Nonlinear Dyn (2012) 69:1995–2007
DOI 10.1007/s11071-012-0402-6

ORIGINAL PAPER

# An intertwining chaotic maps based image encryption scheme

**I. Shatheesh Sam · P. Devaraj · R.S. Bhuvaneswaran**

Received: 17 August 2011 / Accepted: 20 March 2012 / Published online: 6 April 2012

**Abstract** In this paper, a new image encryption scheme is proposed that uses intertwining chaotic maps to enhance security and key length. In the substitution process, six randomly chosen odd integers are used to permute and then XORed with the first chaotic key to shuffle and alter the image pixels. Byte substitution has also been applied and the resultant values are XORed with the second chaotic key to improve the security against the known/chosen-plain text attack and to increase nonlinearity. In the diffusion process, the pixel values are altered sequentially with various operations which include nonlinear diffusion using the first chaotic key, subdiagonal diffusion of adjacent pixels and XORing with the third chaotic key. The security and performance of the proposed image encryption technique have been analyzed using statistical analysis, sensitivity analysis, key space analysis, differential analysis, and entropy analysis. The simulation shows that a single bit of key or pixel difference of the plain-image will change almost all the pixels in the cipher-image (NPCR > 99.63 %), and the unified average changing intensity is high (UACI > 33.43 %). Since the entropy is found to be close to the theoretical value, we observed that the information leakage is negligible, and hence the scheme is highly secure. The experimental results show that the performance of the proposed scheme is secure and fast.

**Keywords** Intertwining chaotic map · Permutation · Byte substitution · Nonlinear diffusion · Subdiagonal diffusion

## 1 Introduction

In any communication system, including the satellite and the Internet, it is almost impossible to prevent unauthorized people from eavesdropping. When information is broadcast from a satellite or transmitted through the Internet, there is a risk of information interception. Security of image and video data has become increasingly important for many applications, including video conferencing, secure facsimile, medical and military applications. The conventional encryption techniques are not suitable for image encryption due to high redundancy, strong correlation and high computation complexity. The chaos based cryptosystems are suitable for the secure transmission of images due to the intrinsic features of chaotic systems such as ergodicity, mixing property, sensitivity to initial conditions, and system parameters. It can be

I. Shatheesh Sam (✉) · R.S. Bhuvaneswaran
Ramanujan Computing Centre, College of Engineering,
Anna University Chennai, Guindy, India
e-mail: shatheeshsam@yahoo.com

R.S. Bhuvaneswaran
e-mail: bhuvan@annauniv.edu

P. Devaraj
Department of Mathematics, College of Engineering, Anna
University Chennai, Guindy, India
e-mail: devaraj@annauniv.edu

considered analogous to ideal cryptographic properties such as confusion and diffusion properties. Hence, many chaos based encryption systems have been proposed [4, 16, 18, 20, 21] in the last two decades.

Most chaotic image encryption systems use the permutation substitution architecture. These two processes are repeated for several rounds, to obtain the final encrypted image. Fridrich [3] suggested a chaotic image encryption method composed of permutation and substitution. All the pixels are moved using a 2D chaotic map. The new pixels moved to the current position are taken as a permutation of the original pixels. In the substitution process, the pixel values are altered sequentially. Chen et al. [2] employed a three-dimensional 3D Arnold cat map and a 3D Baker map in the permutation stage. Lian et al. [9] used a chaotic standard map in the permutation stage and a quantized logistic map in the substitution stage. Sam et al. [13] used improved chaotic map for the substitution and diffusion stages. The maps are generated a series of pseudorandom values and the scheme is highly secure. Block ciphers have been proposed to improve the security level [15, 17]. The cryptanalysis techniques on chaotic maps have also been attempted in recent years [1, 6, 7, 14].

In [10], the logistic and standard maps are used to generate a Pseudo Random Number Sequence (PRNS) controlling two kinds of encryption operations. This scheme was later cryptanalyzed by Rhouma et al. [12] and they found that it was not secure in the sense that an equivalent key can be obtained from only one known/chosen plain-image and the corresponding cipher-image. In order to resist Rhouma et al.'s attack, a modified version of the original scheme was proposed [11] by same authors. It was claimed that the modified image cipher preserves all the good properties of the original cipher and is also capable of withstanding against the chosen/known plaintext attacks. But the scheme is found to be insecure [8] in the sense that an equivalent key can be found. The major steps in the scheme are as follows:

(1) Modified Horizontal Diffusion (mHD):

$$\mathrm{mHD}(X) = \mathrm{HD}(X) \oplus \mathrm{mHD}(\ominus),$$

where $X$ is the input matrix and $\ominus$ is a zero matrix of the same size as $X$.

(2) Modified Vertical diffusion (mVD):

$$\mathrm{mVD}(X) = \mathrm{VD}(X) \oplus \mathrm{mVD}(\ominus).$$

(3) The encryption procedure of equivalent key is as follows:

$$I' = \mathrm{VD}\big(\mathrm{HD}(I)\big) \oplus \tilde{I}_{\mathrm{key}},$$

where $\tilde{I}_{\mathrm{key}} = \mathrm{VD}(\mathrm{HD}(I_{x\mathrm{key}})) \oplus \mathrm{VD}(\mathrm{mHD}(\ominus)) \oplus \mathrm{mVD}(\ominus) \oplus I_{\mathrm{CKS}}$.

(4) From the properties of steps 1 and 2, we can define

$$\begin{aligned} I' &= \mathrm{mVD}\big(\mathrm{mHD}(I \oplus I_{x\mathrm{key}})\big) \oplus I_{\mathrm{CKS}} \\ &= \mathrm{mVD}\big(\mathrm{HD}(I \oplus I_{x\mathrm{key}}) \oplus \mathrm{mHD}(\ominus)\big) \oplus I_{\mathrm{CKS}} \\ &= \mathrm{VD}\big(\mathrm{HD}(I \oplus I_{x\mathrm{key}}) \oplus \mathrm{mHD}(\ominus)\big) \\ &\quad \oplus \mathrm{mVD}(\ominus) \oplus I_{\mathrm{CKS}} \\ &= \mathrm{VD}\big(\mathrm{HD}(I \oplus I_{x\mathrm{key}})\big) \oplus \mathrm{VD}\big(\mathrm{mHD}(\ominus)\big) \\ &\quad \oplus \mathrm{mVD}(\ominus) \oplus I_{\mathrm{CKS}} \\ &= \mathrm{VD}\big(\mathrm{HD}(I)\big) \oplus \mathrm{VD}\big(\mathrm{HD}(I_{x\mathrm{key}})\big) \\ &\quad \oplus \mathrm{VD}\big(\mathrm{mHD}(\ominus)\big) \oplus \mathrm{mVD}(\ominus) \oplus I_{\mathrm{CKS}} \\ &= \mathrm{VD}\big(\mathrm{HD}(I)\big) \oplus \tilde{I}_{\mathrm{key}}. \end{aligned}$$

