

A NEW CONTRIBUTION OF IMAGE ENCRYPTION BASED ON CHAOTIC MAPS AND THE $\mathbb{Z}/n\mathbb{Z}$ GROUP

ELAZZABY FOUZIA^{1*}, ELAKKAD NABIL², SABOUR KHALID³ AND KABBAJ
SAMIR⁴

1,3,4* Department of Mathematics, Faculty of Sciences Tofail University, KENITRA,
14000, Morocco.

2 Laboratory of Engineering, Systems and Applications, ENSA of Fez, Sidi Mohamed Ben
Abdellah University of Fez, Fez, 30200, Morocco.

Corresponding author: Elazzaby Fouzia (fouzia_099@hotmail.com).

ABSTRACT

Focusing on a significant scientific advancement in image encryption, this paper is an excellent example of its kind. It makes use of a 2D sinusoidal logistic modulation map and the advantageous transformation features of the $\mathbb{Z}/n\mathbb{Z}$ group. In which, we have developed a more suitable key flow by which to create our $\mathbb{Z}/n\mathbb{Z}$ groups as a result of the exceptional hyper-chaotic and ergodic features of our 2D-SLMM maps. By randomly rearranging the orientation of its pixels, it is possible to generate a blurring pattern that has no foreseeable relationship to the original image. Because of this, the transmitted image is no longer recognizable as being based on the original, which is now blurred and unreadable, and its transmission is private and safe from prying eyes. In fact, we compared our algorithm to five different methods from the literature and employed metrics including the histogram, entropy, correlation analysis, and differential assaults. Our simulation findings show that it performs well and achieves a high level of security with the optimum algorithmic complexity and adequate protection against unlawful manipulation. In other words, when compared to alternative methods, our method performs well when encrypting images.

Keywords: Image Encryption, Group $\mathbb{Z}/n\mathbb{Z}$, Chaotic Maps, 2D-SLMM And Security

1 INTRODUCTION

The image plays an important role in the modern media more than it ever did in the past. And with the increased use of the internet, emails, the widespread availability of computers and affordable digital cameras, we have witnessed a huge and unprecedented expansion in the dissemination of digital images and photography. The image is used in several disciplines including, among others, cryptography [10, 12], camera self-calibration ([7], [8]) and 3D reconstruction ([9], [25]). Cameras on smartphones are some of the fastest-growing mobile multimedia applications that offer technologies that have not been taken into account. Despite the inferior size of the pictures taken by these cameras, millions of shots are taken every day and are also shared between millions around the world, sometimes they are even used to document important

events, some of which are dangerous. This requires a lot of attention from researchers that make sure that security mechanisms are used to ensure the transmission of these images across networks [13, 14]. To accomplish this requirement, cryptography aims to find the best way to send these images confidentially ([22], [3], [21], [29], [26],[38]). Despite the diversity of these techniques, it is not guaranteed that they are flawless or insensitive to unauthorized attacks. Furthermore, image encryption remains a hot topic that is increasingly attracting more and more researchers that are eager to create even more effective approaches ([33], [1], [30]). Especially since it has been noticed that algorithms such as AES and DES are no longer used in the field of image encryption because the space reserved for the key is limited and the confidentiality of the message to be encrypted is not ensured. In addition, these algorithms waste time, especially at the computational level.

Indeed, traditional encryption schemes are unsuitable for image encryption due to the enormous capacity of the data and its high correlation with the image pixels. For all these reasons, most of the currently adapted encryption methods are based on chaotic encryption. The latter has good capabilities such as :

- Sensitivity to initial conditions and system parameters.
- Non-periodicity.
- Topological transitivity.
- The pseudo-random property.

In addition to all these advantages, its easy implementation and speed of real-time image processing are also noteworthy. As well, it is applicable in all scientific fields (biology, physics, electrical engineering, complex networks, etc.).

This is why we have designed a new image encryption scheme based on the chaotic 2D SLMM maps and with the good properties of this map, which can be refined to simulate the characteristics of a random signal. The latter helps us to build a $\mathbb{Z}/n\mathbb{Z}$ group, which changes the positions of the pixels in the original image according to the matrix generated by 2D-SLMM. It randomly shifts the direction of the pixels vertically and horizontally. Then an equalization is applied to the resulting image by the second 2D-SLMM matrix, which makes chaos a very interesting phenomenon to hide data. Then we performed several evaluation measurements to estimate our new approach and compared it with the approach of Hua[17], Tong [32], zhu [37], Norouzi [28] and Es-sabry[13]. Indeed, the experimental results of our algorithm demonstrate its robustness and efficiency against unauthorized access.

The present research is divided as followed: the first section elaborates the state of the art. The second section focuses on the basic mathematical concepts we have used in this research. Our proposed method is detailed in section 3. Section 4 describes the experimental results that demonstrate the performance and effectiveness of our method. And finally, the last section presents the conclusion.

2 RELATED WORK

There are several types of cryptography in the literature, and data security today is based on calculation algorithms whose confidentiality depends on the number of bits in a key. The increasing power of computational techniques

threatens the confidentiality of these classical cryptographic approaches, to alleviate this concern one of the techniques that have emerged in the last 10 years is chaos ([23], [35], [16], [4], [6]).

