Image encryption based on chaos, elliptic curve, dynamic S-boxes and variable permutations

Victor Manuel Silva Garcia
Instituto Politécnico Nacional
Kevin Brando Garcia-Cuahutle
Instituto Politécnico Nacional
Rolando Flores-Carapia
Instituto Politécnico Nacional
Marlon David Gonzalez-Ramirez (dgonzalezr@ipn.mx)
Instituto Politécnico Nacional
Juan Carlos Chimal-Eguia
Instituto Politécnico Nacional

Research Article

Keywords: Lorenz equations, elliptic curve, chaos, variable S-box, variable permutation

Posted Date: May 17th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1647076/v1

Image encryption based on chaos, elliptic curve, dynamic S-boxes and variable permutations

Victor Manuel Silva Garcia[1], Kevin Brando Garcia-Cuahutle[2†], Rolando Flores-Carapia[1†], Marlon David Gonzalez-Ramirez[1*†] and Juan Carlos Chimal-Eguia[2†]

[1*]Centro de Innovación y Desarrollo Tecnológico en Cómputo, Instituto Politécnico Nacional, Av. Luis Enrique Erro S/N, Unidad Profesional Adolfo López Mateos, Zacatenco, Gustavo A. Madero, 07738, Ciudad de México, México.
[2]Centro de Investigación en Computación, Instituto Politécnico Nacional, Av. Luis Enrique Erro S/N, Unidad Profesional Adolfo López Mateos, Zacatenco, Gustavo A. Madero, 07738, Ciudad de México, México.

*Corresponding author(s). E-mail(s): dgonzalezr@ipn.mx;
Contributing authors: vsilvag@ipn.mx;
dkevinyahppp@gmail.com; rfloresca@ipn.mx; jchimale@ipn.mx;
†These authors contributed equally to this work.

Abstract

The proposed algorithm called Image encryption based on chaos, elliptic curve, dynamic S-boxes and variable permutations (IECC) is a symmetric cryptosystem for encrypting bmp images, in this case 512 × 512 pixel figures are used for testing. This algorithm consists of 15 rounds with a different S-box for each round and each set of S-boxes is different for each image encryption. Based on the above, a permutation is applied before the first round, additionally, in round 15 the inverse permutation of the first round intervenes. Both the S-boxes and the permutations are built using the E. Lorenz equations, which obtain solutions with two different points of the elliptic curve chosen randomly in each process. To measure the resistance to differential attack of the proposed cryptosystem, the following measurements are carried out: Number of Pixels Change Rate

- NPCR, Unified Average Changing Intensity - UACI. Also, taking into account that the generation of the boxes is dynamic, the algebraic attack is avoided; furthermore, with this symmetric cryptosystem it is possible to distribute keys and sign, since an asymmetric system is used in its construction. On the other hand, four types of noise are applied to the encrypted images to evaluate the resistance of the encryption algorithm to this type of attack. Ten instruments are used to measure the quality of encryption; namely: entropy, correlation, discrete Fourier transform, NPCR, UACI, Avalanche Criteria - AC, contrast, energy, homogeneity and a goodness of fit test is proposed using the χ^2 distribution.

Keywords: Lorenz equations, elliptic curve, chaos, variable S-box, variable permutation.

1 Introduction

Images are an important element to contain information, therefore, they can be protected using encryption algorithms, especially symmetric encryption algorithms [1–5]. In this case, the use of dynamic boxes, variable permutation, chaos and transcendental numbers is proposed to give rise to the Image Encryption Algorithm using Permutation, and Dynamic Boxes (IECC). In this work the images are not compressed since there are some countries whose regulations do not allow it, for example, Mexico [6]. In fact, the bmp format is used.

Four points are highlighted in IECC. The first point is related to the resistance of the proposed cryptosystem to attacks. In this case, the attacks are divided into three categories:

A) those carried out using the elliptic curve;
B) those that apply to the proposed symmetric cryptosystem and,
C) those that apply to encrypted images.

The A point refers, because the elliptic curve is involved in the construction of the IECC system, some attacks may be to the curve, which leads to the discrete logarithm problem [7], [8]. The discrete logarithm attack on the elliptic curve can be compared to the integer factorization n of the Rivest Shamir Adleman (RSA). Solving the discrete logarithm problem when the number of points on the curve has a prime factor of 2^{256} is equivalent to factoring in the RSA scheme, a $n \approx 2^{3072}$ [9]; however, an elliptic curve can be constructed whose number of solutions has a prime factor greater than 2^{512} [10]. In this scenario, solving the discrete logarithm problem is equivalent to factoring $n \approx 2^{15000}$ in the RSA scheme [9]. This is higher than what is currently on the market [11]. On the other hand, a brute force attack on the IECC when the number of keys is greater than 2^{512} is more complex than a brute force attack on the Advanced Encryption Standard - AES-256 [12] cryptosystem. The B point is described below: as the substitution boxes (S-box) are unknown in each encryption process, it is not possible to perform the linear attack, at

least as known [13], [14]. Also, because dynamic S-box (8 × 8) are used, the algebraic attack [15] cannot be carried out. The schedule-keys is constructed by means of the chaos and the points of the elliptic curve. Also, an algorithm is applied to generate permutations, which defines a one-to-one function, in fact, a bijective function [16]. Regarding the C point, it is mentioned that the images encrypted with the proposed cryptosystem resist differential attack [17, 18], because the NPCR, UACI and AC parameters have adequate values [19–21] in fact, the results will be presented later.

According the second point, it is mentioned that the proposed symmetric cryptosystem is of the Substitution Permutation Network (SPN) type [22] with a random permutation of the image size at the encryption beginning. This makes attacks on the cryptosystem more complex [23].

The third point refers to the quality of the images encryption, that is, as the proposed encryption cryptosystem is symmetric, it is tested by encrypting one image in black color and another in white. In the results section we will see that the encryption is of quality.

Last point, it is pointed out that the encrypted images are subjected to four types of noise: occlusion, additive, multiplicative and Gaussian [24]. In this sense, a parameter is proposed to evaluate the damage, when the image encrypted with noise is decrypted. This parameter is called Similarity Parameter – SP_c, where the subscript c indicates the color.

The present work is organized as follows: in the Introduction a brief description of the state of the art is made; In Section II, the tools that are used in this research are presented; Section III presents the construction of the elements involved in the encryption algorithm, as well as the test images; Section IV shows how the different noises are constructed, and how they affect the encrypted images; In addition, a high-level description of the median filter 3 × 3 and the SP parameter is made; The results are shown in Section V; In Section VI, the analysis and discussion are presented; Finally, in Section VII, the conclusions and future work are shown.

2 Theoretical tools utilized in IECC

2.1 Lorenz equations

The Lorenz system of differential equations is shown in Eqs.(1, 2, 3) [25].

$$\frac{dx}{dt} = \sigma(-x + y) \tag{1}$$

$$\frac{dy}{dt} = rx - y - xy \tag{2}$$

$$\frac{dz}{dt} = -bx + xy \tag{3}$$

The parameters σ, r and b are real positives; furthermore, the critical points of the Lorenz equations are obtained by setting to zero the Eq.(1), Eq.2 and

Eq.3. From here, the critical points are presented in Eq.4:

$$\begin{aligned} P_1 &= (0,0,0) \\ P_2 &= (\sqrt{b(r-1)}, \sqrt{b(r-1)}, r-1) \\ P_3 &= (-\sqrt{b(r-1)}, -\sqrt{b(r-1}, r-1) \end{aligned} \tag{4}$$

Considering that the Lorenz equations describe the phenomenon of convection in the Earth's atmosphere, the values expressed below are reasonable: $\sigma = 10$ y $b = \frac{8}{3}$. Also, the solution of the Lorenz's equations has the form presented in Eq.5:

$$\vec{X} = \vec{\xi} e^{\lambda t} \tag{5}$$

where $\vec{\xi}$ represent the eigenvectors, and λ the eigenvalues. To calculate the solutions in the neighborhood of the point P_2, the equation Eq.6 is used.

$$X^{'} = AX \tag{6}$$

where the matrices A, X y $X^{'}$ are described in the Eqs.(7, 8, 9);

$$A = \begin{pmatrix} 10 & 10 & 0 \\ r & -1 & -\sqrt{8/3(r-1)} \\ \sqrt{8/3(r-1)} & \sqrt{8/3(r-1)} & -8/3 \end{pmatrix} \tag{7}$$

$$X = \begin{pmatrix} \mathrm{x} \\ \mathrm{y} \\ \mathrm{z} \end{pmatrix} \tag{8}$$

$$X^{'} = \begin{pmatrix} x^{'} \\ y^{'} \\ z^{'} \end{pmatrix} \tag{9}$$

The eigenvalues are calculated from the characteristic polynomial, which is obtained from the Eq.(10).

$$\mid A - \lambda I \mid = 0 \tag{10}$$

Considering the parameter $r = 28$, the characteristic polynomial is written in the Eq.(11).

$$3\lambda^3 + 41\lambda^2 - 50\lambda + 2160 = 0 \tag{11}$$

From the Eq.(11) a real root and two complex ones are obtained; these are shown in the Eqs.(12, 13, 14).