Since the above operations are linear in nature, the scheme is highly vulnerable to known plaintext attacks. Note that the equivalent key $\tilde{I}_{\mathrm{key}}$ can be obtained as

$$\tilde{I}_{\mathrm{key}} = \mathrm{VD}\big(\mathrm{HD}(I)\big) \oplus I'.$$

In order to address this problem, we have introduced nonlinear operations in our scheme. An intertwining chaotic maps based scheme is suggested in this paper to overcome the above weakness. The scheme uses significant features such as sensitivity to initial conditions, permutation of keys, intertwining chaotic maps, byte substitution, nonlinear diffusion, and subdiagonal diffusion. The nonlinearity is used to overcome the limitation of the Patidar et al. [11] scheme. The rest of this paper is organized as follows. Section 2 introduces and compares the logistic map and intertwining maps. Section 3, the new image encryption scheme based on intertwining chaotic map is proposed. Section 4, the security of new scheme is analyzed. Finally, the conclusions are discussed in Sect. 5.

## 2 Logistic map

The logistic map is a simple nonlinear model, but it has complicated dynamic behavior. The chaotic sequence

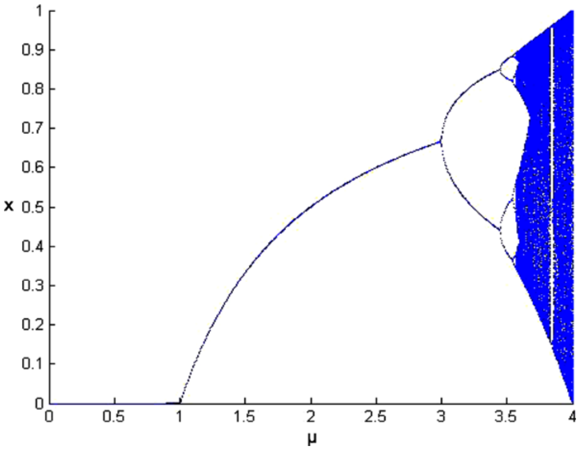

**Fig. 1** Bifurcation of the logistic map

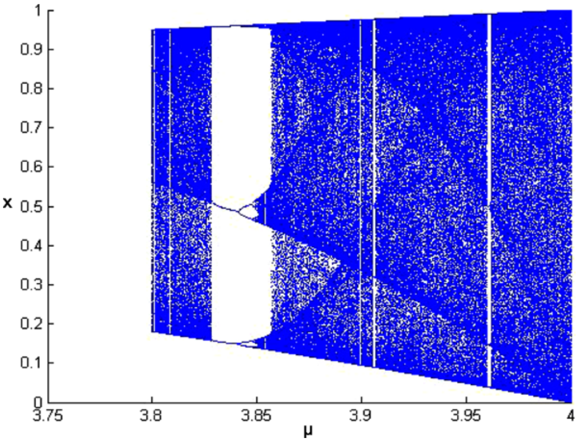

**Fig. 2** Blank Window of the logistic map

produced by the logistic map is extremely sensitive to the change of its initial value. The logistic map is defined as

$$x_{n+1} = \mu x_n(1 - x_n),$$

where $0 < x_n < 1$ and $0 < \mu \leq 4$. The sequences produced by the logistic map are controlled by the parameter value of $\mu$ and the initial value of $x_n$. The system has a different characteristics with different values of $\mu$ called the bifurcation parameter. The process of bifurcation starts from $\mu > 3.564$ to $\mu < 4$. It may be noted that the more closer the value of $\mu$ to four, the system response will be more chaotic. Figure 1 shows the different characteristics for the values of $\mu$. The horizontal axis shows the values of the parameter $\mu$ and the vertical axis shows the possible long term values of $x_n$.

Logistic mapping sequences also have good autocorrelation and cross-correlation properties. The iterative sequences which are produced by the logistic map can replace traditional pseudorandom sequences produced by the linear feedback shift register (LFSR) used in encryption.

In general, the logistic map has some common weaknesses such as stable windows, blank windows, uneven distribution of sequences, and a weak key as suggested by Jianquan et al. [5]. The blank window is a more serious weakness than the other mentioned ones. Figure 2 illustrates the blank window by logistic map when $\mu = 3.828$.

Hence, a new type of intertwining logistic maps are required to alleviate the weaknesses. The maps are mixed well together so as to achieve larger key space and to attain chaotic behavior.

### 2.1 Intertwining logistic map

The proposed intertwining logistic maps are defined as follows:

$$x_{n+1} = \big[\mu \times k_1 \times y_n \times (1 - x_n) + z_n\big] \bmod 1,$$

$$y_{n+1} = \big[\mu \times k_2 \times y_n + z_n \times 1/\big(1 + (x_{n+1})^2\big)\big] \bmod 1,$$

$$z_{n+1} = \big[\mu \times (x_{n+1} + y_{n+1} + k_3) \times \sin(z_n)\big] \bmod 1,$$

where $0 < \mu \leq 3.999$, $|k_1| > 33.5$, $|k_2| > 37.9$, $|k_3| > 35.7$. These are used to increase the chaotic key space. Along with the key $k_i$ the distribution of the sequences becomes better. Figure 3 shows the uniform distribution of sequences. The aforementioned weaknesses such as stable windows, blank windows, uneven distribution of sequences, and weak key are completely resolved.

Thus, the proposed intertwining logistic map does not have security issues which are present in the logistic map. Moreover, the resulting chaotic sequences are uniformly distributed and the key size has been increased greatly.

