INFORMATICA, 2020, Vol. 31, No. 4, 793–820

DOI: https://doi.org/10.15388/20-INFOR426

Efficient Image Encryption Scheme Based on 4-Dimensional Chaotic Maps

Ali KANSO*, Mohammad GHEBLEH, Abdullah ALAZEMI

Department of Mathematics, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait
e-mail: ali.kanso@ku.edu.kw, mohammad.ghebleh@ku.edu.kw, abdullah.alazemi@ku.edu.kw

Received: February 2020; accepted: August 2020

Abstract. This paper proposes a new family of 4-dimensional chaotic cat maps. This family is then used in the design of a novel block-based image encryption scheme. This scheme is composed of two independent phases, a robust light shuffling phase and a masking phase which operate on image-blocks. It utilizes measures of central tendency to mix blocks of the image at hand to enhance security against a number of cryptanalytic attacks. The mixing is designed so that while encryption is highly sensitive to the secret key and the input image, decryption is robust against noise and cropping of the cipher-image. Empirical results show high performance of the suggested scheme and its robustness against well-known cryptanalytic attacks. Furthermore, comparisons with existing image encryption methods are presented which demonstrate the superiority of the proposed scheme.

Key words: cryptography, chaos, cat map, pseudorandom numbers, image encryption.

1. Introduction

The rapid growth in multimedia applications has led to the vast spread of multimedia information across public networks. As a consequence, such information has become vulnerable to eavesdropping. Therefore, the need for safeguarding algorithms has become of major concern. Digital images are amongst the most popular digital media, they are found in a number of applications including military, medical and geographical applications. Due to this wide range of applications, research for developing efficient safeguarding algorithms has grasped the attention of scientists and engineers more than ever.

Cryptography is a field of mathematics and computer science that provide many security services including encryption and data hiding. Data hiding is a process that intends to hide secret information within cover media in such a way that an eavesdropper is incapable to detect the presence of such information within the carrier. On the contrary, encryption is a process that transforms secret information into scrambled data which is totally meaningless to an eavesdropper (Katz *et al.*, 1996; Rijmen and Daemen, 2001; Rivest *et al.*, 1978). Both techniques require a secret key that entitles the recipient to recover back the secret information. One disadvantage of data hiding techniques is that most schemes hide

*Corresponding author.

the raw data within the cover media (Cheddad *et al.*, 2010; Mao and Qin, 2013; Ghebleh and Kanso, 2014; Tang *et al.*, 2014). Furthermore, secret images of large sizes require quite large carriers. Due to some inherent characteristics of digital images such as bulk data capacity, high redundancy and correlation between adjacent pixels, conventional encryption schemes such as the Data Encryption Standard (DES) (Katz *et al.*, 1996), the Advanced Encryption Standard (AES) (Rijmen and Daemen, 2001), the Rivest, Shamir and Adleman's scheme (RSA) (Rivest *et al.*, 1978) are unsuitable for the encryption of digital images.

Chaotic systems have a number of important characteristics such as high sensitive dependence on initial conditions and control parameters, large keyspace, unpredictability, ergodicity, and mixing property. Furthermore, with suitable control parameters and initial conditions, they can generate random looking sequences indistinguishable from random sequences. Confusion and diffusion are two important properties of any suitable encryption scheme (Shannon, 1949). In image encryption, confusion makes the relationship between the cipher-image and the secret key as complex as possible. That is, the impact of a tiny change to the secret key results in a major change in the cipher-image. On the other hand, diffusion makes the statistical relationship between the plain-image and the cipher-image as complex as possible. That is, the impact of a tiny change in the plain-image results in a major change in the cipher-image. This complexity can be obtained by a number of permutations and substitutions. Owing to the strong relationship between the properties of chaotic systems and Shannon's principles of confusion and diffusion (Shannon, 1949), which are ideal properties in the design of a strong image encryption scheme, chaotic systems have become promising building blocks in the construction of such schemes. In 1998, Fridrich (1998) presented an elegant chaos-based image encryption scheme that consists of two phases: a shuffling phase to confuse the relationship between the cipher-image and the plain-image, and a masking phase to spread a small change in the plain-image throughout the whole cipher-image. Despite the fact that Fridrich's scheme is shown to suffer from security issues under chosen cipher-image scenario (Solak *et al.*, 2010; Xie *et al.*, 2017), Fridrich's approach has been adopted in the designs of most proposed chaos-based image encryption schemes. Throughout the last two decades, a number of chaos-based image encryption schemes have been developed (Chen *et al.*, 2004; Guan *et al.*, 2005; Behnia *et al.*, 2008; Zhang *et al.*, 2010; Liu Y. *et al.*, 2016; Hua *et al.*, 2015; Kanso and Ghebleh, 2012, 2015a; Khan *et al.*, 2017; Fu *et al.*, 2018; Khan and Shah, 2015). Chen *et al.* (2004) proposed an image encryption scheme that employs a 3-dimensional (3D) cat map. However, Chen et al.'s scheme (Chen *et al.*, 2004) is shown to be vulnerable to differential attacks (Li and Chen, 2008; Wang *et al.*, 2005). Guan *et al.* (2005) proposed an image encryption scheme based on Arnold cat map and Chen's chaotic system. Cokal and Solak (2009) proved that this scheme suffers from security weaknesses under chosen plain-image and known plain-image scenarios. Behnia *et al.* (2008) proposed a new kind of image encryption scheme based on composition of trigonometric chaotic maps. However, this scheme is shown to suffer from security issues under chosen plain-image scenario and differential attacks (Li *et al.*, 2010). Zhang *et al.* (2010) proposed an image encryption scheme based on DNA addition in conjunction with two chaotic logistic maps. Hermassi *et al.* (2014)

revealed a number of flaws including non-invertibility of Zhang et al.'s scheme (Zhang *et al.*, 2010). In Zhu (2012), Zhu proposed an image encryption scheme based on improved hyper-chaotic sequences. Li *et al.* (2013) showed that Zhu's scheme can be broken with only one known plain-image. In Liu Y. *et al.* (2016), a hyper-chaos-based image encryption algorithm with linear feedback shift registers is proposed. Zhang *et al.* (2017) showed that this scheme has some flaws due to weak security of the diffusion process and it is vulnerable to differential attacks. Hua *et al.* (2015) introduced a new 2D sine logistic modulation map and proposed a chaotic magic transform image encryption scheme. Kanso and Ghebleh (2012) proposed an image encryption scheme based on 3D cat map. In Kanso and Ghebleh (2015a), a new family of 4D cat maps is proposed together with an image encryption scheme for medical applications. Khan *et al.* (2017) proposed a chaos-based image encryption scheme that utilizes a non-linear chaotic algorithm for destroying correlation and diffusion in plain-image. In Fu *et al.* (2018), Fu et al. proposed an algorithm based on a 4D hyper-chaotic system in conjunction with the hash function SHA-224. In addition to the aforementioned schemes, the research committee has proposed a number of schemes such as those presented in Wang *et al.* (2015), Zhou *et al.* (2014), Xu *et al.* (2016), Liu *et al.* (2016), Hua and Zhou (2017), Zhou *et al.* (2013), Wu *et al.* (2014), Cao *et al.* (2018), Hua *et al.* (2019), Khan *et al.* (2017), Fu *et al.* (2018), Liu *et al.* (2019), Sun *et al.* (2020), Hemdan *et al.* (2019) and references therein.

Among the large number of image encryption schemes that have appeared in the literature, security flaws in some of these schemes have been revealed by the cryptographic community. Furthermore, the rapid advancement of digital media technology demands the attention of researchers to develop fast and efficient image encryption schemes. Arnold's cat map (Arnol'd and Avez, 1968) is one of the most studied 2D chaotic maps. Due to its characteristics, it has been widely used in a number of cryptographic applications (Guan *et al.*, 2005; Xiao *et al.*, 2009; Fu *et al.*, 2011; Ghebleh *et al.*, 2014b; Soleymani *et al.*, 2014; Kanso and Ghebleh, 2015a,b). Furthermore, a number of generalizations of the 2D cat map have appeared in the literature (Chen *et al.*, 2004; Kanso and Ghebleh, 2013). In this paper, we propose a new family of 4D chaotic cat maps that is an extension of the generalization suggested in Kanso and Ghebleh (2013) for use in cryptographic applications. The objective of this proposal is to increase the number of control parameters in the coefficient matrix defining the 4D cat map which in turn increases the size of the keyspace of any cryptographic scheme adopting the generalization. We then propose an image encryption scheme based on members of this family. The proposed scheme follows Fridrich's approach. It is composed of a light shuffling phase and a masking phase, which operate on image-blocks. The shuffling phase preforms a circular shift on the rows and columns of the image at hand in conjunction with a zigzag ordering algorithm. The masking phase uses pseudorandom sequences generated by the proposed 4D cat map for diffusion of the resulting shuffle-image. Furthermore, the masking phase applies measures of central tendency to enhance security against a number of cryptanalytic attacks such as differential attacks. The mixing is designed so that while encryption is highly sensitive to the secret key and the input image, decryption is robust against noise and cropping of the cipher-image. Simulation results are presented to demonstrate the high performance of the proposed scheme and its high security level.

The main contributions of this work are as follows:

- The method is simple and efficient.
- The encryption scheme is highly sensitive to its key and input image, while the decryption scheme is robust against various alternations such as noise and cropping of cipher-image.
- The method is block-based. Based on the block size, there is a tradeoff between the security and the speed of the proposed scheme. However, simulations show that the chosen block size makes the scheme robust to existing attacks, insensitive to cipher-image attacks, and faster than existing schemes.

The paper is organized as follows: Section 2 presents the proposed family of 4D cat maps. In Section 3, we give a detailed description of the proposed image encryption scheme. We also demonstrate the randomness of matrices generated by successive iterations of the proposed 4D cat map. Section 4 showcases the efficiency of the proposed scheme. It also presents simulation results that demonstrate the robustness of the proposed scheme against statistical attacks. In Section 5, we further analyse the security of the proposed scheme. In Section 6, we showcase the superiority of the proposed scheme over some of the existing schemes. Finally, we end the paper with some concluding remarks.

