



2010-01-01

# Chaotic Image Encryption Algorithm Based on Frequency Domain Scrambling

Jonathan Blackledge

*Dublin Institute of Technology, jonathan.blackledge@dit.ie*

Musheer Ahmad

*ZH College of Engineering and Technology, AMU, Aligarh, India*

Omar Farooq

*ZH College of Engineering and Technology, AMU, Aligarh, India*

Follow this and additional works at: <http://arrow.dit.ie/engscheleart2>

 Part of the [Digital Communications and Networking Commons](#), [Probability Commons](#), [Signal Processing Commons](#), and the [Systems and Communications Commons](#)

## Recommended Citation

Blackledge, Jonathan; Ahmad, Musheer; and Farooq, Omar, "Chaotic Image Encryption Algorithm Based on Frequency Domain Scrambling" (2010). *Articles*. Paper 16.

<http://arrow.dit.ie/engscheleart2/16>

This Article is brought to you for free and open access by the School of Electrical Engineering Systems at ARROW@DIT. It has been accepted for inclusion in Articles by an authorized administrator of ARROW@DIT. For more information, please contact [yvonne.desmond@dit.ie](mailto:yvonne.desmond@dit.ie), [arrow.admin@dit.ie](mailto:arrow.admin@dit.ie).



# Chaotic image encryption algorithm based on frequency domain scrambling

Musheer Ahmad<sup>a,\*</sup>, Omar Farooq<sup>b</sup>, Jonathan Blackledge<sup>c</sup>

<sup>a</sup>Department of Computer Engineering, ZH College of Engineering and Technology, AMU, Aligarh, India

<sup>b</sup>Department of Electronics Engineering, ZH College of Engineering and Technology, AMU, Aligarh, India

<sup>c</sup>School of Electrical Engineering Systems, Dublin Institute of Technology, Dublin, Ireland

---

## Abstract

This letter proposes an image encryption algorithm using scrambling by exploiting the features of chaotic maps suited for cryptography. The proposed algorithm performs scrambling and masking of image pixels using states of chaotic maps in a secure manner. A novel multi-level blocks scrambling scheme is employed in frequency domain to overcome the drawbacks of spatial domain scrambling. At each level of scrambling, the non-overlapping blocks of frequency coefficients are shuffled using random control parameters. To improve the statistical characteristics from cryptographic viewpoint, mixing operation is done using keystream extracted from one-dimensional chaotic map and the plain-image. As a result, the algorithm resists the chosen-plaintext/chosen-ciphertext/known-plaintext attacks, as mixing depends on plain-image. Moreover, the experimental results of keyspace, sensitivity to secret keys, entropies, gray-level distribution and maximum deviation confirm that the proposed algorithm provides high security and can be applied to protect digital images over communication channels.

*Keywords:* chaotic maps, image encryption, scrambling, frequency domain

---

## 1. Introduction

In today's world of advancement, it is a mandatory task to share, distribute and exchange the electronic information across public wired/wireless networks. Modern telecommunications technologies facilitate to transmit large amount of information in relatively short time. This brings challenges to build credible security methods for the protection of confidential and sensitive information to be transmitted. As inadequate information security leads to unauthorized access, usage, disruption or destruction of information assets. So, the information security is a hot topic of research for decades to deal the prevailing security issues. Information security relies on traditional cryptographic techniques to develop methods which can meet the security and privacy requirements. Traditional encryption schemes such as simple-DES, triple-DES, RSA, IDEA, AES are not suited to build cryptosystems for digital images, this is due to inherent features of image data like bulk data capacity and high redundancy. To encrypt digital images data, lots of encryption techniques have been proposed [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. In most of the efficient image encryption techniques, many researchers utilized chaos systems to fulfill the demand of reliable and secure protection/storage/transmission of digital images over public networks. This is because of the fact that the chaotic signals have cryptographically desirable features such as high sensitivity to initial conditions/parameters, long periodicity, high randomness and mixing [8]. These features make chaos-based image cryptosystems excellent and robust against statistical attacks. The properties like high randomness, balancedness, confusion and diffusion needed in traditional cryptographic algorithms are achieved using states of chaotic maps obtained on iterative processing.