#### *2.1.1 Comparison between logistic map and intertwining chaotic map*

In order to determine whether a map is chaotic or not, the simplest way is to calculate the map's Lyapunov exponent. A chaotic system is sensitive to small

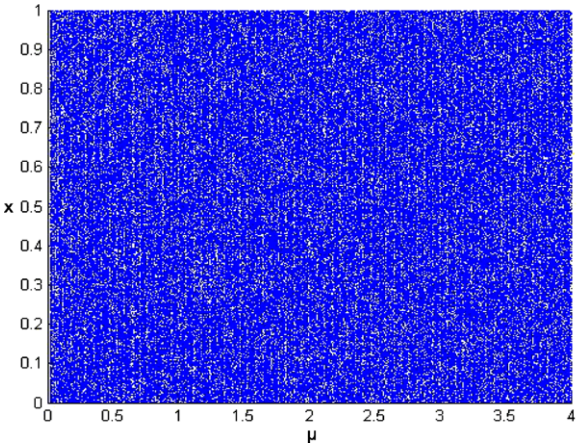

**Fig. 3** Distribution of the sequences for intertwining map

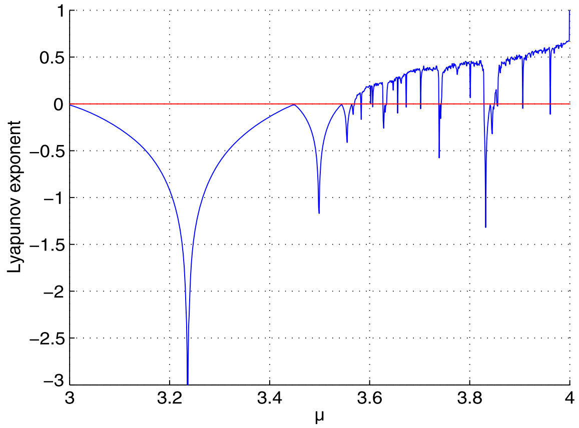

**Fig. 4** Lyapunov exponents of the logistic map

changes in the initial state. The parameter is positive; the new map is extremely sensitive to small changes in the values. The basic expression of the discrete Lyapunov exponent is defined as

$$\lambda_F = \frac{1}{M}\sum_{i=0}^{M-1} \ln \frac{d(F(m_{i+1}), F(m_j))}{d(m_{i+1}, m_j)},$$

where $m_i$ is the subset of the trajectory of a digitalized map $F$ in length $M$ and $d(m_i, m_j)$ is the distance between $m_i$ and $m_j$. The computation of the Lyapunov exponents for logistic map is shown in Fig. 4.

Figure 5 shows that the complex degrees of the intertwining chaotic model are larger and more random than logistic map. The positive frequency indicates the sequence are more random and complex.

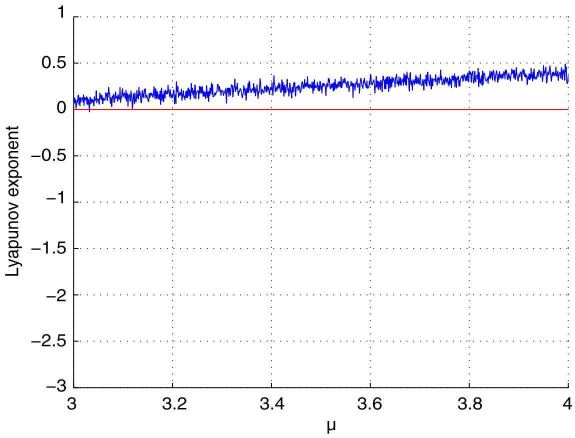

**Fig. 5** Lyapunov exponents of the intertwining map

We have constructed a histogram to display the frequency in which the states along a trajectory fall into a given region in the state space. We have divided the state space $[0, 1]$ into $n = 256$ discrete nonintersecting intervals, where the $i$th interval is $[\frac{i-1}{n}, \frac{i}{n}]$; for $i = 1, 2, \ldots, n = 256$. Then a long trajectory of length 100000 is calculated, using an initial system state $x_0$ as follows:

For the logistic map,

$$L(x) = \mu x(1 - x),$$

$$x_0, L^1(x_0), L^2(x_0), \ldots, L^{100000}(x_0),$$

$$x_i = L(x_{i-1}),$$

where $i = 1, 2, 3, \ldots, 100000$. Figure 6 shows the histogram of the logistic map.

For the intertwining map,

$$S(x, y, z) = \big(\mu \times k_1 \times y \times (1 - x) + z\big) \bmod 1,$$

$$T(x, y, z) = \big(\mu \times k_2 \times y + z \times 1/\big(1 + x^2\big)\big) \bmod 1,$$

$$U(x, y, z) = \big(\mu \times (x + y + k_3) \times \sin(z)\big) \bmod 1.$$

The trajectory of length 100000 using the initial values of the system $(x_0, y_0, z_0)$ are generated as follows:

$$x_0, x_1 = S(x_0, y_0, z_0), \quad x_2 = S(x_1, y_1, z_1), \quad \ldots,$$

$$y_0, y_1 = T(x_1, y_0, z_0), \quad y_2 = T(x_2, y_1, z_1), \quad \ldots,$$

$$z_0, z_1 = U(x_1, y_1, z_0), \quad z_2 = U(x_2, y_2, z_1), \quad \ldots,$$

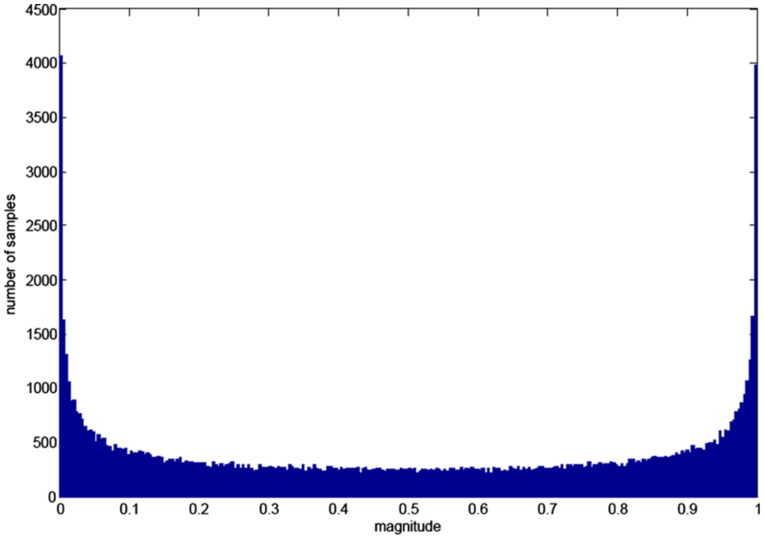

**Fig. 6** Histogram of the logistic map

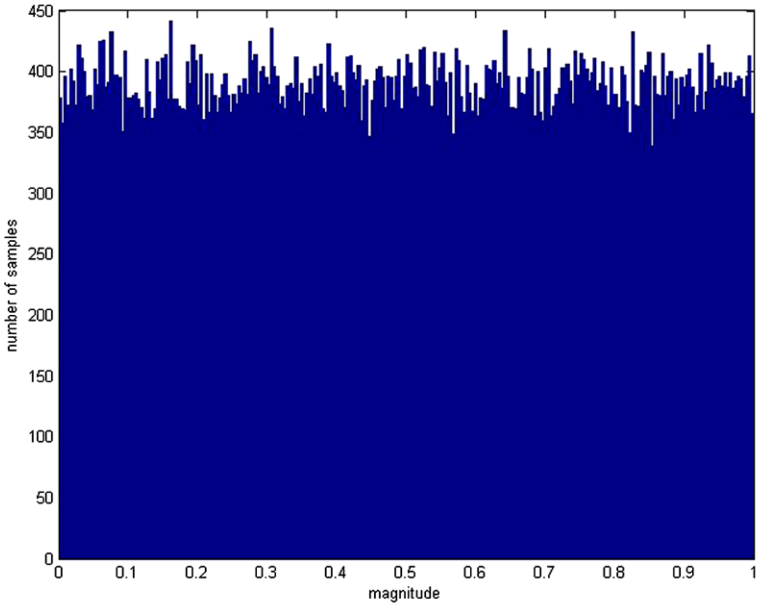

**Fig. 7** Histogram of the intertwining map

$$x_i = S(x_{i-1}, y_{i-1}, z_{i-1}),$$

$$y_i = T(x_i, y_{i-1}, z_{i-1}),$$

$$z_i = U(x_i, y_i, z_{i-1}).$$

Note that, in the logistic map (Fig. 6) the intensity values are not uniformly distributed and the intensity values are high near zero and near one. But the histogram of the intertwining map is uniformly distributed as shown in Fig. 7. Hence, uniform distribution is obtained for each proposed maps and also the key space of the intertwining chaotic system is larger than the logistic map. It is better and more suitable for image encryptions.

## 3 Proposed scheme

The architecture of the proposed intertwining chaotic maps based image cryptosystem is shown in Fig. 8. The scheme consists of four major phases, permutation, byte substitution, nonlinear diffusion, and subdiagonal diffusion. The permutation of pixel position,

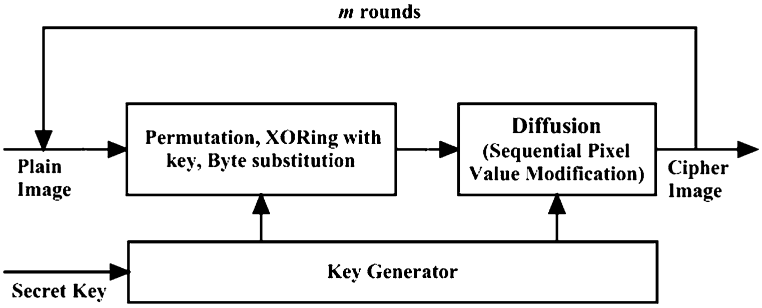
*m* rounds
Plain Image
Permutation, XORing with key, Byte substitution
Diffusion (Sequential Pixel Value Modification)
Cipher Image
Secret Key
Key Generator

**Fig. 8** Architecture of the proposed image cryptosystem

the change of pixel value, and byte substitution are carried out to enable the confusion process. Two rounds of operations are carried out. The pixel value mixing effect of the whole cryptosystem is altered greatly.

The plain image is stored in a two-dimensional array of $\{R_{i,j}, G_{i,j}, B_{i,j}\}$ pixels. In this, $1 \leq i \leq H$ and $1 \leq j \leq W$, where $H$ and $W$ represent the height and width of the plain-image in pixels.

### 3.1 Key generation

Three initial values are used for the key generation. They are randomly chosen float numbers stored in $x_{1,1}, y_{1,1}$, and $z_{1,1}$. They are used as the secret keys for the scheme. The corresponding integer values are $X_{1,1} = \lfloor x_{1,1} \times 256 \rfloor$, $Y_{1,1} = \lfloor y_{1,1} \times 256 \rfloor$and $Z_{1,1} = \lfloor z_{1,1} \times 256 \rfloor$, respectively. The key stream is generated with the help of the proposed intertwining chaotic maps as follows:

```
for $i = 1$ to $H$ step $1$
  for $j = 1$ to $W$ step $1$
    $x_{i,j+1} = (\mu \times k_1 \times y_{i,j} \times (1 - x_{i,j}) + z_{i,j}) \bmod 1$
    $y_{i,j+1} = (\mu \times k_2 \times y_{i,j} + z_{i,j} \times 1 / (1 + (x_{i,j+1})^2)) \bmod 1$
    $z_{i,j+1} = (\mu \times (x_{i,j+1} + y_{i,j+1} + k_3) \times \sin(z_{i,j})) \bmod 1$
    $X_{i,j} = \lfloor x_{i,j+1} \times 256 \rfloor$
    $Y_{i,j} = \lfloor y_{i,j+1} \times 256 \rfloor$
    $Z_{i,j} = \lfloor z_{i,j+1} \times 256 \rfloor$
  end
  $x_{i+1,1} = x_{i,j+1}$
  $y_{i+1,1} = y_{i,j+1}$
  $z_{i+1,1} = z_{i,j+1}$
end
```

where $X_{i,j}, Y_{i,j}, Z_{i,j}$ are the set of chaotic keys. The $\mu$ values are in between 3.567 to 3.999 to achieve chaotic behavior. The size is the same as plain-image. Moreover, we use three float numbers as multipliers $k_1, k_2, k_3$ in the proposed maps to increase the randomness and uniform distribution of the key values.

### 3.2 Initial permutation

Permutation transformations are a basic operations in many scrambling and encryption systems. There are two iterative stages in the chaos based image cryptosystem. Generally, the confusion effect is obtained in the permutation stage, while the diffusion effect is performed in the pixel value diffusion stage. Confusion makes the relationship between the key and the ciphertext as complex as possible.

The confusion stage permutes the pixels in the image, without changing its value. The pixel values are modified sequentially in the diffusion stage, so that a small change in one pixel in the image causes an enormous difference in the whole image. In order to decorrelate the relationship between adjacent pixels, the permutation of pixels is introduced in the confusion stage. The confusion stage of the proposed scheme is composed of position permutation, byte substitution, and simple pixel value modification. Here, the process uses six odd random secret key values for scrambling the plain-image and then XORing it with the first chaotic key for pixel value modification simultaneously. The pixels are permuted using the following operations:

```
for $i = 1$ to $H$
  for $j = 1$ to $W$
    $CR_{i,j} = R[1 + (p_1 \times i + 3) \bmod H, 1 + (p_2 \times j + 3) \bmod W] \oplus X_{i,j}$
```

```
        $CG_{i,j} = G\big[1 + (p_3 \times i + 3) \bmod H,$
                $1 + (p_4 \times j + 3) \bmod W\big] \oplus X_{i,j}$
        $CB_{i,j} = B\big[1 + (p_5 \times i + 3) \bmod H,$
                $1 + (p_6 \times j + 3) \bmod W\big] \oplus X_{i,j}$
    end
end
```

where $X_{i,j}$ is the first chaotic key, $R[i, j]$, $G[i, j]$, $B[i, j]$ represent the red, green, blue channels in the plain-image and $CR_{i,j}, CG_{i,j}, CB_{i,j}$ denote the $(i, j)$th pixel of the permuted image. The method uses $p_1, p_2, p_3, p_4, p_5, p_6$ as odd random values for scrambling the image. In order to get a reversible permutation, $p_1, p_3, p_5$ must be chosen so that to relatively prime to $H$ and similarly $p_2, p_4, p_6$ are relatively prime to $W$. When the typical images height and width are even numbers, the $p_1, p_2, p_3, p_4, p_5, p_6$ must be odd. The above permutation operations produce good scrambling of the image, and hence enhance the security.

### 3.3 Byte substitution

Each individual RGB pixel byte of the state is replaced with a new byte by using the S-box of the AES (Advanced Encryption Standard) algorithm. The size of the S-box is 16 × 16 values. Here, the RGB component of each pixel is divided into two parts; the left half consists of the left most four bits and the right half consists of the right most four bits. They are denoted by LR, RR, LG, RG, LB, RB. For the red channel, the byte substitution is performed treating LR as the row number and RR as the column number of the S-box. Similarly, the other channel substitutions are done. The resultant values are XORed with the second chaotic key. It improves the security against the known/chosen plaintext attacks.

### 3.4 Nonlinear diffusion

Diffusion refers to the property that redundancy in the statistics of the plaintext is dissipated in the statistics of the cipher text. The RGB diffusion is obtained by the 5 Least Significant Bits (LSB) circular shift method. The resultant values are again XORed with the first chaotic key to all the red, green, and blue channels. The procedure for the nonlinear diffusion is as follows:

```
for i = 1 to H
    for j = 1 to W
        $CR_{i,j} = (R_{i,j} \ggg 5) \bmod 256$
        $CG_{i,j} = (G_{i,j} \ggg 5) \bmod 256$
        $CB_{i,j} = (B_{i,j} \ggg 5) \bmod 256$
        $CSR_{i,j} = CR_{i,j} \oplus X_{i,j}$
        $CSG_{i,j} = CG_{i,j} \oplus X_{i,j}$
        $CSB_{i,j} = CB_{i,j} \oplus X_{i,j}$
    end
end
```

where $X_{i,j}$ is the first chaotic key, $CR_{i,j}, CG_{i,j}, CB_{i,j}$ denotes the resultant values of the circular shift operation and $CSR_{i,j}, CSG_{i,j}, CSB_{i,j}$ denotes the nonlinear diffusion image of the XORed operation. The combination of the 5 bit circular shift and XORing make the encryption operation nonlinear, and hence the system becomes strong against known/chosen-plaintext attacks.

### 3.5 Subdiagonal diffusion

Diffusion is obtained with the help of subdiagonal XORing and XORing with the third chaotic key and so on. The subdiagonal operation is shown in Fig. 9.

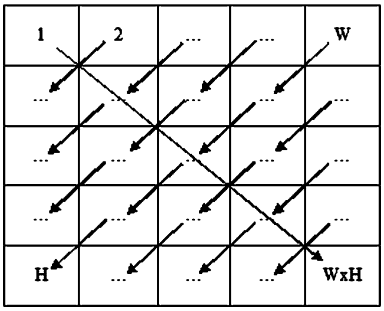

**Fig. 9** Subdiagonal pixel value reading

The procedure for the red channel is as follows:

Choose three random integers $R_0$, $G_0$, $B_0$ in the range 1 to 256.

```
$\mathrm{Iv}R = R_0$
$\mathrm{Iv}G = G_0$
$\mathrm{Iv}B = B_0$
for $i = 1 : \max$
    $\mathrm{out}R(i, \max - i + 1) = \mathrm{in}R(i, \max - i + 1) \oplus \mathrm{Iv}R$
    $\mathrm{Iv}R = \mathrm{out}R(i, \max - i + 1) \oplus Z_{i,j}$
end
for $j = 1 : \max - 1$
    for $i = 1 : \max - j$
        $\mathrm{out}R\bigl(i, \max - (j-1) - i\bigr)$
            $= \mathrm{in}\bigl(i, \max - (j-1) - i\bigr) \oplus \mathrm{Iv}R$
        $\mathrm{Iv}R = \mathrm{out}R(i, \max - j - 1) \oplus Z_{i,j}$
    end
    for $i = 1 : \max - j$
        $\mathrm{out}R\bigl(i + j, (\max - i + 1)\bigr)$
            $= \mathrm{in}\bigl(i + j, (\max - i + 1)\bigr)$
        $\mathrm{Iv}R = \mathrm{out}R(i + j, \max - i + 1) \oplus Z_{i,j}$
    end
end
```

Here, max is the maximum size of the image, in$R$ and out$R$ are the input and output of the image and Iv$R$, Iv$G$, Iv$B$ are the initial vector of each channel which may also be treated as an 8-bit secret key. $Z_{i,j}$ is the third chaotic key. The pixel is modified by XORing the first and second pixels with the chaotic key, the third pixel is modified by XORing modified second and third pixels with key and the process continues until the end of the image. The similar procedure is applied for the other channels. These operations enhance the diffusion property and hence improve the security levels.

## 3.6 Rounds

The whole confusion-diffusion steps 3.2 to 3.5 are repeated from beginning to end to achieve a satisfactory level of security. Simulation of the scheme is discussed in Sect. 4, shows that the desired level of security can be achieved only in two rounds.

## 3.7 Decryption

The decryption algorithm is just the reverse of the encryption one. In order to get the original image, encrypted image pixel values are XORed with the same set of secret keys which were used in the encryption process.

### 3.7.1 *Inverse subdiagonal diffusion*

The reverse procedure for the red channel is as follows:

```
$\mathrm{Iv}R = R_0$
$\mathrm{Iv}G = G_0$
$\mathrm{Iv}B = B_0$
for $i = 1 : \max$
    $\mathrm{Iv}R1 = \mathrm{in}(i, \max - i + 1)$
    $\mathrm{out}R(i, \max - i + 1) = \mathrm{in}(i, \max - i + 1) \oplus \mathrm{Iv}R$
    $\mathrm{Iv}R = \mathrm{Iv}R1 \oplus Z_{i,j}$
end
for $j = 1 : \max - 1$
    for $i = 1 : \max - j$
        $\mathrm{Iv}R1 = \mathrm{in}\bigl(i, \max - (j-1) - i\bigr)$
        $\mathrm{out}R\bigl(i, \max - (j-1) - i\bigr)$
            $= \mathrm{in}\bigl(i, \max - (j-1) - i\bigr) \oplus \mathrm{Iv}R$
        $\mathrm{Iv}R = \mathrm{Iv}R1 \oplus Z_{i,j}$
    end
    for $i = 1 : \max - j$
        $\mathrm{Iv}R1 = \mathrm{in}\bigl(i + j, (\max - i + 1)\bigr)$
        $\mathrm{out}R\bigl(i + j, (\max - i + 1)\bigr)$
            $= \mathrm{in}\bigl(i + j, (\max - i + 1)\bigr)$
        $\mathrm{Iv}R = \mathrm{Iv}R1 \oplus Z_{i,j}$
    end
end
```

