ E_{LSB} &= L' \oplus Y_{2'} \end{aligned} \tag{3.14}$$

and finally both XORed parts are unified to get E as cipher image and the whole method is shown graphically in Fig. 2.

$$E = Cat(E_{LSB}, E_{MSB});$$

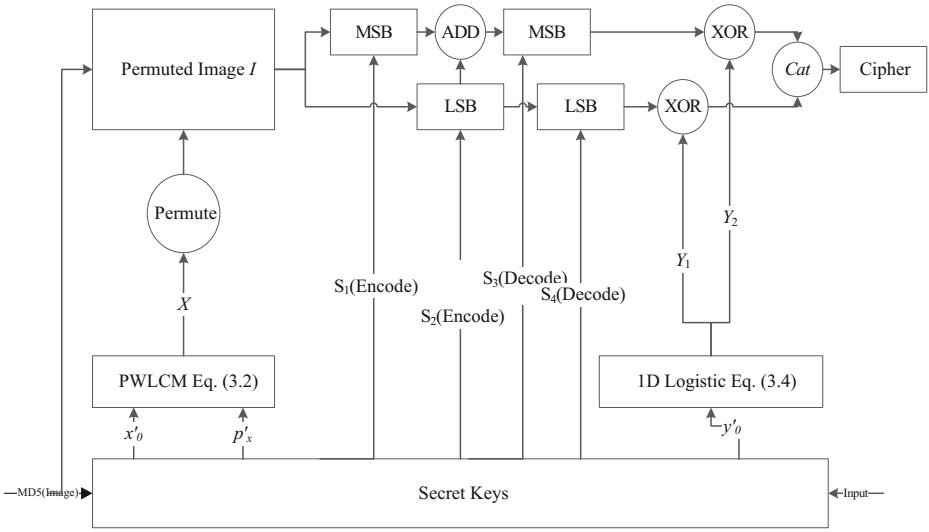


Fig. 2 Schematic diagram of proposed cipher

3.3 Image encryption steps

Suppose that the size of the original grayscale image I is $H \times W$, the complete encryption process consists of the following steps.

> **Input**: Image I, the initial value $x_0^{'}$ and control parameter $p_x^{'}$ for PWLCM, the initial value $y_0^{'}$ for logistic map.
> **Output**: The encrypted image.

Step 1 Iterate Eq. (3.2) with new $p_x^{'}$ and $x_0^{'}$ get sequence X to permute the Image I according to the section 3.2.1 to form I'.
Step 2 Generate new initial condition $y_0^{'}$ and s_j from 128-bit hash according to section 3.1.
Step 3 Split binary image I' into LSB and MSB part whereas the size of each is $H \times 4W$, encode them using s_1 and s_2 to get L and M shown in Eq. (3.10).
Step 4 Perform DNA addition on L and M to get R and then decode both parts using s_3 and s_4 according to Table 1 to get L', R' respectively.
Step 5 Iterate Eq. (3.4) with $y_0^{'}$ to get Y of size $H \times 4W$ and transform it into uniform distributed sequence according to Eq. (3.5), divide it into two sequences $Y_1^{'}$ and $Y_2^{'}$ as described in section 3.2.2.
Step 6 Convert floating point values of $Y_1^{'}$ and $Y_2^{'}$ into integer in the range of 0 to 15 using Eq. (3.13).
Step 7 XOR R' with $Y_1^{'}$ and L' with $Y_2^{'}$ and then combine XORed part to get cipher image.

3.4 Image decryption steps

Decryption process is similar to encryption in reverse order where first on LSB and MSB parts, XOR operation is performed then s_3 and s_4 are used to encode, DNA subtraction operation is

applied at step 4. Finally s_1 and s_2 are used for decoding to get the original permuted image. Reversal of permutation is applied to get back an original image.

4 Simulation results and analysis

A good encryption scheme is satisfactory only when it is robust and possesses the attribute of resisting all sorts of known attacks, like brute force, statistical and differential attacks. Couples of tests and analysis have been made to ascertain the security of the proposed cryptosystem, including the most imperative ones like key space analysis, key sensitivity analysis, statistical analysis, differential analysis. The results of these tests demonstrate that the new scheme owns high security and efficiency. The results of each of these tests and the performance of the proposed cipher are elaborated and analyzed in detail in the subsequent section.

4.1 Key space

Quoting from [28]:

> "A necessary, but usually not sufficient, condition for an encryption scheme to be secure is that the key space be large enough to preclude exhaustive search."

The total number of different keys used in the encryption procedure integrated together to form the key space of a cryptosystem. If the key space of an encryption algorithm is large enough (more than 128-bit which is considered to be secure for most common cryptographic applications in view of the speed of present day computing machines) then the brute force attack on such algorithm becomes infeasible [29]. In this paper, the encryption algorithm consists of three key variables, (i) For PWLCM, initial value x_o and control parameter p_0 with the precision 10^{-16}. (ii) Initial condition with precision 10^{-16} of Logistic map.(iii) Eight DNA complementary rules for encoding and decoding. Thus, the total key space of the proposed system is $S=(0.5\times10^{16}\times10^{16})\times10^{16}\times2^8=2^{167}$, sufficiently larger than 2^{128} [16]. An image encryption algorithm with such a long key makes the brute force attack unworkable and infeasible.

4.2 Key sensitivity analysis

In secure encryption schemes, extreme key sensitivity is an essential factor. Chaotic maps have high sensitivity to initial value and control parameter. Both chaotic maps, i.e., logistic and PWLCM are highly sensitive to initial conditions and control parameter. The encrypted image of lena is shown in Fig. 3b with $p_x=0.345678901234567$ while Fig. 3c is the decrypted image with a key of only one bit difference $p_x=0.345678901234568$ that results in failure. By using the same key only, the original image can be decrypted as is shown in Fig. 3d.