The proposed image encryption algorithm consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete state variables of chaotic maps. The purpose of scrambling is to transform a meaningful image into a meaningless, disordered and unsystematic image to obscure real meaning of image. A secret

---

\*Corresponding author. Tel.: +91 571 272 1194; fax: +91 571 272 1194.

Email addresses: musheer.cse@gmail.com (Musheer Ahmad), omar.farooq@amu.ac.in (Omar Farooq), jonathan.blackledge@dit.ie (Jonathan Blackledge)

scrambling increases the computational complexity of potential chosen-plaintext attack, thereby making cryptanalysis of image encryption much more complicated. Many schemes have been suggested to achieve secure image scrambling; these schemes are based on Baker map [6, 10], Arnold cat map [14, 15, 17], Standard map [12] etc. These scrambling schemes have few shortcomings. Firstly, one iteration of these schemes scrambles all the pixels of an image individually and more iterations consequently require a lot of computation. Secondly, the scrambling control parameters used in the schemes are usually key independent. Lastly, these schemes scramble the image in spatial domain. Spatial domain scrambling has drawback that it keeps the statistical characteristics of image intact after scrambling. So, it is not secure to perform scrambling in spatial domain as the attacker can utilize the characteristics of scrambled image to recover the plain-image. In mixing operation, the pixels gray values are masked to enhance the statistical characteristics of image. If the keystream used in mixing operation is determined only by the key and independent of plain-image as in [11, 14, 15, 16], then such algorithms cannot resist the chosen-plaintext (*CP*) and known-plaintext (*KP*) attacks [18, 19, 20]. An efficient image encryption algorithm should have features such as: (i) high sensitivity to secret key, (ii) sufficiently large keyspace and (iii) ability to resist the cryptographic attacks through statistical analysis like gray level distribution, correlation, entropies etc [21]. Keeping all these facts under consideration, the four improvements are to be incorporated to strengthen the security of scrambling based image encryption methods:

1. Scramble blocks instead of all individual pixels to save computation.
2. Randomly generate control parameters to make scrambling key dependent.
3. Perform scrambling in frequency domain to overcome the drawbacks of spatial domain scrambling.
4. Keystream used in mixing operation must depends also on the plain-image to resist the chosen-plaintext and known-plaintext attacks.

In this letter, a chaos-based image encryption algorithm using novel multi-level blocks scrambling (MLBS) is proposed. The MLBS scrambling is performed in discrete cosine transform (DCT) domain to withstand the security threats of spatial domain scrambling. MLBS scrambling scheme reduces the number of computations require to get desirable scrambling effect. Two chaotic maps are used to perform MLBS scrambling: one map is utilized to scramble blocks of DCT coefficients, while the control parameters are randomly generated using other map. To further enforce the security, the mixing operation is done to mask the gray values of image pixels using keystream extracted from third chaotic map and the plain-image.

Rest of the letter is organized as follows: Section 2 discusses the novel multi-level blocks scrambling applied in frequency domain. Section 3 discusses the proposed image encryption algorithm. The experimental results are discussed in Section 4 followed by conclusions drawn in Section 5.

## 2. Multi-level blocks scrambling

To achieve secure image scrambling, a multi-level blocks scrambling in DCT domain is applied by employing two chaotic maps given in (2) and (3). In multi-level blocks scrambling scheme, the plain-image is broken into  $8 \times 8$  macroblocks. The DCT  $G(u, v)$  of a macroblock  $B(i, j)$  with size  $M \times M$  is determined as follows [22].