### 3.7.2 *Inverse nonlinear diffusion*

The inverse nonlinear diffusion is obtained by the 5 bit reverse circular shift method. The resultant values are

XORed with the same RGB channels. The procedure for the inverse nonlinear diffusion is as follows:

```
for $i = 1$ to $H$
  for $j = 1$ to $W$
    $CR_{i,j} = (R_{i,j} \lll 5) \bmod 256$
    $CG_{i,j} = (G_{i,j} \lll 5) \bmod 256$
    $CB_{i,j} = (B_{i,j} \lll 5) \bmod 256$
    $CSR_{i,j} = CR_{i,j} \oplus X_{i,j}$
    $CSG_{i,j} = CG_{i,j} \oplus X_{i,j}$
    $CSB_{i,j} = CB_{i,j} \oplus X_{i,j}$
  end
end
```

#### *3.7.3 Inverse byte substitution*

The inverse S-box is used for byte substitution. Each individual RGB pixel byte of the state is replaced with a new byte by using the inverse S-box of the AES algorithm. The same technique is followed as for encryption to replace the substituted values. Finally, the inverse resultant values are XORed with the second chaotic key.

#### *3.7.4 Inverse permutation*

The permutation is replaced by the inverse value permutation. The inverse method is described by:

```
for $i = 1$ to $H$
  for $j = 1$ to $W$
    $R_{i,j} = R\big[1 + (p_1^{-1} \times i - 4) \bmod H,$
        $1 + (p_2^{-1} \times j - 4) \bmod W\big] \oplus X_{i,j}$
    $G_{i,j} = G\big[1 + (p_3^{-1} \times i - 4) \bmod H,$
        $1 + (p_4^{-1} \times j - 4) \bmod W\big] \oplus X_{i,j}$
    $B_{i,j} = B\big[1 + (p_5^{-1} \times i - 4) \bmod H,$
        $1 + (p_6^{-1} \times j - 4) \bmod W\big] \oplus X_{i,j}$
  end
end
```

where $p_1^{-1} \bmod H, p_2^{-1} \bmod W, \ldots$ inverse odd random values. The original image can be recovered once the above decryption process is completed.

## 4 Security analysis

A good encryption scheme should resist all kinds of known attacks, such as known-plaintext, ciphertext only, statistical, differential, and various brute force attacks. Some security analyzes have been performed on the proposed image encryption scheme, including the most important ones like the key sensitivity, statistical, and differential analyses, which have demonstrated the robust security of the new scheme, as shown in the following.

### 4.1 Statistical analysis

Statistical analysis has been performed on the proposed image encryption scheme, demonstrating its superior confusion-diffusion properties which strongly resist statistical attacks. This is shown by the test on the histograms of the enciphered images and on the correlations of the adjacent pixels in the ciphered image.

#### *4.1.1 Histogram analysis*

The histogram analysis is used to illustrate the confusion and diffusion properties in the encrypted data. We have chosen USC-SIPI image database (freely available at http://sipi.usc.edu/database/) for testing purposes. In the permutation process, the odd values are taken as $p_1 = 7$, $p_2 = 31$, $p_3 = 23$, $p_4 = 9$, $p_5 = 15$, $p_6 = 91$. In the inverse permutation process the values are used as $p_1^{-1} = 183$, $p_2^{-1} = 223$, $p_3^{-1} = 167$, $p_4^{-1} = 57$, $p_5^{-1} = 239$, $p_6^{-1} = 211$. The histogram of the plain image "Lena" and the histogram of the encrypted image are shown in Fig. 10. Comparing the two histograms, it may be observed that the histogram of the encrypted image is uniform and is significantly different from that of the original image, and that the encrypted images transmitted do not provide any suspicion to the attacker, which can strongly resist statistical attacks.

#### *4.1.2 Correlation of two adjacent pixels*

The effect of image scrambling is related to the correlation of adjacent pixels. A better scrambling effect is indicated the lower correlation value. In order to test the correlation between two adjacent pixels in plain-image and cipher-image, we have analyzed the correlation between pairs of plain-image channels and cipher-image channels. The following formulae is used to calculate the correlation coefficients in the horizontal, vertical and diagonal directions. The calculated results are listed in Table 1.

$$r_{\alpha\beta} = \frac{\operatorname{cov}(\alpha, \beta)}{\sqrt{D(\alpha)}\sqrt{D(\beta)}},$$

$$E(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\alpha_i,$$

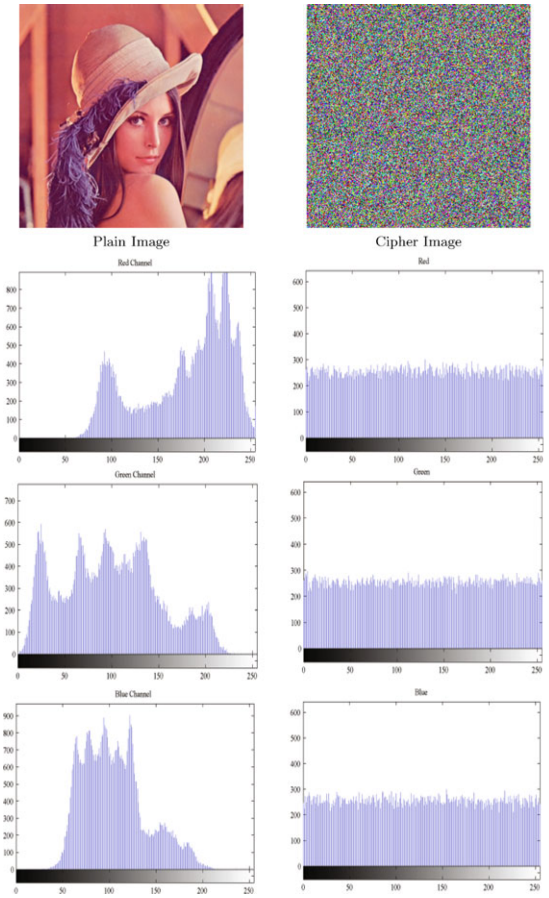

**Fig. 10** Histogram of plain image ‘Lena’ and its encrypted image

$$D(\alpha) = \frac{1}{N}\sum_{i=1}^{N}\left(\alpha_i - E(\alpha)\right)^2,$$

$$\operatorname{cov}(\alpha, \beta) = \frac{1}{N}\sum_{i=1}^{N}\left(\alpha_i - E(\alpha)\right)\left(\beta_i - E(\beta)\right),$$

where $\alpha$ and $\beta$ denote two adjacent pixels and $N$ is the total number of duplets $(\alpha, \beta)$ obtained from the image.

The proposed cipher image channel values are close to zero and shows a better scrambling effect.

### 4.2 Key space analysis

An ideal encryption scheme should have larger secret key length, such that the key space should be large enough to make brute-force attacks infeasible. In the proposed scheme, the initial conditions and parameters of three maps are used as keys. The multiplier $k_1$, $k_2$, and $k_3$ treated as key in the intertwining maps and the key space is approximately $2^{192}$. Iv$R$, Iv$G$, Iv$B$ are also used as part of the key, then the key space is increased up to $2^{216}$. The combination of the key space is large enough in the proposed scheme to resist the attacks.

As shown in Table 2, the proposed scheme has larger key size than other schemes.

### 4.3 Sensitivity analysis

Key sensitivity means that the change of a single bit in the secret key should produce a completely different encrypted image. The two cipher-images are compared pixel-by-pixel. Different images and different

**Table 2** Key space size of the proposed scheme and different encryption scheme

| Scheme | Proposed | Patidar et al. [11] | Patidar et al. [10] |
|---|---|---|---|
| Key space size | $2^{216}$ | $2^{128}$ | $2^{157}$ |

**Table 1** Correlation coefficients between adjacent pixels of plain-image and cipher-images

| Directions | Plain image | | | Cipher image | | |
|---|---|---|---|---|---|---|
| | Red | Green | Blue | Red | Green | Blue |
| Horizontal | 0.9518 | 0.9587 | 0.9168 | 0.0017 | 0.0021 | 0.0048 |
| Vertical | 0.9753 | 0.9747 | 0.9724 | 0.0019 | 0.0045 | 0.0027 |
| Diagonal | 0.9317 | 0.9378 | 0.9403 | 0.0042 | 0.0051 | 0.0036 |

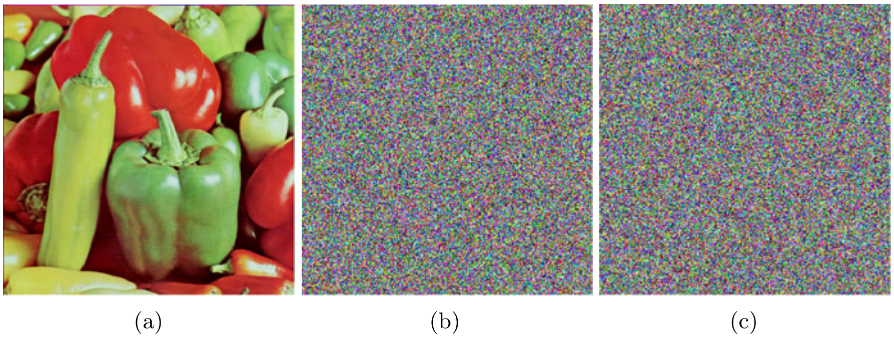

**Fig. 11** Key sensitivity analysis of the proposed scheme on the test image "pepper". (**a**) Plain-image. (**b**) Cipher-image using single bit change of plain text. (**c**) Cipher-image using single bit change of secret key

key values are tested. A test image "pepper" is encrypted with the following set of secret key: $x_0 = 0.41324738544344$, $y_0 = 0.52638928350638$, $z_0 = 0.98644737157579$, $k_1 = 33.1, k_2 = 37.3, k_3 = 35.7$, and $\text{Iv}R = 35, \text{Iv}G = 25, \text{Iv}B = 65$. The output cipher is shown in Fig. 11(a).

In order to test key and plaintext sensitivity a single bit is changed any one of the key or plaintext. Here, we changed the key as: $x_0 = 0.41324738544345$, $y_0 = 0.52638928350638$, $z_0 = 0.98644737157579$, $k_1 = 33.1, k_2 = 37.3, k_3 = 35.7$ and $\text{Iv}R = 35$, $\text{Iv}G = 25$, $\text{Iv}B = 65$. The output cipher is shown in Fig. 11(b).

There is a 99.82 % difference between the two cipher-images. It shows that this algorithm has a great sensitivity to the key and plain text.

### 4.4 Differential analysis

In order to assess the changing a single bit of key or any pixel value in the plain-image on the cipher-image, the number of pixel change rate (NPCR) and the unified averaged changing intensity (UACI) are computed in the proposed scheme. The NPCR is used to measure the change rate of the number of pixels of the cipher-image when only one bit of key or pixel is modified. The UACI measures the average intensity of two one bit changes of cipher-images. Let us assume, the two ciphered images $C^1$ and $C^2$ whose corresponding plain images have only one-pixel difference. The color RGB-level values of ciphered images $C^1$ and $C^2$ at row $i$, column $j$ are labeled as $C^1(i, j)$ and $C^2(i, j)$, respectively. The NPCR is defined as

$$\text{NPCR} = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} D(i, j)}{W \times H} \times 100\ \%,$$

where $W$ and $H$ are the width and height of two random images and $D(i, j)$ is defined as

$$D(i, j) = \begin{cases} 0 & C^1(i, j) = C^2(i, j), \\ 1 & C^1(i, j) \neq C^2(i, j). \end{cases}$$

Further, the UACI, is used to measure the average intensity difference in a color component between the two cipher images $C^1(i, j)$ and $C^2(i, j)$. It is defined as

$$\text{UACI} = \frac{1}{W \times H} \left[ \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{|C^1(i, j) - C^2(i, j)|}{2^L - 1} \right] \times 100\ \%,$$

where $L$ is the number of bits used to represent the color channels of red, green, and blue, respectively. The results of NPCR and UACI are presented in Table 3.

The performance of each stage of the difference between the cipher and plain-images is measured by the mean absolute error (MAE) is defined as

$$\text{MAE} = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} |P_{i,j} - C_{i,j}|,$$

where the parameters $P_{i,j}$ and $C_{i,j}$ are pixel values of plain and cipher images. The MAE indicates the better security. The results for the MAE values are shown in Table 4.

The value is found that in the proposed scheme is high. Thus, the cryptosystem is better security.

Wu et al. [19] tested and claimed that many existing image encryption methods are actually not as good as they are purported, although some methods do pass these randomness tests. The results show that a small change in the original image will result in a significant

**Table 3** NPCR and UACI criteria of the proposed scheme

| Cipher images | NPCR % | | | UACI % | | |
|---|---|---|---|---|---|---|
| | Red | Green | Blue | Red | Green | Blue |
| Lena | 99.5621 | 99.5773 | 99.6689 | 33.4324 | 33.4958 | 33.4774 |
| Baboon | 99.6214 | 99.6105 | 99.6082 | 33.4392 | 33.4436 | 33.4579 |
| House | 99.6328 | 99.6278 | 99.6109 | 33.4431 | 33.4521 | 33.4651 |
| Pepper | 99.6292 | 99.6154 | 99.6032 | 33.4273 | 33.4309 | 33.4474 |

**Table 4** A comparison of MAE of different stages

| Proposed stages | MAE % |
|---|---|
| Permutation | 80.9610 |
| Byte Substitution | 81.5108 |
| Nonlinear diffusion | 82.1309 |
| Subdiagonal diffusion | 84.2461 |

difference in the cipher-image, proposed scheme can be found that the NPCR > 99.63 %, MAE > 84.24 %, and the UACI > 33.43 %. So the scheme has a good ability to withstand a differential attack.

### 4.5 Performance analysis

Apart from the security consideration, the running speed of the algorithm is also an important aspect for a good encryption scheme. The simulator for the proposed scheme is implemented using MATLAB 7.4. The performance is measured on a 3.0 GHz Pentium Core 2 Duo with the 4 GB RAM running Windows Vista Business Edition. Simulation results show that the total encryption time is 0.8645 s and 1.4609 s for decryption.

### 4.6 Information entropy analysis

Information entropy is one of the criteria to measure the strength of a symmetric cryptosystem. The entropy $H(m)$ of a message $m$ can be calculated as

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

where $p(m_i)$ represents the probability of the occurrence of symbol $m_i$ and log denotes the base 2 logarithm. If there are 256 possible outcomes of the message $m$ with equal probability, it is considered as random. In this case, $H(m) = 8$, is an ideal value.

As shown in Table 5, we notice that the values obtained in the proposed scheme are closer to the theoretical value of 8, than the other schemes. This means that information leakage in the encryption process is negligible and the encryption system is secure against entropy attack.

**Table 5** The entropy analysis of the proposed and other schemes

| Cipher | Proposed | RC4 | RC6 |
|---|---|---|---|
| Lena | 7.9994 | 7.9728 | 7.9829 |
| House | 7.9992 | 7.9637 | 7.9761 |

## 5 Conclusion

In this paper, an intertwining chaotic maps based image encryption scheme is proposed. The proposed cipher provides good confusion and diffusion properties that ensures high security. Confusion and diffusion have been achieved using permutation, byte substitution, nonlinear diffusion, and subdiagonal diffusion. This scheme is immune to various types of cryptographic attacks like known/chosen plain text attacks and brute force attacks. We have carried out statistical analysis, key sensitivity analysis, key space analysis differential analysis, and entropy analysis to demonstrate the security of the new image encryption procedure. Based on the various analyses, it is shown that the proposed scheme is more secure and fast, and hence more suitable for real time image encryption for transmission applications.

**Acknowledgement** This research is partially supported by the All India Council for Technical Education, New Delhi, India.

## References

1. Alvarez, G., Shujun, L.: Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. Commun. Nonlinear Sci. Numer. Simul. **14**, 3743–3749 (2009)
2. Chen, G.R., Mao, Y.B., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals **21**, 749–761 (2004)
3. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurc. Chaos Appl. Sci. Eng. **8**(6), 1259–1284 (1998)
4. Guan, Z.H., Huang, F., Guan, W.: Chaos based image encryption algorithm. Phys. Lett. A **346**, 153–157 (2005)
5. Jianquan, X., Chunhua, Y., Qing, X., Lijun, T.: An encryption algorithm based on transformed logistic map. In: IEEE Proc. Network Security, Wireless Communications and Truested Computing, pp. 111–114 (2009)
6. Li, C., Li, S., Alvarez, G., Chen, G., Lo, K.T.: Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. Phys. Lett. A **369**(1–2), 23–30 (2007)
7. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G.: On the security defects of an image encryption scheme. Image Vis. Comput. **27**, 1371–1381 (2009)
8. Li, C., Li, S., Lo, K.T.: Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **16**, 837–843 (2011)
9. Lian, S., Sun, J., Wang, Z.: A block cipher based on a suitable use of chaotic standard map. Chaos Solitons Fractals **26**, 117–129 (2005)
10. Patidar, V., Pareek, N.K., Sud, K.K.: A new substitution diffusion based image cipher using chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **14**(7), 3056–3075 (2009)
11. Patidar, V., Pareek, N.K., Purohit, G., Sud, K.K.: Modified substitution–diffusion image cipher using chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **15**(10), 2755–2765 (2010)
12. Rhouma, R., Solak, E., Belghith, S.: Cryptanalysis of a new substitution-diffusion based image cipher. Commun. Nonlinear Sci. Numer. Simul. **15**(7), 1887–1892 (2010)
13. Sam, I.S., Devaraj, P., Bhuvaneswaran, R.S.: Chaos based image encryption scheme based on enhanced logistic map. In: LNCS Proc. ICDCIT, vol. 6536, pp. 290–300 (2011)
14. Sam, I.S., Devaraj, P., Bhuvaneswaran, R.S.: A novel image cipher based on mixed transformed logistic maps. Multimed. Tools Appl. (2012). doi:10.1007/s11042-010-0652-6
15. Wang, X., Teng, L.: An image blocks encryption algorithm based on spatiotemporal chaos. Nonlinear Dyn. (2011). doi:10.1007/s11071-011-9984-7
16. Wang, Y., Wong, K.W., Liao, X., Xiang, T., Chen, G.: A chaos-based image encryption algorithm with variable control parameters. Chaos Solitons Fractals **41**, 1773–1783 (2009)
17. Wang, X., Wang, X., Zhao, J., Zhang, Z.: Chaotic encryption algorithm based on alternant of stream cipher and block cipher. Nonlinear Dyn. **63**, 587–597 (2011)
18. Wong, K.W., Kwok, B.S.H., Law, W.S.: A fast image encryption scheme based on chaotic standard map. Phys. Lett. A **372**, 2645–2652 (2008)
19. Wu, Y., Noonan, J.P., Agaian, S.: NPCR and UACI randomness tests for image encryption. Cyber J., Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. 31–38 (2011)
20. Xiaojun, T., Minggen, C.: Image encryption with compound chaotic sequence cipher shifting dynamically. Image Vis. Comput. **26**, 843–850 (2008)
21. Zhang, L., Liao, X., Wang, X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals **24**, 759–765 (2005)