It is based on the use of several types of cards. One-dimensional [1D] chaotic maps which consists of a single variable and several parameters. Their structures and chaotic orbits are simple for example, logistic, Gaussian, sine and Tent maps. The application of these maps is limited due to its weakness especially at the security level: technological development has allowed the estimation of chaotic signs in case of extraction of a limited amount of information because the orbits can be estimated and the parameters predicted for image encryption, when based on these maps, several algorithms prove to be unsafe, as an example: M.Z.Talhaoui et al [31] have designed a new relevant image encryption scheme based on the new 1-DCP map. They have combined the permutation and substitution steps to increase the speed and security of encryption. This new card is defined by a simple iterative mathematical equation, and through several analytical tests, it shows a very high chaotic behavior over a wide range of its positive real control parameter.

Chaotic [HD] cards that have more complex structures and high performance. Their orbits are difficult to predict and therefore they are weak and secure. Note that the implementation of these maps is relatively complex and quite expensive.

For example, H. Guo et al [15] presented a general condition for quadratic functions which will help generate pseudo-random sequences in chaotic digital image encryption by topological conjugation of these quadratic functions with the logistic map and tent map, while A.Mansouri, X.Wang [24] constructed an image encryption scheme based on an Arnold map enhanced by the inclusion of a split operation, rotation, and pixel scrambling. The evaluation of this improved map shows better results in terms of confusion and time cost. JAN and AL used chaotic maps and adopted the TD-ERCS system to produce 2 random sequences [35]. HUA and AL [18] used one-dimensional and no-linear (1D-NLM) models. Comparing the existing chaotic cards with these new cards, one can be sure that they are more efficient since their capacities are larger, their outputs more random and the freedom of their attractors is higher. As for Mollaeefar and Al, [27] they have based

themselves on color image encryption to adapt chaotic cards with a high level of protection with a lower computing time; less correlation between pixels and more performance: Cosine-Arcsine and Sinus-Power Logistic map. Zhu and Al [19] involved a high-security algorithm based on analysis and simulations. It is a two-dimensional hyperchaotic system encrypting a single image into a local binary pattern. Note that the high security depends on the proposed algorithm and the performance of the chaotic maps, and they can be easily broken and this was the case for Belzani and Al [2] who had broken a DNA encoding and chaotic systems based on an RGB scheme through algebraic analysis. To enhance the competence of chaotic maps, chaotic modulation must be used through the reinforcement of its communication system because chaotic trajectories depend on time and information. In short, this technique is very effective for secure communication.

3 MATHEMATICAL CONCEPTS

3.1 The group $\mathbb{Z}/n\mathbb{Z}$


Let n be a non-negative integer. We define an equivalence relation \sim on \mathbb{Z} by putting: $x \sim y$ if and only if n divides $x - y$. We then write $\mathbb{Z}/n\mathbb{Z}$ the set of equivalence classes.

The equivalence class of an integer x is the subset of \mathbb{Z} formed by integers of the form: $n + x$, where $k \in \mathbb{Z}$. In the following, we will represent the equivalence class of x by the remainder $r \in \{0, 1, \dots, n - 1\}$ of the Euclidean division of x by n . We also note $x \bmod n$ the equivalence class of x .

We can define a multiplicative law on $\mathbb{Z}/n\mathbb{Z}$ by posing: $(x \bmod n) \times (y \bmod n) = xy \bmod n$. The set $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z}) - \{0\}$ with the previous law is not a group in general. In fact, $(\mathbb{Z}/n\mathbb{Z})^*$ is a group if and only if n is a prime number (we recall that, if n is not prime, an equivalence class does not always have reverse). In this work, $n = 257$ which is a prime number. So that, the set $((\mathbb{Z}/257\mathbb{Z})^*, \times)$ is a group and hence the invertible elements in $\mathbb{Z}/257\mathbb{Z}$ are the elements represented by the integers: 1, 2, 3, 4, 5, 6, 7, 8, ..., 255 and 256.

Example:

Multiplication table in the set $\mathbb{Z}/5\mathbb{Z}$.



*	[3]	[2]	[4]	[1]
[1]	[3]	[2]	[4]	[1]
[3]	[4]	[1]	[2]	[3]
[4]	[2]	[3]	[1]	[4]
[2]	[1]	[4]	[3]	[2]

[3]	[2]	[4]	[1]
[4]	[1]	[2]	[3]
[2]	[3]	[1]	[4]
[1]	[4]	[3]	[2]

Remark :

In the previous example, we only used the invertible elements in $\mathbb{Z}/5\mathbb{Z}$, i.e. the elements: 1, 2, 3 et 4.

4 THE PROPOSED TECHNIQUE

This section will discuss the inductive approach of our new encryption method regrouping the 2D chaotic maps and the excellent property of the $\mathbb{Z}/n\mathbb{Z}$ group. Then we will describe it by a graphical representation (flow chart) in Fig 2..