$$G(u, v) = \alpha(u)\alpha(v) \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} B(i, j) \cos \left[ \frac{(2i+1)u\pi}{2M} \right] \cos \left[ \frac{(2j+1)v\pi}{2M} \right] \quad (1)$$

$$\alpha(x) = \begin{cases} \sqrt{\frac{1}{M}} & \text{for } x = 0 \\ \sqrt{\frac{2}{M}} & \text{for } x = 1, 2, \dots, M-1 \end{cases}$$

where  $i, j, u, v = 0, 1, \dots, M-1$ . The macroblock DCT transformed image  $F(u, v)$  of plain-image  $P(i, j)$  is evaluated and then it is split into non-overlapping blocks of DCT coefficients. The size of blocks depends on the level of scrambling. MLBS scheme begins with large size blocks and the size of blocks gets reduced to half iteratively at each level. The blocks of DCT coefficients are permuted using 2D Arnold cat map given in (2).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod}(N) \quad (2)$$

Where  $(x', y')$  is new position of coordinate  $(x, y)$  and  $x', y' \in [0, N-1]$ . The control parameters  $a$  and  $b$  of scrambling are randomly generated through 2D coupled Logistic map given in (3). The 2D coupled logistic map reported in [23] has three quadratic coupling terms to strengthen its complexity. The map is chaotic when  $2.75 < \mu_1 \leq 3.4$ ,  $2.7 < \mu_2 \leq 3.45$ ,  $0.15 < \gamma_1 \leq 0.21$ ,  $0.13 < \gamma_2 \leq 0.15$  and generate chaotic sequences  $x_1, x_2 \in (0, 1)$ .

$$\left. \begin{aligned} x_1(n+1) &= \mu_1 x_1(n)(1-x_1(n)) + \gamma_1 x_2^2(n) \\ x_2(n+1) &= \mu_2 x_2(n)(1-x_2(n)) + \gamma_2 (x_1^2(n) + x_1(n)x_2(n)) \end{aligned} \right\} \quad (3)$$

To randomly generate the control parameters, first the map given in (3) is iterated for  $T$  times, these  $T$  values of  $x_1$  and  $x_2$  are discarded. The map is again iterated to generate  $x_1(i), x_2(i)$  sequences. The control parameters  $a(i), b(i)$  are evaluated from  $x_1(i), x_2(i)$  using (4).

$$\left. \begin{aligned} \psi(x_1(i)) &= 10^{14}(10^6 x_1(i) - \text{floor}(10^6 x_1(i))) \\ \psi(x_2(i)) &= 10^{14}(10^6 x_2(i) - \text{floor}(10^6 x_2(i))) \\ \theta(x_1(i)) &= (\psi(x_1(i)) \bmod 83) + 17 \\ \theta(x_2(i)) &= (\psi(x_2(i)) \bmod 107) + 19 \\ a(i) &= (\psi(x_1(i)) \bmod \theta(x_2(i))) + 1 \\ b(i) &= (\psi(x_2(i)) \bmod \theta(x_1(i))) + 1 \end{aligned} \right\} \quad (4)$$

The description of multi-level blocks scrambling scheme is as follows:

- Step 1. Evaluate macroblock DCT  $F(u, v)$  of plain-image  $P(i, j)$ .
- Step 2. Set  $I(u, v) = F(u, v)$ ,  $k = 1$ ,  $L = \log_2(N) - 1$ ,  $m = L$ .
- Step 3. Repeat Steps 4 to 7 while  $k \leq L$ .
- Step 4. Split  $I(u, v)$  into  $2^m \times 2^m$  size blocks.
- Step 5. Generate control parameter  $a(k)$  and  $b(k)$  for level- $k$  scrambling using (3) and (4).
- Step 6. Apply (2) to scramble the blocks using control parameters  $a(k)$  and  $b(k)$ , let we get  $S_k(u, v)$  scrambled image as output of level- $k$  scrambling.
- Step 7. Set  $I(u, v) = S_k(u, v)$ ,  $k = k + 1$  and  $m = m - 1$ .
- Step 8. Take inverse DCT to get final scrambled image  $S(i, j)$ .