2. The 4-Dimensional Cat Map

Arnold's cat map (Arnol'd and Avez, 1968) is a chaotic map defined on the torus $\mathbb{R}^2/\mathbb{Z}^2$ by

$$\Gamma(x, y) = (x + y,\ x + 2y) \quad \bmod 1.$$

The discrete cat map can be defined accordingly by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \quad \bmod 1,$$

which starting from any initial state (x_0, y_0) defines an infinite sequence of 2-vectors. This map can be generalized (Chen *et al.*, 2004) using two positive integer parameters a and b as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \quad \bmod 1. \tag{1}$$

Further generalizations of this map to higher dimensions are also known (Chen *et al.*, 2004; Kanso and Ghebleh, 2013). Chen *et al.* (2004) proposed a generalization of the 2D cat map into a 3D cat map, where the coefficient matrix consists of six control parameters. Kanso and Ghebleh (2013) extended the generalization of the 2D cat map into a 4D cat map, where the coefficient matrix consists of four control parameters. Despite existing generalizations, in this paper we extend the generalization of the 4D cat map suggested in Kanso and Ghebleh (2013) so that the number of control parameters of the coefficient matrix increases to twelve positive integers. The increase in the number of control parameters is very beneficial to cryptographic applications since it leads to a larger keyspace of the cryptographic scheme.

We consider the following path to define a new 4 × 4 coefficient matrix for a 4D cat map. The building blocks for this definition are maps which fix two coordinates and apply Eq. (1) to the other two coordinates. More specifically, we use the six matrices

$$M_{12} = \begin{bmatrix} 1 & a_1 & 0 & 0 \\ b_1 & a_1b_1+1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad M_{23} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a_2 & 0 \\ 0 & b_2 & a_2b_2+1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$M_{34} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & a_3 \\ 0 & 0 & b_3 & a_3b_3+1 \end{bmatrix}, \qquad M_{41} = \begin{bmatrix} a_4b_4+1 & 0 & 0 & b_4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ a_4 & 0 & 0 & 1 \end{bmatrix},$$

$$M_{31} = \begin{bmatrix} a_5b_5+1 & 0 & a_5 & 0 \\ 0 & 1 & 0 & 0 \\ b_5 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad M_{24} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & a_6 \\ 0 & 0 & 1 & 0 \\ 0 & b_6 & 0 & a_6b_6+1 \end{bmatrix},$$

where $a_1, \ldots, a_6, b_1, \ldots, b_6$ are constant positive integers. Note that each M_{ij} is obtained from the identity matrix I_4 via replacing a 2 × 2 principal minor by the coefficient matrix of Eq. (1) using parameters $a = a_k$ and $b = b_k$. The 4 × 4 coefficient matrix is now defined to be

$$A = M_{12}M_{23}M_{34}M_{41}M_{31}M_{24}. \tag{2}$$

In turn, this matrix can be used in defining the 4D cat map

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \\ w_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \\ w_n \end{bmatrix} \mod 1. \tag{3}$$

It is easy to see that each matrix M_{ij} has determinant 1, thus $\det(A) = 1$. On the other hand, since this construction involves no subtraction, and since all its parameters are positive integers, each entry of the matrix A of Eq. (2) is greater than or equal to its corresponding entry in the matrix A_0 obtained with all parameters set to 1:

$$A_0 = \begin{bmatrix} 7 & 3 & 4 & 5 \\ 10 & 5 & 6 & 8 \\ 6 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 \end{bmatrix}.$$

In particular, $\operatorname{tr}(A) \geqslant \operatorname{tr}(A_0) = 20$. Now if $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ denote the (possibly complex) eigenvalues of A, then

$$\lambda_1\lambda_2\lambda_3\lambda_4 = \det(A) = 1, \quad \text{and} \quad \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 = \operatorname{tr}(A) \geqslant 20.$$

Thus at least one eigenvalue of A has modulus greater than 1, which justifies chaotic behaviour of the map of Eq. (3). See Ott (2002), Hua *et al.* (2017), Wang *et al.* (2018) for more information.

For all the experimental results presented in this work, we use the values

$$(a_1, a_2, a_3, a_4, a_5, a_6) = (1, 2, 3, 1, 7, 11) \quad \text{and}$$
$$(b_1, b_2, b_3, b_4, b_5, b_6) = (2, 1, 3, 5, 3, 3)$$

for the control parameters of the 4D cat map, while yield the coefficients matrix

$$A = \begin{bmatrix} 270 & 34 & 86 & 385 \\ 678 & 87 & 216 & 985 \\ 207 & 28 & 66 & 317 \\ 229 & 30 & 73 & 340 \end{bmatrix}, \tag{4}$$

whose eigenvalues are

$$\lambda_1 \approx 758.8966, \qquad \lambda_2 \approx 4.1140, \quad \text{and} \quad \lambda_3, \lambda_4 \approx -0.0053 \pm 0.0171\,i.$$

Since A has more than one eigenvalue greater than 1, the 4D cat map of Eq. (3) exhibits hyper-chaotic behaviour (Hua *et al.*, 2017).

3. Description of the Proposed Scheme Pr-IES

In this work, we propose an image encryption scheme that follows Fridrich's approach. The proposed scheme consists of three phases (i) a preprocessing phase for reshaping the input image, (ii) a shuffling phase for destroying any correlation between adjacent intensity values, and (iii) a masking phase that acts on the shuffle-image to change its intensity values in such a way that a tiny change in one intensity value spreads out to almost all intensity values in the cipher-image. Algorithm 1 depicts the phases of the proposed image encryption scheme.

3.1. *The Preprocessing Phase*

The size of the input image plays an important role in the performance of the proposed scheme. In the preprocessing phase, the input image J, typically a 2D (for grayscale images) or 3D (for colour images) array of bytes, is reshaped into an almost square 2D matrix J_0. This step is necessary if the number of rows of the 2D matrix is more than twice

```
Algorithm 1: The proposed image encryption scheme Pr-IES
    Data: Plain-image $J$ and the number of rounds $r$ and $s$
    Data: Initial conditions and control parameters from secret key $\mathbb{K}$
    Result: The encrypted image $J_{\text{cipher}}$
    $J_0 \leftarrow \text{Preprocess}(J)$
    $J_{\text{shuffled}} \leftarrow \text{Shuffle}(J_0, r, K_1)$, where $K_1 \in \mathbb{K}$
    $J_{\text{masked}} \leftarrow \text{Mask}(J_{\text{shuffled}}, s, K_2)$, where $K_2 \in \mathbb{K}$
    Reshape $J_{\text{masked}}$ into the shape of the input matrix $J$ to produce the encrypted
      image $J_{\text{cipher}}$
```

the number of columns or vice versa. If this condition is not attainable (e.g. if the number of rows and columns of J are primes far apart), then a padding scheme can be applied to the input image. We refer to the number of rows and columns of the resulting matrix J_0 from the preprocessing phase by m and n, respectively.

3.2. *The Shuffling Phase*

This phase aims to destroy correlations between adjacent pixels in the input image. It performs an (a, b)-circular shift on the matrix at hand in conjunction with a zigzag reordering of the entries. By an (a, b)-circular shift we mean shifting all entries of the matrix $a - 1$ places up and $b - 1$ places left, so that the (a, b)-entry is moved to the $(1, 1)$ position. Note that entries exiting the matrix from the top or from the left, enter from the opposite side in a circular fashion. This phase requires $2r$ pseudorandom numbers, where r is the number of rounds. These numbers can be obtained from a chaotic map such as the skew tent map

$$u_{i+1} = \begin{cases} \frac{u_i}{p} & \text{if } u_i \leqslant p, \\ \frac{1-u_i}{1-p} & \text{if } u_i > p, \end{cases}$$

where $p \in (0, 1)$ is a control parameter and $u_0 \in (0, 1)$. The skew tent map is widely used in cryptographic applications (Alvarez and Li, 2006; Ghebleh *et al.*, 2014a). Algorithm 2 depicts the shuffling phase of the proposed image encryption scheme.

To illustrate the shuffling phase, we present a one round toy example on the 4 × 5 matrix

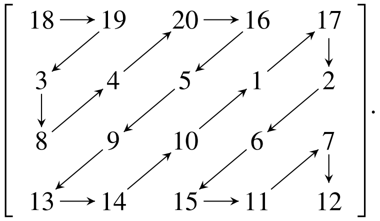
$$P_0 = J_0 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{bmatrix}.$$

```
Algorithm 2: The shuffling of the matrix $J_0$
  Data: The array $J_0$ from the preprocessing phase and the number of rounds $r$
  Data: Initial condition $u_0$ and control parameter $p$ of the skew tent map from
        secret key $\mathbb{K}$
  Result: Shuffled matrix $J_{\text{shuffled}}$
  $P_0 \leftarrow J_0$
  for $k = 1$ to $r$ do
      Generate two numbers $u$ and $v$ by successive iterations of the skew tent map
      $a \leftarrow 1 + \lfloor mu \rfloor$
      $b \leftarrow 1 + \lfloor nv \rfloor$
      $T_1 \leftarrow$ perform an $(a, b)$–circular shift on the matrix $P_{k-1}$
      $T_2 \leftarrow$ traverse $T_1$ in a zigzag order
      $P_k \leftarrow$ reshape $T_2$ into an $m \times n$ matrix
  $J_{\text{shuffled}} \leftarrow P_r$
```

Suppose $a = 4$ and $b = 3$. Performing a (4, 3)–circular shift on the matrix J_0 gives

$$T_1 = \begin{bmatrix} 18 & 19 & 20 & 16 & 17 \\ 3 & 4 & 5 & 1 & 2 \\ 8 & 9 & 10 & 6 & 7 \\ 13 & 14 & 15 & 11 & 12 \end{bmatrix}.$$

Traverse T_1 in a zigzag order as follows



This gives the 1D array

$$T_2 = [18\ \ 19\ \ 3\ \ 8\ \ 4\ \ 20\ \ 16\ \ 5\ \ 9\ \ 13\ \ 14\ \ 10\ \ 1\ \ 17\ \ 2\ \ 6\ \ 15\ \ 11\ \ 7\ \ 12].$$

Reshaping T_2 back to 4×5 matrix yields

$$P_1 = \begin{bmatrix} 18 & 4 & 9 & 1 & 15 \\ 19 & 20 & 13 & 17 & 11 \\ 3 & 16 & 14 & 2 & 7 \\ 8 & 5 & 10 & 6 & 12 \end{bmatrix}.$$

3.3. *The Masking Phase*

The masking phase acts on the shuffled matrix J_{shuffled}. It masks the rows and columns of J_{shuffled} using entries of matrices $\Omega_1, \Omega_2, \dots, \Omega_s$ consisting of pseudorandom bytes (integers in $[0, 255]$) derived from output sequences of the 4D cat map defined in Eq. (3). More specifically, each Ω_k is a $4 \times \ell$ matrix of bytes where 4ℓ is greater than or equal to the number of entries of J_{shuffled}. Columns of Ω_1 are generated via iterations of the 4D cat map with chosen control parameters. For $2 \leqslant k \leqslant s$, we define Ω_k by applying a (possibly different) 4D cat map to columns of Ω_{k-1}. It is demonstrated in Subsection 3.4 that this transition of matrices preserves pseudorandomness of entries. The masking phase also mixes the rows and the columns of the image at hand using measures of central tendency. Algorithm (3) presents a detailed description of the masking phase.