Algorithm

Step 1: Load and transform the source image I into three primary colors R, G, and B, denoted by I_r, I_g, I_b , and $I_r = (:, :, 1), I_g = (:, :, 2), I_b = (:, :, 3)$.

Step 2: U_1, U_2 and U_3 be three 2D chaotic matrices of size $N \times M$ generated by the 2D-SLMM sinusoidal logistic modulation map which is defined by equation (1).

$$\begin{cases} x_{i+1} = a(\sin(\pi y_i) + b)x_i(1 - x_i) \\ y_{i+1} = a(\sin(\pi x_{i+1}) + b)y_i(1 - y_i) \end{cases} \quad (1)$$

Where a and b are control parameters. $a \in [0, 1]$ and $b \in [0, 3]$

This generation is done using a 256-bit secret key $(x_0, y_0, a, H, G_1, G_2)$ Its structure is shown in Fig. 1

key

52 bits	52bits	52bits	52bits	24bits	24bits
↓	↓	↓	↓	↓	↓
x_0	y_0	a	H	G_1	G_2

Figure 1: The security key's structure

(x_0, y_0) are the initial values and a is a control parameter. H, G_1 and G_2 are designed to change

the initial values and parameters to widen the space of the security key.

x_0, y_0, α et H are decimal numbers that are generated by a 52 -bit string $\{b_1, b_2, \dots, b_{52}\}$ using the IEEE 754 format [21], as shown in equation (2)

$$x = \frac{\sum_{i=1}^{52} b_i 2^{52-i}}{2^{52}} \quad (2)$$

G1 and G2 are two integer coefficients generated by a 24 –bit string $\{b_1, b_2, \dots, b_{24}\}$. The initial values and control parameters of 2 D-SLMM to generate two chaotic matrices are defined by equation (3)

$$\begin{cases} x_{0i} = (x_0 + G_i H) \bmod 1 \\ y_{0i} = (y_0 + G_i H) \bmod 1 \\ \alpha_i = 0.9 + ((\alpha + G_i H) \bmod 0.1) \end{cases} \quad (3)$$

where the round number i is 1 or 2.

In equation (3), the initial values generated will fall within the range of $[0,1]$ and the control parameter a will be limited within $[0,9,1]$.

Thus, 2 D-SLMM has good chaotic performance under these parameters.

In our simulations we randomly generate a bitstream to produce the security key.

Step 3: we sorted the generated data in step 2 in each row, and designed three mixed index matrices of size $N \times M$, U_1', U_2' and U_3' .

Step 4: in this case, we take the first and the middle rows of these matrices (U_1', U_2' and U_3') denoted respectively by L_1, L_2 and L_3 .

L_1 is used to calculate the product of two vectors in the multiplicative group $((\mathbb{Z}/n\mathbb{Z})^*, \times)$, denoted Z_1 as for L_2 , it is used to generate the product of two vectors in the multiplicative group $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ Z_2 and we do the same for Z_3 See section II.

Step 5: For each plane I_k , each pixel is encrypted using ITGZ (image transformation by the group $\mathbb{Z}/n\mathbb{Z}$) defined by the equation below

$$\Phi_k = \frac{F(I_k)}{I_k(i, j)} = v \quad v \in [0,255], k \in 1,2,3$$

$$, I_k = I_r, I_g, I_b$$

F is the image transformation by the group $\square / n\square$ (TIGZ) which changes the positions of the pixel in each plane of the original image I (I_r, I_g, I_b) according to respectively to the matrix Z_1, Z_2 and Z_3 matrix generated by 2D -SLMM. It seems random and unpredictable to move the pixel positions in both directions, vertically and horizontally.

Step 6: Use U_1', U_2', U_3' to execute

equalization transformation for pixel values after scrambling:

$$\Psi_k = \Phi_k(i, j) \times U_k'(i, j) \bmod 256,$$

$$k \in \{1,2,3\} \text{ and } U_k' \in \{U_1', U_2', U_3'\}$$

where $\varphi_1, \varphi_2, \varphi_3$ are pixel values after the rearrangement carried out in the previous steps

Step 7: In the end, the sequence of pixels encrypted for each plane is transformed into a matrix of size $M \times N$ resulting in the encrypted image

Flowchart of the proposed method

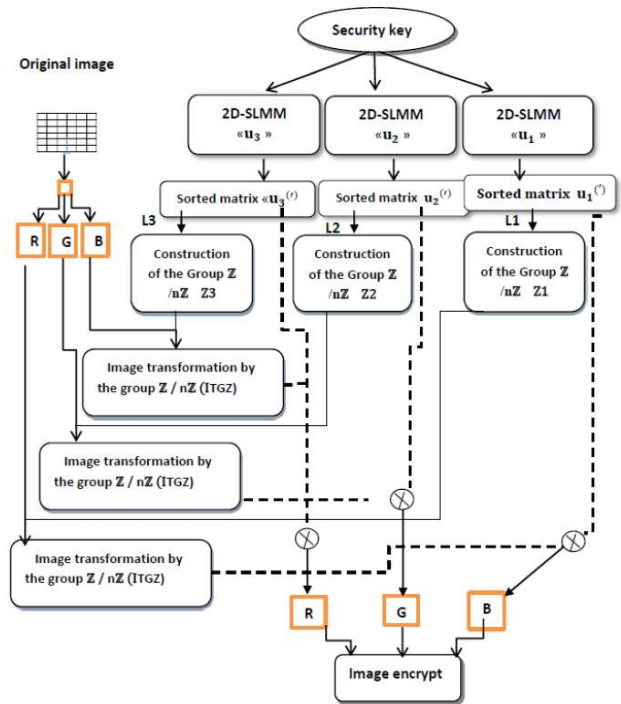


Figure 2: Flowchart of the proposed method.

4.1 Example:

This section presents step by step an illustrative example of image encryption mixing the 2D sinusoidal logistic modulation map and the group $\mathbb{Z}/5\mathbb{Z}$. First of all, we keep three sorted matrices of size 5×4 U_1', U_2' and U_3' which are streams generated by the 2D chaotic maps, the first and the middle of these three sorted matrices will be divided into two vectors, one will take the vertical part and the other the horizontal part respectively of the matrices Z_1, Z_2, Z_3 which allow us to procreate them as shown in Fig 3.

0.0239	0.0823	0.0691	0.1064
0.0551	0.0716	0.0589	0.0808
0.1432	0.0377	0.0824	0.1133
0.0914	0.0277	0.0824	0.1011
0.0931	0.0533	0.0628	0.0761



1	3	2	4
1	3	2	4
4	1	2	3
3	1	2	4
4	1	2	3



1	3	2	4
4	1	2	3



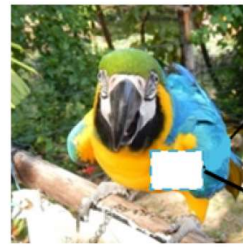
Z/5Z	[1]	[3]	[2]	[4]
[4]	[4]	[2]	[3]	[1]
[1]	[1]	[3]	[2]	[4]
[2]	[2]	[1]	[4]	[3]
[3]	[3]	[4]	[1]	[2]

Figure 3: An example of the generation of index matrix I.

Fig. 4 shows the process of reordering the pixels of a plane I_k the original I-image according to the positions of the Z_1 matrix, which indicates the references of the locations where the I-pixels are changed. For example, $Z_1[1,1] = 4$ means that the $I_k[1,1]$ position of the I_k matrix is permuted by the $I_k[4,1]$ location; $Z_1[1,2] = 2$ will permute the $I_k[1,2]$ position by $I_k[2,2]$. Since group Z_1 has four lines, the rearrangement processes can be divided into four steps as follows:

The first line of the $Z_1(4,2,3,1)$ matrix allows us to take the positions $[I_k(4,1), I_k(2,2), I_k(3,3), I_k(1,4)]$ of the original image as the first line of the mixed matrix φ_k . The same for the second row of the matrix $Z_1(1,3,2,4)$, the mixed matrix φ_k becomes $[I_k(1,1), I_k(3,2), I_k(2,3), I_k(4,4)]$. For the third row $Z_1(2,1,4,3)$ becomes $[I_k(2,1), I_k(1,2), I_k(4,3), I_k(3,4)]$. And the last line $Z_1(3,4,1,2)$ becomes

$[I_k(3,1), I_k(4,2), I_k(1,3), I_k(2,4)]$.



Ir

201	159	87	65
149	144	86	50
111	112	80	51
99	101	92	70

99	144	80	65
149	159	92	51
201	112	86	70
111	101	87	50

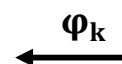


Figure 4: An example of pixel blending processes

After changing the pixels of an original image according to the positions of the Z_1 matrix. An ordinary matrix product is applied between the result of the image transformation with the Z_1 matrix (TIGZ) and the U'_1 matrix (EIGZ), and this contributes to an equalization of the pixel values to have an unpredictable blurring pattern that eliminates any resemblance or correlation with the original image and we do the same for the others plans

$$U'_1 \begin{pmatrix} 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix} \otimes \varphi_k \begin{pmatrix} 99 & 144 & 80 & 65 \\ 149 & 159 & 92 & 51 \\ 201 & 112 & 86 & 70 \\ 111 & 101 & 87 & 50 \end{pmatrix} = \begin{pmatrix} 139 & 31 & 240 & 65 \\ 149 & 220 & 184 & 204 \\ 145 & 112 & 87 & 210 \\ 76 & 147 & 87 & 100 \end{pmatrix} \text{mod } [257]$$

\otimes Is the Product of Hadamard.

The values of the resulting matrix are between 1 and 256 (because 0 has no reverse in $Z=257z$). For not having the value 256, we will subtract the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Thus, we will get the encrypted image

$$\begin{pmatrix} 138 & 30 & 239 & 64 \\ 148 & 219 & 183 & 203 \\ 144 & 111 & 86 & 209 \\ 75 & 146 & 86 & 99 \end{pmatrix}$$

For decryption, we add the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

at the decrypted matrix then we obtain

$$\begin{pmatrix} 139 & 31 & 240 & 65 \\ 149 & 220 & 184 & 204 \\ 145 & 112 & 87 & 210 \\ 76 & 147 & 87 & 100 \end{pmatrix}$$

And then, we will decrypt the image

$$\begin{pmatrix} 193 & 129 & 86 & 1 \\ 1 & 86 & 129 & 193 \\ 129 & 1 & 193 & 86 \\ 86 & 193 & 1 & 129 \end{pmatrix} \otimes \begin{pmatrix} 139 & 31 & 240 & 65 \\ 149 & 220 & 184 & 204 \\ 145 & 112 & 87 & 210 \\ 76 & 147 & 87 & 100 \end{pmatrix} \\ = \begin{pmatrix} 99 & 144 & 80 & 65 \\ 149 & 159 & 92 & 51 \\ 201 & 112 & 86 & 70 \\ 111 & 101 & 87 & 50 \end{pmatrix} \text{ mod } [257]$$

would like to point out that

$$\begin{pmatrix} 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix} \otimes \begin{pmatrix} 193 & 129 & 86 & 1 \\ 1 & 86 & 129 & 193 \\ 129 & 1 & 193 & 86 \\ 86 & 193 & 1 & 129 \end{pmatrix} \\ = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

i.e. the inverse matrix of $\begin{pmatrix} 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

modulo 257 is $\begin{pmatrix} 193 & 129 & 86 & 1 \\ 1 & 86 & 129 & 193 \\ 129 & 1 & 193 & 86 \\ 86 & 193 & 1 & 129 \end{pmatrix}$

5. STATISTICAL ANALYSIS

This part demonstrates the efficiency and resistance of our proposed image cryptosystem against all illicit attacks that exist in the literature either in terms of statistical, cryptanalytic or brute force attacks.

To do this, we applied these different security measures to 8 images of size 256 x 256 using the java programming language.

5.1. Histograms

A histogram is one of the most common criteria for making a comparison between the graphical representation of the intensity distribution of the encrypted images and the original images. This is why we have compared the histograms of 8 original images with very different contents and the histogram of their encrypted images using

our new method.

According to Figures 6 and 7, we found that the distribution of pixels in the histograms of the encrypted images is almost uniform, while the distribution of the original images has very high and very low values. This obvious difference between the two histograms leads us to say that our new approach demonstrates its robustness in terms of security and ensures the protection of the images against statistical attacks.

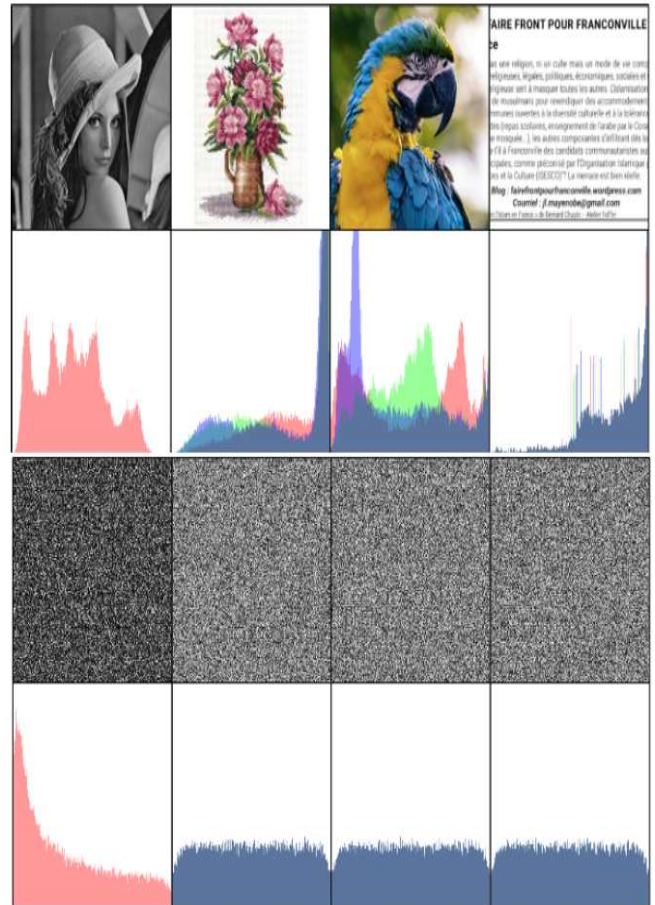


Figure 5. Example 1 shows the results of the simulation of 4 images. The first line represents the original images, the second line shows their histograms and the third and fourth lines represent the encrypted images and their histograms. (i1) Lena image; (i2) owers image; (i3) Parrot image; (i4) image text.

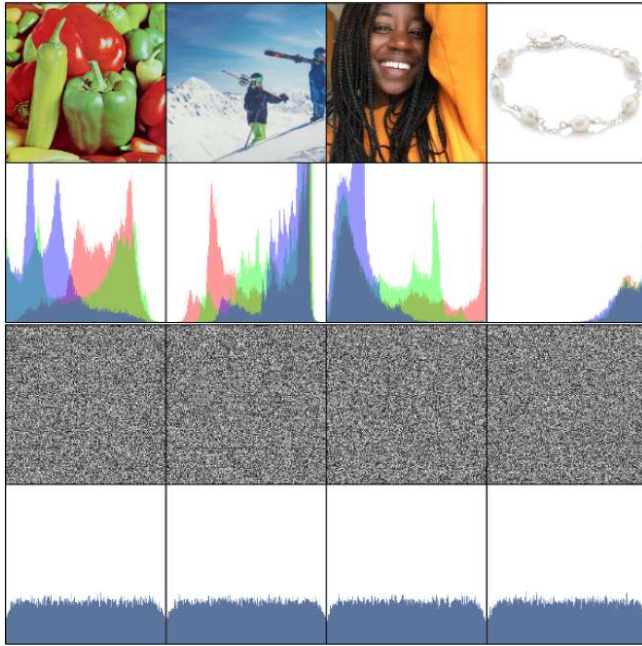


Figure 6. Example 2 shows the results of (i5) Peppers image; (i6) ski image; (i7) girl image; (i8) image bracelet.

5.2. Correlation coefficient of two adjacent pixels

Each image is made up of many key internal pieces of information, including the "correlation coefficient of the adjacent pixels", which is the target of any statistical attack. So it is necessary to strengthen the competence of this coefficient while minimizing and even getting rid of it to have the weakest and hardest to decipher original images. To reach this level of security, the following test was put into practice: 5 000 pairs of adjacent pixels were arbitrarily selected in three directions horizontally, vertically and diagonally from the original image and the encrypted image, this calculation is applied to the images in figures 6 and 7, using the following equations

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D_x} \sqrt{D_y}} \quad (4)$$

$$Cov(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - E_x)(y_i - E_y) \quad (5)$$

$$D_x = \frac{1}{N} \sum_{i=1}^N (x_i - E_x)^2 \quad (6)$$

$$E_x = \frac{1}{N} \sum_{i=1}^N x_i \quad (7)$$

After the test (see table 1), we conclude that:

– The coefficient of the original image takes values close to 1:

– The coefficient of the encrypted image takes values close to 0.

This leads us to say that our method is more efficient in destroying the dependency between adjacent pixels.

This test (see table 2) informs that the degree of reliability of our method and its high performance are better than the approaches of Hua[17], Tong[32] and Es-Sabry[13]. And proves that it can eliminate any resemblance between the original image and the encrypted image.

5.3 Correlation coefficient between the original image and the encrypted image

We reiterate that the above-mentioned test was based on 3 directions. Now we will calculate the correlation coefficient for each pixel of the original image with that of the image to be encrypted according to this formula:

$$CC = \frac{\sum_{i=1}^M \sum_{j=1}^N (I_{ij} - \bar{I})(I'_{ij} - \bar{I}')}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (I_{ij} - \bar{I})^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N (I'_{ij} - \bar{I}')^2}} \quad (8)$$

$$\bar{I} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N I_{ij} \quad (9)$$

$$\bar{I}' = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N I'_{ij} \quad (10)$$

I : original image and \bar{I} its average.

I' : encrypted image and \bar{I}' its average.

N,M: Represent respectively the length and the width of the matrices I and I'.

Encrypted image	Our Method	Es-sabry[13]	ZHU [37]
Lena	-1.8735E-4	0.001744	0.002851
Peppers	8.9482E-4	-0.001332	-0.001650

Table 3: Comparison of CC of our method with that of ZHU.

Our method achieves better results than those found by the zhu [37] and Es-sabry [13] methods because the values obtained are close to '0'.

5.4 Differential attacks

To assess the reliability of our approach to differential attacks, we took the image of lena. We made a small change in a single pixel of this image and then calculated the NPCR and ICAU as shown in equations (11) and (12). The values found are respectively greater than 99.6% and 33.8%(see table 4).

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\% \quad (11)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (12)$$

$$D(i, j) = \begin{cases} 0, & \text{if } C_1(i, j) = C_2(i, j) \\ 1, & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases} \quad (13)$$

5.5 Entropy information

The entropy of an image is an indicator of its complexity, the higher the entropy, the more random the image is. To calculate entropy, we use the following formula.

$$H(s) = \sum_{i=0}^{2^n-1} P(s_i) \log_2 [P(s_i)] \quad (14)$$

- $P(s_i)$ represents the probabilities of occurrence of each Si
- 2^n marks the total number of states of the information source (note the entropy should be equal to n for the random information source to be perfect and having 2n states).

As far as we are concerned we will use each channel and we will calculate their entropy information then the number of states will be 256 and the ideal entropy $n = 8$.

Images	Original Entropy	Encrypted Entropy
Lena	7.610197	7.9989244
Peppers	7.5867806	7.9997215

Table 5: Entropy of the original image and the encrypted image

According to Table 5, the values found are close to the ideal 8. This ensures the resistance of our approach against any illicit attacks.

6 CONCLUSION

In this article, a novel encryption algorithm that is based on a 2D chaotic map and the transformation of the Z/nZ group is presented. This algorithm has the potential to significantly improve the cryptosystem's level of safety. The scheme is described in detail.

For the purpose of determining whether or not the proposed encryption method is secure, various security analyses, such as correlation analysis, histogram analysis, and key sensitivity analysis, are carried out. The findings of the experiment provide evidence that the encryption

algorithm offers a high level of security.

REFERENCES

- [1] Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V., On the security of a new image encryption scheme based on chaotic map lattices, *Chaos: Interdiscip. J. Nonlinear Sci.* 18 (2008).
- [2] Belazi, A., Hermassi, H., Rhouma, R., et al., Algebraic analysis of a rgb image encryption algorithm based on dna encoding and chaotic map, *Nonlinear Dyn.* 76, 1989–2004 (2014).
- [3] Borujeni, S.E., Eshghi, M., Chaotic image encryption system using phase-magnitude transformation and pixel substitution, *J. Telecommun. Syst.* 52, 525–537 (2013).
- [4] C. Ling, X. Wu, S. Sun, A general efficient method for chaotic signal estimation, *IEEE Trans. Signal Process.* 47, 1424–1428(1999).
- [5] Elazzaby, F., El Akkad, N., Kabbaj, S., A New Encryption Approach Based on Four-Square and Zigzag Encryption (C4CZ), *Embedded Systems and Artificial Intelligence* (Springer). 1076, 589-597(2020).
- [6] Elazzaby, F. EL akkad, N., kabbaj, S., Advanced encryption of image based on S-box and chaos 2D (LSMCL), 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). DOI: 10.1109/IRASET48871.2020.9092254 (2020).
- [7] El akkad, N. Merras, M. Saaidi, A. and Satori, K., Camera self-Calibration with Varying Parameters from Two views, *Wseas Transactions on Information Science and Application*, Vol. 10, No. 11, pp. 356-367, 2013.
- [8] El akkad, N. Merras, M. Saaidi, A. and Satori, K., Robust Method For Self-Calibration Of Cameras Having The Varying Intrinsic Parameters, *Journal Of Theoretical And Applied Information Technology* 50 (1): 57-67, (2013).
- [9] El akkad, N. El Hazzat, S. Saaidi, A. and Satori, K., Reconstruction of 3D Scenes by Camera Self-Calibration and Using Genetic Algorithms, *3D Research*, 6 (7): 1-17, (2016).

- [10] Es-Sabry, M., El Akkad, N., Merras, M., Saaidi, A., Satori K., A novel text encryption algorithm based on the two-square Cipher and Caesar Cipher, *Int Conf Big Data Cloud Appl.* 872, 78–88, (2018).
- [11] Es-sabry, M., El akkad, N., Merras, M., Saaidi, A., Satori, K., A New Color Image Encryption Using Random Numbers Generation And Linear Functions, *Embedded Systems and Artificial Intelligence (Springer)*, 581-588, (2020).
- [12] Es-Sabry, M., El Akkad, N., Merras, M., Saaidi, A., Satori, K., Grayscale image encryption using shift bits operations, *International Conference on Intelligent Systems and Computer Vision.* 1-7, (2018).
- [13] Es-sabry, M., El akkad, M., Merras, M., Saaidi, A., Satori, K., A Novel Color Image Encryption Approach Based On Random Numbers Generation Of Two Matrices And Bit-Shift Operators, *Soft Computing (Springer)*, (2019). <https://doi.org/10.1007/s00500-019-04151-8>.
- [14] Essaid, M., Akharraz, I., Saaidi, A., Mouhib, A., Mohamed, E., Ismail, A., Abderrahim S., Ali M., A new color image encryption algorithm based on iterative mixing of color channels and chaos, *Advances in Science, Technology and Engineering Systems Journal.* 2, 94-99 (2017).
- [15] GUO, H., ZHANG, X., ZHAO, X., YU, H., ZHANG, L., Quadratic Function Chaotic System and Its Application on Digital Image Encryption, 8, 55540 – 55549(2020).
- [16] Hilborn, R.C., *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, second ed., Oxford University Press, USA, 2001.
- [17] Hua, Z., Zhou, Y., Pun, C.M., Chen, P.C., 2D Sine logistic modulation map for image encryption, *Inf Sci.* 297, 80–94 (2015).
- [18] Hua, Z., Zhou, Y., One-dimensional nonlinear model for producing chaos, *IEEE Trans. Circuits Syst. I Reg. Papers.* 65(1), 235-246(2018).
- [19] H. Zhu, X. Zhang, H. Yu, C. Zhao, Z. Zhu, An image encryption algorithm based on compound homogeneous hyper-chaotic system, *Nonlinear Dyn* 89, 61–79 (2017).
- [20] Khan, J.S., Ahmad, J., Chaos based efficient selective image encryption, *Multidim Syst Sign Process.* 30, 943–961 (2019).
- [21] Liu, C.X., Lu, J.J., A novel fractional-order hyperchaotic system and its circuit realization, *Int. J. Mod. Phys. B.* 24(10), 1299–1307 (2010).
- [22] Lu, L., Luan, L., Meng, L., Li, C.R., Study on spatiotemporal chaos tracking synchronization of a class of complex network, *Nonlinear Dyn.* 70, 89–95 (2012).
- [23] Lesne, A., Chaos in biology, *Riv. Biol.* 99(3), 467–481 (2006).
- [24] Mansouri, A., Wang, X., Image encryption using shuffled Arnold map and multiple values manipulations, *Vis Comput (2020)*. <https://doi.org/10.1007/s00371-020-01791-y>.
- [25] Merras, M., Saaidi, A., El akkad, N., Satori, K., Multi-view 3D reconstruction and modeling of the unknown 3D scenes using genetic algorithms, *Soft computing (Springer)*. 22(19), pp. 6271-6289, 2017.
- [26] Mitchell, G., Richter, E. A., Weidenmüller, H. A., Random matrices and chaos in nuclear physics, nuclear structure. *Rev. Mod. Phys.* 81(2), 539–589 (2009).
- [27] Mollaefar, M., Sharif, A., Nazari, M., A novel encryption scheme for colored image based on high level chaotic maps, *Multimed. Tools Appl.* 76(1), 607-629(2017).
- [28] Norouzi, B., Seyezadeh, S.M., Mirzakuchaki, S. Mosavi; M.R., A novel image encryption based on hash function with only two-round diffusion process, *Multimedia Systems.* 20, 45–64(2014).
- [29] Patidar, V., Pareek, N., Sud, K., A new substitution-diffusion based image cipher using chaotic standard and logistic maps, *Communications in Nonlinear Science and Numerical Simulation.* 14 (7) 3056–3075(2009)

- [30] Skrobek, A., Cryptanalysis of chaotic stream cipher, *Phys. Lett. A.* 363, 84–90(2007)
- [31] Talhaoui, M.Z., Wang, X., Midoun, M.A., A new one-dimensional cosine polynomial chaotic map and its use in image encryption, *Vis Comput* (2020). <https://doi.org/10.1007/s00371-020-01822-8>.
- [32] Tong, X.J., Wang, Z., Zhang, M., Liu, Y., Xu, H., Ma, J., An image encryption algorithm based on the perturbed high-dimensional chaotic map, *Nonlinear Dyn.* 80, 1493–1508 (2015)
- [33] Tong, X., Cui, M., Wang, Z., A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator, *J. Opt. Commun.* 282, 2722–2728(2009).
- [34] Wang, X.Y., Guo, K., A new image alternate encryption algorithm based on chaotic map, *Nonlinear Dyn.* 76, 1943–1950(2014).
- [35] Wikipedia, Double-precision Floating-point Format – Wikipedia, the Free Encyclopedia, 2013 (online; accessed 10.12.13).
- [36] Wu, X., Hu, H., Zhang, B., Parameter estimation only from the symbolic sequences generated by chaos system, *Chaos Solitons Fractals.* 22, 359–366(2004).
- [37] Zhu, C.: A novel image encryption scheme based on improved hyperchaotic sequences, *J. Opt. Commun.* 285, 29–37 (2012).
- [38] AZZABY, Fouzia El, AKKAD, Nabil El, SABOUR, Khalid, et al. An RGB Image Encryption Algorithm Based on Clifford Attractors with a Bilinear Transformation. In : International Conference On Big Data and Internet of Things. Springer, Cham, 2022. p. 116-127.

Table 1: Correlation Coefficients Of Two Adjacent Pixels In The Plain-Image And Cipher-Image.

Image	plain-image			+		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.975406	0.931383	0.937071	-0.000157	-0.001046	0.014203
flowers	0.8779182	0.954342	0.900693	-0.003239	0.0011912	0.004434
Parrot	0.9785220	0.9765191	0.9510852	-0.000742	0.008564	0.0133476
text	0.7931710	0.702597	0.553564	-0.003533	-0.009137	0.0010205
Peppers	0.956327	0.9460656	0.954976	0.0120298	0.0014030	-0.009772
ski	0.9818879	0.9506004	0.946533	-0.003344	-0.013221	0.0076130
girl	0.9931496	0.8818434	0.965882	0.003811	0.0137725	0.0036377
bracelet	0.976975	0.929243	0.936798	0.018107	0.010126	-0.001253

Table 2: Comparison Of Correlation Coefficients Of Two Adjacent Pixels In Different Directions Using The Proposed Algorithm With Some Other Algorithms.

Encryptedimage	Directions			Average
	Horizontal	Vertical	Diagonal	
Hua [17]	0.002383	0.008576	0.040242	0.017067
Tong [32]	0.003800	0.005800	0.013300	0.007633
Es-Sabry[13]	-0.007205	0.025854	-0.009817	0.002944
Proposed method	-0.005587	-7.195377E-4	0.006429	0.000121

Table 4: The Sensitivity Of The Algorithm For A Change Of A Single Pixel Of The Original Image.

Image	Proposed Method		Es-Sabry [13]		Tong [32]		Norouzi [28]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.7323	33.61894	99.67576	33.59832	99.62739	33.35064	99.66890	33.55610