In order to evaluate the number of computations required to scramble an image using Arnold cat map, we calculate the number of times the map given in (2) is executed. Scrambling with  $R \geq 1$  iterations needs  $65536 \times R$  computations of map (2) to permute individual pixels of an image with size  $256 \times 256$ . However, only  $2^2 + 4^2 + 8^2 + 16^2 + 32^2 + 64^2 + 128^2 = 21844$  computations are required to scramble the same image with good scrambling effect using proposed MLBS scheme in addition to DCT computation. This results into a saving of about 66.6% ( $R=1$ ), 83.3% ( $R=2$ ), 88.8% ( $R=3$ ), 91.6% ( $R=4$ ) computations as compared to the pixel level scrambling used in [14, 15, 17]. Since, the control parameters are made sensitive to secret keys, therefore the scrambling of an image becomes highly sensitive to small changes in secret keys  $x_1(0), x_2(0), T, \mu_1, \mu_2, \gamma_1, \gamma_2$ . Moreover, due to the application of scrambling in frequency domain, the statistical characteristics like gray value distribution, mean of gray values, entropy etc of scrambled image get changed. In this way, the security of scrambling is enhanced, thereby making the attack more difficult.

### 3. Proposed encryption algorithm

In the proposed encryption algorithm, the well known one-dimensional Logistic map is employed to mask the pixels gray values during mixing operation. The 1D Logistic map is defined as:

$$x_3(n+1) = \lambda x_3(n)(1-x_3(n)) \quad (5)$$

where  $x_3(0)$  is initial condition,  $\lambda$  is system parameter,  $n$  is number of iterations and  $x_3(n) \in (0, 1)$  for all  $n \geq 0$ . The map is chaotic for  $3.9 < \lambda < 4$ . The initial condition  $x_3(0)$ , parameter  $\lambda$  and an initial value  $S(0)$  constitutes the mixing

Table 1: Mean gray values of plain-images and cipher-images

Test Images	Plain-image	Cipher-image
Airplane	129.17	127.41
Baboon	129.41	127.33
Barbara	127.39	127.40
Boat	129.71	127.17
Goldhill	112.21	127.11
Lena	124.09	127.29

key. The mixing keystream is extracted from discrete state variables  $x_3(i)$  generated from (5) to improve the statistical characteristics of image  $S(i, j)$  resulted from frequency domain scrambling. The steps of proposed image encryption algorithm is as follows:

- Step 1. Apply scrambling as discussed in Section 2. Let  $S(i, j)$  be the final scrambled image obtained.
- Step 2. Arrange the pixels of scrambled image  $S(i, j)$  from left to right and then top to bottom, we get sequence  $S(1), S(2), \dots, S(N \times N)$ .
- Step 3. Perform mixing operation using  $x_3(0)$ ,  $\lambda$  and  $S(0)$  as illustrated below:
  - (a) Repeat (b) to (e) for  $i = 1$  to  $N \times N$ .
  - (b) Evaluate modified key  $x'_{3(i-1)}$  as:
$$x = \left( x_3(i-1) + \frac{S(i-1)}{256} \right)$$

$$x'_{3(i-1)} = (x - \text{floor}(x))$$
  - (c) Iterate map (5) using  $x'_{3(i-1)}$  as initial condition to get next chaotic state.
  - (d) Obtain keystream  $\Phi(i)$  from the current state of the map as:
$$\Phi(i) = \left[ x_3(i) \times 10^{14} \right] \text{mod}(256)$$
  - (e) Calculate pixel gray value  $C(i)$  of cipher-image as:
$$C(i) = S(i) \oplus \Phi(i)$$
- Step 4. Arrange the sequence of encrypted pixels  $C(1), C(2), \dots, C(N \times N)$  into a 2D cipher-image  $C(i, j)$ .

The plain-image can be recovered by executing the proposed encryption algorithm in reverse order as the proposed algorithm is symmetric and deterministic in nature.