$$\lambda_1 = -22.558424 \tag{12}$$

$$\lambda_2 = 4.445878 + 3.485904i \tag{13}$$

$$\lambda_3 = 4.445878 - 3.485904i \tag{14}$$

In relation to the eigenvectors, it is necessary to generate two to obtain the general solution. The Eqs.(15, 16) show the eigenvectors $\vec{\xi_1}$ y $\vec{\xi_2}$.

$$\vec{\xi_1} = \begin{pmatrix} 9.163288 \\ -11.507650 \\ 1 \end{pmatrix} \tag{15}$$

$$\vec{\xi_2} = \begin{pmatrix} 0.359510 + 0.116796i \\ 0.478680 + 0.294040i \\ 1 + 0i \end{pmatrix} \tag{16}$$

Also, it is pointed out that the solution $\vec{\xi_2}e^{(4.445878+3.485904i)t}$ it has a real part and a complex part. The real part is $\vec{u}$ and the complex $\vec{v}$; furthermore, if $\vec{w} = \vec{\xi_1}e^{-22.558424t}$ is denoted, then, the general solution is written in the Eq.(17).

$$X\vec{(t)} = C_1\vec{w}(t) + C_2\vec{u}(t) + C_3\vec{v}(t) \tag{17}$$

Taking the first coordinate of the vectors in Eq.(17) the function $\varphi_x(t)$ is getting. In this research the values of $C_1 = 0$ y $t_0 = 1/(4.445878)$ are taken; the result is expressed in Eq.(18).

$$\varphi_x(t_0) = (0.172089)C_2e + (0.336590)C_3e \tag{18}$$

2.2 Elliptic Curve

IECC is a symmetric cryptosystem based on two points of the elliptic curve and chaos. In this vein, a brief description of the elements used in the development of an elliptic curve is made below. The equation of an elliptical curve is presented in Eq.(19):

$$y^2 \equiv x^3 + ax + b \mod p \tag{19}$$

However, in this developed a curve with: $b = 0$ y $a = -k$ is applied. The above is expressed in the Eq.(20).

$$y^2 \equiv x^3 - kx \mod p \tag{20}$$

The conditions that the curve must meet to avoid known cryptanalysis like attack MOV [26], or construct trace one curves, which are considered weak, are shown in the Eqs.(21,22).

$$\#E(F_q) \not\equiv 1 \mod p \tag{21}$$

$$\#E(F_q) \neq p \tag{22}$$

Where $\#E(F_q)$ is the prime number of solutions of the curve. To guarantee that the curve has three different real roots it is necessary that it be non-singular, the above is expressed in the Eq.(23).

$$4((-k)^3) \not\equiv 0 \mod p \tag{23}$$

The sum operation $(+)$ is defined on the set of solution points of the curve, so that this set $(E, +)$ is an Abelian group [27]. Theorem 1 is applied to calculate the number of solutions:

Theorem 1 *Let p be an odd prime number, $k \not\equiv 0 \mod p$, and $\#E(F_p)$ the number of solutions for the elliptic curve defined by Eq.(20). Additionally, $p \equiv 1 \mod 4$, where p can be written as in Eq.(24),*

$$p = a^2 + b^2 \tag{24}$$

such that a, b are positive integers, b is an even number, and $a + b \equiv 1 \mod 4$. The number of solutions is given by Eq.(25) when k is not a fourth power mod p of some element in the field F_p, but a square power mod p.

$$\#E(F_p) = p + 1 + 2a \tag{25}$$

Additionally, the number of solutions $\#E(F_p)$ must has a prime factor as large enough such that the discrete logarithm attack cannot be carried out, at least with the currently available technology [7]. On the other hand, k must meet the condition of being not a fourth power mod p of some element of F_p. In this sense, such condition is the following: $k^{(p-1)/4} \mod p \not\equiv 1$. The Euler criterion is used for finding out if k is a square power mod p of some element in the F_p field [29]. To obtain the prime number of solutions, if it exists, it is calculated according to Eq.(26). In fact, the number of solutions is always divisible by 4 [10].

$$q = (p + 1 + 2a)/4 \tag{26}$$

Furthermore, the Theorem 2 gives information to construct a cyclic subgroup in the solution set.

Theorem 2 *Let E be an elliptical curve defined on Z_p, where p is a prime number ¿ 3. Then, there are two positive integers n_1, n_2 such that there is an isomorphism from $(E, +)$ to $Z_{n_1} \times Z_{n_2}$. Also, $n_2 \mid n_1$ and $n_2 \mid (p - 1)$.*

For this case, $n_2 = 1$ and $n_1 = q$, which is a prime factor of $\#E(F_p)$, and q is defined in Eq.(26). Sometimes, q is not prime. But if this the case, it is necessary to look for other prime number p that meets the conditions of Theorem 1, such that number q be prime. To find the first solution and the

elliptic curve equation, it is applied Eq.(27); where only is necessary to know a initial point (x, y).

$$k \equiv \left(x^3 - y^2\right)\left(x^{-1}\right) \mod p \tag{27}$$

There are researches where the elliptic curve and the generator element, α, are calculated according the concepts mentioned above[16]. To reduce times in the calculation of the multiplicative inverse modulo p in the sum of points, the following theorem is proposed to obtain it.

Theorem 3 *Given a prime number p, and an element* $x \epsilon Z_p$ *such that* $x \neq 0$*, then the multiplicative inverse of* $x \mod p$ *is obtained as* $x^{-1} = x^{p-2} \mod p$

Proof Since p is a prime number, and $x \neq 0$, ϵZ_p, it follows that gcd(x, p) = 1. Hence, the inverse of x exists and is unique [23]. □

So, $x \times x^{p-2} \mod p = x^{p-1}p$. However, $x^{p-1} \mod p \equiv 1$according to Lagrange and considering that Euler's ϕ satisfies $\phi(p) = p^-1$[29] . Therefore, $x^{p-2}$is the multiplicative inverse of x.

Below is an example: Given $a = 4139$ and $b = 314$, it follows that p is 17229917. It can be verified that $p \bmod 4 \equiv 1$, and $a + b \equiv 1 \bmod 4$. A solution point $\alpha = (11199810, 4614456)$ is selected, and k is calculated according to Eq.(27) resulting in $k = 4167325$. Then, k is verified using Eqs.(28) and (29).

$$(4167325)^{17229917-1/4} \mod 17229917 \not\equiv 1 \tag{28}$$

$$(4167325)^{17229917-1/2} \mod 38873 \equiv 1 \tag{29}$$

The resulting curve is described in Eq.(30):

$$y^2 \equiv x^3 - 4167325x \mod 17229917 \tag{30}$$

Thus, according to Theorem 1 the number of solutions is $\#E(F_{17229917}) = 17238196$, and the prime $q = 17238196/4 = 4309549$. Additionally, 4309549 mod 17229917 $\not\equiv$ 1, $4\,(-4167325)^3 \mod 17229917 \not\equiv 0$ and $\#E(F_{4309549}) \neq 17229917$. From these conditions, it is concluded that the curve is non-singular, non-supersingular and not even trace one.

The next step is to verify if $\alpha = (11199810,4614456)$ is a primitive element, so $(q-1)\alpha = (11199810, -4614456)$ must be met [23]. The following values are calculated: $2\alpha = (4995846, 1046698)$; $4\alpha = (12063429, 15977680)$;$\cdots$ $4194304\alpha = (2413044, 15455227)$. The remaining points are: $4259840\alpha = (15791514, 845101)$; $4292608\alpha = (16173401, 14902172)$; $\cdots$ $4309548\alpha = (11199810, 12615461)$. Note that $12615461 \equiv -4614456 \bmod 17229917$, it follows that $4309548\alpha + \alpha = \infty$.

2.3 Entropy

Entropy is a parameter that measures the quality of encrypted images, that is, the distribution of color levels must be random. The entropy is calculated according to Eq.(31) [30]:

$$H(x) = -\sum_{x \varepsilon X} P(x) log_2 P(x) \tag{31}$$

Images can have 256 gray levels, defined in a Byte. Instead, if the image is in color, three Bytes are used for the colors red, green, and blue. In this sense, an image is well encoded if the histogram of the different levels of each color resembles a uniform distribution. In this order of ideas, if the distribution of color levels is exactly a uniform distribution, then the entropy is 8. It is clarified that, if a histogram has entropy 8, the color distribution is not necessarily random, because it is possible for construct a theoretical distribution with entropy 8, which is not random. However, the randomness of the color distribution is measured according to various instruments to ensure that this property is met. In practice, an entropy close to 8 is considered to have a good degree of randomness [31].

2.4 Correlation Coefficient

Correlation coefficient or simply correlation is other parameter to measure the quality of encrypted images. This analysis is carried out as follows: n pixels are randomly chosen from the encrypted image, and the correlation is calculated taking the adjacent pixels of each one of them. That is, in the horizontal vertical and diagonal directions. Measurement of this parameter is carried out in a large part of the image encryption work [32] - [33].