3.4. *Randomness of the Masking Matrices*

In Bassham *et al.* (2010), the National Institute of Standards and Technology (NIST) proposes a Statistical Test Suite (STS) which is one of the most popular tools for validation of random number generators and pseudorandom number generators for cryptographic applications. To assess randomness of their entries, we subject the matrices $\Omega_1, \Omega_2, \dots, \Omega_{50}$ constructed in 50 rounds of Algorithm 3 to the STS. These matrices are computed using the 4D cat map coefficient matrix A of Eq. (3) which is used also as the transition matrix in all rounds. That is, $A_2 = A_3 = \cdots = A_{50} = A$. Further parameters used in the generation of these matrices are $m = 256$, $n = 512$, and randomized initial condition $\mathbf{x}_0$. Hence each Ω_k is a 4×32768 matrix, which is passed to the STS as a sequence of 1048576 bits. Table 1 presents the results generated by the STS. On the basis of these results, we conclude that the matrices $\Omega_1, \Omega_2, \dots, \Omega_{50}$ all possess excellent randomness properties.

4. Statistical Analysis of Cipher-Images

In this section, we showcase the efficiency of the proposed scheme. We then evaluate the randomness of cipher-images corresponding to standard test images. Furthermore, we consider cipher-images corresponding to bank of test plain-images.

4.1. *Test Images and Parameters*

This section shows the efficiency of the proposed image encryption scheme Pr-IES. Figure 1 depicts standard grayscale test images Barbara of size 256×256, Lena of size 512×512 and Elaine of size 1024×1024.

Figure 2 presents the shuffle-images corresponding to the test images Barbara, Lena and Elaine for $r = 1, 2, 3$ and 4. It is evident that for $r > 3$ the shuffle-images show no pattern. On the basis of these results and the fact that a shuffle-image is almost free of correlation for $r = 5$ (as shown in Fig. 3), we consider the number of rounds for the shuffling phase to be set to 5. Similarly, it is shown in Section 5 that the image encryption

Algorithm 3: Generation of the scrambled matrix J_{masked}

```
Data: $J_{\text{shuffled}}$ from the shuffling phase and the number of rounds $s$
Data: Initial condition $\mathbf{x}_0$ and control parameters of the 4D cat map from secret
      key $\mathbb{K}$
Data: Control parameters of the coefficient matrices $A_2, A_3, \ldots, A_s$ from secret
      key $\mathbb{K}$
Result: Encrypted matrix $J_{\text{masked}}$

for $j = 1$ to $\lceil mn/4 \rceil$ do
    $\mathbf{x}_j \leftarrow A\mathbf{x}_{j-1} \mod 1$
$\Omega_1 \leftarrow \lfloor 256X \rfloor$ where $X$ is the matrix whose $j$–th column is $\mathbf{x}_j$
$\Gamma_1 \leftarrow$ reshape the first $mn$ entries of $\Omega_1$ into an $m \times n$ matrix
for $k = 2$ to $s$ do
    $\Omega_k \leftarrow A_k \Omega_{k-1} \mod 256$
    $\Gamma_k \leftarrow$ reshape $\Omega_k$ into an $m \times n$
$P_0 \leftarrow J_{\text{shuffled}}$
Initialize two $m \times n$ matrices $Q_1$ and $R_1$
for $k = 1$ to $s$ do
    for $j = 1$ to $n$ do
        if $j = 1$ then
            $\mathbf{p} \leftarrow \text{col}_n(P_{k-1})$
        else
            $\mathbf{p} \leftarrow \text{col}_{j-1}(Q_k)$
        $\mu \leftarrow$ mean of $\text{col}_j(\Gamma_k)$
        $\mathbf{p} \leftarrow \lfloor \mu \mathbf{p} \mod 256 \rfloor$
        $\mathbf{g} \leftarrow \big(\text{col}_j(P_k) + \text{col}_j(\Gamma_k)\big) \mod 256$
        $\text{col}_j(Q_k) \leftarrow \mathbf{p} \oplus \mathbf{g}$
    for $i = 1$ to $m$ do
        if $i = 1$ then
            $\mathbf{p} \leftarrow \text{row}_m(Q_k)$
        else
            $\mathbf{p} \leftarrow \text{row}_{i-1}(R_k)$
        $\mu \leftarrow$ mean of $\text{row}_i(\Gamma_k)$
        $\mathbf{p} \leftarrow \lfloor \mu \mathbf{p} \mod 256 \rfloor$
        $\mathbf{g} \leftarrow \big(\text{row}_i(Q_k) + \text{row}_i(\Gamma_k)\big) \mod 256$
        $\text{row}_i(R_k) \leftarrow \mathbf{p} \oplus \mathbf{g}$
    $Q_{k+1} \leftarrow Q_k$
    $R_{k+1} \leftarrow R_k$
    $P_k \leftarrow$ flip matrix $P_{k-1}$ in up/down direction
$J_{\text{masked}} \leftarrow P_s$
```

Table 1
Statistical Test Suite results for a matrix Ω_1 and 49 of its consecutive cat transition matrices $\Omega_2, \Omega_3, \dots, \Omega_{50}$ as described in 3.4. Each matrix is processed as a sequence of 1048576 bits. According to the STS documentation, a minimum pass rate for each statistical test is 96%.

Statistical test	Set of matrices	
	P-value	Result
Frequency	0.455937	50/50
Block-frequency	0.983453	49/50
Cumulative-sums (forward)	0.350485	50/50
Cumulative-sums (reverse)	0.383827	50/50
Runs	0.779188	49/50
Longest-runs	0.191687	48/48
Rank	0.616305	50/50
FFT	0.494392	50/50
Non-overlapping-templates	0.616305	50/50
Overlapping-templates	0.289667	50/50
Universal	0.494392	50/50
Approximate entropy	0.657933	50/50
Random-excursions	0.324180	33/33
Random-excursions variant	0.706149	33/33
Serial 1	0.383827	48/50
Serial 2	0.816537	48/50
Linear-complexity	0.213309	49/50

Barbara Lena Elaine

Fig. 1. Test plain-images Barbara of size 256 × 256, Lena of size 512 × 512 and Elaine of size 1024 × 1024.

scheme Pr-IES is robust against differential attacks when the number of rounds for the masking phase $s > 3$. Thus, $r = s = 5$ is ideal for the robustness of the proposed encryption scheme.

Figure 3 depicts the shuffle-images and cipher-images corresponding to the test plain-images Barbara, Lena and Elaine, with $r = s = 5$. It is evident that one cannot distinguish between the cipher-images and a random image.