#### 4. Experimental results

The proposed encryption algorithm is experimented with various plain-images like *Airplane*, *Baboon*, *Barbara*, *Boat*, *Goldhill* and *Lena* of  $256 \times 256$  in size. Among them, the plain-image of *Lena* and its histogram is shown in Fig. 1. The initial conditions and parameters taken for experimentation are:  $x_1(0) = 0.0215$ ,  $x_2(0) = 0.5734$ ,  $x_3(0) = 0.3915$ ,  $t = 500$ ,  $S(0) = 127$ ,  $\mu_1 = 2.93$ ,  $\mu_2 = 3.17$ ,  $\gamma_1 = 0.197$ ,  $\gamma_2 = 0.139$  and  $\lambda = 3.9985$ . The cipher-image of *Lena* and its histogram using proposed encryption algorithm is shown in Fig. 2. It is clear from the Fig. 2 that the cipher-image is indistinguishable and completely disordered. The gray value distribution of cipher-image is fairly uniform and very much different from the histogram of plain-image shown in Fig. 1. The statistical characteristics of plain-images are enhanced in such a manner that cipher-images has uniform gray level distribution and good balance property. To quantify the balance property, the mean gray values of plain-images and cipher-images are evaluated and listed in Table 1. It evident from the mean values that no matter how gray values of plain-images are distributed, the mean values for cipher-images are around 127. This shows that the cipher-images doesn't provide any information regarding the distribution of gray values to the attacker. Hence, the proposed algorithm can resist any type of histogram based attacks and strengthen the security of cipher-images significantly.

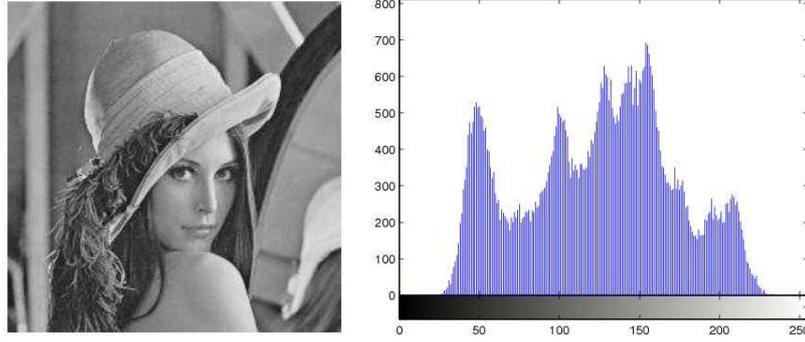


Figure 1: Plain-image of *Lena* and its histogram

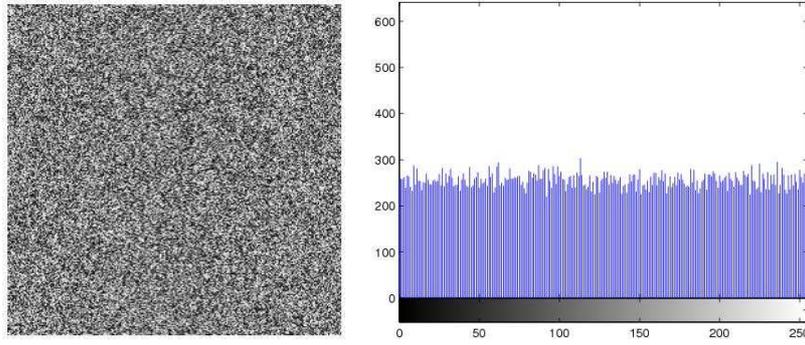


Figure 2: Cipher-image of *Lena* and its histogram

#### 4.1. Key space

Key space is the total number of different keys that can be used in a cryptosystem. A good cryptosystem should have sufficiently large key space to resist brute-force attack. In proposed algorithm, secret key consists of  $x_1(0)$ ,  $x_2(0)$ ,  $x_3(0)$ ,  $T$ ,  $S(0)$ ,  $\mu_1$ ,  $\mu_2$ ,  $\gamma_1$ ,  $\gamma_2$ ,  $\lambda$  where  $T \geq 0$  and  $0 \leq S(0) \leq 255$ . In the proposed algorithm, all the variables are declared as Matlab type *long* which is scaled fixed point format with 15 digits precision for *double*. After considering the permitted range of all initial conditions and parameters involved, the key space comes out to be  $256 \times (3.4 - 2.75) \times (3.45 - 2.7) \times (0.21 - 0.15) \times (0.15 - 0.13) \times (4 - 3.9) \times (10^{14})^8 \times T = 1.4976 \times 10^{110} \times T \approx 2^{360}$ . Thus, the key space of the proposed algorithm is extensively large enough to resist the exhaustive brute-force attack.

