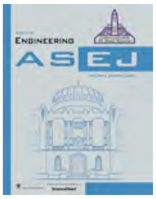
Contents lists available at ScienceDirect

Ain Shams Engineering Journal

journal homepage: www.sciencedirect.com



Engineering Physics and Mathematics

A new cryptographic algorithm via a two-dimensional chaotic map

Aesha Elghandour, Ahmad Salah, Abdelrahman Karawia [*]

Mathematics Department, Faculty of Science Mansoura University, Mansoura 35516, Egypt

ARTICLE INFO

Article history:
Received 9 October 2020
Revised 20 February 2021
Accepted 1 May 2021
Available online xxxx

Keywords:
Chaotic map
Two-dimensional piecewise smooth chaotic map
Confusion-diffusion model
Security analysis

ABSTRACT

In this paper, a new cryptographic algorithm using a two-dimensional piecewise smooth nonlinear chaotic map is suggested. It depends on the confusion-diffusion model (permutation-substitution model). Firstly, the plain image is shuffled using the logistic map (confusion). Secondly, chaotic sequences are produced by two-dimensional piecewise smooth nonlinear chaotic map. Then, the produced sequences are preprocessed to integers between 0 and 255. Finally, the shuffled image is masked using the chaotic sequences (diffusion). The suggested algorithm is tested by different types of images. Furthermore, the decryption algorithm is implemented to retrieve the plain (original) image using the secret key. Experimental results and security analyses are applied using the suggested algorithm and its performances are validated with recent cryptographic algorithms. The security and performance analyses conclude that the suggested algorithm is secure, fast, and resists various attacks.

1. Introduction

In the current era where our lives depend on technology and the exchange of information, information security has become an important challenge. This information can take several forms, such as images, video, audio, text, and others. Moreover, images specifically have many applications in many sensitive areas, such as medical, military, and personal data, among others. This is why scientists are trying to protect the security of images while transferring them through various communication channels and preventing attacks that hackers may perform. The security of information can be achieved in three different ways: encryption, steganography and watermarking.

Encryption was one of the famous algorithms used for information security long time ago. Evidence was found that the ancient Egyptians, Babylonians and the Romans used encryption, and that the Romans were the first to use encryption for military purposes. With the increase in data size transferred through images, the traditional encryption failed to perform their mission, as they needed a lot of time and high capabilities. Now, faster and more efficient methods are being sought. In fact, the encryption was previously based on permutation or substitution. In either case, encryption and decryption are used the same secret key. Now, most authors are using the permutation-substitution model. Definitely, it will increase secrecy and make the encryption difficult to break. Permutations are used first to reduce the strong association between pixels (confusion) and then substitution is made (diffusion). In this case, the security key becomes stronger because it consists of two parts, one for permutation and the other for substitution.

The encryption key must be unpredictable and highly sensitive to very small changes in its value. This is why chaos maps are so important because they have these properties. Chaos maps generate random numbers with certain characteristics like bifurcation, unpredictability, and the initial conditions sensitivity. These complex properties of chaotic maps can be expressed in a comparison to several features of perfect ciphers like balance, confusion, diffusion, and avalanche in the cryptographical process.

This paper is divided into several sections as follows. Section 2 introduces the literature survey. A brief introduction to 2D piecewise smooth nonlinear chaotic map is presented in Section 3. In Section 4, the shuffling algorithm using logistic map is given. The suggested cryptographic algorithm is introduced in more details in Section 5. Experimental results are given in Section 6. Section 7 presents security analyses and some comparisons with algorithms in literature. The conclusion is placed in Section 8.

2. Literature survey

In [20], the author was the first who published the algorithm of encryption via chaotic map. After that, many authors used chaotic maps to develop image encryption algorithms. In these algorithms,

[*] Corresponding author.
E-mail addresses: aaeshaelghandour@mans.edu.eg (A. Elghandour), asalah@mans.edu.eg (A. Salah), abibka@mans.edu.eg (A. Karawia).

https://doi.org/10.1016/j.asej.2021.05.004
2090-4479/

some of them used only permutation [23] while the others used only substitution like in [13]. In addition, many authors have merged permutation and substitution in image encryption algorithms using different types of chaotic maps. For example, in [6,5] encryption algorithms based on one-dimensional chaotic economic maps are suggested. Ref. [18] presented an image encryption algorithm using 1-D Sine Powered chaotic map. A new encryption algorithm using two-dimensional chaotic economic map is proposed in [4]. Ref. [24] presented a cryptographic algorithm via two-dimensional Henon-Chebyshev map (2D-HCM). An encryption algorithm using both pixel level and bit level permutation with Henon chaotic map is presented in [27]. Ref. [28] suggested a cryptographic algorithm using 2D chaotic map. Image encryption algorithm via image shuffling and 3D dimensional chaotic economic map was proposed by [10]. Based on three-dimensional Lorenz chaotic, a novel image encryption system was presented in [19]. Ref. [12] proposed a cryptographic algorithm via different chaotic maps. Other algorithms for color image encryption via chaotic map and DNA sequence operations are presented in [35,32,31]. Ref. [29] developed a cryptographic algorithm using Spatiotemporal chaos. Ref. [7] used a new chaotic system which consists of joining the cubic chaotic map and the logistic chaotic map to design image encryption algorithm. Optical encryption algorithm using hybrid 3D chaotic maps and discrete cosine transform is proposed in [15]. In [16], a parameter-varying Baker map (PVBM) has been introduced into process of image encryption. Ref. [34] suggested a novel chaotic map combined with delay and cascade to encrypt images. On the other hand, to improve high computational complexity for generating a big number of chaotic values using chaotic maps, some researchers have used various methods to reduce the number of values to be generated [26,11], while others have improved the characteristics of maps to consume a less time [30,17,14]. Ref. [30] presented new real time image encryption algorithms based on one-dimensional cosine polynomial. Fast Fourier Transform and various chaotic maps have been introduced for real time image encryption in [26]. A novel image encryption based on logistic-sine system (LSS) and a new S-Box has been proposed in [17]. In [14], the authors suggested a cryptographic algorithm via 32-bit piecewise linear chaotic maps. Ref. [11] proposed an algorithm for a 2D image encryption based on 2D piecewise linear chaotic maps (PWLCM). In the current paper, a cryptographic algorithm is designed using two different kinds of chaotic maps. Initially, 1-D logistic map was used to perform the permutation process to reduce the correlation between pixel values. Then a new chaotic map was used to perform the substitution process. This new map is two-dimensional, piecewise, nonlinear and smooth. The goal of the current paper is to study the effect of this new map on improving image encryption by increasing the efficiency and security of the image encryption. Experimental results of the suggested algorithm have been compared with many new encryption algorithms that have used other types of chaotic maps.

This paper is divided into several sections as follows. In Section 2, A brief introduction to 2D piecewise smooth nonlinear chaotic map. Shuffling algorithm using logistic map is given in Section 3. The suggested cryptographic algorithm is introduced in more details in Section 4. Experimental results are given in Section 5. Section 6 presents security analyses and some comparisons with algorithms in literature. The conclusion is placed in Section 7.

3. Two-dimensional piecewise smooth nonlinear chaotic map (2DPSNCM)

Now, a new chaotic map have studied in [3]. It takes the following form:

$$q_{1,t+1} = q_{1,t} + k_1 q_{1,t}[1 - 2(1+c_1)q_{1,t} - \theta q_{2,t}], q_{2,t+1} = \left\{ \begin{array}{lll} q_{2,t} + k_2 q_{2,t}[\theta(1 - q_{1,t} - 2q_{2,t}) - 2c_2 q_{2,t}] & if & q_{1,t} \geqslant f(q_{2,t}), \\ q_{1,t} & if & q_{1,t} < f(q_{2,t}), \end{array} \right\} \quad (1)$$

where

$$f(q_{2,t}) = \frac{q_{2,t}[1 + \theta k_2 - 2k_2(c_2 + \theta)q_{2,t}]}{1 + \theta k_2 q_{2,t}}.$$

$q_{1,t}$ and $q_{2,t}$ reflect the production's quantities reached to the store by Company 1 and Company 2, respectively. Map (1) shows the 2DPSNCM's chaotic behavior with five different parameters. From an economic point of view, these parameters are significant. c_1 and c_2 are the shift cost parameters where c_1 is greater than c_2. The parameter θ stands for the fraction where customers will pay for buy new remanufactured goods such that $c_2 < \theta$ and $0 < \theta < 1$. The functions $k_1 q_1$ and $k_2 q_2$ are used to capture the speed of a company's quantity adjustment with the change that can occur in the marginal profit of a company. The chaotic behavior of 2DPSNCM is observed by the values of the parameters: $c_1 = 0.55$, $c_2 = 0.3, \theta = 0.35, k_1 = 2.95, k_2 = 2$ and initial values $q_{1,0} = 0.0002, q_{2,0} = 0.0008$. Fig. 1 shows the bifurcation diagram of 2DPSNCM regarding the parameter k_1. Lyapunov exponent of a 2DPSNCM regarding the parameter k_1 is shown in Fig. 2. Based on

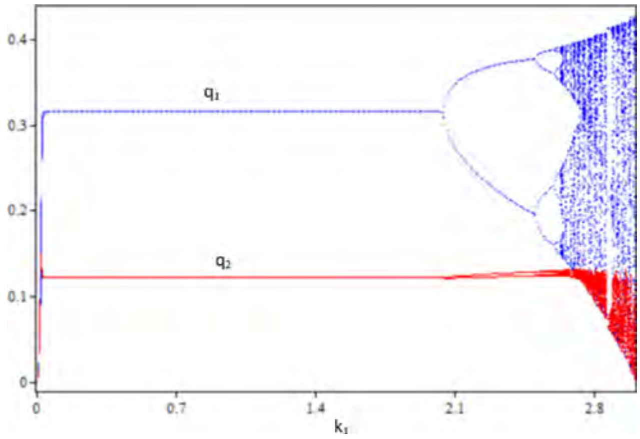


Fig. 1. Bifurcation diagram of 2DPSNCM regarding the parameter k_1 at $c_1 = 0.55, c_2 = 0.3, \theta = 0.35, k_2 = 2, q_{1,0} = 0.0002; q_{2,0} = 0.0008$ and $k_1 \in [0, 3]$.

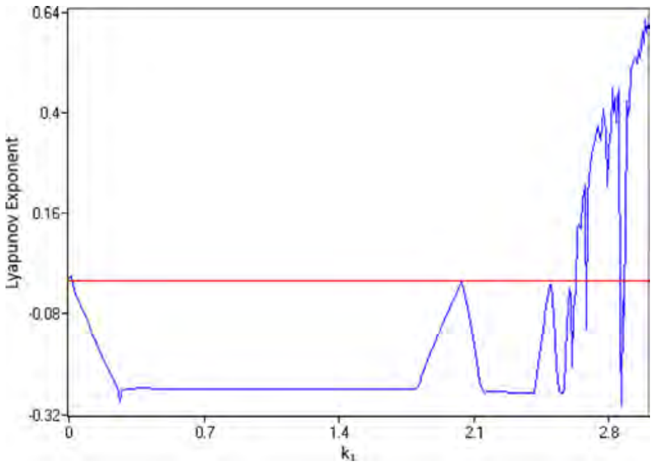


Fig. 2. Lyapunov exponent of 2DPSNCM regarding the parameter k_1.

the chaotic behavior and Lyapunov exponent of map (1), we will study its effect on improving the image encryption. The chaotic map (1) is very sensitive to initial conditions and control parameters which make it suitable for image encryption.

4. Shuffling algorithm using a logistic map

To destroy the high correlations among pixels of the plain image, the shuffling of rows and columns for the plain image are required to modify the pixel positions. The position of the pixel is shuffled randomly using the logistic map. The procedure is used to produce random different values between 1 and the dimension of the plain image. It can be processed as in **algorithm.** 1.

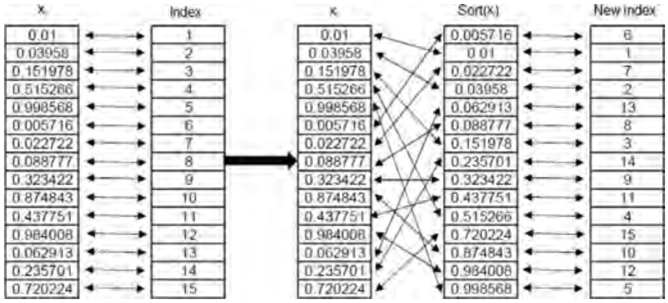
Algorithm 1. Shuffling algorithm

```
Input: Size of random numbers, $n$, the initial value, $x_0$ and the parameter $\mu$.
Output: The random numbers, $R(i), i = 1, 2, \ldots, n$.
Step 1: Set $X(1) = x_0$
Step 2: For $i = 2$ to $n$, compute
    $X(i) = \mu * X(i-1) * (1 - X(i-1))$
End
Step 3: For $i = 1$ to $n$, compute
    max=$X(i)$
    index = 1
    For $j = 2$ to $n$, compute
        If $X(j) >$ max then
            max=$X(j)$
            index = j
        End
    End
    $R(i)$=index
    $X(index) = 0$
End
```

After calling the **algorithm.** 1, change the pixels of the plain image according to the new indices. Fig. 3 shows the generation of a 1 × 15 size key.

5. The suggested work

The algorithm uses a chaotic system (logistic map) to scramble the original image using the shuffling algorithm. Then, the cipher image is obtained by diffusing the image via **2DPSNCM**. The suggested algorithm in the current paper encrypts the image significantly and includes good encryption performance. In this section, the generation of secret key, shuffling, and the image encryption/decryption algorithms are presented.



x	Index	x	Sort(x)	New index
0.01	1	0.01	0.005716	6
0.03958	2	0.03958	0.01	1
0.151978	3	0.151978	0.022722	7
0.515266	4	0.515266	0.03958	2
0.998568	5	0.998568	0.062913	13
0.005716	6	0.005716	0.088777	8
0.022722	7	0.022722	0.151978	3
0.088777	8	0.088777	0.235701	14
0.323422	9	0.323422	0.323422	9
0.874843	10	0.874843	0.437751	11
0.437751	11	0.437751	0.515266	4
0.984008	12	0.984008	0.720224	15
0.062913	13	0.062913	0.874843	10
0.235701	14	0.235701	0.984008	12
0.720224	15	0.720224	0.998568	5

Fig. 3. Shuffling process using logistic map with $x_0 = 0.01$.

5.1. The key generation

Assume that $\mathbf{P} = (p_{ij}), \quad i = 1, 2, \ldots, M,$ and $j = 1, 2, \ldots, N,$ be the plain. Now, the key mixing proportion factor K is used to generate the key as follows [8]:

$$K_z = \frac{1}{256} mod\left(\sum_{i=\left[\frac{(z-1)M}{4}\right]+1}^{\left[\frac{zM}{4}\right]} \sum_{j=1}^{n} p_{ij}, 256 \right) \tag{2}$$

and, the initial condition ξ_0 is changed via the following formula:

$$\xi_0 \leftarrow \frac{(\xi_0 + K_z)}{2}, \tag{3}$$

where $\xi_0 = xr_0, xc_0, q_{1,0}, q_{2,0}$ and $[x]$ is the nearest integer number of the number x.

Then, for the logistic map, select two initial values, xr_0, xc_0, and one parameter μ for the shuffling stage, two initial values for the **2DPSNCM**, $q_{1,0}, q_{2,0}$, with five parameters $c_1, c_2, \theta, k_1, k_2$ for diffusion stage.

5.2. Encryption algorithm

Suppose that the plain image is $P = (p_{ij}), 1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N$ and p_{ij} is the pixel value at position i, j. The suggested encryption algorithm is given as in **algorithm.** 2.

Algorithm 2. Encryption Algorithm

```
Input: Plain image, $P = (p_{ij})_{1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N}, xr_0, xc_0, \mu$ for Logistic
    map, and $c_1, c_2, \theta, k_1, k_2, q_{1,0}, q_{2,0}$ for 2DPSNCM.
Output: Cipher image $C = (c_{ij})_{1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N}$.
Step 1: Read the plain image, and convert it to gray image $A$.
Step 2: Permute the columns and the rows of $A$ using the
    shuffling algorithm, say $Shuf_A$.
Step 3: Change $Shuf_A$ from decimal to binary vector
B=$\{b_1, b_2, \ldots, b_{MN}\}$.
Step 4: Generate two sequences of $MN$ values using 2DPSNCM
as follows:
$Q_{1,1} \leftarrow q_{1,0}$
$Q_{2,1} \leftarrow q_{2,0}$
for i = 1:MN + 299
$Q \leftarrow Q_{2,i} * (1 + k_2\theta - 2k_2(c_2 + \theta)Q_{1,i})/(1 + \theta k_2 Q_{2,i})$
if $Q_{1,i} \geqslant Q$ then
$Q_{1,i+1} \leftarrow Q_{1,i}(1 + k_1(1 - 2(1 + c_1)Q_{1,i} - \theta Q_{2,i})$
$Q_{2,i+1} \leftarrow Q_{2,i}(1 + k_2(\theta(1 - Q_{1,i} - 2Q_{2,i}) - 2c_2Q_{2,i})$
else
$Q_{1,i+1} \leftarrow Q_{1,i}(1 + k_1(1 - 2(1 + c_1)Q_{1,i} - \theta Q_{2,i})$
$Q_{2,i+1} \leftarrow Q_{1,i}$
end if
end for
Step 5: Pre-process the produced sequences as follows:
$Y_1 = floor(mod(Q_{1,300:MN+299} \times (10^{14}), 256))$
$Y_2 = floor(mod(Q_{2,300:MN+299} \times (10^{14}), 256))$
Step 6: Convert $Y_1$ and $Y_2$ to binary vectors and compute the
Map = $XOR(Y_1, Y_2)$.
Step 7: Do bit-wise $XOR$ among B and Map, say
B_Map = $XOR$(B,Map).
Step 8: Change B_Map to decimal vector, say
$\mathbf{D} = \{d_1, d_2, \ldots, d_{MN}\}$.
Step 9: Rechange the D to $M \times N$ array, say C as the cipher
    image.
```

5.3. Decryption algorithm

The decryption algorithm is the inverse of the encryption algorithm. The decryption algorithm may be given as in **algorithm.** 3.

Algorithm 3. Decryption Algorithm

```
Input: Cipher image, $C = (c_{ij})_{1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N}$, $xr_0, xc_0$ for logistic
  map, and $c_1, c_2, \theta, k_1, k_2, q_{1,0}, q_{2,0}$ for 2DPSNCM.
Output: Plain image $P = (p_{ij})_{1 \leqslant i \leqslant M, 1 \leqslant j \leqslant N}$.
Step 1: Read the cipher image, $C$.
Step 2: Reshape $C$ into vector of size $1 \times MN$.
Step 3: Change the array $C$ to the binary vector
  D=$\{b_1, b_2, \ldots, b_{MN}\}$.
Step 4:Generate two sequences of $MN$ values using 2DPSNCM
  as
follows:
$Q_{1,1} \leftarrow q_{1,0}$
$Q_{2,1} \leftarrow q_{2,0}$
for i = 1:MN + 299
$Q \leftarrow Q_{2,i} \; * (1 + k_2\theta - 2k_2(c_2 + \theta)Q_{1,i})/(1 + \theta k_2 Q_{2,i})$
if $Q_{1,i} \geqslant Q$ then
$Q_{1,i+1} \leftarrow Q_{1,i}(1 + k_1(1 - 2(1 + c_1)Q_{1,i} - \theta Q_{2,i})$
$Q_{2,i+1} \leftarrow Q_{2,i}(1 + k_2(\theta(1 - Q_{1,i} - 2Q_{2,i}) - 2c_2 Q_{2,i})$
else
$Q_{1,i+1} \leftarrow Q_{1,i}(1 + k_1(1 - 2(1 + c_1)Q_{1,i} - \theta Q_{2,i})$
$Q_{2,i+1} \leftarrow Q_{1,i}$
end if
end for
Step 5: Pre-process the produced sequences as follows:
$Y_1 = floor(mod(Q_{1,300:MN+299} \times (10^{14}), 256))$
$Y_2 = floor(mod(Q_{2,300:MN+299} \times (10^{14}), 256))$
Step 6: Convert $Y_1$ and $Y_2$ to binary vectors and compute the
Map = $XOR(Y_1, Y_2)$.
Step 7: Do bit-wise $XOR$ among D and Map, say
D_Map = $XOR$(D,Map).
Step 8: Change D_Map to decimal vector, say
Z = $\{z_1, z_2, \ldots, z_{MN}\}$.
Step 9: Rechange the vector Z to $M \times N$ array, say $O$.
Step 10: Reshuffle the columns and the rows of $O$ using
inverse of the shuffling algorithm, say $P$.
Step 11: $P$ is the plain image.
```

6. Experimental results

Now, we investigate the result of the suggested algorithm. Eight gray images of different sizes are tested. All codes are implemented via Matlab R2016b and Laptop has the features: Intel(R) Core(TM) i7-4700MQ, 2.40 GHz and 12 GB RAM. The secret key of our algorithm is divided to $xr_0 = 0.01, xc_0 = 0.02$, and $\mu = 3.998$ for the logistic map, and $q_{1,0} = 0.0002, q_{2,0} = 0.0008$, $\theta = 0.35, c_1 = 0.55, c_2 = 0.3, k_1 = 2.95$, and $k_2 = 2$ for **2DPSNCM**. Figs. 4 and 5 display the plain, cipher images and their corresponding histograms.

7. Security analyses

The suggested algorithm must be tested efficiently using some tests that confirm the results.

7.1. Histogram Analysis

A good algorithm has cipher images that have uniform distribution histograms. Fig. 4(b,f,j,n) and Fig. 5(b,f,j,n) show the histograms for the images in Fig. 4(a,e,i,m) and Fig. 5(a,e,i,m), respectively, while the histograms of cipher images (Fig. 4(c,g,k,o) and Fig. 5(c,g,k,o)) are displayed in Fig. 4(d,h,l,p) and Fig. 5(d,h,l,p), respectively.

Based on Fig. 4 and Fig. 5, the histograms of the cipher images have an almost uniform distribution. Therefore, the suggested algorithm can hold out against the statistical attacks.

On the other hand, to validate whether the cipher image's histogram has the uniform distribution, the cipher image is checked by chi-square test as follows [10]:

$$\chi^2 = \sum_{n=1}^{256} \frac{(O_n - E_n)^2}{E_n} \tag{4}$$

where O_n: the observed occurrence frequencies of $n - 1$,

E_n: the expected occurrence frequencies of $n - 1$. Table 1 displays the χ^2 values of the cipher images for the suggested algorithm. Moreover, $\chi^2(n - 1, \alpha) = \chi^2(255, 0.05) = 293$. From Table 1, all values are less than 293. Therefore, we can conclude that the cipher image histograms obey the uniform distribution.

7.2. Information entropy analysis

Information entropy [33] checked the randomness of the cipher image. It can be evaluated as follows:

$$H(s) = \sum_{i=1}^{2^n - 1} P(s_i) log(\frac{1}{P(s_i)}) \tag{5}$$

where 2^n: the total states of the information source s,

$P(s_i)$: the probability of symbol s_i.

The information entropies for the images before and after the encryption using **algorithm** 2 are presented in Table 2. Based on Table 2, the information entropies of the cipher images are close to the theoretical value 8. Moreover, 100 different blocks of size 16×16 are selected randomly from the cipher image. For each block, the information entropy and the average entropy are evaluated. A comparison with algorithms in [10,9,2] is performed and the result is given in Table 3. From Tables 2 and 3, we can decide that the randomness of cipher images is achieved using **algorithm** 2 and it has good information entropy.

7.3. Correlation Analysis

Adjacent pixels of the plain image have a solid relationship. If the relationship of adjacent pixels for the cipher image is low enough, the cipher image avoids statistical attacks. The relationship of adjacent pixels is measured by correlation coefficient. It can be calculated by [10]:

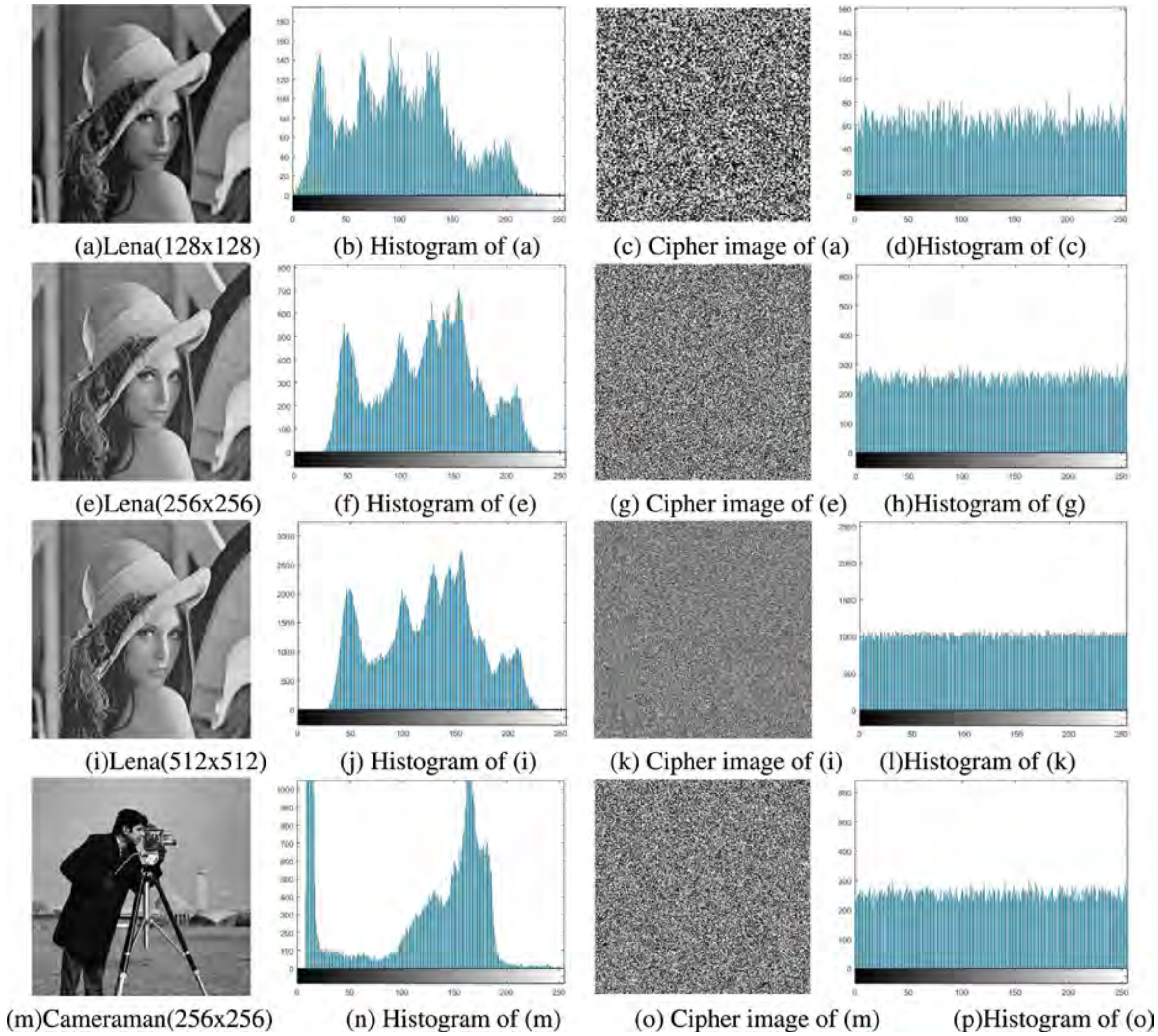
$$r_{xy} = \frac{Cov(x, y)}{\sqrt(D(x)D(y))} \tag{6}$$

where

$$Cov(x, y) = \frac{1}{N} \sum_{j=1}^{N} (x_j - E(x))(y_j - E(y)), \tag{7}$$

$$E(x) = \frac{1}{N} \sum_{j=1}^{N} x_j, \tag{8}$$

and



(a)Lena(128x128) (b) Histogram of (a) (c) Cipher image of (a) (d)Histogram of (c)

(e)Lena(256x256) (f) Histogram of (e) (g) Cipher image of (e) (h)Histogram of (g)

(i)Lena(512x512) (j) Histogram of (i) (k) Cipher image of (i) (l)Histogram of (k)

(m)Cameraman(256x256) (n) Histogram of (m) (o) Cipher image of (m) (p)Histogram of (o)

Fig. 4. Plain images, cipher images and their corresponding histograms.

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2. \tag{9}$$

From the three directions of both images, plain and cipher, adjacent pixels are chosen randomly. Then, the correlation coefficients are evaluated. Moreover, the correlation between adjacent pixels in the plain image and the cipher image is discussed. Table 4 displays its values for the image, before and after the encryption, in the three directions. For all the plain images in Table 4, the values are close to 1, whereas the values are close to 0 for all cipher images and that goes back to the solid relationship between pixels in the plain image whereas the relationship between pixels in the cipher image is a significant correlation among pixels in the three directions. The relationship of adjacent pixels for the plain images, under the suggested algorithm, is not existed. Fig. 6 displays the correlation coefficients of adjacent pixels for the Lena(256 × 256) before and after the encryption in all directions. Table 5 shows comparison between the suggested algorithm and the algorithms in literature based on the correlation coefficient measurement.

7.4. Sensitivity analyses

Sensitivity analyses are important measurements in the image encryption field. They are used to measure the sensitivity to: (i) the secret key and (ii) the plain image. In the efficient algorithm, a few modifications in any one of them lead to a nonidentical cipher image [21].

7.4.1. Key sensitivity analysis

An effective cryptographic algorithm should be oversensitive to secret keys. In the process of restoring plain images (decryption process), small changes in the true key will fail to restore the plain image. Now, the suggested algorithm is checked to the key sensitivity. Suppose that a is initial value or parameter value in the true secret key. It will be modified to $a + 10^{-14}$ and the modified key will be applied to decrypt the cipher image. Table 6 displays the decrypting images by using the true key and the modified true keys. When any one of the initial values or parameters in the true key is changed, the plain image cannot be restored. Therefore, the suggested algorithm is sensitive to the secret key.

7.4.2. Plain image sensitivity analysis

In this type, the sensitivity is tested by modifying only one pixel's value of the plain image and we have compared the cipher images of the plain image and the cipher images of the modified plain image. Two measurements will be used to measure the sensitivity to the plain image. The first is the number of pixels change rate (NPCR) and the second is the unified average changing inten-

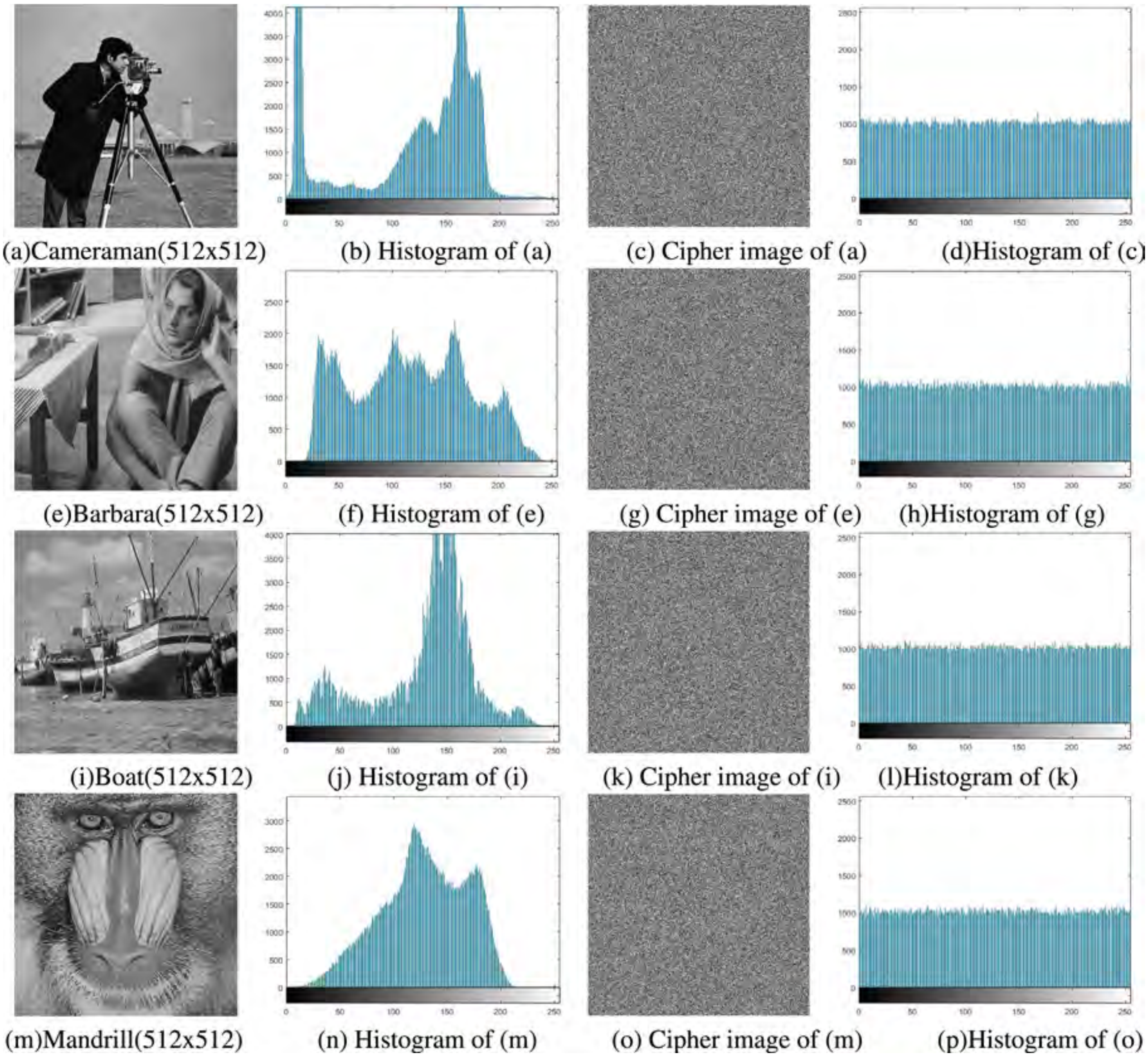


Fig. 5. Plain images, cipher images and their corresponding histograms.

Table 1
Chi-square values before and after encryption at $xr_0 = 0.01$, $xc_0 = 0.02, \mu = 3.998, q_1(0) = 0.0002, q_2(0) = 0.0008, \theta = 0.35, c_1 = 0.55, c_2 = 0.3$, $c_2 = 0.3, k_1 = 2.95$, and$k_2 = 2$.

Image	Chi-square	
	Plain Image	Cipher Image
Lena(128 × 128)	7.9348×10^3	239.3750
Lena(256 × 256)	3.9613×10^4	240.4609
Lena(512 × 512)	1.5808×10^5	287.1660
Cameraman(256 × 256)	1.0658×10^5	281.0547
Cameraman(512 × 512)	4.1651×10^5	265.6914
Barbara(512 × 512)	9.7202×10^5	237.9238
Boat(512 × 512)	3654926	258.1367
Mandrill(512 × 512)	2.1121×10^5	266.0781

sity (UACI). NPCR and UACI are evaluated by the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{10}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%. \tag{11}$$

where

$$D(i,j) = \begin{cases} 0 & \text{if} C_1(i,j) = C_2(i,j), \\ 1 & \text{otherwise} \end{cases} \tag{12}$$

M and N are the height and the width of the plain and the cipher images, C_1 and C_2 are the cipher images before and after one pixel is modified from the plain image, respectively. The exact values of NPCR and UACI are 99.61% and 33.46%, respectively. Table 7 displays the NPCR and UACI of the tested images by applying the suggested algorithm. The average values of NPCR and UACI are 99.63% and 33.52%. These values are the nearest to the theoretical values. On the other hand, a comparison among the suggested algorithm and the algorithms in literature are displayed in Table 8. From the result of Tables 7 and 8, it can be concluded that the suggested algorithm is oversensitive to the modifications in the plain image and the small modification in the plain image leads to obtain completely different cipher image. Therefore, the suggested algorithm can hold out against the differential attacks.

Table 2
Information entropy before and after encryption at $xr_0 = 0.01, xc_0 = 0.02, \mu = 3.998, q_{1,0} = 0.0002, q_{2,0} = 0.0008, \theta = 0.35, c_1 = 0.55, c_2 = 0.3, c_2 = 0.3, k_1 = 2.95$, and $k_2 = 2$.

Image	Plain	Cipher			
		Entropy	Actual entropy of the block	Theoretical entropy of the block	
				$\alpha = 0.01$ 7.16276745	$\alpha = 0.05$ 7.16634107
Lena(256 × 256)	3.4594	7.9974	7.1798	Pass	Pass
Lena(512 × 512)	3.4594	7.9994	7.1779	Pass	Pass
Cameraman(256 × 256)	3.5778	7.9969	7.1723	Pass	Pass
Cameraman(512 × 512)	3.5778	7.9993	7.1748	Pass	Pass
Barbara(512 × 512)	3.1820	7.9993	7.1847	Pass	Pass
Boat(512 × 512)	3.4594	7.9993	7.1753	Pass	Pass
Mandrill(512 × 512)	3.7736	7.9993	7.1825	Pass	Pass

Table 3
Comparison among the suggested algorithm and the algorithms in literature based on the information entropy.

Image	Suggested algorithm	Ref. [10]	Ref. [9]	Ref. [2]
Lena	7.9994	7.9992	7.9983	7.9086
Boat	7.9993	7.9993	7.9986	7.9025

Table 4
Correlation coefficient of two adjacent pixels of the image before and after the encryption.

Image		Plain Image	Suggested Algorithm	Image		Plain Image	Suggested Algorithm
Lena	H	0.8826	0.0072	Lena	H	0.9206	-0.0092
	V	0.9480	0.0073		V	0.9578	0.0008
	D	0.8447	0.0015		D	0.8992	-0.0035
Lena	H	0.9697	−0.0010	Cameraman	H	0.9327	0.0035
	V	0.9848	-0.0017		V	0.9082	0.0025
	D	0.9571	0.0002		D	0.9585	0.0002
Cameraman	H	0.9830	0.0001	Barbara	H	0.8938	0.0015
	V	0.9900	−0.0036		V	0.9583	0.0003
	D	0.9731	-0.0009		D	0.8817	−0.0036
Boat	H	0.9355	-0.0008	Mandrill	H	0.9320	-0.0026
	V	0.9699	−0.0034		V	0.9117	0.0006
	D	0.9204	0.0026		D	0.8654	0.0006

7.5. Key Space Analysis

One of the famous features of an effective cryptographic algorithm is the large key space. It must be greater than or equal to 2^{100} [36]. In the suggested algorithm, the key space has four parts: the initial values of the logistic map, the parameter of the logistic map, the initial values of **2DPSNCM**, and the parameters of **2DPSNCM**. The key space will be $10^{154} (\gg 2^{100})$ if the accuracy was 10^{-14}. Table 9 displays the key space of the suggested algorithm and the algorithms in literature. The key space is large enough ($\gg 2^{100}$). Therefore, the security standard of the key space is reached.

7.6. Noise attack analysis

While transmitting cipher images over the Internet or any transmission tool, it can be distorted by noise and it is difficult to retrieve the plain images. So, the performance of the suggested algorithm must be tested against noise attack. To test that, the Lina's cipher image of size (256 × 256) is modified by adding Gaussian noise and Salt&Pepper noise with diverse variances and densities, respectively.

Fig. 7 shows the decrypted images for all cases. The mean square error (MSE) and the peak signal-to-noise ratio (PSNR) are utilized to compute the effect of noise on the cipher image. MSE and PSNR are defined by the following formulas:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{N} (p_{ij} - c_{ij})^2, \tag{13}$$

$$PSNR = 10 \log_{10} \left(\frac{Max_I^2}{MSE} \right) \tag{14}$$

where

p_{ij}: the pixel value at the position i, j for the plain image,
c_{ij}: the pixel value at the position i, j for the cipher image,
Max_I: the largest pixel value of the image I.

Table 10 displays the MSE and PSNR for different noises. The comparison with other algorithms is added to Table 10. The decryption algorithm for the image with the Salt&Pepper noise produces result better than the image with Gaussian noise. The suggested algorithm gives result better than the algorithms in [10,22]. Therefore, the suggested algorithm can hold out against the noise attacks (see Table 11).

7.7. Chosen plaintext attack analysis

Since the suggested algorithm is oversensitive to the key mixing proportion factor K_z in eqn(2) then any change of pixel values in the plain image leads to changing in the generating sequences of **2DPSNCM**. So, the suggested algorithm can hold out against the plaintext attacks. For testing the chosen plaintext attack (CPA), the cipher image and the running of the encryption machine for

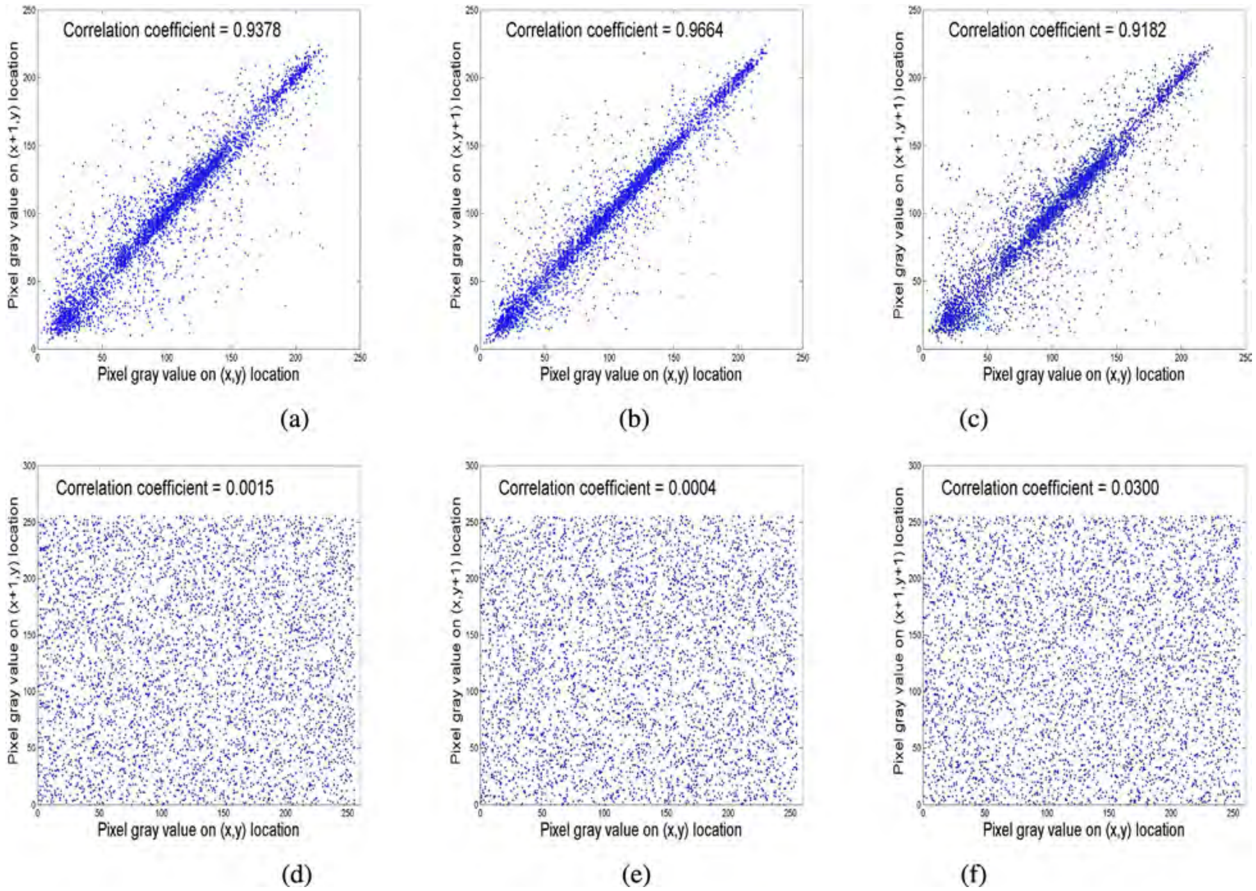


Fig. 6. Correlation coefficients of adjacent pixels for the plain image (Lena(256 × 256)) and its cipher image in all directions: (a,d) Horizontal direction, (b,e) Vertical direction, and (c,f) Diagonal direction.

Table 5
Comparison among the suggested algorithm and the algorithms in literature based on Correlation coefficient measurement.

Image		Suggested	Ref. [10]	Ref. [9]	Ref. [2]
		Algorithm			
Lena	H	−0.0010	0.0025	−0.0045	−0.0048
	V	0.0017	−0.0016	−0.0103	−0.0112
	D	0.0002	−0.0037	0.0022	−0.0045
Boat	H	−0.0008	−0.0013	−0.0130	−0.0100
	V	−0.0034	−0.0020	0.0111	−0.0124
	D	0.0026	−0.0009	−0.0182	−0.0185

Table 6
key sensitivity analysis result.

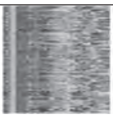
Image	Cipher image	Wrong key decryption $x_{01} + 10^{-14}$	Wrong key decryption $q_{1,0} + 10^{-14}$	Wrong key decryption $\theta + 10^{-14}$	Wrong key decryption $c_1 + 10^{-14}$	Wrong key decryption $k_1 + 10^{-14}$	True key decryption
Lena (256 × 256)							

Table 7
NPCR and UACI of the tested images.

Image	NPCR(%)	UACI%
Lena(128 × 128)	99.63	33.7986
Lena(256 × 256)	99.62	33.5188
Lena(512 × 512)	99.63	33.4198
Cameraman(256 × 256)	99.64	33.4553
Cameraman(512 × 512)	99.62	33.4769
Barbara(512 × 512)	99.62	33.5803
Boat(512 × 512)	99.63	33.5271
Mandrill(512 × 512)	99.63	33.4001
Average	99.63	33.5221

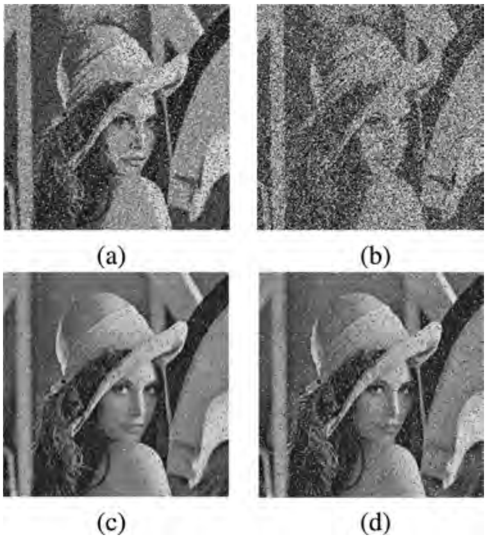


Fig. 7. (a) Decrypted image with Gaussian noise(mean = 0, variance = 0.01); (b) Decrypted image with Gaussian noise(mean = 0, variance = 0.1); (c) Decrypted image with Salt&Pepper noise(density = 0.05); (d) Decrypted image with Salt&Pepper noise(density = 0.1).

Table 8
Comparison of NPCR and UACI of Lena (256 × 256) between the suggested algorithm and the algorithms in literature.

Algorithm	NPCR(%)	UACI(%)
Expected exact value	99.61	33.46
Suggested algorithm	99.62	33.52
Ref. [9]	99.63	33.51
Ref. [10]	99.61	31.54
Ref. [2]	99.62	33.81

short time are available for the attacker. So, let P be the plain image, C is the corresponding cipher image and $D = (d_{ij})$; $d_{ij} = 0; 1 \leqslant i \leqslant M; 1 \leqslant j \leqslant N$ is the designed image to find the decimal array C_D.

CPA may be processed via the algorithm in [1] as follows:

Step 1: Implement **Algorithm 2** to encrypt D; the cipher. image is referred by C_D,

Step 2: Do $R(Restoreplainimage) = XOR(C, C_D)$,

Step 3: Compare the plain image P and the restored plain image R.

Fig. 8 shows that the restored plain image is perfectly unlike the plain image. Therefore, the suggested algorithm can resist the chosen plaintext attack.

7.8. NIST Statistical Tests

Nist is the famous standard test for pseudo-randomness. The statistical package (NIST) contains 15 tests that were created to test the randomness of generating sequences given by cryptographic algorithms[25]. To check our results, the NIST is used to test the randomness of a sequence which consists of 100 cipher images of length $256 \times 256 \times 8 = 524288$ bits. Those cipher images were generated by using random secret keys. Table 7 shows the results for 15 tests and the sequences are all passed.

7.9. Computational complexity analysis

The computational cost of the current algorithm is the total of the permutation-substitution operations. For the generating key, $(M \times N)$ operations are required. The permutation process is needed to $(M \times N)$ operations for the shuffling process and $(2 \times M \times N)$ operations for generating the sequences from **2DPSNCM**. $(M \times N)$ operations are needed for the preprocessing of these sequences. At the end, for the substitution process, the XOR is required to $(M \times N)$ operations. Therefore, the computational cost of the suggested algorithm is required to $\Theta(M \times N)$ operations.

8. Conclusion

In this paper, a new cryptographic algorithm, based on a two-dimensional piecewise smooth nonlinear chaotic map, has been proposed. **2DPSNCM** produces chaotic sequences necessary to digital image encryption. NIST test has been executed on these sequences and it has confirmed that the **2DPSNCM** is appropriate to digital image encryption. The security of the proposed algorithm has been proved over many experimental analyses: histogram analysis, information entropy analysis, correlation analysis,

Table 9
Comparison of key space between the suggested algorithm and the algorithms in literature.

Algorithm	Suggested algorithm	Ref. [9]	Ref. [10]	Ref. [2]
Key space	$10^{154} \approx 2^{500}$	2^{237}	$10^{182} \approx 2^{605}$	2^{312}

Table 10
The MSE and PSNR between decrypted images with and without noise.

Noise		Suggested algorithm		Ref. [10]		Ref. [22]	
		MSE	PSNR	MSE	PSNR	MSE	PSNR
Gaussian	var = 0.01	1967.8	15.2	2348.4	14.4	4410.1	11.7
noise	var = 0.1	4665.3	11.4	5272.1	10.9	5631.4	10.6
Salt&Pepper	d = 0.05	406.6	22.0	444.1	21.7	869.9	18.7
noise	d = 0.1	782.0	19.2	909.3	18.5	1829.6	15.5

Table 11
NIST statistical test for 100 cipher images by the suggested algorithm.

Statistical test	Suggested algorithm	Result
Frequency monobit test	100/100	PASS
Block frequency test	98/100	PASS
Runs test	99/100	PASS
Longest runs test	99/100	PASS
Rank test	98/100	PASS
Discrete Fourier transform	99/100	PASS
Cumulative sums test	100/100	PASS
Random excursion test	57/58	PASS
Random excursion variant test	57/58	PASS
Approximate entropy	97/100	PASS
Universal test	99/100	PASS
Serial	100/100	PASS
Linear complexity test	99/100	PASS
Non Overlapping templates test	99/100	PASS
Overlapping templates test	100/100	PASS

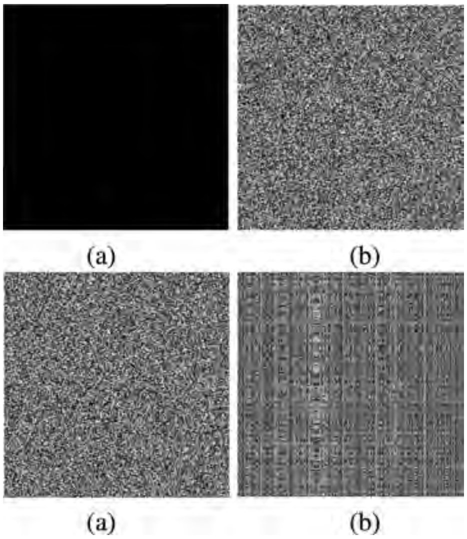


Fig. 8. CPA analysis: (a) designed image *D*, (b) decimal code matrix E_D, (c) cipher image *C*, (d) restored image *R*.

sensitivity analyses, key space analysis, noise attack analysis, and chosen plaintext attack analysis. The experimental results have concluded that the proposed algorithm can be used to image encryption efficiently. Finally, the quantum image encryption algorithm via **2DPSNCM** will be proposed to increase the current algorithm's security in the future.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

I deeply thank Dr. A. Elsherif and Dr. S. S. Askar for their proof reading of the paper.

References

[1] Ahmad M, Shamsi U, Khan I. An enhanced image encryption algorithm using fractional chaotic systems. Procedia Comput Sci 2015;57:852–9.

[2] Alawida M, Samsudin A, Teh JS, Alkhawaldeh RS. A new hybrid digital chaotic system with applications in image encryption. Signal Process 2019;160:45–58.

[3] Askar SS, Al-khedhairi A. The dynamics of a business game, A 2d-piecewise smooth nonlinear map. Phys. A 2020;537:122766.

[4] Askar SS, Karawia AA, Al-Khedhairi A, Alammar FS. An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. Entropy 2019;21(1):1–17.

[5] Askar SS, Karawia AA, Alammar FS. Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map. IET Image Process 2018;12(1):158–67.

[6] Askar SS, Karawia AA, Alshamrani A. Image encryption algorithm based on chaotic economic model, Math Probl Eng, vol. 2015, Article ID:341729; 2015.

[7] N.F. Elabady, H.M. Abdalkader, M.I. Moussa and S.F. Sabbeh, Image encryption based on new one-dimensional chaotic map, International Conference on Engineering and Technology (ICET), Cairo, Egypt, 2014.

[8] D. Enzeng, C. Zengqiang, Y. Zhuzhi and C.A. Zaiping, Chaotic images encryption algorithm with the key mixing proportion factor, International Conference on Information Management, Innovation Management and Industrial Engineering, Taipei, Taiwan, pp. 169-174, 2008.

[9] Jin X, Duan X, Jin H, Ma Y. A novel hybrid secure image encryption based on the shuffle algorithm and the hidden attractor chaos system. Entropy 2020;22(6):640.

[10] Karawia A. Image encryption based on fisher-yates shuffling and three dimensional chaotic economic map. IET Image Process 2019;13(12):2086–97.

[11] G. Kaur, R. Agarwal and V. Patidar, Chaos based multiple order optical transform for 2d image encryption, Engineering Science and Technology, In Press, 2020, DOI: 10.1016/j.jestch.2020.02.007.

[12] Khade PN, Narnaware PM. 3d chaotic functions for image encryption. International Journal of Computer Science Issues 2012;9(3):323–8.

[13] Li C, Luo G, Qin K, Li C. An image encryption scheme based on chaotic tent map. Nonlinear Dynam 2017;87(1):127–33.

[14] Li H, Deng L, Gu Z. A robust image encryption algorithm based on a 32-bit chaotic system. IEEE Access 2020;8:30127–51.

[15] Fath Allah MI, Eid MM. Chaos based 3D color image encryption. Ain Shams Engineering Journal 2020;11(1):67–75.

[16] Liu L, Miao S. An image encryption algorithm based on baker map with varying parameter. Multimed Tools Appl 2017;76(15):16511–27.

[17] Lu Q, Zhu C, Deng X. An efficient image encryption scheme based on the lss chaotic map and single s-box. IEEE Access 2020;8:25664–78.

[18] Mansouri A, Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inform Sciences 2020;520:46–62.

[19] Masood F, Ahmad J, Shah SA, Jamal SS, Hussain I. A novel hybrid secure image encryption based on julia set of fractals and 3d lorenz chaotic map. Entropy 2020;22(3):274.

[20] Matthews R. On the derivation of a "chaotic" encryption algorithm. Cryptologia 1989;13(1):29–42.

[21] Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map, image and vision computing. Image Vision Comput 2006;24(9):926–34.

[22] Parvin Z, Seyedarabi H, Shamsi M. A new secure and sensitive image encryption scheme based on new substitution with chaotic function. Multimed Tools Appl 2016;75:10631–48.

[23] Prasad M, Sudha KL. Chaos image encryption using pixel shuffling. Computer Science Information Technology 2011;2:169–79.

[24] F. Qi, S. Huang, T. Li, H. Yang and X. Kang, 2d henon-chebyshev chaotic map for image encryption, Proceedings - 21st IEEE International Conference on High Performance Computing and Communications, 17th IEEE International Conference on Smart City and 5th IEEE International Conference on Data Science and Systems, Zhangjiajie, China, pp. 774-781, 2019.

[25] A. Rukhin, J. Soto, J. Nechvatal, M. Smid and E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800–822, 2001.

[26] Sathiyamurthi P, Ramakrishnan S. Speech encryption algorithm using fft and 3d-lorenz–logistic chaotic map. Multimed Tools Appl 2020. doi: https://doi.org/10.1007/s11042-020-08729-5.

[27] Shahna KU, Mohamed A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Appl Soft Comput 2020;90:106162.

[28] Sharma M. Image encryption based on a new 2d logistic adjusted logistic map. Multimed Tools Appl 2020;79:355–74.

[29] Song CY, Qiao YL, Zhang XZ. An image encryption scheme based on new spatiotemporal chaos. Optik - International Journal for Light and Electron Optics 2013;124(18):3329–34.

[30] Talhaoui MZ, Wang X, Midoun MA. A new one-dimensional cosine polynomial chaotic map and its use in image encryption. Visual Comput 2020. doi: https://doi.org/10.1007/s00371-020-01822-8.

[31] Wang X, Zhang HL, Bao XM. Color image encryption scheme using cml and dna sequence operations. Biosystems 2016;144:18–26.

[32] Wang X, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using dna sequence operations. Opt Laser Eng 2015;73:53–61.

[33] Wu XJ, Wang KS, Wang XY, Kan HB. Lossless chaotic color image cryptosystem based on dna encryption and entropy. Nonlinear Dynam 2017;90:855–75.

[34] Zhang G, Ding W, Li L. Image encryption algorithm based on tent delay-sine cascade with logistic map. Symmetry 2020;12(3):355.

[35] J. Zhang, D. Fang and H. Ren, Image encryption algorithm based on dna encoding and chaotic maps, Math Probl Eng, vol. 2014, Article ID:917147, 10 pages, 2014.

[36] Zhang LY, Li C, Wong K, Shu S, Chen G. Cryptanalyzing a chaos-based image encryption algorithm using alternate structure. J Syst Software 2012;85(9):2077–85.

Aesha Elghandour received her B.Ed. degree in Mathematics from the faculty of education, Mansoura University, in 2012 and B.Sc. degree in Statistics and Computer Science from the faculty of Science, Mansoura University, in 2016. She is working now as a demonstrator at Computer Science Division, Mathematics Department, faculty of Science, Mansoura university, Egypt. She has many areas of research, including: cryptography, image processing, and chaos theory.

Ahmed M. Salah is lecturer of computer science at mathematics department, faculty of Science, Mansoura University, Egypt. He got his BSc. in Mathematics (majored in Statistics and Computer Science) from the faculty of Science, Mansoura University and then continued his studies obtaining an MSc in Artificial Intelligence in 2012, followed by a PhD in 2019 that explored the use of immunology as an inspiration for computing, examining a range of techniques applied to optimization and data classification problems. He was a member of the Centre for Algorithms, Visualization and Evolving Systems (CAVES) 2014-2016 at the School of Computing in Edinburgh Napier University, UK.

A.A. Karawia received his B. Sc. degree in Statistics and Scientific Computation, M.Sc. in Statistic and Computer Science and Ph.D. in Computer Science from the faculty of Science, Mansoura University, in 1994, 1999, and 2004 respectively. He is working now as an Associated Professor at Computer Science Division, Mathematics Department, Mansoura University, Egypt. He has numerous areas of research, including: cryptography, steganography, medical image processing, chaos theory, wavelets, inverse of banded matrices, linear systems and parameter estimation.