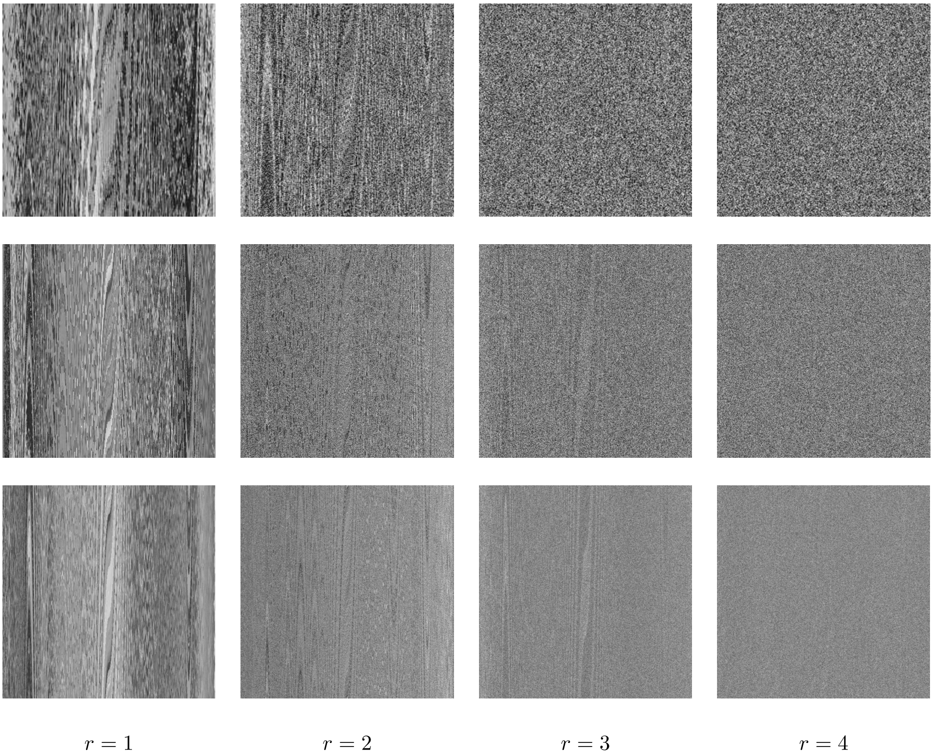


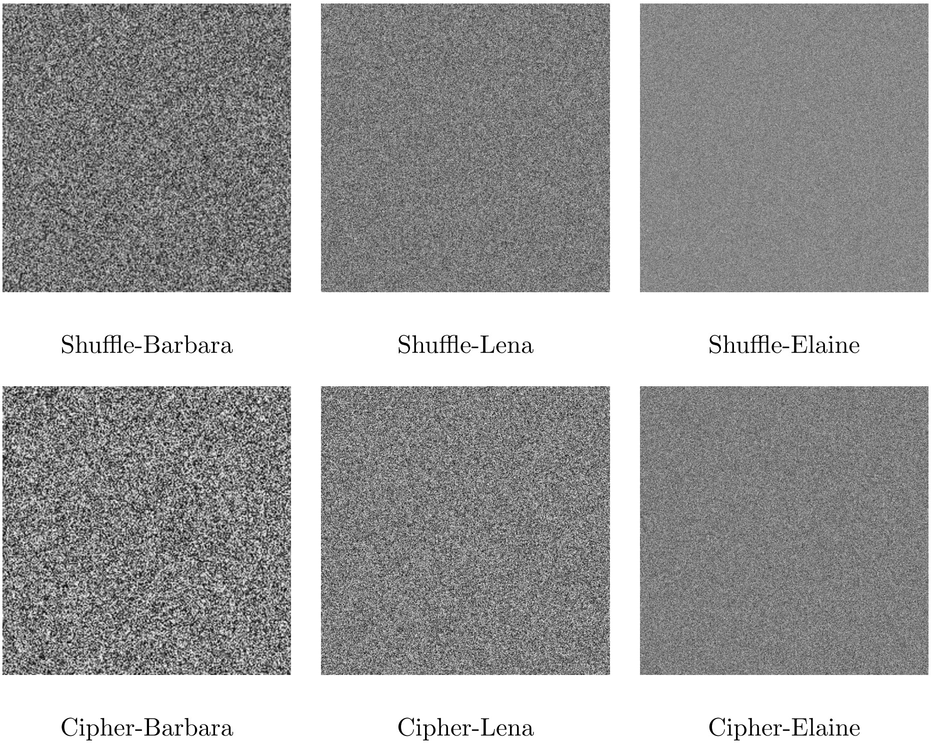
Fig. 2. The shuffle-images corresponding to the test images Barbara, Lena and Elaine.

4.2. *Histogram Analysis*

Histogram analysis is an important test which shows the distribution of the intensity values of the pixels within an image. A secure image encryption scheme produces cipher-images whose pixel intensity values are uniformly distributed in the interval [0, 255]. It is evident from Fig. 4, which depicts the histograms of the test images Barbara, Lena, Elaine and their corresponding cipher-images, that the histograms of the cipher-images are almost flat and hence show no useful information about the plain-images. Furthermore, the average pixel intensity of the cipher-images is approximately 127.50, which is the ideal value. Moreover, Table 2 reports the chi-square test (Kwok and Tang, 2007) for cipher-images and random images. It is evident that the chi-square measures for cipher-images are similar to those of random images and they are less than the upper bound 293 for a significance level 0.05.

4.3. *Correlation Analysis of Adjacent Pixels*

A secure image encryption scheme generates cipher-images almost free of any correlation. The correlation coefficients $r_{\mathbf{xy}}$ between N pairs of randomly chosen adjacent pixels $\mathbf{x} =$



Shuffle-Barbara Shuffle-Lena Shuffle-Elaine

Cipher-Barbara Cipher-Lena Cipher-Elaine

Fig. 3. The shuffle-images (top) and cipher-images (bottom) for $r = s = 5$ corresponding to the test plain-images Barbara, Lena and Elaine. The decipher-images are identical to the plain-images.

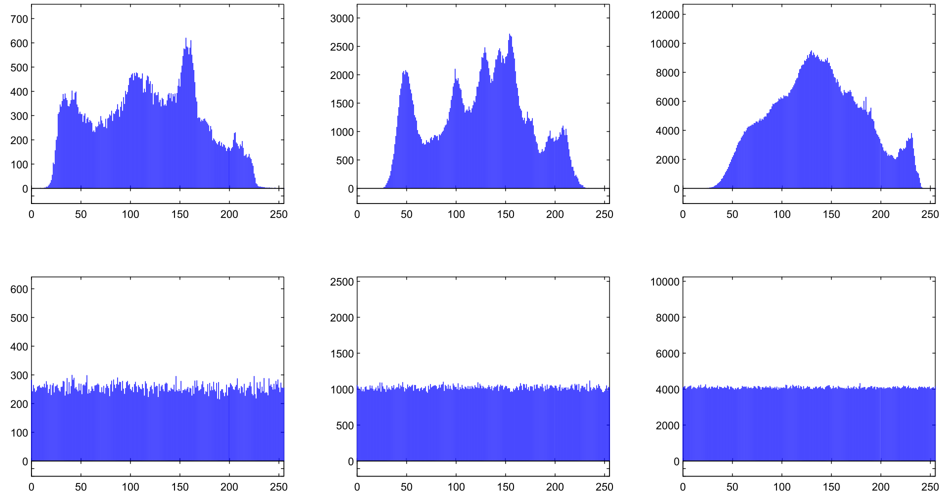
Table 2
The chi-square test results for the cipher-images corresponding to the test images Barbara, Lena and Elaine. This table also reports the chi-square value for a random image.

Cipher-image	χ^2_{test}
Cipher-Barbara	262.5859
Cipher-Lena	248.8477
Cipher-Elaine	222.1147
Random image	235.4453

$\{x_i\}_{i=1}^N$ and $\mathbf{y} = \{y_i\}_{i=1}^N$ in a given image is defined by

$$r_{\mathbf{xy}} = \frac{\operatorname{cov}(\mathbf{x}, \mathbf{y})}{\sigma_{\mathbf{x}}\sigma_{\mathbf{y}}},$$

where $\operatorname{cov}(\mathbf{x}, \mathbf{y}) = \frac{1}{N}\sum_{i=1}^N \big(x_i - E[\mathbf{x}]\big)\big(y_i - E[\mathbf{y}]\big)$, $E[\mathbf{x}]$ and $E[\mathbf{y}]$ are the expected values of the samples $\mathbf{x}$ and $\mathbf{y}$ respectively, and $\sigma_{\mathbf{x}}$ and $\sigma_{\mathbf{y}}$ are their standard deviations.



Barbara Lena Elaine

Fig. 4. Histograms of the test images Barbara, Lena and Elaine (top) and their corresponding cipher-images (bottom).

Table 3
Correlation coefficients of the test plain-images, shuffle-images and cipher-images for $N = 10000$.

Image	Adjacency	Plain-image	Shuffle-image	Cipher-image
Barbara	Horizontal	0.956279	−0.006150	−0.017363
	Vertical	0.971464	0.003786	0.007816
	Diagonal	0.935520	−0.002700	−0.016839
Lena	Horizontal	0.972826	0.006197	0.001692
	Vertical	0.986398	−0.019941	0.020036
	Diagonal	0.962357	−0.015373	−0.004486
Elaine	Horizontal	0.994613	0.015765	−0.009980
	Vertical	0.993920	−0.004081	0.008746
	Diagonal	0.989842	0.003508	−0.009003

Table 3 reports the correlation coefficients for cipher-images corresponding to the test plain-images Barbara, Lena and Elaine. Furthermore, the table presents the correlation coefficients of the shuffle-images corresponding to the test images. It is evident from this table that the correlation coefficients of the cipher-images and the shuffle-images are almost zero. Hence, the cipher-images are almost free of any correlation.

Figure 5 depicts a plot of the points (x_i, y_i), where $1 \leqslant i \leqslant 10000$, in the plain-image Lena and its corresponding shuffle-image and cipher-image. It is evident from this figure that the cipher-image is almost free of any correlation between the values of x_i and y_i. The cipher-images corresponding to the plain-images Barbara and Elaine have similar behaviour, hence are omitted.

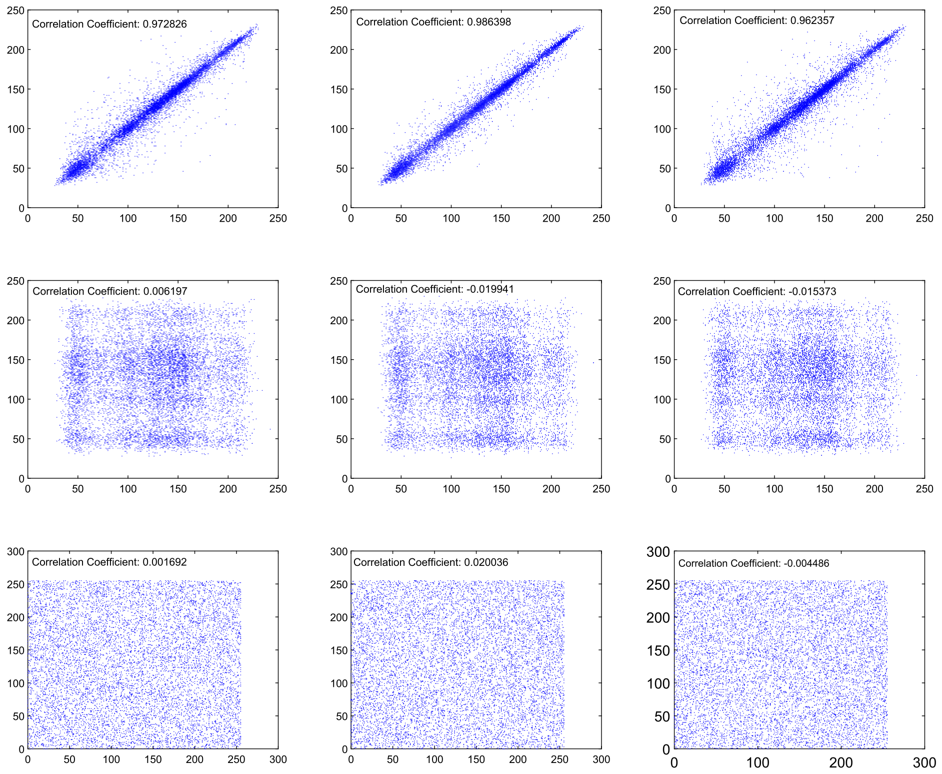


Fig. 5. Point plots of the intensity values of randomly chosen pairs of horizontally, vertically and diagonally adjacent pixels in the plain-image Lena (top), its corresponding shuffle-image (middle) and cipher-image (bottom).