#### 4.2. Key sensitivity

An efficient encryption algorithm should be sensitive to secret key i.e. a small change in secret key during decryption process results into a completely different decrypted image. In proposed algorithm, an incremental change in key; even of the order of  $(\Delta =) 10^{-14}$ , results into completely unrecognizable decrypted image. The cipher-image shown in Fig. 2 is decrypted using  $x_1(0) + \Delta$ ,  $S(0) + 1$  and  $x_3(0) + \Delta$  separately, the resultant decrypted images shown in Fig. 3 are unrecognizable and noise like. Similar sensitivity is obtained for the case of wrong  $x_2(0)$ ,  $T$ ,  $\mu_1$ ,  $\mu_2$ ,  $\gamma_1$ ,  $\gamma_2$  and  $\lambda$ . Hence, it can be said that the proposed algorithm has high sensitivity to secret key.

#### 4.3. Correlation coefficient

In most of the plain-images, there exists high correlation among adjacent pixels. It is mainstream task of an efficient image encryption algorithm to eliminate the correlation of pixels. Two highly uncorrelated sequences have approximately zero correlation coefficient. The correlation coefficients between two adjacent pixels in an image is determined as:

$$\rho(x, y) = \frac{\sum_{i=1}^N [(x_i - E(x))(y_i - E(y))]}{\sqrt{\sum_{i=1}^N [x_i - E(x)]^2} \sqrt{\sum_{i=1}^N [y_i - E(y)]^2}} \quad (6)$$

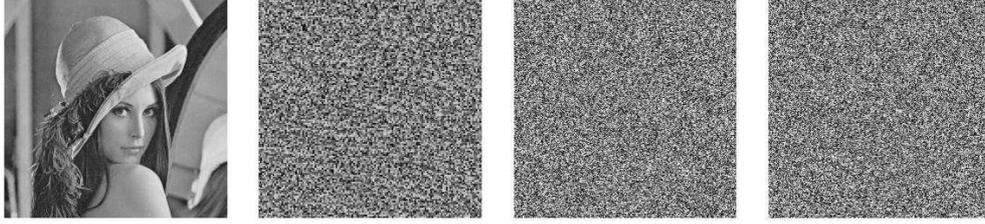


Figure 3: Key sensitivity: decrypted images with correct key,  $x_1(0)+\Delta$ ,  $S(0)+1$  and  $x_3(0)+\Delta$

Table 2: Correlation coefficient of two adjacent pixels in plain- images

Test Images	Vertical	Horizontal	Diagonal
Airplane	0.92944	0.93696	0.88629
Baboon	0.79835	0.84413	0.75661
Barbara	0.95012	0.92208	0.91518
Boat	0.94182	0.91856	0.87697
Goldhill	0.94425	0.94271	0.91066
Lena	0.95967	0.92479	0.90236

where  $E(x)=mean(x_i)$  and  $x, y$  are gray values of two adjacent pixels in the image. In the proposed algorithm, the correlation coefficient of 1000 randomly selected pairs of vertically, horizontally and diagonally adjacent pixels is determined. The average of 50 such correlation coefficients in plain-images and cipher-images in three directions are listed in Table 2 and Table 3 respectively. The values of correlation coefficients show that the two adjacent pixels in the plain-images are highly correlated to each other, whereas the values obtained for cipher-images are close to 0. This shows that the proposed algorithm highly de-correlate the adjacent pixels in cipher-images.

#### 4.4. Shannon entropy

Shannon entropy is the minimum message length require to communicate information. It measures the uncertainty associated with a random variable [24]. Entropy  $H$  of a message source  $M$  can be calculated as:

$$H(M) = - \sum_{i=0}^{255} p(m_i) \log_2(p(m_i)) \quad (7)$$

where  $p(m_i)$  represents the probability of symbol  $m_i$  and the entropy is expressed in bits. If the message source  $M$  emits  $2^8$  symbols as  $M = \{m_0, m_1, \dots, m_{255}\}$ , with equal probabilities, then the entropy of  $M$  is 8, which corresponds to a true random source and represents the ideal value of entropy for  $M$ . If the entropy of a cipher-image is significantly less than the ideal value, then there would be a possibility of predictability which threatens the image security. The

Table 3: Correlation coefficient of two adjacent pixels in cipher-images

Test Images	Vertical	Horizontal	Diagonal
Airplane	0.00108	0.00071	0.00028
Baboon	0.00357	0.00056	0.00203
Barbara	0.00062	0.00211	0.00036
Boat	0.00098	0.00151	0.00097
Goldhill	0.00031	0.00064	0.00055
Lena	0.00074	0.00253	0.00301

Table 4: Entropy of plain-images and cipher-images

Test Images	Plain-image	Cipher-image
Airplane	6.7074	7.9968
Baboon	7.2649	7.9970
Barbara	7.5482	7.9978
Boat	7.1124	7.9973
Goldhill	7.4716	7.9973
Lena	7.4439	7.9973

Table 5: Maximum deviation of cipher-images from their plain-images

Test Images	Max. deviation
Airplane	68118.0
Baboon	54069.5
Barbara	37496.5
Boat	56874.0
Goldhill	45652.5
Lena	42543.0

values of entropies obtained for plain-images and cipher-images are given in Table 4. The entropy values for cipher-images are close to the ideal value 8. This implies that the information leakage in the proposed encryption process is negligible and the encryption algorithm is secure against the entropy based attack.

#### 4.5. Maximum Deviation

The maximum deviation ( $D$ ) is used to measure the quality of encryption and it quantifies the deviation of a cipher-image from its plain-image [25, 26]. The procedure to evaluate  $D$  is as follows:

1. Count the number of pixels of each gray value in the range 0 to 255 using gray level distribution curve of plain-image and cipher-image.
2. Evaluate the absolute difference between the two computed values.
3. Calculate the area under the absolute difference curve by adding the values computed above to get the sum of deviation  $D$ .

The maximum deviation  $D$  is given as:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \quad (8)$$

where  $h_i$  is the amplitude of the absolute difference curve at gray value  $i$ . The higher the value of deviation  $D$ , the more the cipher-image is deviated from plain-image. The values of maximum deviation of cipher-images encrypted using the proposed algorithm are listed in Table 5. The large entries of Table 5 show that the cipher-images are highly deviated from their respective plain-images, which again confirms that the quality of proposed encryption algorithm is high.

#### 4.6. Resistance to KPA/CPA/CCA attacks

In the proposed algorithm, the control parameters of permutation are randomly generated from key of map (3). A tiny different key results in distinct control parameters and non-identical permuted images. Moreover, the keystream  $\Phi(i)$  used in mixing operation is extracted from key of map (5) and it also depends on plain-image. Different keystreams are generated in mixing operation when different plain-images are encrypted using proposed algorithm. Therefore, the known-plaintext ( $KP$ ), chosen-plaintext ( $CP$ ) and chosen-ciphertext ( $CC$ ) attacks are not applicable in case of proposed encryption algorithm. Hence, the proposed algorithm can resist the  $KPA/CPA/CCA$  attacks.

## 5. Conclusions

In this letter, a new chaos-based image encryption algorithm using frequency domain scrambling is presented. A multi-level blocks scrambling is employed to scramble the blocks of coefficients which saves computation. The control parameters of scrambling are randomly generated from secret key to make scrambling key dependent. Moreover, the keystream used to encrypt scrambled image is extracted from a chaotic map and plain-image. As a result, the encryption of different plain-images results in distinct keystreams and thereby resists the known-plaintext, chosen-plaintext and chosen-ciphertext attacks. All the experimental analyses show that the proposed encryption algorithm: (i) has high level of security with less computation; (ii) is highly robust towards cryptanalysis; and (iii) can be applied practically for the protection of digital images over open channels.