In the event that this analysis is performed in the horizontal direction and for the color red: a red point of the encrypted image is chosen at random way, denoted as z_r. Subsequently, the red point adjacent to it in the horizontal direction is chosen, and in the same way as before, this point has three basic colors, including red denoted as w_r. Then, it is possible to calculate the correlation between the variables z_r y w_r, when they have n point pairs. For the other directions and colors the calculation is similar. The formula to calculate the correlation in the horizontal direction and the color red is presented in Eq.(32), and the expressions $\overline{z}_r$, $\overline{w}_r$ are shown in the Eqs.(33) and (34).

$$r_{h;\, z_r, w_r} = \frac{\frac{1}{n}(\sum_{i=1}^{n}(z_{i,r} - \overline{z}_r)(w_{i,r} - \overline{w}_r))}{\sqrt{(\frac{1}{n}\sum_{i=1}^{n}(z_{i,r} - \overline{z}_r)^2(\frac{1}{n}\sum_{i=1}^{n}(w_{i,r} - \overline{w}_r)^2))}} \tag{32}$$

$$\overline{z}_r = \frac{1}{n}\sum_{i=1}^{n} z_{i,r} \tag{33}$$

$$\overline{w}_r = \frac{1}{n}\sum_{i=1}^{n} w_{i,r} \tag{34}$$

2.5 Discrete Fourier Transform

The Discrete Fourier Transform (DFT) is a test included in the NIST standard 800-22, for measuring the randomness degree of a binary chain, that is, there are no repetitive zeros-and-ones patterns, one after another [34]. The parameters involved in the calculation are: N_0, an expected theoretical quantity given by $(0.95) \times n/2$, where n is the string length; and N_1, the number of values lower than the threshold h, calculated from Eq.(35),

$$h = \sqrt{\mathrm{Ln}\frac{1}{0.05}(n)} \tag{35}$$

Then, f_j is obtained using Eq.(36), with $i = \sqrt{-1}$, $j = 1, 2 \ldots \frac{n}{2} - 1$ and x_k = -1, 1; in fact, $x_k = 2\delta_k - 1$ where δ_k is k-th bit of the string,

$$f_j = \sum_{k=1}^{n} x_k e^{\frac{2\pi(i)(k-1)j}{n}} \tag{36}$$

If n is odd, the last string bit is deleted, however, in this case n is always even; on the other hand, f_j is a complex number. The module $\|f_j\|$ is calculated and compared to h. If $\|f_j\| < h$, then 1 is added to N_1. Otherwise, N_1 remains the same. Eq.(37) is evaluated to obtain d and then calculate Eq.(38), where erfc is determined by Eq.(39). The decision rule is: if $P - value$ ¡ 0.01 then the hypothesis that the string is random is rejected, and it is otherwise accepted .

$$d = \frac{N_1 - N_0}{\sqrt{\frac{n(0.95)(0.05)}{4}}} \tag{37}$$

$$P - value = \mathrm{erfc}\frac{|\ d\ |}{\sqrt{2}} \tag{38}$$

$$\mathrm{erfc}\frac{|\ d\ |}{\sqrt{2}} = 2(1 - \Phi(|\ d\ |)) \tag{39}$$

2.6 Parameters to measure the strength of IECC against the differential attack

The parameters Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Avalanche Criteria (AC) are used to evaluate the strength of the proposed system against the differential attack.

NPCR is defined in Eq.(40), where the subscript c indicates the color, and the function $D(i, j)_c$ takes a value 1 when the bytes in position (i, j) of the encrypted images 1 and 2 are different; otherwise, it is 0. It is pointed out that image 1 and image 2 are differences by only one Byte. On the other hand, variables W and H are the width and height of the image, respectively. An appropriate percentage of this parameter to avoid the differential attack is in

the range close to 99.6% [35] [36].

$$\mathrm{NPCR}_c = \frac{\Sigma_{i,j} D(i,j)_c}{W \times H} \times 100\% \tag{40}$$

Regarding the UACI, it is defined in Eq.(41). The byte $C_{1,c}(i,j)$ is defined as follows: it has a position (i,j) and the color c in the first image. Similarly, the byte $C_{2,c}(i,j)$ has a position (i,j) and a color c in the second image.

$$\mathrm{UACI}_c = \frac{1}{W \times H}[\Sigma_{i,j} \frac{\mid C_{1,c} - C_{2,c} \mid}{255}] \times 100\% \tag{41}$$

A good percentage of UACI to endure the differential attack is close to 33.4% [37]. The calculation of AC for a particular color is carried out according to Eq.(42), where T is the total number of bits in the encrypted image, and the function $b(i,j)_c$ is defined by Eq.(43).

$$\mathrm{AC}_c = \frac{\Sigma_{i,j} b(i,j)_c}{T} \times 100\% \tag{42}$$

$$b(i,j)_c = \begin{cases} 0 \\ 1 \end{cases} \tag{43}$$

That is, if a bit in image 1 for color c is equal to the corresponding bit in image 2 for the same color, then $b(i,j)_c = 0$. Otherwise, $b(i,j)_c = 1$. An appropriated value of AC to prevent the differential attack is close to 50% [38].

2.7 Parameters of energy, contrast and homogeneity

Other important parameters to measure the quality of an encryption result are energy, contrast and homogeneity.

The measurement of energy reveals the degree of order or disorder that the information in an image has, that is, when the energy in an encrypted image is close to zero, it means that the degree of clutter is high, which shows that the encrypted image is of high quality. The energy is calculated according to the Eq.(44), where i,j is pixel position and $g(i,j)$ is the value at that point.

$$E = \sum_{i,j} g(i,j)^2 \tag{44}$$

In relation to contrast, it measures the differences in intensity between a pixel and neighboring pixels. Contrast is defined in the Eq.(45).

$$Contrast = \sum_{i,j} \mid i - j \mid^2 g(i,j) \tag{45}$$

Where, $g(i,j)$ is the pixel value at position (i,j). On other hand, an image is said to be well encrypted if the contrast values are high, which is, the higher the contrast values the proposed encryption algorithm shows greater security.

Regarding homogeneity, the lower the homogeneity values, the higher the encryption quality. This is calculated according to the equation (46).

$$H = \sum_{i,j} \frac{g(i,j)}{1+ \mid i-j \mid} \tag{46}$$

2.8 Goodness-of-Fit test

This tool aims to find out if the distributions of the primary colors fit to a uniform distribution [39]. If so, the distribution of the colors is said to be random. However, the above approach leads to a statistical hypothesis test. This test requires two ingredients, namely: a test statistic and a rejection region. In this work, the statistic χ^2 is utilized for each primary color. The χ^2 variable distribution is the Chi-square with k-1 freedom degrees, and is expressed in Eq.(47), where o_i and exp are the observed and expected values, respectively.

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - \exp)^2}{\exp} \tag{47}$$

According to the Central Limit Theorem, the statistic χ^2 approaches to the normal distribution with mean $\mu = 255$ and standard deviation σ, is shown in Eq.(48) [40]. Taking this into account, the threshold can be calculated using the right side of the normal distribution with a significance level of $\alpha = 0.01$, which is approximately 308. Thus, the decision rule is: if $\chi^2 > 308$ the hypothesis that the string is random is rejected, and it is otherwise accepted.

$$\sigma = (2 \times 255)^{0.5} = 22.58 \tag{48}$$

This type of test does not appear in the NIST 800-22 test set to find out the randomness degree of the bit string. That is, the randomness of the tone distribution for the basic colors in the encrypted image is not measured in that standard.

3 Building Elements

3.1 Algorithm for the generation of permutations

Given the set $Z_m = \{n \in N \mid 0 \leq n \leq m! - 1\}$ any element of Z_m can be expressed on a factorial basis as follows:

$$n = D_0(m-1)! + D_1(m-2)! + \ldots D_{m-2}(1)! + D_{m-1}(0)! \tag{49}$$

In fact, according to the Euclidean division algorithm, the constants D_i in the eq.(49) are unique [41], besides that the constant $D_{m-1} = 0$. Also, the constants comply with the property shown in Eq.(50).

$$0 \leq D_i < (m-i) \text{ with } 0 \leq i \leq (m-2) \tag{50}$$

With this information, it is possible to develop an algorithm that generates a permutation in an array of m diverse elements, using the constants D_i of the Eq.(49) [42]. Also, it is shown that this algorithm defines a one-to-one function [43], which is an important property because it means that two different integers $n_1 \neq n_2$ in turn generate two different permutations.

3.2 Similarity Parameter

In this research encrypted images are damaged using four types of noise: additive, multiplicative, Gaussian, and occlusion. For this reason, it is proposed to quantify the difference between the image deciphered with damage and the original image. Specifically, the authors propose using the parameter UACI as shown in the Eq.(51). It is pointed out that the constant 2.994 appears because it is desired that the range of SP_c are between 0 and 100 approximately.

$$\mathrm{SP}_c = |100 - \mathrm{UACI}_c(2.994)| \tag{51}$$

3.3 Encryption procedure

IECC is a symmetric cryptosystem of 15 rounds [44]. In each round a different S-box of 8×8 size is applied[45]. In addition, in each encryption process the 15 S-boxes are generated, this means, they are dynamic. To exemplify a dynamically built box, the S-box in Table 1 was randomly selected. Table 2 displays the properties of the dynamically built S-box.

Table 1 Example of an S-box.

Element	Hex value															
0-15	71	ab	dc	05	a2	bb	65	a1	c4	ea	38	cb	8f	7b	ef	4f
16-31	a8	72	6b	4c	ba	ff	0b	b4	34	f9	11	f2	89	16	ca	3c
32-47	77	2d	94	f4	c9	b9	2a	df	ec	cd	57	88	21	7d	37	7c
48-63	10	8e	41	95	b8	0e	ad	f3	14	6d	e76	97	d4	b2	96	99
64-79	fa	90	7f6	82	e6	00	a7	e1	1f	d5	51	29	7e	75	87	a4
80-95	92	3e	de	07	2e	74	1c	e4	69	db	09	9b	a5	d0	3b	22
96-111	cf	1b	e5	70	3d	59	ce	2c	02	53	c2	91	86	2f	44	a0
112-127	ae	f7	48	4b	55	9f	3a	e0	eb	9c	62	5c	04	50	c5	15
128-143	1d	0d	af	85	f1	fb	4e	78	81	52	d7	32	80	93	b6	45
144-159	c7	5a	26	23	d1	fc	a3	b1	d8	8c	bd	20	b0	98	5f	39
160-175	73	6c	56	24	79	8b	27	40	c8	5b	9d	4a	cc	d3	68	2b
176-191	5e	60	13	35	fd	7a	1e	e8	47	d6	a6	c1	da	76	fe	0a
192-207	1a	b7	67	84	06	19	9e	36	b3	f6	31	be	63	42	6f	d2
208-223	ee	e9	c0	f8	aa	28	83	9a	43	66	c3	e3	d9	25	b5	4d
224-239	0f	e2	6a	61	17	54	f0	64	bc	46	12	0c	ac	bf	8a	c6
240-255	30	dd	58	5d	8d	a9	49	3f	18	33	01	03	f5	ed	6e	08

Similarly, a dynamic permutation is applied before starting the first round and its inverse in round 15, which is the size of the image; so, it alters the order of the pixels in the image. On other hand, the schedule keys involved are also

Table 2 Characteristics of the S-box.

Properties	Result
Balance	0
Nonlinearity	94
Corelation immunity	0
Absolute indicator	88
Sum of square indicator	265984
Correlation immunity	0
Algebraic degree	7
Algebraic immunity	4
Transparency order	7.793
Propagation characteristics	0
Number of fixed points	0
Number of opposite fixed points	2
Composite algebraic immunity	4
Robustness to differential cryptanalysis	0.961
Delta uniformity	10
SNR (DPA) (F)	9.137
Confusion coefficient variance	0.129405

the size of the image. Likewise, it is important to mention that every time an image is encrypted, even if it is the same at a different time, the encryption keys are changed; that is, the schedule keys, the boxes and the permutation are different in each encryption process. Below is a high-level description of the encryption algorithm:

1. Before starting the encryption procedure, the P permutation is applied to the original image. Subsequently, the x-or operation is used, which is performed with the permuted image and the first schedule key. Then, the resulting chain is divided into blocks of one byte and the substitution operation is performed with the first box; it is clarified that the substitution is carried out in the same way as in AES [46].
2. From round 2 to 14, the procedure is as follows: first, the x-or operation is applied between the output of the previous round, and the corresponding schedule key. Subsequently, the substitution is carried out with the S-box that corresponds to it.
3. In the last round, first, the x-or operation is carried out with the exit of round 14. Then, the substitution operation is applied with the last box. Subsequently, the output string of the substitution operation is permuted using P^{-1}, ending with an x-or between the permuted string and the schedule key 16. The result is the encrypted image.

Regarding the generation of the permutation and the boxes, the following section will be reviewed.

3.4 Generation of the schedule keys, S-boxes and permutation

First, the steps for generating the schedule keys are shown.

1. A positive integer is randomly chosen, K^1 such that $0 < K^1 < 2^{512}$.
2. The point $K^1\alpha$ is calculated, which is denoted as: (x_1, y_1). Where α is the generating element of the curve.
3. It is proposed that the constant C_2 de la Eq.(18) take the positive integer value of the following string: $x_1 \parallel y_1$.
4. With the information from step III, the product is carried out $(0.172082 \times e)C_2$.
5. From the result of the previous step, the necessary bits of the decimal point to the right are taken, in such a way that the length of the string is the size of the image. This string will be called k_1. In fact, this is proposed to be the first schedule key.
6. To get the value k_2 proceed as follows: a one-bit circular shift is made to the left of the key k_1, and the result is k_2. So, to calculate the key k_i, a one-bit circular shift is executed to the left of the key k_{i-1}, for $1 < i \leqq 16$.

To generate the permutation, taking into account that the image has m pixels. It is proposed to use the string that was obtained in the above algorithm. That is, the bits to the right of the decimal point of the multiplication result $(0.172082 \times e)C_2$, where $C_2 = x_1 \parallel y_1$. The process of generating permutations is as follows:

1. Three bytes are taken, and the integer value associated with this string is called a_0. It is proposed that $D_0 = a_0 \text{ mod. } m - 0$.
2. For the calculation of a_1 a shift to the right of one byte is carried out, that is, bytes 2, 3 and 4. Then, the value of a_1 is the integer associated with the string of bytes 2, 3 and 4. Hence, the calculation of $D_1 = a_1 \text{ mod. } m - 1$.
3. According to this procedure, the constant D_i is obtained as $D_i = a_i \text{ mod. } m - i$.

Once the constants are obtained, the permutation is calculated according to what is indicated in Subsection A.

Regarding the generation of the boxes, the procedure is as follows:

1. A positive integer is randomly chosen K^2, which meets the condition $0 < K^2 < 2^{512}$.
2. From the curve $K^2\alpha$, the point (x_2, y_2) is calculated. Taking into account that the point α is the generator element of the curve.
3. For the construction of the S-boxes, the constant C_3 of the Eq.(18) is obtained as the positive integer associated with the string $x_2 \parallel y_2$.
4. Multiplication is done by $0.336590C_3e$ and the bit string that is formed from the decimal point to the right is divided into 8-bit blocks. Now, with this information the constants D_i are calculated to construct a 256-elements permutation, using the algorithm mentioned in Subsection A.

To obtain the first constant D_0 proceed as follows: take the first byte of the bit string after the decimal point, and call the integer associated with this byte b_0. Then, the calculation of the constant D_0 is done as follows; $D_0 = b_0 \text{ mod. } 256 - 0$. To get the D_1 the second byte of the string is taken after the decimal point. This byte has an integer associated with it, let's denote it as b_1. With this information the constant D_1 is obtained as follows: $D_1 = b_1 \text{ mod. } 256 - 1$. Then, following this same process the constant D_i is calculated as: $D_i = b_i \text{ mod. } 256 - i$. With $0 \leq i \leq 254$.

5. Once the D_i have been calculated, the information mentioned in subsection A is used to obtain the corresponding box. It is noted that a S-box 8×8 is a permutation of 256 elements. Finally, it is mentioned that all the boxes are obtained by shifting bytes to the right of the decimal point, and applying the modular operation.

The authors consider it convenient to show which is the elliptical curve used in this research; clarifying, that the curve has the shape of the Eq.(20). The values a, b, p, q, k and $\#E(F_p)$ meet the conditions mentioned in Section 2.2. When the solutions number of the elliptic curve is a prime, all the solutions (x_1, x_2) are different and they appear in a pseudo-random way. In addition, the elliptic curve proposed has the following characteristics: the prime p is higher than 2^{512} and the prime in Eq.(52) is approximately the same size. An example is shown below, where the p size is approximately 2^{562}:

$$q = \frac{\#E(F_p)}{4} \tag{52}$$

p = 25657b0e6967bb48772ed69af6b33b1a5dce8b8457ad506886b92222e981ef0884256b5d7c5eda5e36fea7c0f46f583fc42da46089ca9f296825c20db4cbe1b02cea2f664a3dd

p value is constructed using the following values of a and b.

a = 187606ce029ebd22bb08a7676ebd9095598b9c90d89976c517fe0521e6abc53b7270fdb

b = 295e

Regarding the other elements they are shown below:

q = 9595ec39a59eed21dcbb5a6bdaccec69773a2e115eb541a21ae4888ba607bc221095ae39a1b1d98dd1e3b4dc16f89c74fd3b3c4e840f036a6c4d30f6c35895f611d2992cb0e5

k = 122adae68006bdeaff1bfa9b46216275351a0f5109674cb8f29e54eeec332689c725cd46219126cd8c6d9b8bfddfbb8737638b4a0b7f67612a93379530046335b4361ddf70275

The generator point is expressed as: $\alpha = (x_0, y_0)$; where x_0 and y_0 are written below:

x_0 = 3d3e14cf7080ee1ecfd0007bab7bafe88d8fd6bea0e8a432ebd90aac3ebe696ea7611517fbe2d463a8e19ee49d991331096c8d1789d85b6cb35f724f55ea43530193e0b248a7

y_0 = 9f5c4ed872dc026ddeb38916910152a46119799231349f13cccaed2377c0b88c2c863e8e457fa4d277c29c16fe1f3eb5d8be3ab7010177c9b21634c380e488d19eb8386b586c

It can be observed that (x_1, y_1) and (x_2, y_2) are the base for developing the symmetric cryptosystem. So, the sender uses the public key of the receiver "Q", to encrypt (x_1, y_1) and (x_2, y_2). Later the receiver using their private key "m", decrypt the sent points [23]. Also, using the elliptic curve and the value of the Has Sha-512 function it is possible that the sender signs the information, applying the Elliptic Curve Signature Algorithm - ECSA [47].

3.5 Images used for testing

The images used for testing IECC are presented in Fig. 1. These images are 512 × 512 pixels, and have been recurrently employed in previous works for their special characteristics [48]. The Barbara and Cameraman images are black-and-white pictures, and if a inadequate symmetric system is used for encrypting them there is a risk that the encrypted images could not pass the randomness tests proposed in this work. Two more images were employed for testing this algorithm: one completely black and another white, with all the bits in 0 or 1, respectively. Furthermore, the Lena image is widely known in the cipher world. The AES-CBC system is commonly used to encrypt images, however, this encryption mode does not give expected results when the encrypted image is corrupted by noise, as will be seen later. Also, the CBC mode is sequential [23].

Another issue that should be mentioned is that the encrypted images are made up of the three basic colors. In fact, the encrypted image of Barbara, of 256 levels of gray, is shown in the Fig. 3

4 Noise effect on the ciphered images

IECC can endure a certain damage degree produced by noise in a ciphered image. To test this capability, different noise sources were applied to the encrypted images to simulate their effect. Four types were considered: Gaussian, additive, multiplicative, and occlusion noise. A new measure denominated Similarity Parameter is implemented in this work, to evaluate this feature. Also, a median filter was applied to the damaged images to complement the testing.

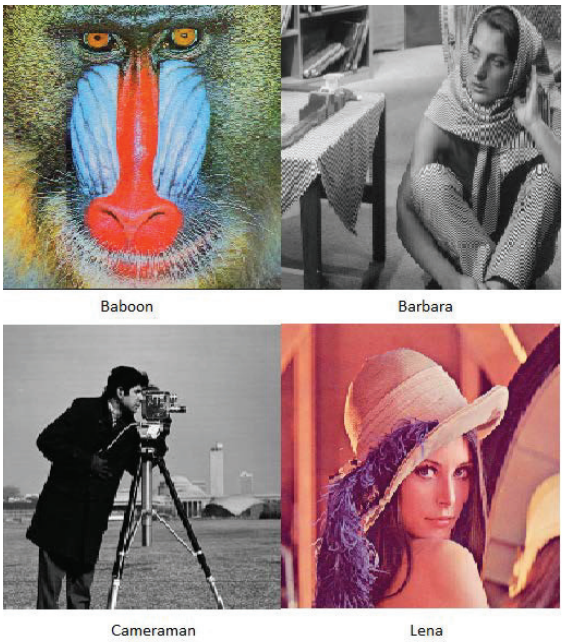

Fig. 1 Images used for testing IECC

4.1 Noise generated by a Gaussian random variable

Mathematical models of the Gaussian noise have been developed in two domains: spatial and frequency. In this work, the standard normal distribution is applied to assign values in the frequency domain, while a uniform distribution is used for choosing points in the spatial domain. The density function of the normal distribution is shown in Eq.(53), where μ is the mean and σ is the standard deviation. The normal distribution of the random variable x with parameters μ and σ is denoted as $x \sim N(\mu, \sigma)$.

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{53}$$

A random variable z has a standard normal distribution if $z \sim N(0, 1)$. Eq.(54) corresponds to the density function for this particular case:

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \tag{54}$$

4.1.1 Spatial domain

The points (x, y) are selected as follows: the points are listed as (0,0) $\leftrightarrow$ 0, $\cdots$, (0,511) $\leftrightarrow$ 511, (1,0) $\leftrightarrow$ 512, $\cdots$, (511,511) $\leftrightarrow$ 262143, since the encrypted images are 512 $\times$ 512 pixels size. Then, it is possible to define the set Y by

Eq.(55). With this information, a sample is randomly selected from Y, with a size up to 40% that of encrypted image.

$$Y = \{y | 0 \leq y \leq 262143\} \tag{55}$$

4.1.2 Frequency domain

For the frequency domain, a random variable w_c is defined in the discrete range 0, 1, 2, $\cdots$, 255, where the subscript c indicates the basic color. A value z is chosen with a number generator, taking into account that $z \sim N(0, 1)$. In addition, $z = -3$ and $z = 3$ are taken if the number generator assigns values lower than -3 or higher than 3, respectively. Then, $-3 \leq z \leq 3$, and the random variable $w_c^{'}$ is defined according to Eq.(56), considering that this type of noise replaces the original intensities of the image with central values; i.e., integers around 127.5.

$$w_c^{'} = 127.5 + z \times (42.5) \tag{56}$$

The symbols $\lfloor, \rfloor$ and $\lceil, \rceil$ are used to discretize $w_c^{'}$. The first pair, $\lfloor w_c^{'} \rfloor$, means that the integer part of the variable is taken, and is applied when the decimal fraction of $w_c^{'}$ is ≤ 0.5. The second case, $\lceil w_c^{'} \rceil$, means that the integer part of $w_c^{'}$ plus one is taken if the fraction is ¿ 0.5.

Summarizing, the process for simulating noise generated by a random Gaussian variable over an encrypted figure is as follows:

- The points (x_1, x_2) are selected from the map of the encrypted figure, and the number of points depends on the noise degree to simulate. Each point (x_1, x_2) is associated with a value $y \varepsilon Y$, where the latter is chosen randomly.
- Every point has an intensity level assigned for each basic color, denoted as w_c. The procedure is carried out separately for each basic color, within an intensity range from 0 to 255.
- The z-value is generated according to the standard normal distribution, and $w_c^{'}$ is computed using Eq.(56).
- The value w_c is replaced by the discrete value of $w_c^{'}$.

4.2 Additive and multiplicative noises

The points (x_1, x_2) were randomly chosen in the previous section, using the integers $y \varepsilon Y$. For generating these types of noise, a set of pairs is randomly chosen, each pair formed by a point (x_1, x_2) and an integer $\eta(x_1, x_2)$. In the frequency domain, the intensity levels w_c are converted to $w_c^{'}$. For additive noise, Eq.(57) is used for the conversion, while Eq.(58) is applied for multiplicative noise:

$$w_c^{'}(x, y) = [w_c(x_1, x_2) + \eta(x_1, x_2)] \mod 256 \tag{57}$$

$$w_c^{'}(x, y) = [w_c(x_1, x_2) \times \eta(x_1, x_2)] \mod 256 \tag{58}$$

4.3 Occlusion noise

For this type of noise, the points (x_1, x_2) are selected according to a concentric parallelogram over the encrypted image. Then, the intensity values of the points inside the parallelogram are replaced by a single color. A cherry color was selected for the simulation in this work. This process is equivalent to deleting the information in a specific central area of the encrypted image, as shown in Fig.2.

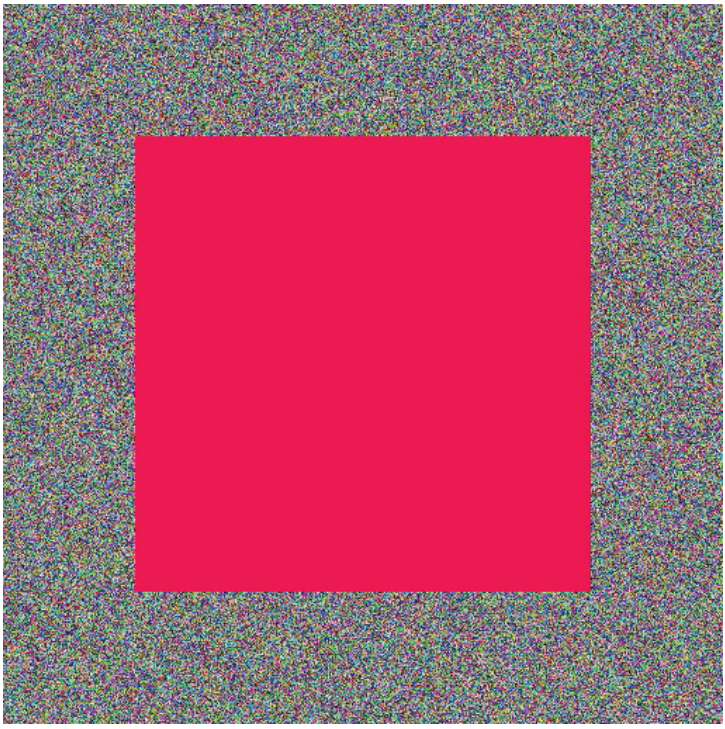

Fig. 2 Occlusion damage in an encrypted image

4.4 Median filter

There are different sizes of median filters. This research use a filter of 3×3. In general, we can say that a filter is a manipulation of $(n \times m)$ pixels in the image map; In this sense, the median filter proceeds as follows: for any pixel in the image (x_1, x_2) analysis is carried out on neighboring pixels. In case of a mask 3×3 adjacent pixels are shown in Table 3.

The levels of the basic colors for each of the neighbor points and the image pixel (x_1, x_2) are ordered. After the points are arranged, their median must be higher or equal than the first $\lceil \frac{n}{2} \rceil$ - 1 elements; (i.e 50%), and lower than the remaining cells. The median for each color is denoted as $M_{r,(x_1,x_2)}$, $M_{g,(x_1,x_2)}$ and $M_{b,(x_1,x_2)}$, respectively.

Table 3 3×3 mask for the median filter

$(x_1 - 1, x_2 - 1)$	$(x_1 - 1, x_2)$	$(x_1 - 1, x_2 + 1)$
$(x_1, x_2 - 1)$	(x_1, x_2)	$(x_1, x_2 + 1)$
$(x_1 + 1, x_2 - 1)$	$(x_1 + 1, x_2)$	$(x_1 + 1, x_2 + 1)$

4.5 Similarity parameter

Four types of noise were considered to test the encrypted images: Gaussian, additive, multiplicative, and occlusion. The test for IECC began with a damage percentage of 20% of the image size, then increased to 30% and 40%, all this carried out for each of the noise types. So, it is important to measure the sharpness-loss percentage for damages in an encrypted image, in respect to the original image. Furthermore, a question arises: what is the sharpness improvement of a damaged image when it passes through a filter? For answering it, a new measure named Similarity Parameter (SP) is proposed in this research. SP is calculated according to Eq.(59):

$$\mathrm{SP}_c = \mid 100\% - \mathrm{UACI}_c(2.994) \mid \tag{59}$$

In Eq.(59) the subscript c appears because the measurement is made for each basic color. Since the range of values for UACI is from 0% to around 33.4%, the factor 2.994 is included to let SP cover an approximate range from 0% to 100%. When both images are equal (that is, without encryption) then SP = 100%. However, if the resulting image is well encrypted UACI $\approx$ 33.4 and SP $\approx$ 0, indicating that there is no similarity between them. As can be seen, SP gives an accurate idea of the damage impact on the sharpness, as well as the improvement on the sharpness when a filter is applied.

5 Test procedure and results

The results of images ciphered without damage, and later the results of images with damage are shown. In this vein, the instruments for measuring the randomness are divided in two: those that present a deterministic result, such as: Entropy, Correlation, NPCR, UACI, AC, Homogeneity, Energy and contrast; and those that perform a hypothesis test: the Discrete Fourier Transform and the Goodness-of-Fit test proposed. As an example of the testing, Fig. (3) presents the Barbara original image, and its encrypted image using the proposed method.

5.1 Correlation, Entropy, NPCR, UACI, AC, Energy, Contrast and Homogeneity

Table 4 presents the results of correlation for the encrypted testing images. The entropy values are described in Table 5. The NPCR value appears in Table 6, for each basic color. Similarly, Table 7 and Table 8 shown the values of UACI

and AC, respectively. On other hand, the energy, contrast and homogeneity are presented in the Tables 9, 10 y 11.

Table 4 Correlation coefficient of the testing images after encryption

Color	Correlation	Baboon	Barbara	Cameraman	Lena
Red	*Horizontal*	−0.0075	0.0208	0.0071	−0.0022
	Vertical	0.0207	0.0088	0.0018	−0.0031
	Diagonal	0.0048	−0.0050	0.0028	−0.0127
Green	*Horizontal*	−0.0087	−0.0113	−0.0106	−0.0087
	Vertical	−0.0119	−0.0109	−0.0064	0.0087
	Diagonal	0.0118	−0.0119	−0.0027	−0.0106
Blue	*Horizontal*	−0.0029	−0.0096	0.0115	−0.0111
	Vertical	−0.0129	−0.0009	−0.0009	0.00002
	Diagonal	−0.0043	−0.0126	−0.0110	0.0194

Table 5 Entropy of test images after encryption

Color	Baboon	Barbara	Cameraman	Lena
Red	7.99921	7.99929	7.99932	7.99926
Green	7.99928	7.99931	7.99935	7.99934
Blue	7.99926	7.99928	7.99938	7.99935

Table 6 NPCR of the test images after encryption

Color	Baboon	Barbara	Cameraman	Lena
Red	99.623	99.598	99.609	99.632
Green	99.605	99.617	99.614	99.613
Blue	99.597	99.603	99.625	99.618

Table 7 UACI of the test images after encryption

Color	Baboon	Barbara	Cameraman	Lena
Red	33.581	33.482	33.438	33.522
Green	33.496	33.462	33.486	33.471
Blue	33.443	33.496	33.516	33.453

Table 8 AC of the test images after encryption

Color	Baboon	Barbara	Cameraman	Lena
Red	50.01	49.98	49.96	50.04
Green	50.01	49.97	50.01	49.97
Blue	49.94	49.96	50.00	49.99

Table 9 Energy of Fig.1 after encryption

Energy	Baboon	Barbara	Cameraman	Lena
Red	0.015627	0.015629	0.015629	0.015628
Green	0.015629	0.015628	0.015629	0.015629
Blue	0.015629	0.015629	0.015628	0.015628

Table 10 Contrast of Fig.1 after encryption

Contrast	Baboon	Barbara	Cameraman	Lena
Red	10.477	10.454	10.478	10.466
Green	10.538	10.480	10.491	10.504
Blue	10.523	10.509	10.502	10.504

Table 11 Homogeneity of Fig.1 after encryption

Homogeneity	Baboon	Barbara	Cameraman	Lena
Red	0.389580	0.389743	0.389507	0.390037
Green	0.389028	0.389829	0.390159	0.389272
Blue	0.389588	0.388325	0.389715	0.389343

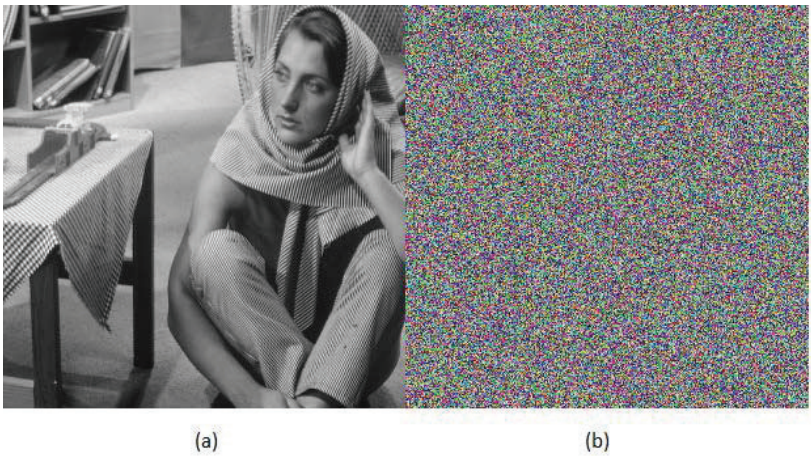

Fig. 3 Barbara image (a) original and (b) ciphered with IECC

5.2 Discrete Fourier Transform and The Proposal Test

Randomness results in the ciphered images measured with DFT are presented in Table 12.

Table 12 The randomness measurement using the DFT(✓ Accept, x Reject), with $\alpha = 0.01$

Color	Baboon	Barbara	Cameraman	Lena
Red	0.35/✓	0.92✓	0.27✓	0.87✓
Green	0.93✓	0.16✓	0.88✓	0.58✓
Blue	0.09✓	0.63✓	0.06✓	0.38✓

An additional test named *Goodness-of-Fit* using the χ^2 distribution was proposed for this measurement. Table 13 shows the results of this test for the four encrypted images.

Table 13 Goodness-of-Fit test results (✓ Accept, x Reject), with $\alpha = 0.01$

Color	Baboon	Barbara	Cameraman	Lena
Red	258/✓	230.3/✓	233.4/✓	258.4/✓
Green	255.7/✓	255.1/✓	230/✓	286.3/✓
Blue	227.1/✓	257.2/✓	259.9/✓	258.9/✓

5.3 Test images completely black or white

The following experiment was carried out in this section: two images were encrypted, one completely black and another completely white, and the resulting values of NPCR, UACI and AC parameters are reported in Table 14.

Table 14 NPCR, UACI and AC values for the completely black and completely white images

Parameter	Color	Black Image	White Image
NPCR	*Red*	99.59	99.59
	Green	99.61	99.61
	Blue	99.59	99.60
UACI	*Red*	33.52	33.44
	Green	33.43	33.49
	Blue	33.40	33.45
AC	*Red*	50.04	49.98
	Green	49.97	50.03
	Blue	49.95	49.98

5.4 Results of the encrypted images with damage

This section presents the results when noise was applied to the encrypted images to simulate damage. Results of images encrypted with AES-CBC mode and a percentage of noise are visualized. Two encryption cases ware analyzed, one with additive noise and another with occlusion. Fig. 4a presents the original Barbara image. Subsequently, this image is encrypted with AES-CBC mode with a 40% additive noise of the image size applied to the encrypted image. Then, it is deciphered and the result appears in Fig. 4b.

Fig. 5 illustrates the second case; i.e., the image is encrypted according with AES-CBC mode and occlusion noise of 40% of the image size is applied.

Fig. 6 shows the Lena's image encrypted and decrypted with 40% damage applying occlusion noise, using IECC. A 3×3 median filter was used to improve the sharpness in the encrypted images with damage. In this vein, Fig.7(a) presents the Baboon image decrypted with IECC, after additive

Fig. 4 Barbara image: (a) original and (b) deciphered when additive noise of 40% image size was applied to the AES-CBC ciphering

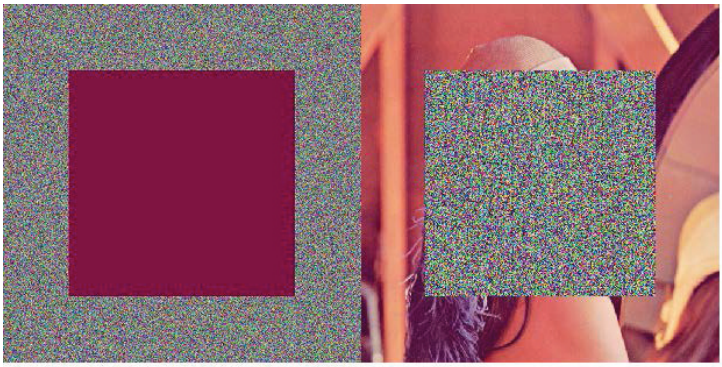

Fig. 5 Lena image: (a) ciphered using AES-CBC with 40% of occlusion damage and (b) deciphered

noise of 40% was inserted to the encrypted image. Subsequently, the filter was applied to the decrypted image with damage, and the result is shown in Fig.7(b).

To end this section, Table 15 presents the value of SP with different percentages of multiplicative noise damage, for the encrypted test images.

Table 16 shows the SP values after applying the filter, inserting a 40% damage for the four noise types. The results in both tables were generated with IECC.

6 Analysis and discussion of results

The section presents a security analysis of IECC. In this sense, the attacks are divided into three: those that apply to the elliptical curve, those that apply to

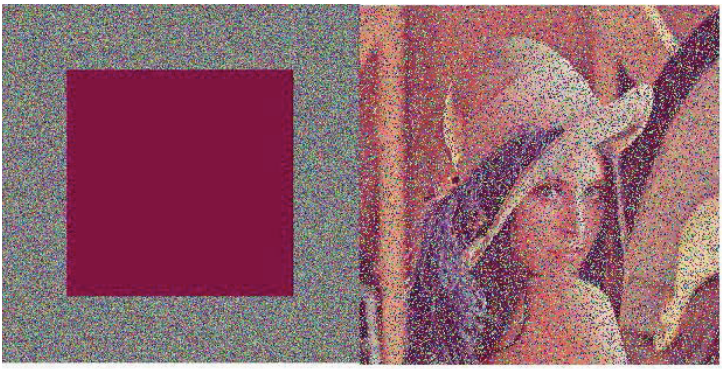

Fig. 6 Lena image (a) ciphered using IECC with 40% of occlusion damage and (b) deciphered

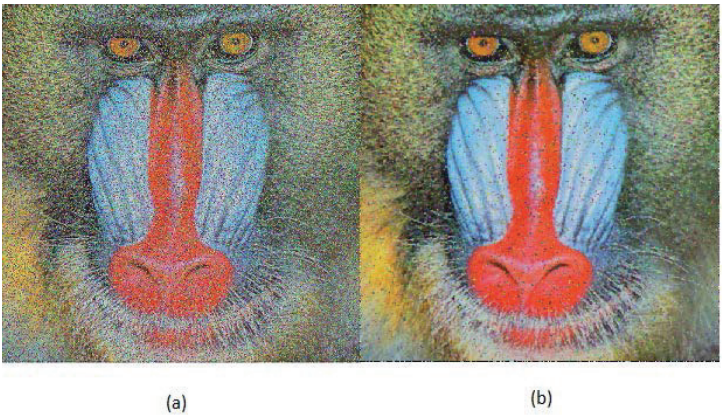

Fig. 7 Baboon image (a) deciphered with noise and (b) deciphered and filtered using median filter

Table 15 SP for different damage size of the testing images after encryption, using multiplicative noise

Color	% Noise	Baboon	Barbara	Cameraman	Lena
Red	20%	82.13	82.42	81.61	80.53
	30%	73.55	73.75	72.55	70.82
	40%	64.73	64.78	63.34	61.07
Green	20%	82.95	82.41	81.60	81.89
	30%	74.82	73.52	72.60	72.85
	40%	66.43	64.90	63.37	63.95
Blue	20%	81.31	82.33	81.55	83.73
	30%	72.51	73.66	72.58	75.53
	40%	63.43	64.97	63.25	67.46

the proposed symmetric cryptosystem, and those that damage the encrypted images with noise.

Table 16 SP when the 3 × 3 median filter was applied to encrypted images with 40% of damage from different noises

Color	Noise Type	Baboon	Barbara	Cameraman	Lena
Red	*Occlusion*	81.00	85.78	91.26	89.70
	Additive	81.00	85.74	91.17	89.59
	Multiplicative	81.19	85.93	91.46	90.15
	Gaussian	80.86	85.78	91.11	89.76
Green	*Occlusion*	80.48	85.87	91.20	89.83
	Additive	80.40	85.80	91.20	89.62
	Multiplicative	80.51	86.06	91.45	89.89
	Gaussian	80.36	85.84	91.04	89.50
Blue	*Occlusion*	79.11	85.83	91.24	91.16
	Additive	79.06	85.72	91.14	91.00
	Multiplicative	79.30	86.12	91.49	91.32
	Gaussian	79.01	85.78	91.12	91.09

1. The elliptic curve attack consists of knowing the private key when the public key is known, which leads to the discrete logarithm problem. Because the prime number of solutions, q, used in this research is greater than or equal to 2^{512}. It follows that solving the discrete logarithm problem in this scenario is equivalent to factoring a n of size 2^{15000}, of an RSA schema, which is much larger than the currently in use version of RSA [11]. Regarding a brute force attack, the following reflections are made: considering that $q \geqq 2^{512}$, then the number of IECC keys to be tested is greater or equal to $(2^{512})^2$, because two points are chosen at random. Therefore, performing a brute force attack is impossible, assuming that the AES-256 cryptosystem of 2^{256} keys resists a [49] brute force attack.
2. Three attacks on the symmetric IECC cryptosystem are considered, namely: linear, algebraic and differential attack. Regarding the linear attack, this cannot be carried out, because the boxes are unknown, and for this same reason the algebraic attack cannot be applied either. Regarding differential attack, it cannot be performed because the NPCR parameters ≈ 99.6 %, UACI ≈ 33.4 % and AC ≈ 50 %, according to the tables 6 and 7, which indicates that IECC is robust against this type of attack.
3. The third aspect, attacking the encrypted images by damaging them, that is, applying additive, multiplicative, Gaussian and occlusion noise. The encryption algorithm can be said to resist damage up to 40% image size, depending on the type of damage.

The proposed symmetric cryptosystem was constructed using the elliptic curve; which makes it possible to distribute the keys of the symmetric system, because only two points of the curve are required, and these can be sent using the same curve. The secure communication scheme only uses a single cryptosystem for image encryption, the elliptical curve, and not two as is the case of the PKI structure. [50].

Regarding the encryption quality of the images, it is carried out in two directions: the first one is carried out according to the results of the DFT, and the proposed goodness of fit test. The second is carried out by analyzing the results of the correlation, entropy, and the parameters NPCR, UACI, AC,

homogeneity, contrast and energy. As can be seen, in both directions the results show that the encryption of the images is robust. In fact, the homogeneity, energy and contrast results are similar to recent research. [51]. To finish this section, Table 17 compares the entropy results with other recent research.

Table 17 Entropy of test images after encryption

Algorithm	Lena	Cameraman	Baboon
IECC	7.9993	7.9993	7.9992
[1]	7.9971	7.9974	7.9972
[2]	7.9975	7.9968	7.9973
[3]	–	–	7.9968
[4]	–	7.9973	–
[5]	7.9960	–	–

7 Conclusion

In this research, a robust cryptosystem was developed to encrypt images, using two points of the elliptic curve. The number of solutions to the curve is $q = 2^{560}$ approximately, so the discrete logarithm attack cannot be carried out. In addition, it resists the following attacks: linear, differential, algebraic and brute force. Also, it is pointed out that the permutation applied in each encryption process is dynamic, so, IECC cryptosystem is safe. Regarding the encryption quality of the images, it was evaluated according to the following parameters: entropy, correlation, DFT, goodness of fit test, NPCR, UACI, AC, homogeneity, energy and contrast. In all cases the results were satisfactory. Finally, two more things are mentioned; the first is in relation to the comparison of results in images encrypted with noise, using the cryptosystem AES-CBC and IECC; where it is observed that IECC is superior to AES-CBC. Regarding the second, the future work intends to distribute the seed using post-quantum algorithms. Finally, in this work no major effort is made to build S-boxes with high nonlinearity, because they are dynamics.

Acknowledgments. The authors would like to thank the Instituto Politécnico Nacional of México (Secretaría Académica, Comisión de Operación y Fomento de Actividades Académicas COFAA, SIP, and CIDETEC), and the CONACyT (SNI) for their support to the development of this work.

Declarations

We confirm that We understand journal Cryptography and Communications is a transformative journal. When research is accepted for publication, there is a choice to publish using either immediate gold open access or the traditional publishing route. The authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper. The results/data/figures in this

manuscript have not been published elsewhere, nor are they under consideration (from you or one of your Contributing Authors) by another publisher. We have read the Springer journal policies on author responsibilities and submit this manuscript in accordance with those policies. The manuscript contains third party material and obtained permissions are available on request by the Publisher.

References

[1] Mahmud M., Lee M. Choi J., Evolutionary-Based image encryption using RNA codons truth table, Optics & Laser Technology, Vol. 121, Elsevier, (2020), pp: 105818.

[2] Abdelfatah, Roayat Ismail, Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography, IEEE Access, IEEE, (2019).

[3] Luo, Yuling and Ouyang, Xue and Liu, Junxiu and Cao, Lvchen, An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems, Vol. 7, IEEE Access, IEEE, (2019) pp: 38507–38522.

[4] Ibrahim, Saleh and Alharbi, Ayman,, Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography, IEEE Access, Vol. 8, IEEE, (2020), pp: 194289—194302.

[5] Benssalah, Mustapha and Rhaskali, Yesser and Drouiche, Karim, An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography, Multimedia Tools and Applications, Vol. 80, Springer, (2021) pp: 2081–2107.

[6] J.G.G. Loza, "NOM-151-SCFI-2002: Uso de la criptografía para la conservación de la información", Ph.D. dissertation, (2012).

[7] Hla, Ni Ni and Aung, Tun Myat, Attack Experiments on Elliptic Curves of Prime and Binary Fields, Emerging Technologies in Data Mining and Information Security, Springer, (2019), pp: 667–683.

[8] Zia, M and Ali, R. Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve, Electronics Letters, Vol. 55, IET, (2019), pp: 457–459.

[9] Hemanth Chakravarthy M. and Kannan E. Hybrid Elliptic Curve Cryptography Using Ant Colony Based Authentication System for Cloud Computing, Journal of Engineering and applied Science, Vol. 10, (2015), pp: 7273–7279.

[10] Silva-García, Víctor Manuel and Flores-Carapia, Rolando and González-Ramírez, Marlon David and Vega-Alvarado, Eduardo and Villarreal-Cervantes, Miguel Gabriel, Cryptosystem Based on the Elliptic Curve With a High Degree of Resistance to Damage on the Encrypted Images, IEEE Access, Vol. 8, IEEE, (2020), 218777–218792.

[11] Yarom Yuval, Genkin Daniel, Heninger Nadia. CacheBleed: a timing attack on OpenSSL constant-time RSA, Journal of Cryptographic Engineering, Vol. 7, Springer, (2017), pp: 99–112.

[12] . Gueron Shay, advanced encryption Standard (AES) new instructions set, Intel Corporation, (2010).

[13] Liu Z, Han S, Wang Q, Li W, Liu Y, Gu D. New insights on linear cryptanalysis. Sci China Inf Sci, Vol. 63, Springer, (2020).

[14] Pedersen Bruce B., Differential power analysis resistant encryption and decryption functions, Google Patents, (2019).

[15] Lavanya, R and Karpagam, M, Enhancing the security of AES through small scale confusion operations for data communication, Microprocessors and Microsystems, Vol. 75, Elsevier, (2020), pp: 103041.

[16] Silva-García, Víctor Manuel and Flores-Carapia, Rolando and Rentería-Márquez, Carlos and Luna-Benoso, Benjamín and Chimal-Eguía, Juan Carlos, Image cipher applications using the elliptical curve and chaos, International Journal of Applied Mathematics and Computer Science, Sciendo, (2020), pp: 377–391.

[17] . Wang X., Zhao H., Wang M., A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices, Optics & Laser Technology, Vol. 115, Elsevier, (2019), pp: 42–57.

[18] Hua Z., Zhou Y., Huang H., Cosine-transform-based Chaotic system for image encryption, Information Sciences, Vol. 480, Elsevier, (2019), pp: 403–419.

[19] Malik, Dania Saleem and Shah, Tariq, Color multiple image encryption scheme based on 3D-chaotic maps, Mathematics and Computers in Simulation,Vol. 178, Elsevier, (2020), pp: 646–666.

[20] Vilardi J.M., Millán M.S., Pérez-Cabré E., Occlusion and noise test on the encrypted image produced by a security system based on a joint transform correlator and Fresnel transform, Journal of Physics: Conference Series, Vol. 1221, IOP Publishing, (2019).

[21] Alawida M., Samsudin A., Teh J., Alkhawaldeh R., A new hybrid digital chaotic system with applications in image encryption, Signal Processing, Vol. 160, Elsevier, (2019), pp: 45–58.

[22] Idrees, Bazgha and Zafar, Sohail and Rashid, Tabasam and Gao, Wei, Image encryption algorithm using S-box and dynamic Henon bit level permutation, Multimedia Tools and Applications, Vol 79, Springer, (2020), pp: 6135–6162.

[23] Stinson D., Patterson M., "CRYPTOGRAPHY: Theory and practice", Fourth Edition, CRC Press, Taylor & Francis group. (2019), pp: 116–122.

[24] Li, Jiaosheng and Li, Yuhui and Li, Ju and Zhang, Qinnan and Li, Jun, Single-pixel compressive optical image hiding based on conditional generative adversarial network, Optics Express, Vol. 28, Optical Society of America, (2020), pp: 22992–23002.

[25] Moon, Sungju and Baik, Jong-Jin and Seo, Jaemyeong Mango, Chaos synchronization in generalized Lorenz systems and an application to image encryption,Communications in Nonlinear Science and Numerical Simulation, Vol. 96, Elsevier, (2021), pp: 105708.

[26] Hernández-Díaz, Erick and Pérez-Meana, Héctor and Silva-García, Víctor and Flores-Carapia, Rolando, Jpeg images encryption scheme using elliptic curves and a new s-box generated by chaos, Electronics, Vol. 10, Multidisciplinary Digital Publishing Institute, (2021), pp: 413.

[27] Lawrence C. Washington, "ELLIPTIC CURVES Number Theory and Cryptography", CHAPMAN & HALL/CRC, (2003).

[28] Hla N., Aung T., Attack Experiments on Elliptic Curves of Prime and Binary Fields, Emerging Technologies in Data Mining and Information Security, Springer, (2019), pp: 667–683.

[29] Gallian J., "Contemporary abstract algebra", seventh edition, Brooks/-Cole, (2011).

[30] Shannon C.E., "A mathematical theory of communication", Bell Syst. Tech. J., Vol.27, no. 3, (1948), pp: 379-423.

[31] Yu, Jiayin and Li, Chao and Song, Xiaomeng and Guo, Shiyu and Wang, Erfu, Parallel mixed image encryption and extraction algorithm based on compressed sensing, Entropy, Vol. 23, Multidisciplinary Digital Publishing Institute, (2021), pp. 278.

[32] Zeng, Jie and Wang, Chunhua, A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata, Security and Communication Networks, Vol. 2021, Hindawi, (2021), pp. 1-15.

[33] Shafique, Arslan and Ahmed, Jameel and Rehman, Mujeeb Ur and Hazzazi, Mohammad Mazyad, Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain, IEEE Access, Vol. 9, IEEE, (2021), pp. 59108–59130.

[34] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert,James Dray, San Vo. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST 800-22,

2010.

[35] Ravichandran, Dhivya and Murthy, BK and Balasubramanian, Vidhyadharini and Fathima, Sherin and Amirtharajan, Rengarajan, An efficient medical image encryption using hybrid DNA computing and chaos in transform domain, Medical & Biological Engineering & Computing, Vol. 59, Springer, (2021), pp. 589–605.

[36] Kamal, Sara T and Hosny, Khalid M and Elgindy, Taha M and Darwish, Mohamed M and Fouda, Mostafa M, A New Image Encryption Algorithm for Grey and Color Medical Images, IEEE Access, Vol. 9, IEEE, (2021), pp. 37855–37865.

[37] Zhang, Duzhong and Chen, Lexing and Li, Taiyong, Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation, Entropy, Vol. 23, Multidisciplinary Digital Publishing Institute, (2021), pp. 361.

[38] Altigani, Abdelrahman and Hasan, Shafaatunnur and Barry, Bazara and Naserelden, Shiraz and Elsadig, Muawia A and Elshoush, Huwaida T, A Polymorphic Advanced Encryption Standard–A Novel Approach, IEEE Access, Vol. 9, IEEE, (2021), pp. 20191–20207.

[39] El-Latif, Ahmed A Abd and Abd-El-Atty, Bassem and Belazi, Akram and Iliyasu, Abdullah M, