Multimedia Tools and Applications (2019) 78:10013–10034
https://doi.org/10.1007/s11042-018-6612-2

An image encryption algorithm based on substitution technique and chaos mixing

Yannick Pascal Kamdeu Nkandeu[1] · Alain Tiedeu[1]

Received: 7 February 2018 / Revised: 8 August 2018 / Accepted: 27 August 2018 /
Published online: 1 September 2018

Abstract

These recent years, countless chaos-based image encryption algorithms have been proposed to meet security needs in real time multimedia communication. However, many of these have exhibited flaws due to the chaotic map inadequacy. In this paper, we proposed a fast and secure image encryption algorithm by using new 1D chaotic systems, with better chaotic properties in the range of their control parameters. These new chaotic systems were obtained from well-known 1D chaotic maps (Logistic, May, Gaussian, Gompertz) with flaws in their chaotic properties. From the chaotic systems designed, we extracted a pseudo random number sequence (PRNS) and generated S-boxes. Then a novel technique of plain image substitution was used to enhance the sensitivity of the original image pixels, followed by a scrambling-masking technique using the generated S-box. Security tests and evaluation metrics confirmed that the proposed cryptosystem was efficient, practicable, and reliable, with high potential to be adopted for network security and secure communications because of its high encryption speed.

Keywords Chaos · Image encryption · Scrambling-masking

1 Introduction

In everyday application, cryptography serves at various levels and scopes of human activities in relation to secured data transfer with the guarantee of privacy [27, 30, 38]. With the rapid expansion of multimedia and internet, the urgent need for appropriate encryption algorithm for image and video online communication have favoured the up-rise of cryptography using chaotic maps.

Chaotic maps were found to be good candidates for cryptography because of the close relationship between chaos properties like ergodicity, sensitivity to initial conditions and control parameters, random-like behaviour, unpredictability, and properties of a good cipher such as sensitivity to key and plaintext, randomness in confusion and diffusion processes [22,

✉ Alain Tiedeu
alain.tiedeu@polytechnique.cm

[1] National Advanced School of Engineering, LAGEMES, PO. Box 8390, Yaoundé, Cameroon

32]. Furthermore chaos-based cryptography was also found suitable for image and video encryption as traditional cryptography (DES, IDEA, AES...) failed [10, 16, 38]. Many techniques and architectures involving different chaotic systems have therefore been published [1–26, 28, 29, 31–37, 39, 41, 43–57].

Permutation–diffusion is the most common architecture used in chaos-based cryptography. It consists of many rounds of crafty association between pixel values relocation (shuffling) and pixel values alteration (diffusion) using chaotic maps [1, 5–7]. Chen et al. [12] proposed a scheme of permutation-diffusion in which the diffusion key stream was extracted from the permutation matrix generated with Baker's map, and used for shuffling. In [7] Belazi et al. used four chaos-based cryptographic phases to design a substitution-permutation network. The author in [50] designed a scheme using a key hash function to generate a hash value from both plain image and a secret hash key, then he used logistic and standard maps and the hash value to perform permutation-diffusion and authentication of the encrypted/decrypted image, to prevent chosen plaintext and middle attack. Paper [35] proposed a secure and lightweight image encryption scheme based on 2D Baker's map, which scheme uses two sets of secret keys, one for permutation and another for diffusion.

In 2011, Zhu et al. [57] proposed a new scheme using a bit-level permutation in which separation of pixels into groups of bits depends on the percentage of pixel information. Afterward they used Cat and Logistic maps to permute and alter the abovementioned bits in pixel values. The scheme was cryptanalyzed and improved in [53]. Zhang et al. [54] proposed a new approach in which he considered an image of M×N size with 2^8 grayscale values as a 3D bit matrix M×N×8, and designed a new bit-level permutation architecture. Another bit-level permutation technique associated with pixel-level substitution and discrete cat map proposed in [17], was quickly cryptanalyzed and improved in [55]. Surprisingly, the improved scheme was broken and proved to have equivalent permutation Keys by Chen et al. in [11].

With the introduction of DNA computing, some researchers proposed image encryption algorithm based on DNA. Pixels in an image are DNA encoded and each nucleotide in the DNA encoded image is transformed to its base pair for DNA addition, complementary rules or replication with the help of chaotic maps and diffusion-confusion technique. However, the DNA image encryption algorithm using the Logistic map proposed in [51] was found non-invertible and prone to known-plaintext attack by authors in [19]. An enhanced version in [31] was cryptanalyzed in [8, 28]. Finally, more suitable versions for colour images using multiple improved 1D chaotic maps [23] and 2D logistic chaotic maps were proposed [21], but with high time consumption.

In 2015, Liu et al. [25] proposed a colour image encryption scheme based on three S-boxes generated in one-time by the complex Chen system. Each S-box randomly took turns to encrypt one of the colour components in each pixel adhering to the switching sequence. The S-box technique is an inheritance of traditional cryptography. The principle is to generate a random number of perfectly distributed 2D or 3D matrices and proceed to substitution, which is a nonlinear transformation, replacing each pixel value with another. In [44], Wang et al. proposed an image encryption based on dynamic S-boxes constructed by chaotic systems but with high time consumption. The encryption algorithm proposed by Belazi et al. [6] applied a lifting wavelet transform (LWT) to the original image in order to encrypt the latter by block permutation based on a chaotic Tent map. Then, a new S-box method based on chaotic system and linear fractional transform (LFT) was used to substitute the permuted image. Wang et al. [46] proposed an encryption algorithm using a discrete wavelet transform (DWT) to split up a digital image into different frequency coefficients before scrambling. Afterwards, the image sequences were encrypted with a multiple chaos encryption matrix.

Earlier in 2014, Eyebe et al. [14] proposed a scrambling-masking technique using a piece wise linear chaotic map (PWLCM) and the Leophantine equation (LDE) for generation of a large pseudo-random key stream. The algorithm achieved fast encryption since the pixel position and value were modified in a single process, but the encryption process was independent of the plain image characteristics. Another scrambling-masking scheme proposed by Huang et al. [20] using a 2D chaotic Chebychev function to scramble and mask pixel images was later proven to have security flaws [43].

Some schemes further analysed, were declared vulnerable to attacks as they were less sensitive to plaintext [5, 13, 15, 26, 29, 33, 34, 41, 47, 52]. The related algorithm suffered from inefficient chaining mode which prevents from different attacks, by creating an "avalanche effect" when a single pixel in the plain image is modified. Wang et al. [47] demonstrated that the sub-image encryption method based on hyperchaos presented by Mirzaei et al. [33] had some security weaknesses to chosen plaintext attack and improved on the scheme. Liu et al. [26] found some security defects in the scheme proposed by El-Latif et al. [13], designing an image cryptosystem based on a hybrid logistic map and a cyclic elliptic curve. Song et al. [41] presented a new spatiotemporal chaos and combined it to Nonlinear Chaotic Algorithm (NCA) to permute and diffuse image pixels. Bechikh et al. [5] analysed the scheme and concluded that the substitution key stream was the same for every cipher image/plain image pair. Murillo-Escobar [34] designed a colour image encryption algorithm using a 1D logistic map, and to avoid chosen/known plain image attack, the scheme relies on the plain image characteristics. Recently these encryption algorithms were successfully cryptanalyzed by Fan et al. [15]. The recent image encryption algorithm based on hyper-chaotic system and dynamic S-box proposed by Liu et al. [29] was proven to be insecure and not suitable for image secure communication by [52].

Other algorithms were prone to attack because their schemes contained chaotic maps (Logistic, Tent…) which had weaknesses like non-uniform data output, small key space, periodic data output, poor ergodic properties for some ranges of control parameter [3, 4, 23, 24]. To overcome these setbacks, some researchers suggested that they should not be used alone [2, 36], others proposed modified or new chaotic systems with better properties [1, 37, 39, 45, 49, 56]. In [56] for example, the author used two existing 1D chaotic maps to generate a number of new chaos with good chaotic properties, and designed an encryption algorithm capable of generating a completely different encrypted image each time it is applied to the same original image. The weakness of this cipher is its high decryption error. Sheela et al. [39] modified the Henon map in order to increase the chaotic region - which in turn improved the range of system parameters - and generated sequences for column and row shift transformation, then carried out diffusion using XOR operator. Yang et al. [49] generalized the chaotic Logistic map to the finite field, and designed a coloured image encryption scheme. Abanda et al. [1] combined outputs of Duffing and Colpitts chaotic systems to encrypt grey and colour images. In [45], Logistic and Kent chaotic mappings were used to produce two sub-matrices of pseudo random number, then a combined matrix was generated from both to perform XOR operation with the original data for encryption.

As can be seen, the common major weaknesses are the use of chaotic map with poor randomness properties outcome, lack of sensitivity to the plaintext in the method, and high computational load. With the purpose to overcome these difficulties, this paper introduces a fast image encryption algorithm built with new chaotic maps (obtained by mixing known 1D seed maps) and using a new encryption technique depending on the plain image. The new chaotic maps constructed proved to have better properties and were used to generate S-boxes by their PRNS. The encryption technique first applies a substitution of the plain image by moving and "XORing" pixels in between themselves, such that the sensitivity to plain image is enhanced. The confusion-diffusion is obtained in one time, exploiting the S-box for the substituted-pixel relocation and masking in a scrambling-masking process. Security tests carried out and evaluation metrics applied to assess the cryptosystem confirm that the aforementioned setbacks were solved.

The rest of this paper is organized as follows. An overview of seed chaotic maps is given in Section 2 while in Section 3, the new chaotic maps are designed and proven to be chaotic. The encryption algorithm proposed, is detailed in Section 4. Section 5 focuses on common security tests like key space, key sensitivity, differential attack, while Section 6 concludes the paper.

2 Presentation of 1D seed chaotic maps

2.1 Logistic map

The Logistic map is one of the most studied chaotic systems and is mathematically translated by the equation:

$$x_{n+1} = rx_n(1-x_n) \tag{1}$$

Where $x_n \in [0, 1]$ is the discrete state of the output chaotic sequence, r is the control parameter with values in the range [0, 4]. The chaotic behaviour of the Logistic map is observed in the range [3.5, 4]. However, its chaotic properties are not so good, as shown in Fig. 1a.

2.2 May map

Published by Robert May [40], the May map has behaviour and properties similar to that of the Logistic map and is expressed by the following equation:

$$x_{n+1} = x_n \exp(a(1-x_n)) \tag{2}$$

Where $x_n \in [0, 10.9]$ and the control parameter a belongs to the range [0, 5].

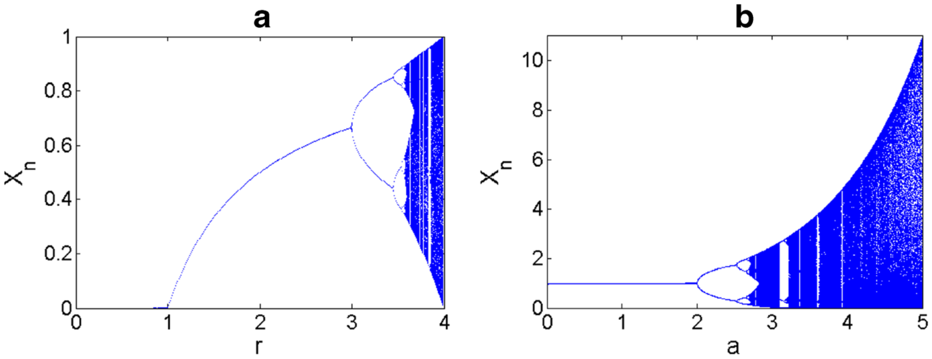

Fig. 1 The bifurcation diagrams of the **a** Logistic map and the **b** May map

Figure 1b illustrates the bifurcation diagram of May map in which, we can observe a non-uniform data output distribution and periodicity (expressed by blank space) in the range of [2.6, 5].

2.3 Gompertz map

First proposed by Gompertz [40], the Gompertz map has a very low level of chaotic behaviour and properties. Its equation is:

$$x_{n+1} = -bx_n \ln x_n \tag{3}$$

Where the control parameter $b \in [0,e]$, e=2.71829… and is the exponential function.

In Fig. 2a, one can see how low the chaocity the Gompertz map exhibits through its bifurcation diagram.

2.4 Gaussian map

The Gaussian map's equation is:

$$x_{n+1} = \exp\left(-\alpha x_n^2\right) + c \tag{4}$$

$\alpha \in [4.7, 17]$, $c \in [-1, 1]$.

Also known as mouse map, this map is a consequence of some mathematical assumptions and approximations over the Gaussian noise function [40]. The bifurcation diagram of the Gaussian map in Fig. 2b shows how their chaotic behaviour and properties are different from the ones of the Logistic, May and Gompertz, and appears in various small intervals of their control parameter c.

3 The proposed chaotic map

The chaotic properties of the above seed maps are not suitable to build a secure cryptosystem [3, 4]. In this section we design new maps with better levels of chaocity and that can therefore be integrated in a good cipher.

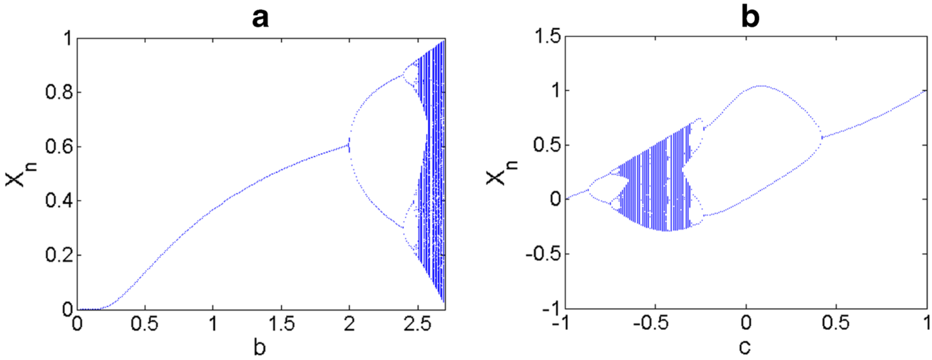

Fig. 2 The bifurcation diagrams of the **a** Gompertz map and the **b** Gaussian map

3.1 Scheme of the designed map

The method proposed by Zhou et al. [56] was adopted to combine the different seed maps. Depicted in Fig. 3, the scheme shows how a new map is obtained from a nonlinear combination of two different 1D chaotic maps.

3.2 The new chaotic maps

From the four 1D chaotic maps (Logistic, May, Gompertz and Gaussian) used as seed, six new chaos will be constructed and analysed, each using two different seeds with unified control parameter r. The criterion for the level of chaocity here will be the maximum Lyapunov exponent.

3.2.1 The Logistic-May system

The first system is made of the Logistic and May maps and is called the Logistic-May System (LOMAS). Its equation is written:

$$x_{n+1} = (x_n \exp((r+9)(1-x_n)) - (r+5)x_n(1-x_n)) \bmod 1 \tag{5}$$

Where $x_n \in [0, 1]$ and $r \in [0, 5]$.

The bifurcation diagram and Lyapunov exponent are shown in Fig. 4 a and d. We then can therefore see that chaotic properties are excellent within [0, 5], with a maximum Lyapunov exponent equal to 8.3.

3.2.2 The Logistic-Gompertz system

Logistic and Gompertz maps are the seeds of the second system called the Logistic-Gompertz system (LOGOS). It is mathematically given by Eq. (6).

$$x_{n+1} = (-(r-31)x_n(1-x_n) - (r+35)x_n \log x_n) \bmod 1 \tag{6}$$

Where $x_n \in [0, 1]$ and $r \in [0, 5]$.

Even though the Gompertz map has poor chaotic properties (Fig. 4), the bifurcation diagram of its combination with Logistic exhibits a rather good level of chaocity (Fig. 4b). The Lyapunov exponent of LOGOS has a mean value of 2.5 (Fig. 4e).

3.2.3 The Logistic-Gaussian system

Constructed with the Logistic and Gaussian maps, the third system is called the Logistic-Gaussian system (LOGAS) and is defined by:

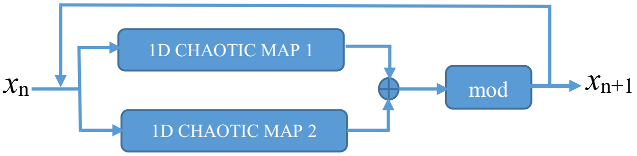

Fig. 3 The new chaotic map scheme

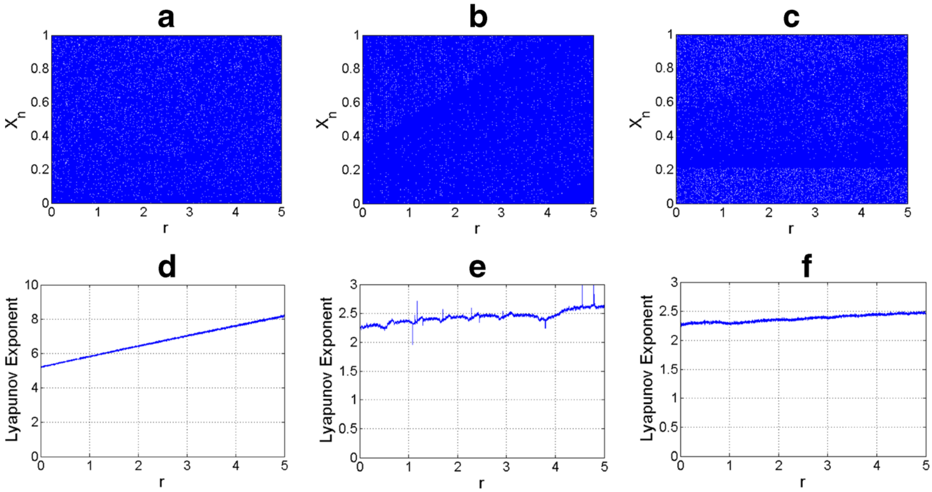

Fig. 4 The bifurcation diagrams and the Lyapunov exponent graphics of the new chaotic maps, **a**-**d** LOMAS, **b**-**e** LOGOS, **c**-**f** LOGAS

$$x_{n+1} = \left(-(r-33)x_n(1-x_n) + \frac{(r+37)}{4} + \exp\left(-\alpha x_n^2\right) \right) \mathrm{mod} 1 \tag{7}$$

Where $x_n \in [0, 1]$, $r \in [0, 5]$, $\alpha \in [4.7, 17]$.

LOGAS's bifurcation diagram depicted by Fig. 4c proves its good chaotic behaviour in the range [0, 5]. Its maximum Lyapunov exponent is equal to 2.5 (Fig. 4f).

3.2.4 The May-Gompertz system

The fourth system derives from the May and Gompertz maps and is named the May-Gompertz system (MAGOS). Its equation is:

$$x_{n+1} = (x_n \exp((r+10)(1-x_n)) - (r+10)x_n \log x_n) \mathrm{mod} 1 \tag{8}$$

Where $x_n \in [0, 1]$ and $r \in [0, 5]$.

Figure 5a and c show how its properties in terms of the bifurcation diagram and Lyapunov exponents (with a maximum value equivalent to 8.7) are excellent in the range of [0, 5].

3.2.5 The May-Gaussian system

The May combined to the Gaussian map form the fifth system called the May-Gaussian system (MAGAS) which is built up by the following equation:

$$x_{n+1} = \left(x_n \exp((r+10)(1-x_n)) + \frac{(r+5)}{4} + \exp\left(-\alpha x_n^2\right) \right) \mathrm{mod} 1 \tag{9}$$

Where $x_n \in [0, 1]$, $r \in [0, 5]$, $\alpha \in [4.7, 17]$.

Through the bifurcation diagram of MAGAS in Fig. 5b, one can see an output sequence uniformly distributed within [0,1]. Figure 5e shows its positive Lyapunov exponents and belonging to the range [2.5, 5.6].

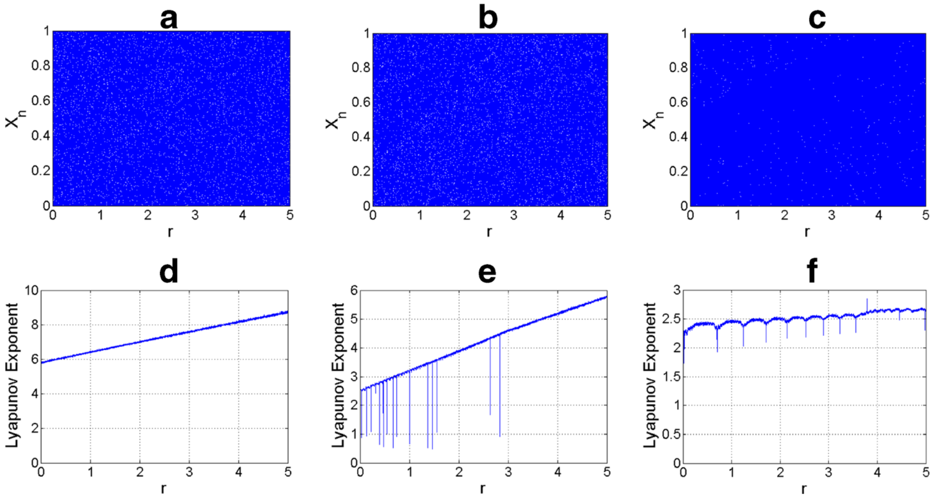

Fig. 5 The bifurcation diagrams and the Lyapunov exponent graphics of the new chaotic maps, **a**-**d** MAGOS, **b**-**e** MAGAS, **c**-**f** GAGOS

3.2.6 The Gaussian-Gompertz system

The last system designed is the Gaussian-Gompertz system (GAGOS). It uses the Gaussian and Gompertz maps and is expressed by the following formula:

$$x_{n+1} = \left(\frac{(r/5+26)}{4} + \exp\left(-\alpha x_n^2\right) - (r/5+26)x_n \log x_n\right) \mathrm{mod} 1 \qquad (10)$$

Where $x_n \in [0, 1]$, $r \in [0, 5]$, $\alpha \in [4.7, 17]$.

The GAGOS bifurcation diagram (Fig. 5c) shows a uniform distribution of sequences like the previous new chaos designed. It also has a mean Lyapunov exponent value around 2.5 (Fig. 5f).

3.3 Advantages of the new maps

All the combined chaotic systems designed above exhibit better chaotic behaviour than those obtained from a single seed. Although the mathematical theory behind chaocity improvement by combining seed maps is not yet established, one easily notices that the bifurcation diagrams of the combined maps have a wider chaotic range and a more uniform distribution of their density functions (Figs. 4a, b and c, 5a, b and c) than their seeds (Figs. 1 and 2.). Furthermore, the maximum Lyapunov exponent values of the Logistic, May, Gompertz and Gaussian maps are respectively equal to 0.6, 0.4, 0.5 and 0.7 [40]. The ones obtained with the LOMAS, LOGOS, LOGAS, MAGOS, MAGAS, GAGOS maps have values of 8.1, 2.6, 2.5, 8.7, 5.6 and 2.5 respectively (Figs. 4d, e and f and 5d, e and f). A high Lyapunov exponent means less iterations and less transient effects to have two totally different PRNS from two very close initial conditions with the same control parameter. It is therefore obvious that the new chaotic maps are better pseudo random number generators (PRNG) than their seeds. We can conclude that these will be more suitable for secure and high speed encryption provided the encryption algorithm is built around a good algebraic structure.

4 Proposed image encryption algorithm

This section presents the new chaotic encryption algorithm based on two main procedures which are a novel plain image substitution technique and a scrambling-masking technique using S-boxes.

4.1 Plain image substitution technique

The plain image substitution technique (PIST) is applied to the plain image for the enhancement of sensitivity such that any change in any pixel in the plain image will cause a substantial change in the corresponding cipher image. It does not depend on a key, and can be applied to any type of images. The steps to apply the PIST to an image are:

- From bottom to top, in each column in an image I of size $M\,X\,N$, replace the value of the pixel in process with the one obtained by bit-wise XOR operation between that value and the value of the previous pixel. The process starts on the second to the last pixel (Eq. (11)).

$$\begin{cases} I(M-i,j) = I(M-i,j)\oplus I(M+1-i,j) \\ i=1,\dots M-1; j=1,\dots N \end{cases} \tag{11}$$

Where (i, j) are indices of an image I of size $M\times N$, and the symbol $\oplus$is the bit-wise XOR operation.

- Repeat the same process in each row (Eq. (12)).

$$\begin{cases} I(i,N-j) = I(i,N-j)\oplus I(i,N+1-j) \\ i=1,\dots M; j=1,\dots N-1 \end{cases} \tag{12}$$

As a consequence of applying the PIST on a plain image, any tiny change in a pixel will spread and affect many pixels in the vertical and horizontal directions and finally the pixels in the first row and the first column (Fig. 6). In the Chaining Block Cipher (CBC) mode or Propagating Chaining Block Cipher (PCBC) mode, a modification of the first pixels in the plain image easily affects the rest when encryption occurs [38]. This technique can be used as a response to the insensitivity to plain images of many cryptosystems as shown in [5, 13, 15, 17, 26, 29, 31, 33, 34, 38, 41, 47, 52, 57]. Figure 6 shows how a grey image Lena is confused when it undergoes the PIST.

4.2 Confusion technique using S-boxes

This section describes the encryption process using as key the initial condition $w_0 = 0.4, x_0 = 0.3, y_0 = 0.2$, $z_0 = 0.1$ and control parameter $r_1 = 1$, $r_2 = 2$, $r_3 = 3$, $r_4 = 4$, $\alpha = 6$, of the new chaos maps (LOMAS, LOGOS, LOGAS, MAGOS). The Plain image I of size $M\times N$ which has undergone the PIST will yield the encrypted image C after a scrambling-masking process using S-boxes, and finally an encrypted image C' after the shuffling process. Below are the steps of the confusion technique.

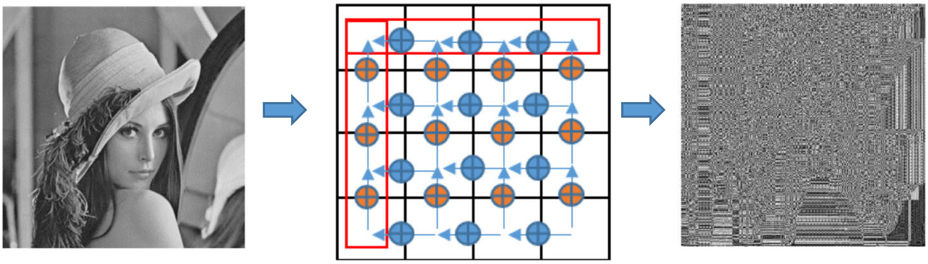

Fig. 6 Effect of PIST process on grey image Lena

Step 1: After 500 iterations to avoid transient effects, iterated LOMAS, LOGOS, LOGAS and MAGOS *M*×*N* times. Build four 1D array vectors *W*, *X*, *Y*, and *Z* of size *M*×*N*, and two 2D vectors S_x (S-box obtained from 1D array *X*) and S_y (S-box obtained from 1D array *Y*) of sizes *M*×*N* respectively with the PRNS obtained from the chaotic systems above.

Step 2: Encrypt the first row and the first column of the image using the PRNS of the 1D vectors *X* and *Y* as expressed by Eq. (13).

$$\begin{cases} j = 2, 3, \ldots N \text{ and } i = 1, 2, \ldots M \\ C(1, j) = I(1, j) \oplus \lfloor \left(X(j+100) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \oplus \lfloor \left(Y(j+100) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \\ C(i, 1) = I(i, 1) \oplus \lfloor \left(X(i+200) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \oplus \lfloor \left(Y(i+200) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \end{cases} \tag{13}$$

Where *i* and *j* are the indices of an image *I* of size *M*×*N*, the symbol $\lfloor t \rfloor$ is to round up the element of *t* to the nearest integer less than or equal to *t*, mod is the modulus operator and the symbol ⊕ denotes bit-wise XOR operation. (Fig. 7)

Step 3: For each encrypted value *C*(*i*,1) and *C*(1, *j*) of the first column and the first row, calculate the number *l(i)* and *k(j)* (Eq. (14)), and use each of them as an index to definitively extract a number respectively in the sets of values {2, 3…*M*} for rows, and {2, 3…*N*} for columns.

$$\begin{cases} i = 2, 3 \ldots N \text{ and } j = 2, 3 \ldots M \\ l(i) = 1 + \big(C(i, 1) \oplus \lfloor \left(Z(i+200) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \times \lfloor \left(W(i+200) \times 10^{15}\right) \rfloor \big) \mathrm{mod}(M + 1 - i) \\ k(j) = 1 + \big(C(1, j) \oplus \lfloor \left(Z(j+100) \times 10^{15}\right) \mathrm{mod} 256 \rfloor \times \lfloor \left(W(j+100) \times 10^{15}\right) \rfloor \big) \mathrm{mod}(N + 1 - j) \end{cases} \tag{14}$$

Where *l*, *k* are 1D arrays respectively of sizes *M* and *N*.

Step 4: Substitute the pixels of indices *i* = {2, 3…*M*} and *j* = {2, 3…*N*} in a scrambling-masking process with the indices *a* and *b* extracted respectively from *l(i)* and *k(j)* following Eq. (15).

$$\begin{cases} i = 2, 3 \ldots M \text{ and } j = 2, 3 \ldots N \\ C(a, b) = I(i, j) \oplus S_x(i, b) \oplus S_y(a, j) \end{cases} \tag{15}$$

Where each element of the S-boxes (S_x and S_y) are grey values obtained calculating (*x* (n) ×10^{15}) mod 256 and (*y* (n) ×10^{15}) mod 256 respectively, with *n* = {1, 2...*M* × *N*}.

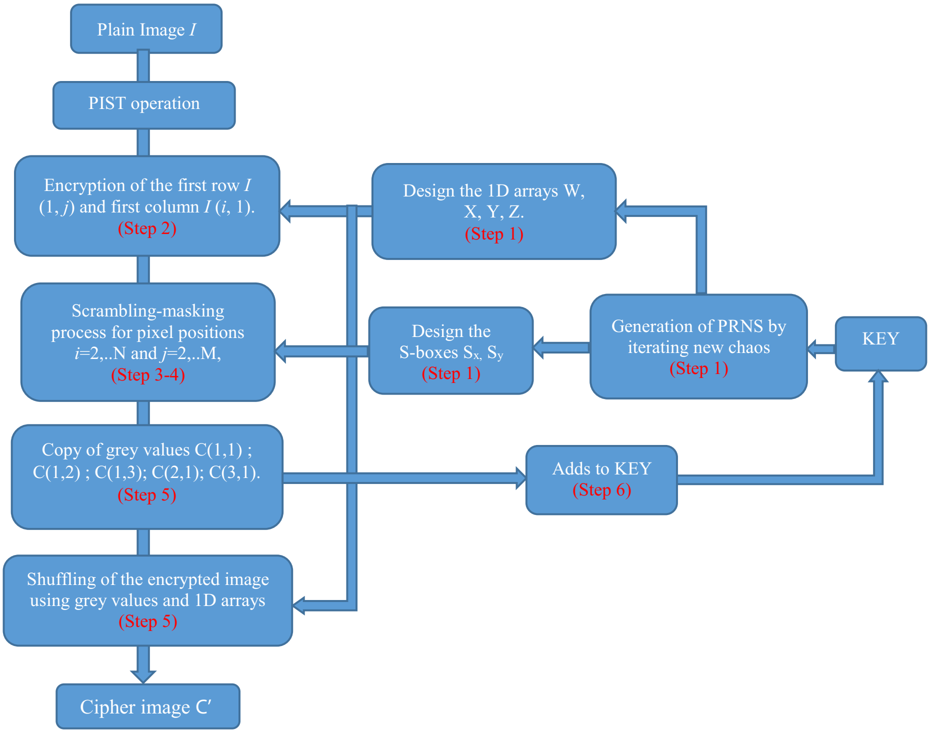
Plain Image I
PIST operation
Encryption of the first row I (1, j) and first column I (i, 1). (Step 2)
Design the 1D arrays W, X, Y, Z. (Step 1)
Scrambling-masking process for pixel positions i=2,..N and j=2,..M, (Step 3-4)
Design the S-boxes Sx, Sy (Step 1)
Generation of PRNS by iterating new chaos (Step 1)
KEY
Copy of grey values C(1,1) ; C(1,2) ; C(1,3); C(2,1); C(3,1). (Step 5)
Adds to KEY (Step 6)
Shuffling of the encrypted image using grey values and 1D arrays (Step 5)
Cipher image C′

Fig. 7 Flowchart of encryption algoritm

Step 5: Determine 1D arrays *u(i)* and *v(j)* using the four systems and the five encrypted values of pixels *C*(1,1), *C*(1,2), *C*(1,3), *C*(2,1), *C*(3,1) as expressed by Eq. (16). And substitute the indices *(i, j)* of each encrypted pixel with the indices *(c, d)*, where *c* and *d* are the values extracted from the sets $\{1, 2\ldots M\}$ and $\{1, 2\ldots N\}$ using *u(i)* and *v(j)* as indices respectively.

$$\begin{cases} i=1,2,\ldots M \ \text{ and } \ j=1,2,\ldots N \\ u(i)=1+\left(C(1,1)\oplus\left\lfloor\left(W(i+C(1,2))\times 10^{15}\right)\mathrm{mod}256\right\rfloor\times\left\lfloor\left(X(i+C(1,3))\times 10^{15}\right)\right\rfloor\right)\mathrm{mod}(M+1-j) \\ v(j)=1+\left(C(1,1)\oplus\left\lfloor\left(Y(j+C(2,1))\times 10^{15}\right)\mathrm{mod}256\right\rfloor\times\lfloor\left(Z\left(j+C(2,3)\times 10^{15}\right)\rfloor\right)\mathrm{mod}(N+1-i) \end{cases} \tag{16}$$

Where *u*, *v* are 1D arrays respectively of sizes *M* and *N*.

Step 1: Send a copy of *C*(1,1), *C*(1,2), *C*(1,3), *C*(2,1), *C*(2,3) values as a part of the key.

4.3 Colour image encryption

The encryption process remains unchanged for coloured images containing R G B components. However, with the purpose of attaining high sensitivity, they will be joined together to form a unique matrix image before encryption, and restored as R G B components at the end.

4.4 Plain image recovering process

Recovering the plain image is done in two steps. Firstly, undo the substitution of indices of all pixels of the encrypted image by using the initial condition and control parameter of the four systems, and also the $C(1,1)$, $C(1,2)$, $C(1,3)$, $C(2,1)$, $C(2,3)$ values (step 6 of Section 4.2). Afterwards, recover confused pixels of indices $i = \{2,3,...M\}$ and $j = \{2,3,...N\}$ using the PRNS of the four systems, the first row and the first column of the confused image. Then decrypt the first row and the first column and apply the PIST to recover the original plain image.

5 Security analysis

The security tests in this section are conducted with a Core(TM) i5-2430 M processor, on a Matlab 2012b platform. The visual results of the encrypted images (Cameraman 256 ×256 image size, Colour Lena 512 ×512, Airport 1024 ×1024) of Fig. 8 are further analysed in terms of statistical attack, brute force attack, differential attack, Chosen plain and cipher image attack, and Speed.

5.1 Statistical analyses

Histogram, correlation analysis, and information entropy of the cipher image are the three main statistical tests (metrics) needed to assess robustness against statistical attack.

5.1.1 Histogram and variance of histogram

The histogram of a noise-like-image must be uniform. In Fig. 8, the histogram of the encrypted images (cameraman, Lena, airport) seem to be uniform. However, the best evaluation is done by calculating the variance of the histogram given by Eq. (18).

$$Var(z) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(z_i - z_j\right)^2 \tag{18}$$

Where Z is the vector of the histogram values and $Z = \{z_1, z_2, ..., z_{256}\}$, z_i and z_j are the numbers of pixels for which the grey values are equal to i and j respectively.

In Table 1, the values of the variance of the histogram of the proposed encryption algorithm are shown with the ones of some recent cryptosystems. It appears that the mean value of the histogram of the proposed cryptosystem is around 5465 which is very close to that of the good cryptosystem proposed in [48], and not far away from the ideal value of 5000 [36]. Histogram analysis proves that the proposed cryptosystem is safe as far as statistical attacks are concerned.

5.1.2 Correlation analysis

In a good encrypted image, there must be no or a very low correlation between neighbouring pixels in every direction. The usual method to assess this is to compute the correlation coefficient Cr of 5000 pairs of randomly chosen pixels in the horizontal (HC), vertical (VC), and diagonal (DC) directions using Eq. (19).

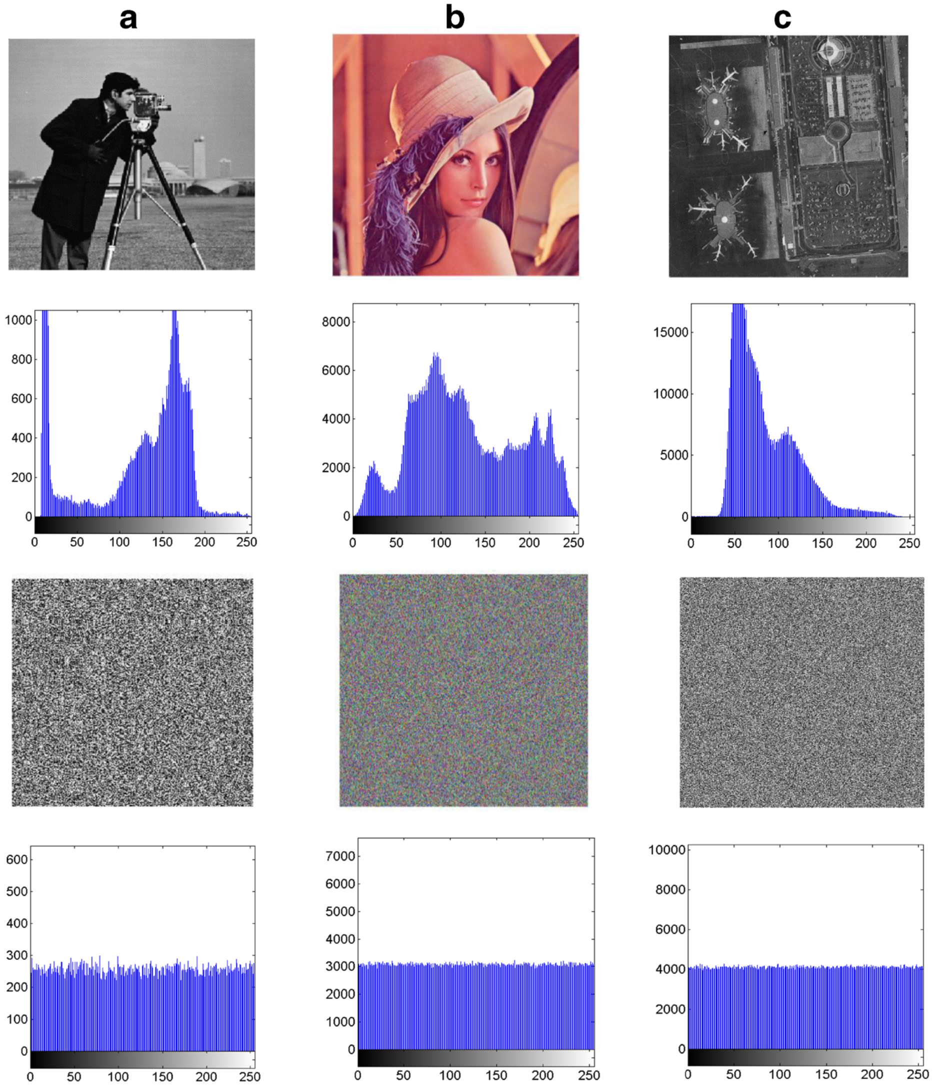

Fig. 8 The grey and colour images encrypted and their histograms. (a) Cameraman, (b) Colour Lena, (c) airport

$$Cr = \frac{K \times \sum_{i=1}^{K} X_i Y_i - \sum_{i=1}^{K} X_i^2 \times \sum_{i=1}^{K} {Y_i}^2}{\sqrt{\left(K \times \sum_{i=1}^{K} (X_i)^2 - \left(\sum_{i=1}^{K} X_i\right)^2\right) \times \left(N \times \sum_{i=1}^{K} (Y_i)^2 - \left(\sum_{i=1}^{K} Y_i\right)^2\right)}} \tag{19}$$

Where X and Y are grey scale values of two adjacent pixels in the image, K is the number of pairs of pixels and Cr is the value of correlation belonging to the [−1,1] range.

Cr tends to be 1 or − 1 for high correlations and tends to be 0 for very low correlations. Table 2 shows the calculated correlation coefficient of a 512×512 Lena image in every

Table 1 Variance of histograms of some cipher images

Grey image	Proposed algorithm	Ref. [48]	Ref. [36]
Cameraman (256 ×256)	5482.61	–	–
Lena (512 ×512)	5450.87	5468.38	5335.83
Airport (1024 ×1024)	5471.65	–	–

direction. A mean value of the proposed encryption algorithm is about 0.007, which tends towards zero. Moreover, Fig. 9 shows how grey values of the cameraman correlated in the horizontal direction in Fig. 9a, are spread in Fig. 9b. From these results, one can conclude that a statistical attack through correlation analysis between adjacent pixels cannot help to break the proposed encryption algorithm.

5.1.3 Information entropy analysis

The information entropy gives an account of the quantum of randomness present in a message (m) as follows.

$$H(m)=\sum_{i=0}^{2^K-1}p(m_i)\log_2(1/p(m_i)) \tag{20}$$

Where $p(m_i)$ represents the probability of symbolm_i, K is the number of bits of the message and 2^K all possible values. For a 256 grayscale image, the pixel data has 2^8 possible values and the ideal entropy of a true random image must be 8.

Table 3 shows entropy values of some images of the proposed encryption algorithm very close to 8 as expected, and slightly better than common ones in literature [48, 38].

5.2 Key analysis

5.2.1 Key space

The key space for an encryption algorithm must be large enough to avoid brute force attack. According to ref. [17], a key size of **10^{30}** is sufficient. The secret key of the proposed algorithm consists of 4 initial conditions (w_0, x_0, y_0, z_0), 5 control parameters ($r_1, r_2, r_3, r_4, \alpha$), and five 8-bit values ($C(1,1)$, $C(1,2)$, $C(1,3)$, $C(2,1)$, $C(3,1)$), giving a total key space of **$(10^{15})^4$**× **$(10^{15})^5$**×

Table 2 Correlation coefficient of two adjacent pixels

Image	Size	Test	Plain image	Encrypted image
Cameraman	(256 ×256)	HC	0.9377	−0.009
		VC	0.9535	0.010
		DC	0.9043	−0.006
Lena	(512 ×512)	HC	0.9679	0.001
		VC	0.9845	−0.014
		DC	0.9580	−0.006
5.3.02	(1024 ×1024)	HC	0.9090	0.002
		VC	0.8989	−0.014
		DC	0.8610	0.018

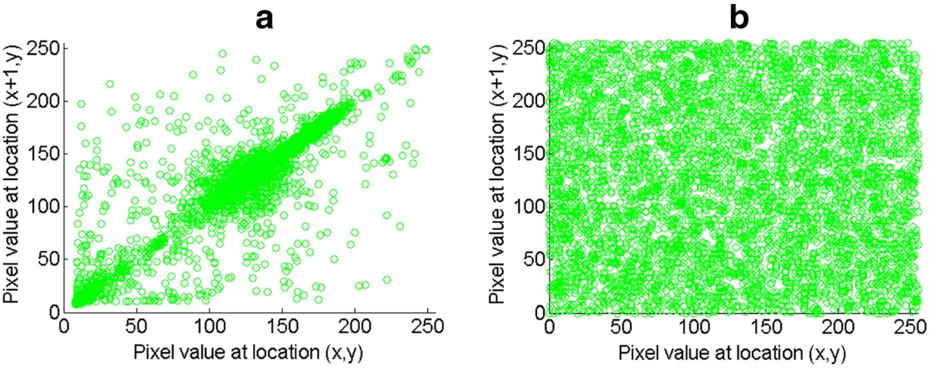

Fig. 9 The horizontal direction correlation graphics. (a) Original cameraman image, (b) encrypted cameraman image

$\mathbf{(2^8)^5 = 10^{142} \approx 2^{475}}$, if the decimal precision is set at 15. This key space is large enough to make brute force attack inefficient.

5.2.2 Key sensitivity

An encryption algorithm must be sensitive to the less significant decimal value of its key to resist chosen plain image or chosen cipher image attack due to an insensitive, weak or equivalent key. Therefore, an original key $K_1 = r_1, r_2, r_3, r_4, \alpha, w_0, x_0, y_0, z_0$, and the modified versions K_2 ($r_2 = r_2 + 10^{-15}$ for K_2, the rest unchanged) and K_3 ($z_0 = z_0 + 10^{-15}$ for K_3, the rest unchanged) on the 15th decimal are used to encrypt the same image. Then, the percentage of difference between pixels of encrypted images is calculated. Table 4 reports that the encrypted images obtained with the K_1, K_2 and K_3 keys differ from one another by at least 99.62%. Such results are not surprising, considering the fact that the Lyapunov exponent of the new chaos is very high (Section 3). Furthermore, the airport image (Fig. 8c) encrypted with K_1 is decrypted with K_2 and K_3 and shown in Fig. 10. The decrypted image with K_2, K_3, has a noise-like appearance.

5.3 Differential attack analysis

A cryptosystem must be sensitive with respect to plain text or plain images, if not, it can undergo a successful differential attack. The sensitivity of a cryptosystem is evaluated through NCPR (Number of Pixel Change Rate) (Eq. (21)) and UACI (Unified Average Change

Table 3 Information entropy of some plain images and their cipher image

Grey image	Proposed algorithm	Ref. [9]	Ref. [34]
Cameraman (256 ×256)	7.9971	7.956	7.9953
Lena (512 ×512)	7.9994	–	7.9975
Baboon (512 ×512)	7.9993	–	–
Airport (1024 ×1024)	7.9998	–	7.9978

Table 4 Proof of key sensitivity

Key	Proposed algorithm	Ref. [42]	Ref. [44]
Key1 Vs Key2	99.61	99.58	99.65
Key2 Vs Key3	99.62	99.59	99.60
Key1Vs Key3	99.65	99.57	99.59

Intensity) (Eq. (22)) metrics [53], which consist of testing the influence of one pixel change on a plain image on the resulting cipher image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{21}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{22}$$

Where C_1 and C_2 are two images with same size $W \times H$. If $C_1(i,j) \neq C_2(i,j)$ then $D(i,j) = 1$, otherwise, $D(i,j) = 0$.

Table 5 gives the measurement of NCPR and UACI between two cipher images of the cameraman, Lena and the airport when a less significant bit (LSB) changed on the grey value in the first, middle, or last pixel's position. The values obtained are around the average of 99.62 for NCPR and 33.51 for UACI. These values are a little better than the ones proposed in literature [18, 34, 44]. Such good values result from the PIST, because the latter accumulates all pixel information in the first row and the first column of the image, which are then used in the confusion step (Section 4). Table 6 shows the effect of one pixel change on component RGB of Lena coloured image.

5.4 Cryptanalysis

Some recent encryption algorithms failed the chosen plain image or/and chosen cipher image attack with all-zero or all-one images [5, 13, 15, 26, 29, 33, 34, 41, 47, 52]. Both attacks are applied to the proposed cryptosystem.

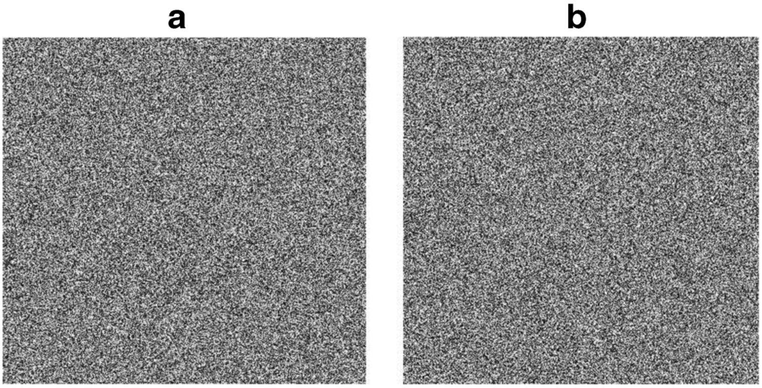

Fig. 10 Decrypted airport image with slightly different keys, (a) K_2, (b) K_3

Table 5 NCPR and UACI measure after a LSB change

		LSB change on the		
Image	Test	First pixel	Middle pixel	Last pixel
Cameraman (256×256)	NCPR	99.63	99.64	99.62
	UACI	33.55	33.55	33.52
Lena (512×512)	NCPR	99.62	99.62	99.61
	UACI	33.46	33.47	33.46
Airport (1024×1024)	NCPR	99.62	99.60	99.62
	UACI	33.47	33.50	33.47

5.4.1 Chosen plain image attack

The opener has an encrypted image *C* but does not know the key. However, he possesses a plain image P_0 of all-zero (or all-one), and its encrypted version C_0 obtained with the same unknown key. He extracts the sub-key used for pixel encryption as follows:

$$Sk_0{}^{i,j} = C_0{}^{i,j} \oplus P_0{}^{i,j} \tag{23}$$

Where $P_0^{i,\,j}$ =0, 0, 0... is a null-image in terms of grey values, and $C_0^{i,\,j}$, its corresponding cipher image, and (i,j) denotes the 2D-position of the pixels. The operation $(C_0^{i,\,j} \oplus P_0^{i,\,j})$extracts the key stream$Sk_0^{i,\,j}$.

Then, the sub-key extracted is used to recover the plain image *P* of the encrypted one *C* with Eq. (24).

$$P^{i,j} = C^{i,j} \oplus Sk_0{}^{i,j} \tag{24}$$

Where $P^{i,\,j}$is an image with the same size as $C_0^{i,\,j}$ and $C^{i,\,j}$ is its encrypted version.

In Fig. 11a, the chosen plain image attack on the airport encrypted image using a null-image has failed because, the scrambling-masking process and the shuffling process rely on the PIST which is highly sensitive to insignificant changes of a grey value. Therefore each encrypted image is specific to its plain image pixel characteristics.

5.4.2 Chosen cipher image attack

This time, the opener possesses an encrypted image C_0 made of all-zero (or all-one) and its corresponding decrypted version P_0. He still wants to determine the key-stream (according to Eq. (23)) necessary to recover the plain image *P* (colour Lena) from its encrypted image *C*

Table 6 NCPR and UACI measures On Lena RGB image

Image component	Test	Proposed algorithm	Ref. [18]	Ref. [34]
R	NCPR	99.63	99.59	99.63
	UACI	33.52	33.33	33.31
G	NCPR	99.61	99.62	99.60
	UACI	33.55	33.35	33.34
B	NCPR	99.64	99.63	99.61
	UACI	33.45	33.12	33.43

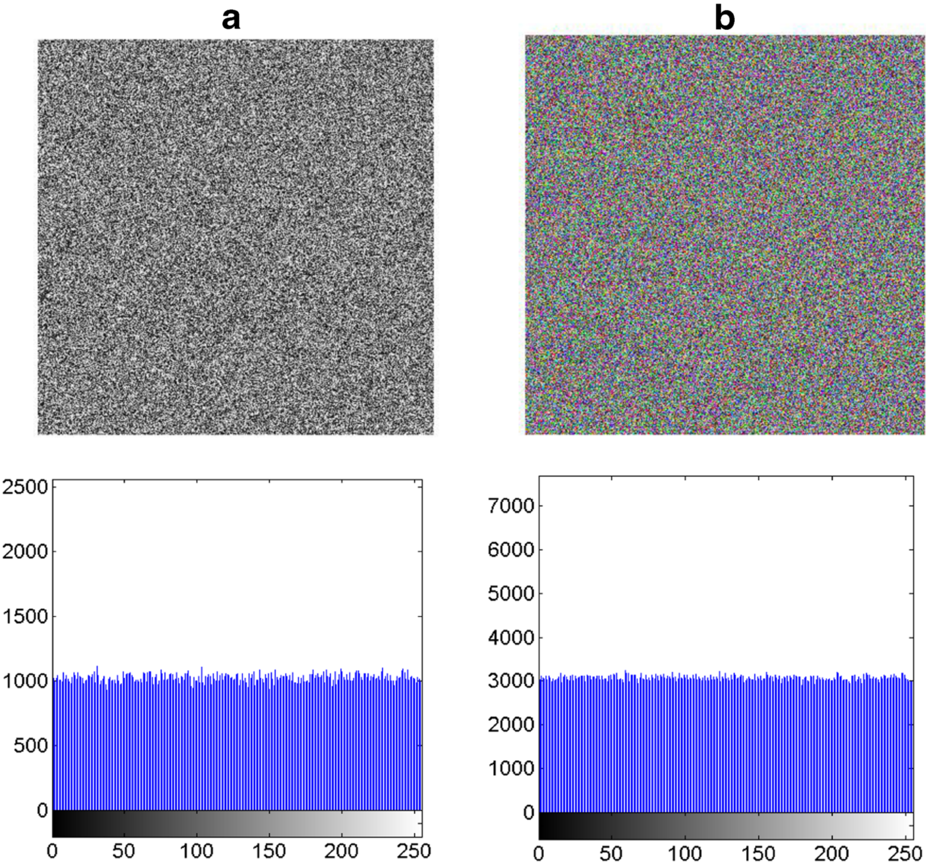

Fig. 11 Cryptanalysis. **a** Chosen plain image attack on grey Airport and its histogram, **b** chosen cipher image attack on colour Lena and its histograms

using Eq. (24). For the same reasons mentioned above (Section 5.4.1), and as shown by Fig. 11b, this type of attack does not work.

5.5 Encryption/decryption time analysis

Table 7 reports a comparison of encryption time by the proposed algorithm with some in literature for different images. The algorithm written under Matlab platform was not optimize.

The computer time consumption is smaller than those of [6, 9], while the proposed algorithm is faster than those in literature.

Table 7 Encryption time in seconds under Matlab 2012b

Image	Size	Type	Proposed algorithm	Ref. [9]	Ref. [6]	Ref. [56]
Cameraman	(256×256)	Grey	0.195	1.673	0.223	0.178
Lena	(512×512)	Grey	0.650	–	–	0.663
Airport	(1024×1024)	Grey	2.897	–	–	3.142
Lena	(512×512)	Colour	2.100	–	–	–

Table 8 Comparison of the proposed algorithm with others

Tests	Proposed cryptosystem	Ref. [42]	Ref. [2]	Ref. [57]
Key space	10^{142}	10^{96}	10^{143}	10^{42}
Key Sensitivity	99.66	–	–	99,61
Average Correlation	0.004	−0.005	0.003	0.004
Entropy	7.9994	7.999	7.9994	7.9993
NCPR	99.62	99.58	99.60	99.59
UACI	33.53	33.25	33.50	33.47
Encryption time in (s)	0.099	0.174 (4 round)	0.105 (4 round)	0.101

5.6 Overall comparison with other encryption algorithms

The performances of the proposed algorithm is here compared (Table 8) to those of some recent and good standing papers of the literature. Test are done using the colour Lena of size 512×512, and the time encryption is evaluated under visual C++ 2010 platform in accordance with real time multimedia application.

The metrics of the proposed cryptosystem reported in Table 8 suggests that, the key space, the NCPR, the encryption time, and the entropy wise are the best values. As far as key sensitivity, correlation and UACI are concerned, the values are in the order of the best values in literature.

6 Conclusion

In this paper, the proposed image encryption algorithm is based on many new 1D chaotic maps, and a substitution technique based plain image and S-boxes. The new chaotic maps are a combination of Logistic, May, Gompertz, and Gaussian maps, and have better maximum Lyapunov exponents, and therefore better chaotic properties than the originals. The encryption uses firstly, the PIST for image sensitiveness enhancement, secondly, S-boxes constructed with PRNS of the new chaos (LOMA, LOGOS, LOGAS, MAGOS, MAGAS, GAGOS, MAGOS); and thirdly, a scrambling-masking technique which permutes and diffuses image pixels in a single process with the help of S-boxes. The evaluation metrics of the proposed cryptosystem NCPR, UACI, correlation coefficient, entropy, key space and key sensitivity are amongst the best values in literature. More interestingly, a LSB change in any pixel value results in a totally different encrypted image, and chosen plaintext attack or chosen cipher image conducted is inefficient, proving the robustness of the cryptosystem. The encryption speed obtained with the non-optimized algorithm is fast enough in his current version for online multimedia communication. This proposed encryption algorithm can surely guarantee security and speed of all types of digital data transfer in a digital network.

Acknowledgement The authors wish to thank Professor Barbara ATOGHO-TIEDEU for proof reading the manuscript.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Abanda Y, Tiedeu A (2016) Image encryption by chaos mixing. IET Image Process 10(10):742–750
2. Ahmed A, El-Latif A, Li L, Niu X (2014) A new image encryption scheme based on cyclic elliptic curve and chaotic system. Multimed Tools Appl 70(3):1559–1584
3. Arroyo D, Alvarez G, Fernandez V (2008) On the inadequacy of the logistic map for cryptographic applications. arXiv:0805.4355v1[nlin.CD]
4. Arroyo D, Alvarez G, Fernandez V (2008) A basic framework for the cryptanalysis of digital chaos-based cryptography. arXiv:0811.1859v1[cs.CR]
5. Bechikh R, Hermassi H, El-Latif AAA, Rhouma R, Belghith S (2015) Breaking an image encryption scheme based on a spatiotemporal chaotic system. Signal Process Image Commun 39:151–158
6. Belazi A, Abd El-Latif AA, Diaconu A-V, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
7. Belazi A, El-Latif AAA, Belghiht S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170
8. Belazi A, Hermassi H, Rhouma R, Belghith S (2014) Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. J NonLinear Dyn 76(4):1989–2009
9. Çavusoglu Ü, Kaçar S, Pehlivan I, Zengin A (2017) A Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons Fractals 95:92–101
10. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption Scheme based on 3D Chaotic cat maps. Chaos, Solitons Fractals 21:749–761
11. Chen L, Wang S (2015) Differential cryptanalysis of a medical image cryptosystem with multiple rounds. Comput Biol Med 65:69–75
12. Chen J-X, Zhu Z-L, Fu C, Yu H, Zhang Y (2015) Reusing the permutation matrix dynamically for efficient image cryptographic algorithm. Signal Process 111:294–307
13. El-Latif A, Niu XM (2013) A hybrid chaotic system and cyclic elliptic curve for image encryption. Int J Electron Commun 67:136–143
14. Eyebe JSA, Effa JY, Alie M (2014) Highly secured chaotic block cipher for fast image encryption. Appl Soft Comput 25:435–444
15. Fan H, Li M, Liu D, AN K (2017) Cryptanalysis of a plaintext-related chaotic RGB image encryption scheme using total plain image characteristics. Multimed Tools Appl 1–25
16. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8(6):1259–1284
17. Fu C, Meng WH, Zhan YF (2013) An efficient and secure medical image protection scheme based on chaotic maps. Comput Biol Med 43(8):1000–1010
18. Guesmi R, Farah MAB, Kachouri A, Sametwang M (2016) A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. Nonlinear Dyn 83(3):1123–1136
19. Hermassi H, Belazi A, Rhouma R, Belghith S (2014) Security analysis of an image encryption algorithm based on a DNA addition combining With chaotic maps. Multimed Tools Appl 72(3):2211–2224
20. Huang XL (2012) Image encryption algorithm using chaotic Chebyshev generator. Nonlinear Dyn 67(4): 2411–2417
21. Jain A, Rajpal N (2015) A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimed Tools Appl 75(10):5455–5472
22. Jakimoski G, Koracev L (2001) Chaos and cryptography: Block encryption ciphers based on chaotic Maps. IEEE Transactions on Circuits and Systems Fund Theo Appl 48(2):163–169
23. Li C, Li S, Lo K-T (2011) Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul 16:837–843
24. Li C, Li S, Muhammad A (2009) On the security defects of an image encryption Scheme. Image Vis Comput 27(9):1371–1381
25. Liu H, Kadir A, Gong P (2015) A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. Optics Comm 338:340–347
26. Liu H, Liu Y (2014) Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. Opt Laser Technol 56:15–19
27. Liu Y, Nie L, Han L, Zhang L, Rosenblum DS (2015) Action2Activity: Recognizing Complex Activities from Sensor Data In: Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence IJCAI, 2015. aaai.org, pp 1617–1623
28. Liu Y, Tang J, Xie T (2014) Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Opt Laser Technol 60:111–115
29. Liu Y, Tong X, Ma J (2015) Image encryption algorithm based on hyper-chaotic system and dynamic S-box. Multimedia Tools Appl 1–21

30. Liu Y, Zhang L, Nie L, Yan Y, Rosenblum DS (2016) Fortune Teller: Predicting Your Career Path. In: Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence AAAI, 2016. aaai.org, pp 201–207
31. Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaotic map. J Comput Electric Eng 28(5):1240–1248
32. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia XIII 1:29–42
33. Mirzaei O, Yaghoobi M, Irani H (2012) A new image encryption method: parallel subimage encryption with hyperchaos. Nonlinear Dyn 67:557–566
34. Murillo-Escobar MA, Cryz-Hernandez C, Abundiz-Pérez F, Lopez-Gutiérrez RM, Del Campo ORA (2015) A RBG image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
35. Noura, M, Noura, H, Chehab A, Mansour M M, Sleem M, Couturier R (2018) A dynamic approach for a lightweight and secure cipher for medical images. Multimed Tools Appl 1–19
36. Pandurang HT, Kumar N, Kiran SK (2014) Image encryption based on permutation-substitution using chaotic map and Latin square image cipher. The European Physical J-Spec Topics 223(8):1663–1677
37. Parvin Z, Seyedarabi H, Shamsi M (2014) A new secure and sensitive image encryption scheme based on new substitution with chaotic function, Multimed Tools Appl 1–18
38. Schneier B (1996) Applied cryptography-protocols, algorithms, and source code in C, 2nd edn. Wiley, Hoboken
39. Sheela S J, Suresh K V, Tandur D (2018) Image encryption based on modified Henon map using hybrid chaotic shift transform. Multimed Tools Appl 1–29
40. Skiadas CH, Skiadas C (2009) Chaotic Modelling and Simulation; Analysis of Chaotic Models, Attractors and Forms. Chapman & Hall/CRC Taylor & Francis Group, New York
41. Song C-Y, Qia Y-L, Zhang X-Z (2013) An image encryption scheme based on new spatiotemporal chaos. Optik 124:3329–3334
42. Wang X, Liu L, Zhang Y (2015) A Novel Chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
43. Wang X, Luan D, Bao X (2014) Cryptanalysis of an image encryption algorithm using Chebyshev generator. Digital Signal Process 25:244–247
44. Wang X, Qiang W (2014) A Novel image encryption algoritm based on dynamic S-boxes constructed by chaos. Nonlinear Dyn 75:567–576
45. Wang W, Si M, Pang Y, Ran P, Wang H, Jiang X, Liu Y, Wub J, Wu W, Chilamkurti N, Jeon G (2018) An encryption algorithm based on combined chaos in body area networks. Comput Electr Eng 65:282–291
46. Wang W, Tan H, Sun P, Yu P, Ren B (2015) A novel digital image encryption algorithm based on wavelet transform and multi-chaos. In: Proceeding of the International Conference Wireless Communications and Sensor Network, WCSN 2015, pp 711–71946.
47. Wang X-Y, Zhang Y-Q, Liu L-T (2016) An enhanced sub-image encryption method. Opt Lasers Eng 86: 248–254
48. Wua X, Kan H, Kurths J (2015) A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Appl Soft Comput 37:24–39
49. Yang B, Liao X (2018) A new color image encryption scheme based on logistic map over the finite field ZN. Multimed Tools Appl 1–19
50. Yang H, Wong K-W, Liao X, Zhang W, Wei P (2010) A fast image encryption and authentification scheme based on chaotic maps. Commun Nonlinear Sci Numer Simul 15:3507–3517
51. Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. J Math Comput Modeling 52:2028–2035
52. Zhang X, Nie W, Ma Y et al (2017) Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box. Multimed Tools Appl 76(14):15641–15659
53. Zhang Y-Q, Wang X-Y (2014) Analysis and improvement of a chaotic-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 77(4):687–698
54. Zhang W, Yu H, Zhao Y-I, Zhu Z-L (2016) Image encryption based on three-dimensional bit matrix permutation. Signal Process 118:36–50
55. Zhang LB, Zhu ZL, Yang BQ, Liu W-Y, Zhug H-F, Zou M (2015) Cryptanalysis and improvement of an efficient and secure medical image protection scheme. Math Probl Eng 2015:1–11
56. Zhou Y, Bao L, Chen CLP (2014) A new 1D chaotic system for image encryption. Signal Process 97:172–182
57. Zhu ZL, Zhang W, Wong KW, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 181:1171–1186

Yannick Pascal Kamdeu Nkandeu is a holder of a Master degree in Physics from the University of Yaoundé I since 2014. He is currently on a Ph.D. program at the LAGEMES, Ecole Nationale Supérieure Polytechnique, University of Yaoundé I. He is specializing in image encryption.

Alain Tiedeu received his doctorate degree from the University of Yaoundé I, Cameroon, in 1995. He has been teaching electronics, digital signal processing, artificial neural networks, digital image processing, and related subjects at the National Advanced School of Engineering for many years. Professor Tiedeu has also served as reviewer, program committee member, and on editorial advisory board of a number of international conferences and journals (IEEE SITIS conference series, IEEE SETIT conference series, WSEAS conference series, RPBME, etc.). A former regular associate member of the Abdus Salam International Centre for Theoretical Physics, his research interests include biomedical instrumentation and modelling, medical signal and image processing and analysis and image encryption.