4.4. *Information entropy analysis*

Information entropy (Shannon, 1948) is an important measure for evaluating the strength of an image encryption scheme. It measures the distribution of gray-values in an image. The entropy $H(\mathbf{s})$ of a source $\mathbf{s}$ emitting 256 symbols $s_1, s_2, \ldots, s_{256}$ is defined by

$$H(s) = -\sum_{i=1}^{256} P(s_i) \log_2 P(s_i),$$

where $P(s_i)$ represents the probability of occurrence of s_i. For a random source $\mathbf{s}$, $H(\mathbf{s}) = 8$. Table 4 reports the entropy measures for the test plain-images and their corresponding cipher-images. The reported measures are very close to the ideal value 8. Hence, the proposed scheme is robust against entropy attacks.

To further showcase the randomness of the proposed image encryption scheme we measure the entropy over local cipher-images blocks (Wu *et al.*, 2013). Table 5 reports the mean of entropy measures over local cipher-images blocks, where the block sizes are 16×16, 32×32 and 64×64. It is evident from this table that the reported measures are

Table 4
Entropy measures for the test plain-images Barbara, Lena, Elaine and their corresponding cipher-images.

Image	Entropy	
	Plain-image	Cipher-image
Barbara	7.6019	7.9971
Lena	7.4455	7.9993
Elaine	7.5029	7.9998

Table 5
Average entropy of image blocks.

Image	Plain-image			Cipher-image		
	16 × 16	32 × 32	64 × 64	16 × 16	32 × 32	64 × 64
Barbara	5.7160	6.5322	7.0868	7.1766	7.8076	7.9549
Lena	4.9910	5.6328	6.2260	7.1763	7.8098	7.9550
Elaine	4.7618	5.3754	5.9626	7.1759	7.8095	7.9546
Random	7.1750	7.8097	7.9542	7.1738	7.8090	7.9542

close to the theoretical mean of Shannon entropy measures for a random image, that is 7.174966353, 7.808756571 and 7.954588734 for 16 × 16, 32 × 32 and 64 × 64 blocks, respectively (Wu *et al.*, 2013). Table 5 also includes the mean of local entropy measures for a random image and its corresponding cipher-image.

4.5. *Randomness Analysis*

In this section, we evaluate the randomness of cipher-images generated by the proposed scheme Pr-IES using the STS proposed by the National Institute for Standards and Technology (NIST) (Bassham *et al.*, 2010). For this regard, we consider the first 100 images from the test bank of images in BOWS2 (2019). We encrypt each 512 × 512 image by the proposed scheme, and subject the resulting cipher-image to the STS. Each cipher-image consists of 2097152 bits and is processed in STS as a single sequence. Table 6 reports the STS results for a collection of 100 cipher-images, each of length 2097152 bits. According to documentation of the STS documentation (Bassham *et al.*, 2010), the minimum pass rate for each test is 96%. Thus, it is evident that the cipher-images pass all 15 test and hence, they possess very good randomness properties.

4.6. *Speed Analysis*

In this section, we report the running speed of the proposed image encryption scheme Pr-IES in MATLAB on a desktop machine with an Intel® Core™ i7-4770 processor and 8GB of memory, running Windows 10. Table 7 reports the running time for encrypting the test images by the proposed scheme. Furthermore, Fig. 6 shows a sample of the running times for encrypting grayscale images of different sizes by the proposed image encryption scheme with $r = s = 5$.

Table 6
Statistical Test Suite results for 100 cipher-images, each of length 2097152 bits.

Statistical test	Cipher-images	
	P-value	Result
Frequency	0.911413	98/100
Block-frequency	0.366918	100/100
Cumulative-sums (forward)	0.924076	97/100
Cumulative-sums (reverse)	0.851383	98/100
Runs	0.334538	100/100
Longest-runs	0.419021	99/100
Rank	0.816537	99/100
FFT	0.108791	99/100
Non-overlapping-templates	0.897763	100/100
Overlapping-templates	0.739918	100/100
Universal	0.994250	98/100
Approximate entropy	0.657933	98/100
Random-excursions	0.534146	72/72
Random-excursions variant	0.846579	72/72
Serial 1	0.719747	99/100
Serial 2	0.191687	99/100
Linear-complexity	0.289667	99/100

Table 7
Running time of the proposed encryption scheme.

Size	Encryption time in seconds
256 × 256	0.0644554
512 × 512	0.2422222
1024 × 1024	1.0021399

5. Security Analysis

In this section, we evaluate the security level of the proposed scheme. We show that the proposed scheme Pr-IES is highly sensitive to a slight modification in the plain-image. We further show that the scheme has a large keyspace, and it is highly sensitive to its secret key and control parameters. Moreover, we analyse the security of the proposed scheme under cipher-image scenario and chosen plain-image scenario. In addition to that, we demonstrate the robustness of its decryption to various alterations in the cipher-image.

5.1. *Differential analysis*

Differential analysis of an image encryption scheme investigates the affect of a slight modification in the plain-image on the corresponding cipher-image. In this section, we measure the sensitivity of the proposed image encryption against slight modification in the plain-image. The Number of Pixels Change Rate (NPCR) and Unified Average Chang-

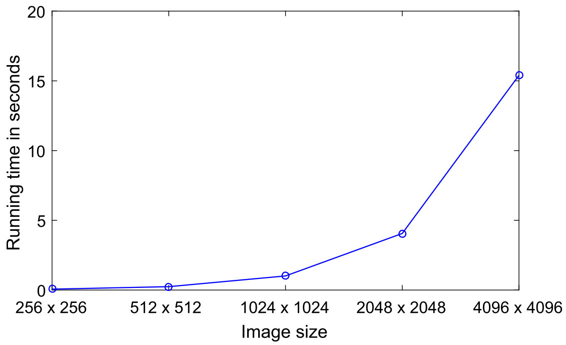


Fig. 6. Encryption time versus image size.

Table 8
Acceptance intervals for the null hypothesis with different levels of significance (Wu *et al.*, 2011).

Parameter	Size	0.05-level	0.01-level	0.001-level
NPCR	256 × 256	[99.5693, 100]	[99.5527, 100]	[99.5341, 100]
	512 × 512	[99.5893, 100]	[99.5810, 100]	[99.5717, 100]
	1024 × 1024	[99.5994, 100]	[99.5952, 100]	[99.5906, 100]
UACI	256 × 256	[33.2824, 33.6447]	[33.2255, 33.7016]	[33.1594, 33.7677]
	512 × 512	[33.3730, 33.5541]	[33.3445, 33.5826]	[33.3115, 33.6156]
	1024 × 1024	[33.4183, 33.5088]	[33.4040, 33.5231]	[33.3875, 33.5396]

ing Intensity (UACI) are two measures used to evaluate the strength of image encryption schemes against differential attacks (Wu *et al.*, 2011). Suppose C_1 and C_2 are two $m \times n$ matrices, then the NPCR and UACI between C_1 and C_2 are given by

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{m \times n},$$

where

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j), \\ 0 & \text{otherwise}, \end{cases}$$

and

$$\mathrm{UACI} = \frac{1}{m \times n} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}.$$

According to Wu *et al.* (2011), the theoretical ideal NPCR and UACI measures for C_1 and C_2 to be random-like in comparison are approximately 99.6094% and 33.4635%, respectively. Furthermore, Table 8 reports the acceptance intervals for the null hypothesis with different significance levels for the NPCR and UACI measures.

Table 9
NPCR and UACI measures between cipher-images C_1 and C_2 corresponding to the test images Barbara, Lena and Elaine, with slight modifications.

Measures	Cipher-images of Barbara			Cipher-images of Lena			Cipher-images of Elaine		
	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max
NPCR	99.5483	99.6093	99.6796	99.5819	99.6110	99.6399	99.5972	99.6089	99.6252
UACI	33.2820	33.4913	33.6932	33.3231	33.4388	33.5638	33.4136	33.4649	33.5160

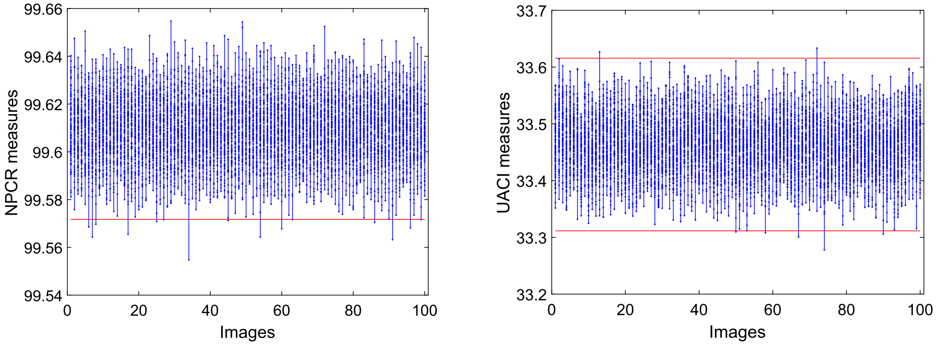


Fig. 7. NPCR (left) and UACI (right) measures for plain-image sensitivity of the proposed scheme. Each point represent an NPCR/UACI measure resulting from repeating the test 100 for each test image in (BOWS2).

We evaluate the robustness of the proposed image encryption scheme by considering two plain-images P_1 and P_2, where P_1 and P_2 differ in a single bit. We encrypt P_1 and P_2 using the proposed image encryption scheme, with the same secret key and parameters, to get cipher-images C_1 and C_2, respectively. We then compute the NPCR and UACI measures between C_1 and C_2. For each test image Barbara, Lena and Elaine, we repeat this test 100 times, where each time we flip the least significant bit of a randomly selected intensity value in the plain-image (including the first and the last intensity value). The minimum, mean and maximum NPCR and UACI measures of the ciphers-images of the original plain-image for each of the 100 cipher-images resulting from a slight modification to the original plain-image are reported in Table 9.

We further evaluate the robustness of the proposed scheme by subjecting each of the first 100 test images from (BOWS2) to the plain-image sensitivity test. For each plain-image we repeat the test 100 times, where each time we make a change to the least significant bit of a randomly chosen intensity value of the original plain-image. It turns out that the pass rate for the NPCR is 99.85% and that for the UACI is 99.93%. Figure 7 depicts a point plot, where each point corresponds to an NPCR/UACI measure resulting from repeating the sensitivity test 100 times for each of the 100 images from (BOWS2). It is evident from this figure that the proposed scheme is robust against plain-image sensitivity.

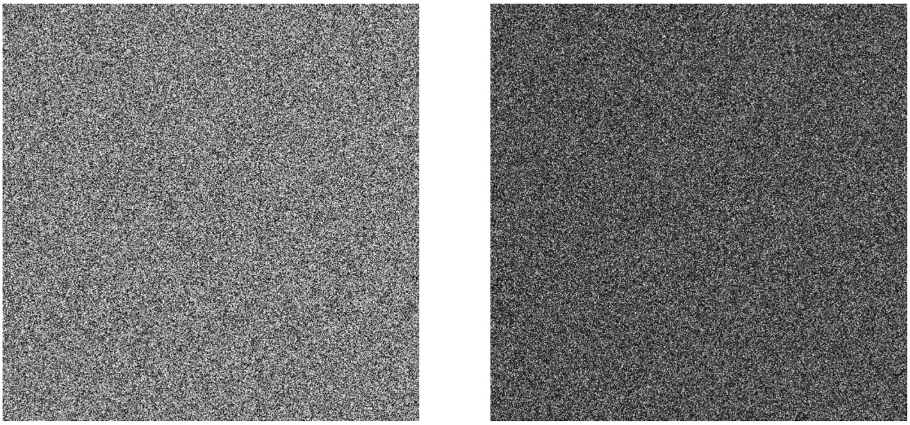


Fig. 8. Bitwise xor between cipher-images C_1 and C_2 corresponding to Lena with $\mathbb{K}_1$ and $\mathbb{K}_2$. Left: $\mathbb{K}_2$ differs from $\mathbb{K}_1$ by 10^{-14} in one component of the initial condition of the 4D cat map. Right: $\mathbb{K}_2$ differs from $\mathbb{K}_1$ in the least significant bit of one control parameter of the 4D cat map.

5.2. *Keyspace*

The secret key $\mathbb{K}$ of the proposed scheme is composed of two doubles $p, u_0 \in (0, 1)$ for the shuffling phase, as well as control parameters and initial conditions of the 4D cat map(s) used in the masking phase. In the latter, there are at least 12 positive integers (for control parameters) and four doubles in $(0, 1)$. Under the assumption that 64-bit doubles and 8-bit integers are used to initialize the cat map, and with the commonly used precision of 10^{-14} for 64-bit doubles, the secret key of the proposed scheme has size at least $\left(2^8\right)^{12} \cdot \left(10^{14}\right)^6 > 2^{375}$. This number renders key search attacks impractical. The keyspace may further expand if we consider distinct transition matrices $A_2, A_3, \ldots, A_s$ in Algorithm (3). In such a case the size of the keyspace becomes $\left(2^8\right)^{12s} \cdot \left(10^{14}\right)^6$, which with $s = 5$ yields a keyspace of size larger than $> 2^{759}$.

Figure 8 depicts the bitwise xor (exclusive or) of two cipher-images C_1 and C_2 corresponding to the test image Lena with slightly different keys $\mathbb{K}_1$ and $\mathbb{K}_2$. Figure 9 shows histograms of the images presented in Fig. 8. Furthermore, Table 10 reports the NPCR and UACI measures between cipher-images C_1 and C_2 of the three test images Barbara, Lena and Elaine generated using slightly different keys.

The experimental results presented in Fig. 8, Fig. 9, and Table 10 demonstrate high sensitivity of the proposed scheme to its secret key, hence its robustness against key search attacks.

5.3. *Cipher-Image and Plain-Image Analysis*

In this section, we show that the proposed scheme is robust against cipher-image and plain-image analysis. In a cipher-image attack, the intruder has only access to the cipher-image. Since the above tests show that no useful information about the plain-image can be gained

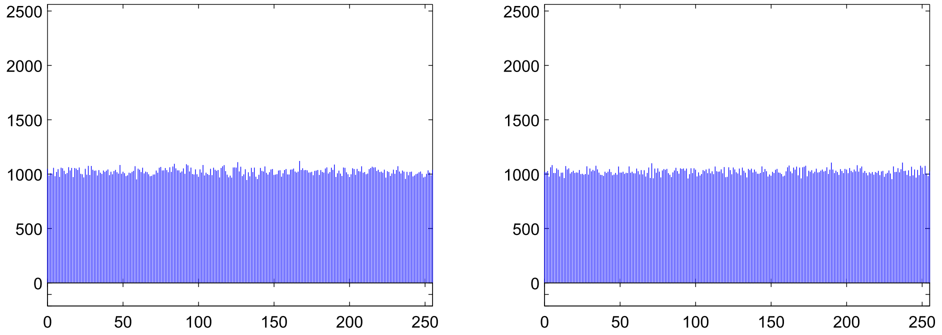


Fig. 9. Histograms of the two images of Fig. 8, respectively.

Table 10
NPCR and UACI measures between cipher-images C_1 and C_2 corresponding to the test images Barbara, Lena and Elaine, with slight modifications in the secret key.

Measures	Cipher-images of Barbara		Cipher-images of Lena		Cipher-images of Elaine	
NPCR	99.6338	99.6124	99.6002	99.6101	99.6215	99.6066
UACI	33.6906	33.4831	33.3946	33.4988	33.4807	33.4435

from the corresponding cipher-image, we conclude that the proposed scheme is robust against this type of attack. In a plain-image attack, the intruder can choose any part of the plain-image and request its corresponding cipher-image part. The aim of this attack is to reconstruct some other plain-image parts. The fact that the chaotic map possesses the one-way property due to floating point errors makes the inverse computation very difficult. Furthermore, since the proposed scheme is highly dependent on its secret key, one cannot predict further outputs of the 4D cat map. Thus, the scheme is robust against this type of attacks.

5.4. *Robustness to Noise and Data Loss*

Earlier, we have shown that the proposed scheme is highly sensitive to its secret key, and it is also highly sensitive to a tiny change in its input plain-image. That is, a change in a plain-image intensity value spreads over all intensity values in the corresponding cipher-image. In this section, we show that a change in intensity values in the cipher-image affects only few intensity values in the corresponding plain-image. The importance of this feature is that with distortion of cipher-images due to salt and pepper noise or data loss one can still successfully recover the corresponding plain-image. Figure 10 depicts median filtered recovered plain-image Lena resulting from subjecting its corresponding cipher-image to salt and pepper noise for different levels of added noise. Figure 11 depicts the median filtered recovered plain-image Lena resulting from subjecting its corresponding cipher-image to data loss for different sizes of data loss.

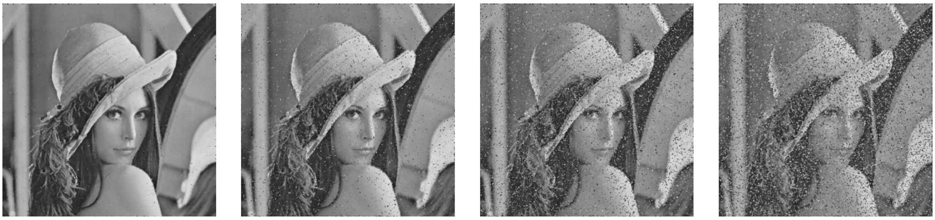


Fig. 10. The reconstructed plain-image Lena resulting from subjecting its corresponding cipher-image to a 1%, 2%, 3% and 4% salt and pepper noise.

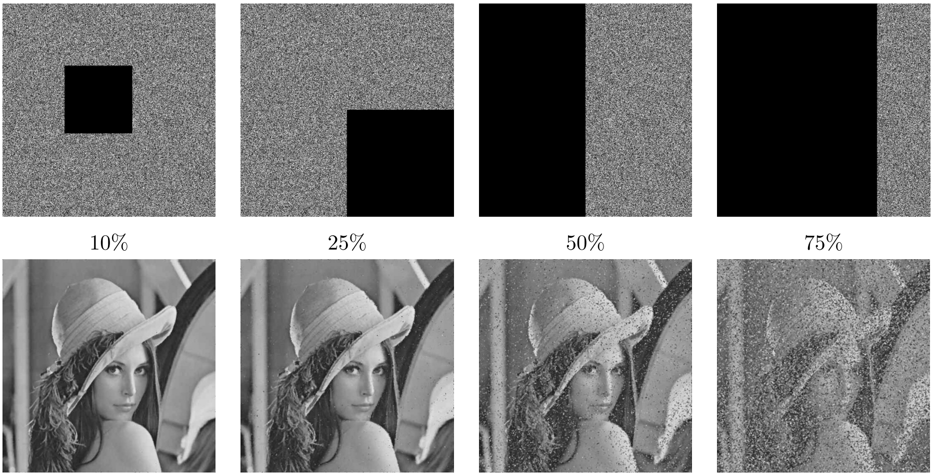


Fig. 11. The reconstructed plain-image Lena (bottom) resulting from subjecting its corresponding cipher-image to a 10%, 25%, 50% and 75% data loss (top).

6. Comparison with Existing Work

In this section, we compare the performance of the proposed scheme Pr-IES with existing ones. Figure 12 presents NPCR and UACI measures for cipher-images corresponding to 25 test images in Test-images (2019) for a number of existing schemes. There are 7 test images of size 256 × 256 (top), 15 of size 512 × 512 (middle) and 3 of size 1024 × 1024 (bottom). Figure 12 shows that the pass rate for the proposed scheme is 25/25 with $\alpha = 0.05$ significance level for the NPCR and UACI measures. Table 11 reports the schemes under comparison and the pass rate of each scheme.

We further compare the correlation coefficients between adjacent pixels of the proposed scheme and existing ones. Figure 13 depicts the correlation coefficients between adjacent intensity values in the horizontal, vertical and diagonal directions for the test image Lena and its corresponding cipher-images generated by the proposed scheme and existing schemes. Note the schemes proposed in Fu *et al.* (2011) and Liao *et al.* (2010) are referred to by FLMLC and LLZ, respectively.

Table 11
The NPCR and UACI pass rates of the proposed scheme and some existing schemes. The pass rates for the schemes under comparison are quoted from Hua *et al.* (2019).

Scheme	Pass rate	
	NPCR	UACI
WWZ (Wang *et al.*, 2015)	23/25	22/25
ZBC1 (Zhou *et al.*, 2014)	15/25	6/25
XLLH (Xu *et al.*, 2016)	23/25	23/25
LSZ (Liu *et al.*, 2016)	23/25	23/25
HZ (Hua and Zhou, 2017)	24/25	24/25
ZBC2 (Zhou *et al.*, 2013)	23/25	7/25
WZNA (Wu *et al.*, 2014)	23/25	22/25
CSL (Cao *et al.*, 2018)	24/25	25/25
HZH (Hua *et al.*, 2019)	25/25	25/25
Pr-IES	25/25	25/25

Table 12
Running time in seconds for encrypting a single image by existing schemes and the proposed encryption scheme Pr-IES. The running times for the schemes under comparison are quoted from Hua *et al.* (2019) used under license CC BY-NC-ND 4.0 (License, 2020).

Image size	128 × 128	256 × 256	512 × 512	1024 × 1024
(Diaconu, 2016)	0.0579	0.2224	0.9731	3.8377
(Ping *et al.*, 2018)	0.0902	0.3440	1.3357	5.3223
(Chai *et al.*, 2017)	0.2757	0.9810	3.8539	15.4565
(Hua and Zhou, 2017)	0.1531	0.6347	2.4913	9.9185
(Xu *et al.*, 2016)	0.0247	0.1164	0.4924	20.144
(Zhou *et al.*, 2014)	0.0933	0.3843	1.4824	5.8175
(Liao *et al.*, 2010)	0.0323	0.1440	0.5510	2.0864
(Hua *et al.*, 2019)	0.0244	0.0949	0.4010	1.9857
Pr-IES	0.0217	0.0645	0.2422	1.0021

Table 12 reports the running time in seconds for encrypting a single image with some existing schemes and the proposed scheme. The reported running times for the schemes under comparison are quoted from Hua *et al.* (2019). According to Hua *et al.* (2019), the reported running times for existing schemes are obtained on a computer under the following environments: Intel® Core™ i7-7700 CPU @3.60 GHz and 8 GB of memory, running Windows 10 operating system. While the reported running times for the proposed scheme Pr-IES are obtained on a desktop machine with an Intel® Core™ i7-4770 processor @3.40 GHz and 8GB of memory, running Windows 10 operating system.

It is evident from the obtained results that the proposed scheme has superiority over existing schemes and competitive with others.

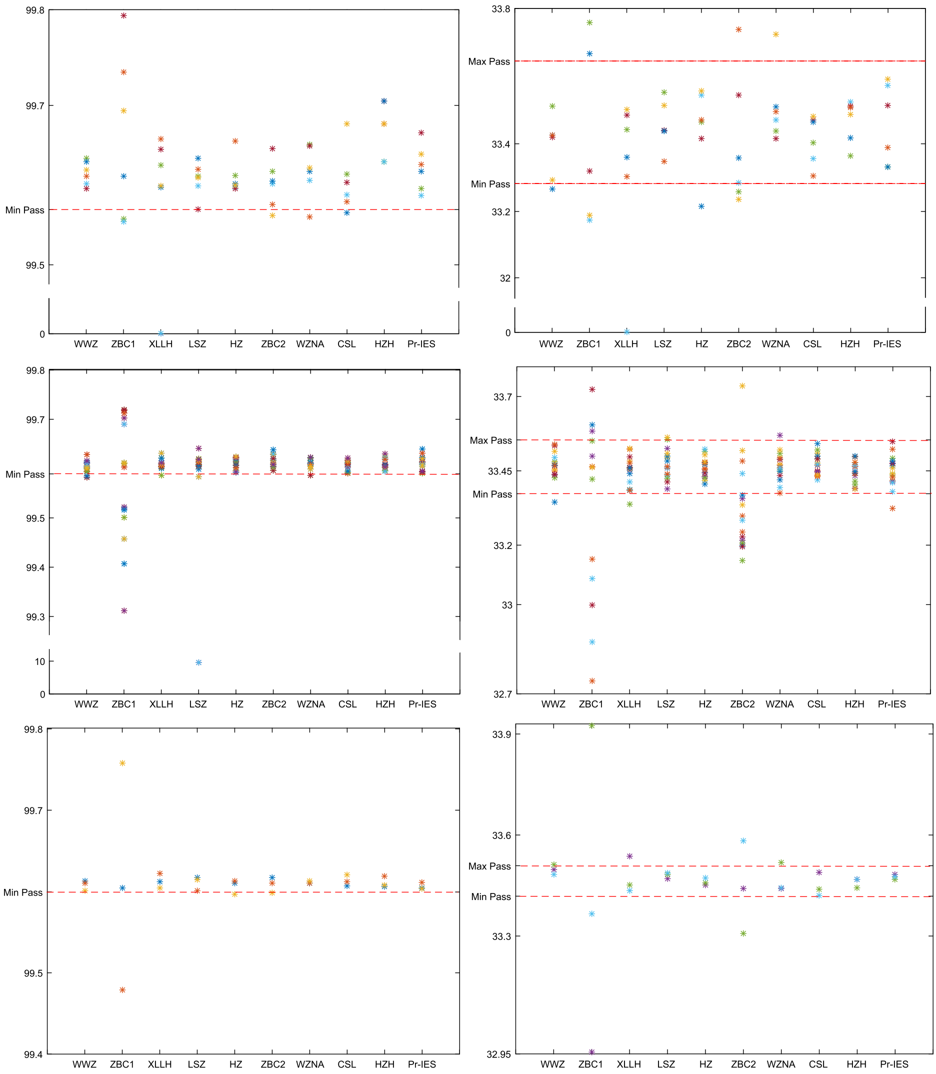


Fig. 12. NPCR (left) and UACI (right) measures for cipher-images generated by existing image encryption schemes and the proposed scheme. The measures for existing schemes are obtained from Hua *et al.* (2019).

7. Conclusion

We propose a new family of 4D chaotic cat maps. As an application of these maps, we present a novel block-based image encryption scheme utilizing them. This scheme consists of a light shuffling phase and a masking phase which uses measures of central tendency for mixing the image blocks. While encryption is highly sensitive to the secret key and the input image, decryption is robust against noise and cropping of the cipher-image. Simulations show that the proposed scheme generates cipher-images possessing high ran-

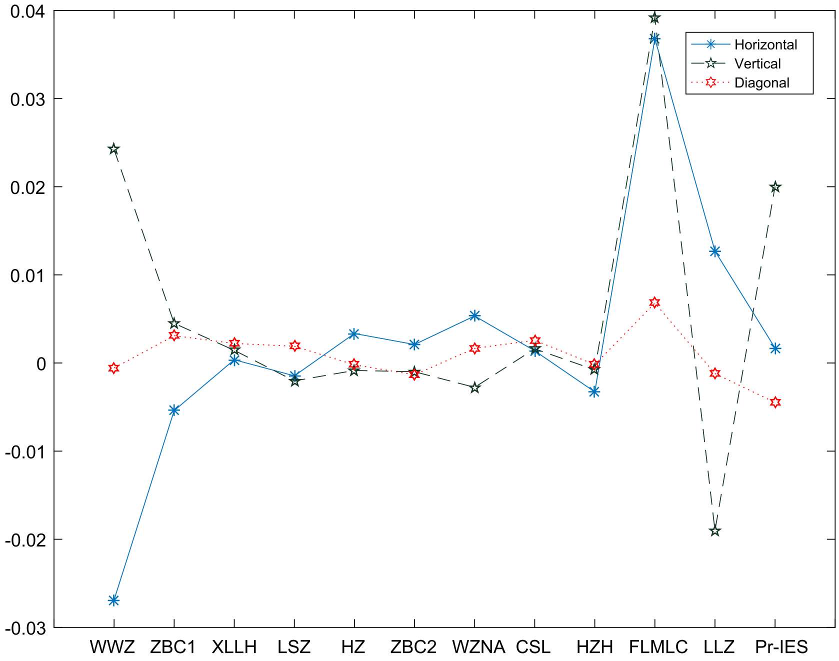


Fig. 13. Adjacent intensity values correlation coefficients for the test image Lena and corresponding cipher-images generated by existing schemes and the proposed scheme. The values for existing schemes are obtained from Hua *et al.* (2019).

domness properties. Furthermore, the scheme is shown to be robust against differential cryptanalysis. With respect to existing works, the proposed scheme is shown to have superior performance over existing image encryption algorithms and to be competitive with others.

Acknowledgements

The authors are grateful to the anonymous referees whose remarks helped improve the presentation of this work.

References

Alvarez, G., Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, 16(08), 2129–2151.

Arnol'd, V.I., Avez, A. (1968). *Ergodic Problems of Classical Mechanics*. WA Benjamin.

Bassham, L.E. III., Rukhin, A.L., Soto, J., Nechvatal, J.R., Smid, M.E., Barker, E.B., Leigh, S.D., Levenson, M., Vangel, M., Banks, D.L. (2010). Sp 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications.

Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A. (2008). Chaotic cryptographic scheme based on composition maps. *International Journal of Bifurcation and Chaos*, 18(01), 251–261.

Cao, C., Sun, K., Liu, W. (2018). A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Processing*, 143, 122–133.

Chai, X., Chen, Y., Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, 88, 197–213.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P. (2010). Digital image steganography: survey and analysis of current methods. *Signal Processing*, 90(3), 727–752.

Chen, G., Mao, Y., Chui, C.K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3), 749–761.

Cokal, C., Solak, E. (2009). Cryptanalysis of a chaos-based image encryption algorithm. *Physics Letters A*, 373(15), 1357–1360.

Diaconu, A.-V. (2016). Circular inter-intra pixels bit-level permutation and chaos-based image encryption. *Information Sciences*, 355, 314–327.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, 8(06), 1259–1284.

Fu, C., Lin, B-b., Miao, Y-s., Liu, X., Chen, J-j. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics Communications*, 284(23), 5415–5423.

Fu, C., Zhang, G.-Y., Zhu, M., Chen, J.-X., Lei, W.-M. (2018). A fast chaos-based colour image encryption algorithm using a hash function. *Informatica*, 29(4), 651–673.

Ghebleh, M., Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. *Communications in Nonlinear Science and Numerical Simulation*, 19(6), 1898–1907.

Ghebleh, M., Kanso, A., Noura, H. (2014a). An image encryption scheme based on irregularly decimated chaotic maps. *Signal Processing: Image Communication*, 29(5), 618–627.

Ghebleh, M., Kanso, A., Own, H.S. (2014b). A blind chaos-based watermarking technique. *Security and Communication Networks*, 7(4), 800–811.

Guan, Z.-H., Huang, F., Guan, W. (2005). Chaos-based image encryption algorithm. *Physics Letters A*, 346(1–3), 153–157.

Hemdan, A.M., Faragallah, O.S., Elshakankiry, O., Elmhalaway, A. (2019). A fast hybrid image cryptosystem based on random generator and modified logistic map. *Multimedia Tools and Applications*, 78(12), 16177–16193.

Hermassi, H., Belazi, A., Rhouma, R., Belghith, S.M. (2014). Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. *Multimedia Tools and Applications*, 72(3), 2211–2224.

Hua, Z., Zhou, Y. (2017). Design of image cipher using block-based scrambling and image filtering. *Information Sciences*, 396, 97–113.

Hua, Z., Zhou, Y., Pun, C.-M., Chen, C.P. (2015). 2D Sine Logistic modulation map for image encryption. *Information Sciences*, 297, 80–94.

Hua, Z., Yi, S., Zhou, Y., Li, C., Wu, Y. (2017). Designing hyperchaotic cat maps with any desired number of positive Lyapunov exponents. *IEEE Transactions on Cybernetics*, 48(2), 463–473.

Hua, Z., Zhou, Y., Huang, H. (2019). Cosine-transform-based chaotic system for image encryption. *Information Sciences*, 480, 403–419.

Kanso, A., Ghebleh, M. (2012). A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(7), 2943–2959.

Kanso, A., Ghebleh, M. (2013). A fast and efficient chaos-based keyed hash function. *Communications in Nonlinear Science and Numerical Simulation*, 18(1), 109–123.

Kanso, A., Ghebleh, M. (2015a). An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation*, 24(1–3), 98–116.

Kanso, A., Ghebleh, M. (2015b). A structure-based chaotic hashing scheme. *Nonlinear Dynamics*, 81(1–2), 27–40.

Katz, J., Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Khan, M., Shah, T. (2015). An efficient chaotic image encryption scheme. *Neural Computing and Applications*, 26(5), 1137–1148.

Khan, J.S., Khan, M.A., Ahmad, J., Hwang, S.O., Ahmed, W. (2017). An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes. *Informatica*, 28(4), 629–649.

Kwok, H., Tang, W.K. (2007). A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, Solitons & Fractals*, 32(4), 1518–1529.

Li, C., Chen, G. (2008). On the security of a class of image encryption schemes. In: *2008 IEEE International Symposium on Circuits and Systems*. IEEE, pp. 3290–3293.

Li, C., Arroyo, D., Lo, K.-T. (2010). Breaking a chaotic cryptographic scheme based on composition maps. *International Journal of Bifurcation and Chaos*, 20(08), 2561–2568.

Li, C., Liu, Y., Xie, T., Chen, M.Z. (2013). Breaking a novel image encryption scheme based on improved hyperchaotic sequences. *Nonlinear Dynamics*, 73(3), 2083–2089.

Liao, X., Lai, S., Zhou, Q. (2010). A novel image encryption algorithm based on self-adaptive wave transmission. *Signal Processing*, 90(9), 2714–2722.

Liu, H., Zhang, Y., Kadir, A., Xu, Y. (2019). Image encryption using complex hyper chaotic system by injecting impulse into parameters. *Applied Mathematics and Computation*, 360, 83–93.

Liu, W., Sun, K., Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84, 26–36.

Liu, Y., Tong, X., Ma, J. (2016). Image encryption algorithm based on hyper-chaotic system and dynamic S-box. *Multimedia Tools and Applications*, 75(13), 7739–7759.

Mao, Q., Qin, C. (2013). A novel turbo unequal error protection scheme for image steganography. *Informatica*, 24(4), 561–576.

Ott, E. (2002). *Chaos in Dynamical Systems*. Cambridge University Press.

Ping, P., Xu, F., Mao, Y., Wang, Z. (2018). Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing*, 283, 53–63.

Rijmen, V., Daemen, J. (2001). Advanced encryption standard. In: *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 19–22

Rivest, R.L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.

Shannon, C.E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27(3), 379–423.

Shannon, C.E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4), 656–715.

Solak, E., Çokal, C., Yildiz, O.T., Biyikoğlu, T. (2010). Cryptanalysis of Fridrich's chaotic image encryption. *International Journal of Bifurcation and Chaos*, 20(05), 1405–1413.

Soleymani, A., Nordin, M.J., Sundararajan, E. (2014). A chaotic cryptosystem for images based on henon and arnold cat map. *The Scientific World Journal*, *2014*.

Sun, Y-J., Zhang, H., Wang, X-Y., Wang, X-Q., Yan, P-F. (2020). 2D non-adjacent coupled map lattice with q and its applications in image encryption. *Applied Mathematics and Computation*, 373, 125039.

Tang, M., Hu, J., Song, W. (2014). A high capacity image steganography using multi-layer embedding. *Optik-International Journal for Light and Electron Optics*, 125(15), 3972–3976.

Wang, C., Fan, C., Ding, Q. (2018). Constructing discrete chaotic systems with positive Lyapunov exponents. *International Journal of Bifurcation and Chaos*, 28(07), 1850084.

Wang, K., Pei, Zou, L., Song, A., He, Z. (2005). On the security of 3D cat map based symmetric image encryption scheme. *Physics Letters A*, 343(6), 432–439.

Wang, X., Wang, Q., Zhang, Y. (2015). A fast image algorithm based on rows and columns switch. *Nonlinear Dynamics*, 79(2), 1141–1149.

Wu, Y., Noonan, J.P., Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2), 31–38.

Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P. (2013). Local shannon entropy measure with statistical tests for image randomness. *Information Sciences*, 222, 323–342.

Wu, Y., Zhou, Y., Noonan, J.P., Agaian, S. (2014). Design of image cipher using latin squares. *Information Sciences*, 264, 317–339.

Xiao, D., Liao, X., Wei, P. (2009). Analysis and improvement of a chaos-based image encryption algorithm. *Chaos, Solitons & Fractals*, 40(5), 2191–2199.

Xie, E.Y., Li, C., Yu, S., Lü, J. (2017). On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Processing*, 132, 150–154.

Xu, L., Li, Z., Li, J., Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 78, 17–25.

Zhang, Q., Guo, L., Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, 52(11–12), 2028–2035.

Zhang, X., Nie, W., Ma, Y., Tian, Q. (2017). Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box. *Multimedia Tools and Applications*, 76(14), 15641–15659.

Zhou, Y., Bao, L., Chen, C.P. (2013). Image encryption using a new parametric switching chaotic system. *Signal Processing*, 93(11), 3039–3052.

Zhou, Y., Bao, L., Chen, C.P. (2014). A new 1D chaotic system for image encryption. *Signal Processing*, 97, 172–182.

Zhu, C. (2012). A novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications*, 285(1), 29–37.

The 2nd BOWS contest. http://bows2.ec-lille.fr. Accessed: 2019-12-14.

Attribution-noncommercial-noderivatives 4.0 international (CC BY-NC-ND 4.0). https://creativecommons.org/licenses/by-nc-nd/4.0/. Accessed: 2020-02-20.

Signal and Image Processing Institute: Miscellaneous volume. http://sipi.usc.edu/database/database.php?volume=misc, Accessed: 2019-12-14.

A. Kanso is an associate professor of mathematics at Kuwait University, Kuwait. He received his BSc degree in mathematics from Queen Mary and Westfield College (University of London), in 1994. He earned his MSc degree in applied computing technology in the Electronic Engineering Department of Middlesex University, in 1996. In 1999 he obtained his PhD in mathematics from Royal Holloway and Bedford New College (University of London). His research interests include chaos-based encryption systems, information hiding, hash functions, secret sharing, and graph theory.

M. Ghebleh is an associate professor of mathematics at Kuwait University, Kuwait. He received his BSc and MSc in mathematics from Sharif University of Technology, Tehran, Iran (1997 and 1999), and his PhD in mathematics from Simon Fraser University, Burnaby, British Columbia, Canada (2007). His research interests include graph theory, combinatorics, and digital security topics such as encryption, data hiding, hash functions, and secret sharing.

A. Alazemi is an associate professor of mathematics at Kuwait University, Kuwait. He received his BSc in mathematics from Kuwait University, Kuwait. He earned his MSc and PhD in mathematics from Colorado State University, Colorado, the United States (2004 and 2007). His research interests include incidence structures, classification problems, spectral graph theory, graph theory, combinatorics and algebra.