It is obvious from the figures of the proposed scheme that the image can be correctly decrypted only when the encryption and decryption keys are even. Else, as long as there exists minute differences in the key, the original image can't be extracted and the information of the original image cannot be reflected by the decrypted image. A swift change in the original image results a significant change in the ciphered image. The high sensitivity of the proposed algorithm demonstrates that it has sufficient ability of resisting exhaustive attack.

4.3 Resistance to statistical attack

Statistical analysis on cipher image is of crucial importance for a cryptosystem. Indeed, an ideal cipher should be robust against statistical attacks. In order to prove the security of the proposed image encryption scheme, following statistical tests are analyzed.

4.3.1 The gray histogram analysis

An Image histogram is a graphical representation that illustrates the number of pixels at each different intensity level found in that image. The histogram of the encrypted image should have uniform distribution and should be entirely different from that of the original image. The grayscale histograms of the plain-image and the cipher-image are plotted in Fig. 4. It is

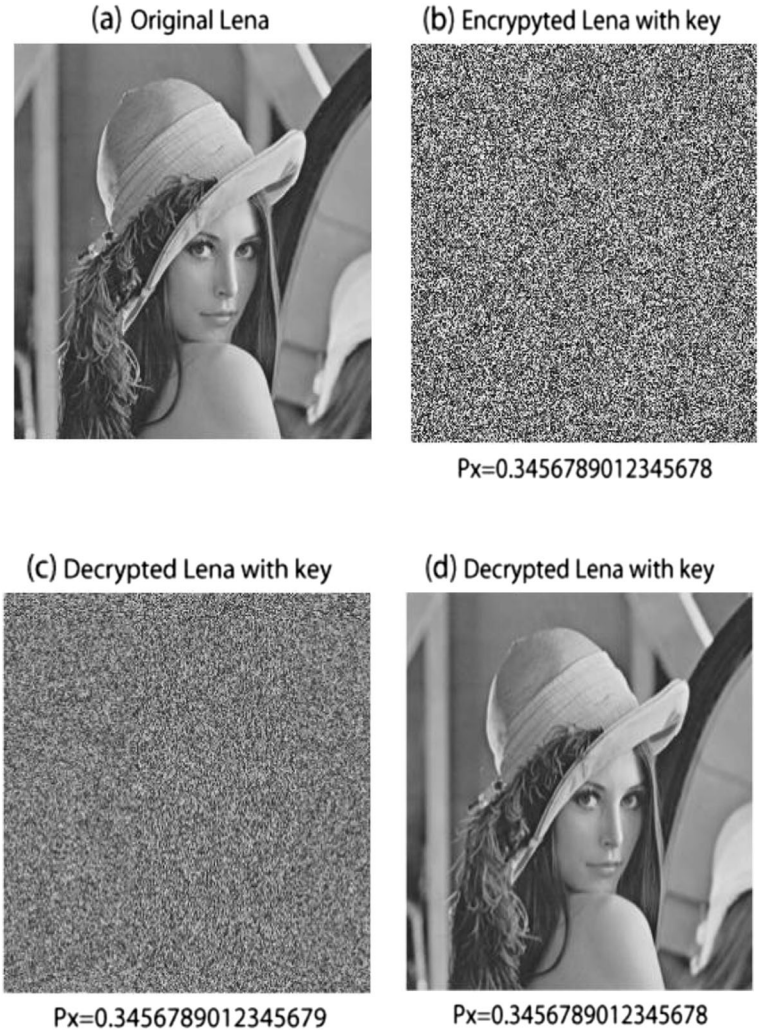


Fig. 3 Key sensitivity analysis for gray image Lena

obvious from the simulation results that the primitive pixel grayscale values of the original image are concentrated within the specified region but they are relatively uniform after encryption.

From Fig. 4, we can see that the histograms of the cipher images are fairly uniform and entirely different from the respective histograms of the plain images, Lena and Pepper. The encrypted images cannot provide any statistical information of plain images to the attacker. In other words eliciting any information is quite impossible.

4.3.2 Auto correlation coefficient analysis

One of the mainstream tasks of an efficient image encryption algorithm is to reduce the correlation of adjacent pixels in order to make statistical attacks infeasible. Usually, there exists strong correlation among the adjacent pixels in the multimedia data. In this section, correlation coefficient of two adjacent pixels in original and encrypted images in all three directions i.e., horizontal, vertical and diagonal is calculated by random selection of 2,500 pairs of adjacent pixels by using the following formula [27].

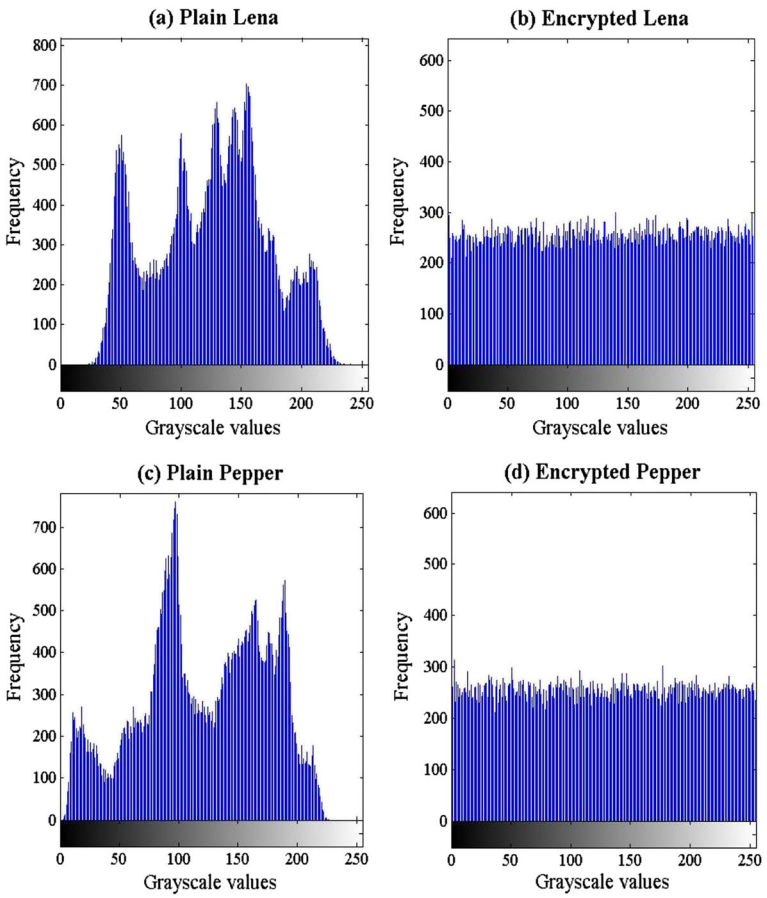


Fig. 4 The histograms of the plain and encrypted images of Lena and Pepper

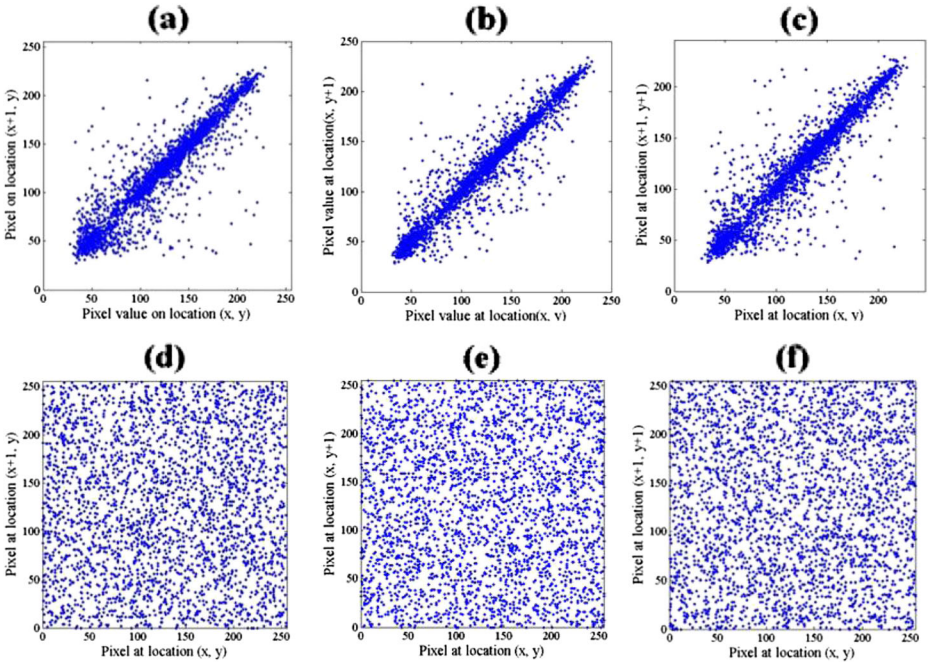


Fig. 5 Auto correlation analysis of plain and ciphered Lena in *horizontal*, *vertical* and *diagonal* directions

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)D(y)}}$$

where

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (4.1)$$

In the above Eq. (4.1), x and y denote gray values of the two adjacent pixels in the image, N is the total number of pairs selected from the image for the calculation, $E(x)$ and $D(x)$ are the expectation and variance of x, respectively. Three images of first row of Fig. 5 demonstrate the strong correlation effect in adjacent pixels of plain image Lena in all three directions while images in the second of row of Fig. 5 reveal significant reduction of correlation effect in encrypted image of Lena in the corresponding directions (Vertical, Horizontal, Diagonal). Table 4 indicates the results of correlation coefficients of two adjacent pixels of encrypted images obtained from proposed system which are comparatively better than the Refs. [27] and

Table 4 The comparison of the auto correlation coefficient of Lena in all three directions with Ref. [27]

Images	Horizontal	Vertical	Diagonal
Plain Lena	0.9449	0.9697	0.9388
Ref. [27]	0.0004	0.0021	−0.0038
Ref. [31]	−0.0007	0.0006	−0.0031
Proposed	0.0027	0.0005	−0.0045

Table 5 Comparison of information entropy of the plain images and ciphered images

Images	Lena	Airplane	Barbara	Pepper
Plain	7.4428	7.5807	7.6321	6.7297
Ref. [27]	7.9874	7.9780	7.9867	7.9860
Ref. [31]	7.9972	7.9973	7.9972	7.9972
Proposed	7.9972	7.9972	7.9973	7.9958

[31]. The proposed method justifies the claim that no significant correlation exists between the original and its corresponding encrypted images.

4.4 Information entropy analysis

The information entropy is considered amongst the most imperative feature of randomness. For measuring the strength of a cipher in symmetric cryptosystems, the information entropy is calculated as follows:

$$H(m) = \sum_{i=0}^{2^{n-1}} p(m_i) log_2 \frac{1}{p(m_i)}. \tag{4.2}$$

where $P(m_i)$ is the emergence probability of m_i. For any gray image, there are 2^8 states of information and for an ideal random image, the value of the information entropy of the encrypted image should tend to 8. The more closely it gets to the ideal value, the harder for the cryptosystem to divulge information. Equation (4.2) is used to compute the information entropy of the plain images and their corresponding cipher images. Table 5 lists the data pertinent to the comparison of the entropy of the proposed scheme and the comparable scheme Refs. [27] and [31]. It is notable that the obtained entropy value of four images encrypted by the proposed method is in close proximity to the theoretical value 8 which means that the ciphered images are very close to a true random source. It is further evident from the fact that the entropy values of the proposed scheme for different images are better than that of the compared scheme. Thus, the proposed algorithm is robust as the information leakage in the image enciphering process is exiguous.

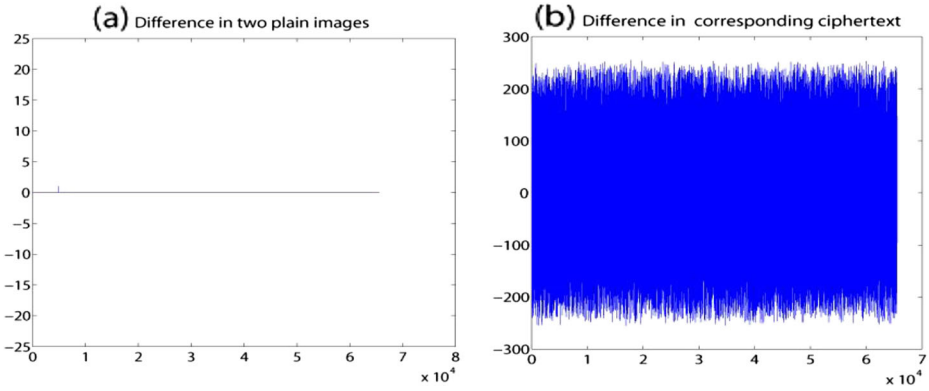


Fig. 6 Avalanche effect (**a**) Plaintext difference (**b**) Ciphertext difference

Table 6 Comparison analysis of Corr., NPCR and UACI between plain and ciphered images

Image	Lena			Pepper		
Parameters	Corr.	NPCR (%)	UACI (%)	Corr.	NPCR (%)	UACI (%)
Ref. [27]	−0.0169	99.6017	28.1370	−0.0125	99.6185	29.1988
Ref. [31]	0.0036	99.6170	29.9238	0.0040	99.6118	29.0492
Proposed	−0.0125	99.6143	28.6098	−0.0103	99.6173	29.5664

4.5 Avalanche criterion

Avalanche effect is evident if, change of one bit in the plaintext causes significant difference in the cipher bits. Accordingly, for proving the claimed sensitivity to the plaintext, two cipher images are generated from two plain images with just one-pixel difference. The bits change rate of the cipher is 49.81 % i.e., very close to the ideal value of the avalanche criterion. Thus the change of one bit in the plaintext results in a drastic change in the ciphers bits, exhibiting a substantial avalanche effect. Figure 6 demonstrates the effect of one bit change in the plain text.

4.6 Quantitative and qualitative analysis of NPCR and UACI

The discovery of differential cryptanalysis is usually attributed to Eli Biham and Adi Shamir [4, 5]. For obtaining meaningful relationship between the plain image and its cipher image, a cryptanalyst may make a slight change in the plain image such as modifying one pixel of the plain image. If this one minor change in the plain image leads to significant and unpredictable changes in the ciphered image then such differential cryptanalysis will become wasteful and defeasible. Quantitative and qualitative differential analysis on our proposed scheme shows great confusion and diffusion effect making the cipher image strongly robust against differential attacks. In image encryption, the cipher resistance to differential attacks is commonly analyzed via two widely used performance indices known as the number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI). The NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired ciphertext images, when the difference between plaintext images is subtle (usually a single pixel).

NPCR score of a secure cipher should be very close to 100 % and UACI value shall be greater than 33 %. These two measurements can be mathematically defined by Eqs. (4.3) and (4.4) where L is the gray levels. Results reveal that the proposed algorithm is able to generate secure enough ciphertext against differential attacks by offering NPCR score over 99.60 % and UACI score over 33.40 %. Table 6 lists the correlation, NPCR and UACI of the proposed scheme and the comparable cryptosystems [27, 31] calculated between plaintext and encrypted images of Lena and Pepper. The mean and standard deviation for correlation, NPCR and UACI scores of 100 encrypted images of Lena are shown in Table 7.

Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks, however it is not clear how high NPCR/UACI should be such that the image cipher indeed could have a high security level and can reflect true randomness of ciphertext. This problem is approached by Y. Wu et al. [37] who established a mathematical model for ideally encrypted images and then derived expectations, variances and hypothesis tests of NPCR and UACI (randomness tests) in order to yield qualitative results so as to test the

Table 7 Comparison of mean values for 100 encrypted images of Lena

Image	Lena					
Parameters	Corr.		NPCR (%)		UACI (%)	
	Mean	σ	Mean	σ	Mean	σ
Ref. [10]	0.0015	0.0011	99.60	0.01	33.46	0.04
Ref. [31]	−0.0009	0.0021	99.61	0.01	33.47	0.04
Proposed	0.0011	−0.0001	99.61	0.01	33.46	0.04

quality of cipher to resist the differential attacks. To calculate NPCR qualitative score, under different significance level for different sizes of image, a critical NPCR score N_a^* is exhibited in Eq. (4.4). If the actual NPCR score of encrypted image is above N_a^* then it is considered to be a true random image like image. In addition, the two critical scores U_α^{*-} and U_α^{*+} extracted by Y. Wei et al. [17] under the α level of significance are shown in Eq. (4.6). If the actual UACI score of an encrypted image falls in the range of U_α^{*-} and U_α^{*+}, it is considered to be a random like image and consequently, the UACI test is passed. While the mean and Standard deviation of UACI can be calculated using the Eqs. (4.7) and (4.8), respectively.

In Table 9, NPCR and UACI scores of 500 encrypted images, generated by changing one bit of plaintext alongwith their means, standard deviation are calculated. It is noticeable that the qualitative results of our proposed image encryption algorithm are satisfying the high performance requirements. NPCR and UACI scores of the proposed method are up to mark and pass the randomness test at a threshold of 5 % percent under significance level α=0.01 and α=0.05 for NPCR and UACI. The work outperforms some previous methods for either high NPCR and UACI quantitative or qualitative scores as evident from comparison made in Table 9. Only one image of the proposed method failed to pass the qualitative test for α=0.05. Thus, the proposed method demonstrates that the ciphertext image is true random-like. Actual scores of NPCR, UACI alongwith their mean and standard deviation are close to the ideal values.

$$N\left(C^1, C^2\right) = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{D(i,j)}{T} \times 100\% \tag{4.3}$$

$$N_\alpha^* = \frac{L - \phi_{-1}(\alpha)\sqrt{(L/H \times W)}}{L+1} \tag{4.4}$$

Table 8 Comparison of EDT of 8-bit gray level images for different image size

Image size	Ours	Ref. [10]	Ref. [15]	Ref. [31]	Ref. [19]
64×64	0.019	–	0.07	0.61	0.19
128×128	0.053	–	0.29	2.17	0.29
256×256	0.202	<0.4/<0.4	1.86	7.73	6.01
512×512	0.741	1/1	15.88	31.59	35.59
1024×1024	2.826	3/3	90.22	169.21	253.88
2048×2048	5.561	14/14	–	–	–

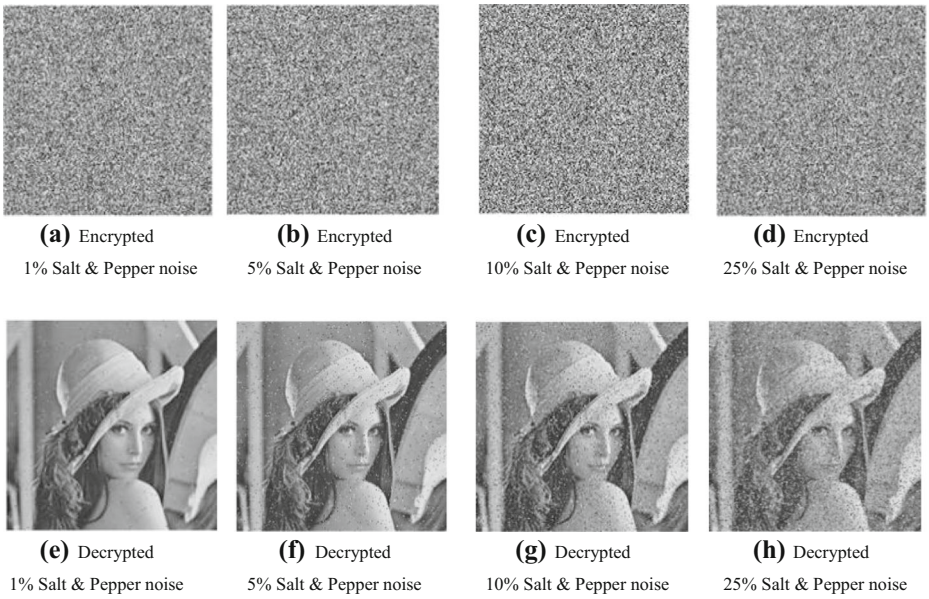


Fig. 7 The encrypted images of Lena with 1–25 % of noise and their decrypted images

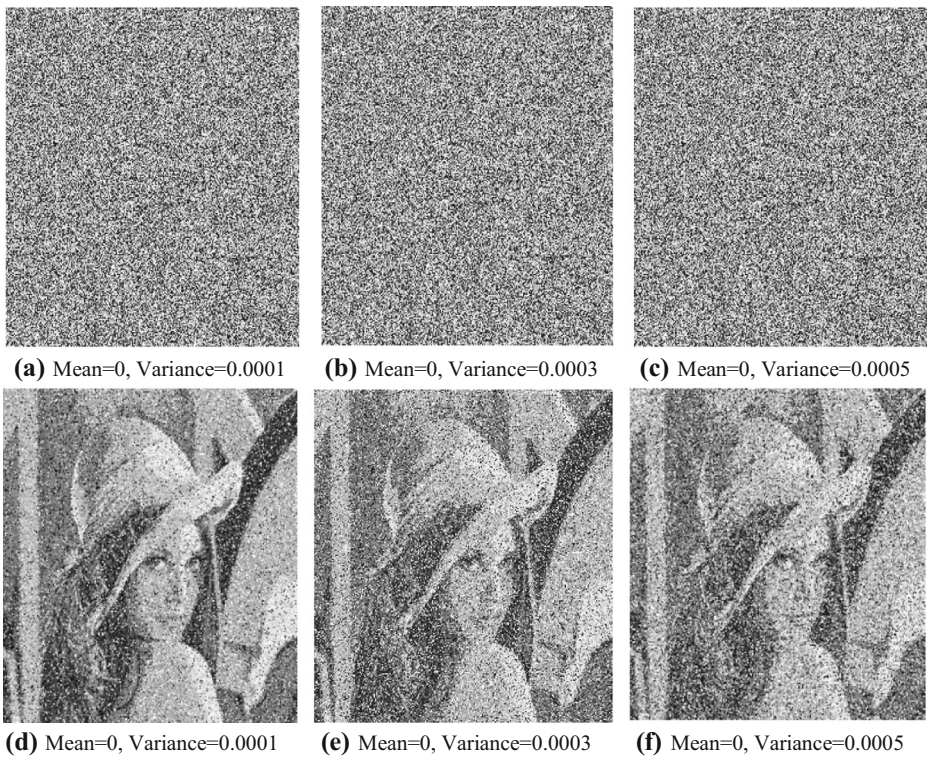


Fig. 8 The encrypted images with Guassian noise and the decrypted images

Table 9 Quantitative and qualitative NPCR and UACI analysis

Image size	Encryption method	Image	NPCR scores %					UACI scores %				
			Actual NPCR (%)	Theoretical NPCR		Actual σ	Ideal σ	Actual UACI	Theoretical UACI		Actual σ	Ideal σ
				$N^*_{0.01}$	$N^*_{0.05}$				$U^{*-}_{0.01}/U^{*+}_{0.01}$	$U^{*-}_{0.05}/U^{*+}_{0.05}$		
256×256				99.5527	99.5693		0.0244		33.2255/33.7016	33.2824/33.6447		0.0924
	Our	5.1.09	99.6144	99.6	96.0	0.0226	Pass	33.4663	100	96.0	0.0922	Pass
	Our	5.1.10	99.6085	99.2	95.4	0.0232	Pass	33.4642	99.8	97.2	0.0885	Pass
512×512	Our	5.1.11	99.6103	98.8	95.0	0.0240	Pass	33.4709	99.6	95.0	0.0883	Pass
	Our	5.1.12	99.6108	98.8	95.0	0.0254	Pass	33.4604	99.2	95.1	0.0968	Pass
	Our	5.1.13	99.6102	99.6	95.0	0.0242	Pass	33.4693	99.6	95.1	0.0964	Pass
	Our	5.1.14	99.6077	99.2	97.4	0.0240	Pass	33.4618	99.4	97.8	0.0897	Pass
	Behnia [37]	–	41.962	Fail	Fail	–	–	33.25	Fail	Fail	–	
	Our	elaine.512	99.6096	99	95.9	0.0143	Pass	33.4644	99.7	95.5	0.0452	Pass
	Our	gray21.512	99.6097	98.9	95.5	0.0136	Pass	33.4650	99.8	95.6	0.0452	Pass
	Our	5.2.08	99.6095	97.5	96.3	0.0134	Pass	33.4639	99.6	93.1	0.0469	Pass
	Our	5.2.09	99.6098	99.0	95.0	0.0122	Pass	33.4639	99.8	96.4	0.0448	Pass
	Our	5.2.10	99.6103	99.6	95.4	0.0118	Pass	33.4656	100	96.6	0.0444	Pass
	Our	7.1.02	99.6098	99.5	95.0	0.0121	Pass	33.4615	99.1	95.1	0.0449	Pass
	Our	7.1.05	99.6095	99.0	96.2	0.0119	Pass	33.4633	100	95.2	0.0461	Pass
	Chen [3]	–	99.669	Fail	Fail	–	–	25.21	Fail	Fail	–	–
1024×1024				99.5952	99.5994		0.0061		33.4040/33.5231	33.4183/33.5088		0.0231
	Our	5.3.01	99.60942	99.0	95.5	0.0060	Pass	33.4639	99.3	95.1	0.0226	Pass
	Our	5.3.02	99.60892	98.8	93.6	0.0061	Pass	33.4652	99.5	98.8	0.0240	Pass
	Our	7.2.01	99.60915	99.1	95.5	0.0060	Pass	33.4642	99.3	96.4	0.0238	Pass
	Our	testpat.1 k	99.60948	98.6	96.3	0.0061	Pass	33.4639	99.8	94.6	0.0235	Pass

Table 10 Corr., NPCR and UACI between plain and decrypted image under various level of noise

Noise (%)	Image	Corr.	NPCR (%)	UACI (%)
1	Figs. 3a and 7a	0.9820	25.6134	0.3037
5	Figs. 3a and 7b	0.9185	28.7765	1.4058
10	Figs. 3a and 7c	0.8371	32.3287	2.9360
25	Figs. 3a and 7d	0.6429	43.7149	7.1220

$$D(i,j) = \begin{cases} 0 & \text{if } C^1(i,j) = C^2(i,j) \\ 1 & \text{if } C^1(i,j) \text{¿} \neq C^2(i,j) \end{cases} \tag{4.5}$$

$$\begin{aligned} U_{\alpha}^{*-} &= \mu_U - \phi_{-1}(\alpha/2)\sigma_U \\ U_{\alpha}^{*+} &= \mu_U - \phi_{-1}(\alpha/2)\sigma_U \end{aligned} \tag{4.6}$$

$$\mu_U = \frac{L+2}{3L+3} \tag{4.7}$$

$$\sigma_U = \frac{(L+2)\left(L^2+2L+3\right)}{18(L+1)_2 L \cdot T} \tag{4.8}$$

4.7 Analysis of speed performance

Besides security consideration, EDT of the algorithm is also an important aspect for a good image cipher. In terms of computational complexity and speed performance, the algorithm is required to be fast enough so that it can be used efficiently in real time applications. Generally, EDT depends on the three factors i.e., Complexity of mathematical operations [25], Mode of operation (Block or Stream), No. of rounds required in the encryption process. In this section, speed performance of the proposed cryptographic system is analyzed. Time taken by the proposed cipher to encrypt/decrypt various different sized grayscale images have been measured. For improving speed, the above stated three measures are exercised in the proposed scheme. Fast and less complex integer

Table 11 Comparison of robustness against Gaussian Noise with Ref. [27]

Image	Proposed			Ref. [27]		
	Corr.	NPCR (%)	UACI (%)	Corr.	NPCR (%)	UACI (%)
Figs. 3a and 8a	0.6476	69.2490	11.8556	0.9584	99.2094	28.4417
Figs. 3a and 8b	0.5619	77.6642	15.0367	0.9198	99.6125	28.6448
Figs. 3a and 8c	0.4793	81.8283	17.2158	0.9079	99.6155	28.8007

operators DNA addition and subtraction (+and −), exclusive or (XOR) and modulus (mod) are employed in stream mode and one round of permutation and diffusion is enough to achieve the satisfactory result. The EDT is measured on Intel (R) Pentium 1,700 MHz with 2 GB RAM, running windows 7 Home Basic as operating system. The programming environment is MATLAB 7.13.

In Table 8, the EDT of the proposed algorithm is compared with the EDT of those reported in [31, 10, 15, 19] and it is observed that the operation speed of the proposed scheme is quite fast in comparison to the speed performance of the algorithms depicted in Table 8. They can barely appease any colossal performance requirement. In addition, with image size increasing, the time complexity of ours scheme increase linearly and attain a gain factor of 3.18 on average, relatively low to the described methods, which have multiplying factor of 3.62, 4.13, 6.19 and 8.64, respectively. Hence, the speed of our system is more stable and better for small size to large size images. Moreover, as the proposed cryptosystem indeed leads to a faster encryption speed so with such a speed, it is appropriate to be used for real time applications.

4.8 Robustness against noise and cropping

Robustness of cryptosystem against noise in a real world communication technology is one of the significant problems. When an image is transmitted electronically over the transmission channel, usually it gets infected with noise. A good encryption algorithm shall have the potential to immune such noise as a minor change in the encrypted image may induce a strong distortion in the decrypted image and thus might have the probability of not recuperating the original image. The method described in [31, 30] also have the same demerit as it does not allow to recover the image just because of an error in one pixel. A secure encryption scheme should consider the robustness against noise and shall be designed to avoid the propagation error in the decrypted image. The simulation results of the noise analysis for the proposed method depicted in Figs. 7 and 8 show that our algorithm is robust against salt & pepper noise and as well as Gaussian noise.

The top row of Fig. 7 shows the encrypted images of Lena with different saturation of Salt & Pepper noise from 1 to 25 %. The bottom row of Fig. 7 shows the correspondent decrypted

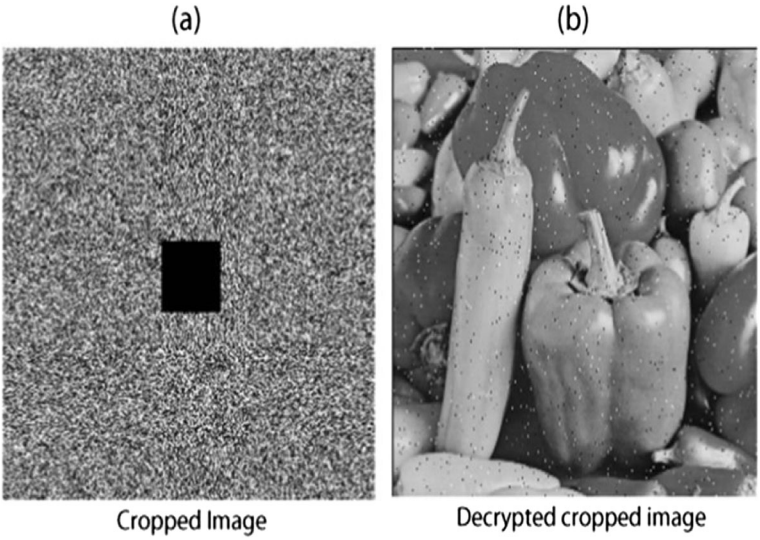


Fig. 9 Cropping effect in image Pepper

images which reflect that the proposed system is robust against noise even to one fourth of the disturbed pixel. Supplementary to above, statistically we have calculated the cross correlation, NPCR and UACI of decrypted images of Fig. 7e–h to plain image Lena of in Table 9. The fact dawns that our proposed system is not only robust against decrypting the noisy image but can also retain the high correlation and low UACI values. For better comprehension of the performance of the proposed cryptosystem, same level of Salt & Pepper noise (1–25 %) is added in the plain image shown in Fig. 3a and then the correlation, NPCR and UACI between the plain image Lena and noisy plain images are calculated. The statistical results of salt & pepper noise are shown in Table 10 while the comparative analysis of Table 11 reveals that proposed cipher is better than Ref. [27] for Gaussian noise. Hence our proposed system is not only able to decrypt the noisy encrypted image but still can also retain the high correlation and low UACI with pleasant visual quality of an image.

Likewise, an encryption algorithm should have the capability to immune the cropping effect as during transmission the data can be partially modified or lost due to some noisy system. If any part of an encrypted image gets damage during transmission, our system has the potential to recover it substantially. To validate this effect, we have cropped some part of the encrypted image Pepper as shown in Fig. 9a and its recovered image is shown in Fig. 9b. The simulation results demonstrate that the proposed image encryption scheme resists cropping effect effectively

5 Conclusion

This paper puts forward a simple yet an efficient selective grayscale image encryption scheme based on combination of 1D chaotic systems and DNA encoding. By employing complete set of DNA rules for encoding and decoding of an image alongwith MD5 hash, the proposed work outperforms in terms of speed. To augment the efficiency of the proposed algorithm and to increase the ciphertext unpredictability, the half of the image containing maximum visual information is encrypted using quaternary DNA addition operation instead of binary. 128 bit hash of plain image is used to calculate initial conditions of PWLCM and Logistic map. In addition, it is also used to calculate control parameter of PWLCM and for selection of DNA rule. Simulation results justify the high resistance of the proposed cryptosystem against different attacks. Moreover, the light of encouraging Qualitative and Quantitative analysis show that the proposed method is strong to encrypt the digital grayscale images. The predominant advantage of this approach is robustness against noise and cropping effect. In a nut shell, the glaring feature of efficiency makes the algorithm feasible for image encryption in real time applications as in terms of efficiency, it outperforms the competitive image encryption algorithms.

Acknowledgments This work was supported in part by Natural Science Foundation Project of CQ CSTC under Grant No. 201440001 and National Natural Science Foundation of China under Grant No. 61070246.

References

1. Anderson R, Schneier B (1994) Description of a new variable-length key, 64 bit block cipher (Blowfish). In: Lecture notes in computer science. Springer, Berlin Heidelberg, pp 191–204
2. Behnia S, Akhshani A, Ahadpour S, Mahmodi H, Akhavand A (2007) A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Phys Lett A 366:391–396

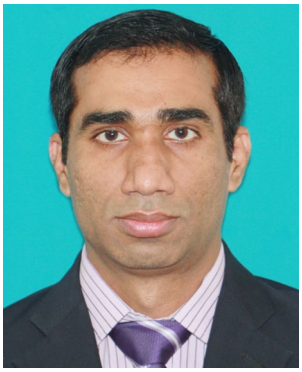
3. Behnia S, Akhshani A, Mahmodi H, Akhavan A (2008) A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons Fractals 35:408–419
4. Biham E, Shamir A (1991) "Differential cryptanalysis of DES-like cryptosystems." In: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag
5. Biham E, Shamir A (1993) "Differential cryptanalysis of the Full 16-round DES." In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag
6. Brown R, Chua LO (1996) Int J Bifurcat Chaos 6(2):219
7. Chang WC, Wong KW, Yu H, Zhu ZL (2012) An image encryption scheme using light weight bit level confusion and cascade cross circular diffusion. Opt Commun 285:2343–2354
8. Chen W, Chen X (2010) Space-based optical image encryption. Opt Express 18:27095–27104
9. Chen W, Chen X (2011) Optical image encryption using multilevel Arnold transform and non interferometric imaging. Opt Eng 50(11):117001
10. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons Fractals 21:749–761
11. Corrochano EB, Mao Y, Chen G (2005) "Chaos-based image encryption." In: Handbook of geometric computing. Springer, Berlin Heidelberg, pp 231–265
12. Enayatifar R, Abdullah AH, Isnin IF (2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt Laser Eng 56:83–93
13. FIPS PUB 197 (2001) Advanced encryption standard. New York, NY
14. FIPS PUB 46 (1977) Data encryption standard
15. Francois M, Grosges T, Barchiesi D, Erra R (2012) A new image encryption scheme based on a chaotic function. Signal Process Image Commun 27:249–259
16. Françoisa M, Grosgesa T, Barchiesia D, Errab R (2012) A new image encryption scheme based on a chaotic function. Signal Process Image Commun 27:249–259
17. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. J Bifurcat Chaos 8:1259–1262
18. Furht B, Muharemagic E, Socek D (2005) Multimedia encryption and watermarking. Springer, New York
19. Gao T, Chen Z (2007) Image encryption based on a new total shuffling algorithm. Chaos, Solitons Fractals. doi:10.1016/j.chaos.2006.11.009
20. Gehani A, LaBean TH, Reif JH (2000) DNA based cryptography. DIMACS series in discrete mathematics. Theor Comput Sci 54:233–249
21. Head T, Rozenberg G, Bladergroen RS, Breek CKD, Lommerse PHM, Spaink HP (2000) Computing with DNA by operating on plasmids. Biosystems 57(2):87–93
22. Hennelly B, Sheridan JT. Optical image encryption by random shifting in fractional fourier domains. Opt Lett 28:269–271
23. Hui CG, Kai H, Yi D (2012) Image permutation scheme based on modified logistic map, IPCSIT 52
24. King OD, Gabroit P (2007) Binary templates for comma free DNA codes. Discret Appl Math 155:831–839
25. Kumar A, Ghose MK (2011) Extended substitution-diffusion based image cipher using chaotic standard map. Commun Nonlinear Sci Numer Simul 16:372–382
26. Liu HJ, Wang XY (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
27. Liu H, Wang X, Kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12:1457–1466
28. Menezes AJ, van Oorschot PC, Vanstone SA (1997) Handbook of applied cryptography. CRC Press, Boca Raton
29. Patidara V, Pareekb NK, Purohita G, Sud KK (2011) A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Opt Commun 284(19):4331–4339
30. Pisarchik AN, Flores-Carmona NJ, Carpio-Valadez M (2006) Encryption and decryption of images with chaotic map lattices. Chaos 16(3):033118-1/6
31. Rehman A, Liao XF, Kulsoom A, Abbas SA. "Selective encryption for gray images based on chaos and DNA complementary rules". Multimed Tools Appl. doi:10.1007/s11042-013-1828-7
32. Schneier B (1999) The two fish encryption algorithm: a 128 bit block cipher. J. Wiley, New York
33. Shi X, Zhao D (2011) Color image hiding based on the phase retrieval technique and Arnold transform. Appl Opt 50:2134–2139
34. Shiu HJ, Ng KL, Fang JF, Lee RCT, Huang CH (2010) Data hiding methods based upon DNA sequences. Inf Sci 180(11):2196–2208
35. Watson JD, Crick FHC (1953) A structure for DNA. Nature 171:737–738
36. Wei X, Guo L, Zhang Q, Zhang J, Lian S (2012) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 85:290–299

37. Wu Y, Noonan JP, Agaian S (2011) "NPCR and UACI randomness tests for image encryption." In: Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), pp 31–38
38. Xiao D, Liao XF, Deng SJ (2008) Parallel keyed hash function construction based on chaotic maps. Phys Lett A 372(26):4682–4688
39. Yang M, Bourbakis N, Li S (2004) Data-image-video encryption. IEEE Pot 23(3):28–34
40. Ye G (2010) Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recogn Lett 31:347–354
41. Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. Math Comput Model 52:2028–2035
42. Zhang Q, Guo L, Wei X (2013) A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Opt Int J Light Electron Opt 124:3596–3600
43. Zhu B, Liu S, Ran Q (2000) Optical image encryption based on multifractional Fourier transforms. Opt Lett 25(16):1159–1161

Ayesha Kulsoom received her B.S. degree in Information Technology from Kohat University of Science and Technology, Kohat, Pakistan and M.S. degree in Computer Engineering from University of Engineering and Technology, Taxilla, Pakistan. Currently, she is a PhD student in College of Computer Science and Engineering, Chongqing University, China. Her primary areas of research incorporates Cryptography and Image Processing.

Xiao Di received the PhD Degree and Post Doctorate Degree in Computer Science in 2009 and 2008, respectively from Chongqing University. Currently, working as Assistant Professor at Chongqing University.

His research include papers in IEEE Transactions on Circuits and Systems-II, Information Sciences, Chaos, Solitons and Fractals, Physics Letters A, Neurocomputing, Communications in Nonlinear Science and Numerical Simulation, International Journal of Innovative Computing, Information and Control, Optics Communications and has other domestic published in academic journals related to more than 50 papers, was retrieved by SCI 37 (first author 15), EI retrieval 40 . In recent years, mainly engaged in information security, multimedia security, steganography and cryptography aspects of chaos.



Aqeel Ur Rehman received his M.Sc degree in Computer Science from The Islamia University of Bahawalpur. He received his second Master degree from Computer Engineering from UET Taxilla (CASE campus) Islamabad, Pakistan. Recently, he has completed his PhD degree in Computer Science from Chongqing University, PR. China. His primary areas of research are Non-linear dynamics and cryptography.

Syed Ali Abbas received the B.Sc degree in Mathematics from the University of Azad Jammu & Kashmir. He received his Masters in Computer Science degree from the University of the Punjab, Pakistan. Recently he has completed his PhD in computer Science from Chongqing University, PR. China. His primary areas of research are regression analysis diagnostics specifically related to software effort estimation. He is Assistant Professor in University of Azad Jammu and Kashmir.