## References

- [1] G. Chen, X. Y. Zhao, A self-adaptive algorithm on image encryption, *Int. J. Software* 16 (1987) 1975–1982.
- [2] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN patterns, *Pattern Recognition* 25 (1992) 567–581.
- [3] K. L. Chung, L. C. Chang, Large encrypting binary images with higher security, *Pattern Recognition Lett.* 19 (1998) 461–468.
- [4] J. C. Yen, J. I. Guo, A new image encryption algorithm and its VLSI architecture, *IEEE Workshop Signal Process. Syst.* 3 (1999) 430–437.
- [5] H. Cheng, X. B. Li, Partial encryption of compressed images and videos, *IEEE Trans. Signal Process.* 48 (2000) 2439–2451.
- [6] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurc. Chaos* 8 (1998) 1259–1284.
- [7] J. Scharinger, Fast encryption of image data using chaotic kolmogorov flows, *J. Electron. Imaging* 2 (1998) 318–325.
- [8] M. S. Baptista, Cryptography with chaos, *Phys. Lett. A* 240 (1999) 50–54.
- [9] X. Liao, X. Li, J. Pen, G. Chen, A digital secure image communication scheme based on the chaotic chebyshev map, *Int. J. Commun. Syst.* 17 (2004) 437–445.
- [10] F. Han, X. Yu, S. Han, Improved baker map for image encryption, *Int. Symp. Syst. Control in Aerosp. Astronaut.* 2 (2006) 1273–1276.
- [11] N. K. Pareek, V. Patidar, K. K. Sud, Cryptography using multiple one-dimensional chaotic maps, *Commun. Nonlinear Sci. Numer. Simul.* 10 (2005) 715–723.
- [12] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of chaotic standard map, *Chaos Solitons Fract.* 26 (2005) 117–129.
- [13] B. He, F. Zhang, L. Luo, M. Du, Y. Wang, An image encryption algorithm based on spatiotemporal chaos, *Int. Congress on Image and Signal Process.* (2009) 1–5.
- [14] G. Y. Chen, Y. B. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solitons Fract.* 21 (2004) 749–761.
- [15] Z. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, *Phys. Lett. A* 346 (2005) 153–157.
- [16] T. Gao, Z. Chen, Image encryption based on a new total shuffling algorithm, *Chaos Solitons Fract.* 38 (2008) 213–220.
- [17] Z. Liehuang, L. Wenzhou, L. Lejian, L. Hong, A novel image scrambling algorithm for digital watermarking based on chaotic sequences, *Int. J. Comput. Sci. Netw. Secur.* 6 (2006) 125–130.
- [18] K. Wang, W. Pei, L. Zou, A. Song, Z. He, On the security of 3d cat map based symmetric image encryption scheme, *Phys. Lett. A* 343 (2005) 432–439.
- [19] J. Wei, X. Liao, K. Wong, T. Zhou, Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps, *Commun. Nonlinear Sci. Numer. Simul.* 12 (2007) 814–822.
- [20] D. Arroyo, C. Li, S. Li, G. Alvarez, W. A. Halang, Cryptanalysis of an image encryption based on a new total shuffling algorithm, *Chaos, Solitons and Fractals* 41 (2009) 2613–2616.
- [21] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *Int. J. Bifurc. Chaos* 16 (2006) 2129–2151.
- [22] K. R. Rao, P. Yip, *Discrete cosine transforms: algorithms, advantages and applications*, Academic Press Boston, 1990.
- [23] X. Wang, Q. Shi, New type crisis: hysteresis and fractal in coupled logistic map, *Chin. J. Appl. Mech.* 4 (2005) 501–506.
- [24] C. E. Shannon, A mathematican theory of communication, *Bell Syst. Tech. J.* 27 (1948) 379–423(Part I), 623–856(part II).
- [25] I. Ziedan, M. Fouad, D. Salem, Application of data encryption standard to bitmap and JPEG images, in: *Twentieth National Radio Sci. Conference*, pp. C16–5.
- [26] N. Fishawy, O. M. A. Zaid, Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms, *Int. J. Netw. Secur.* 5 (2007) 241–251.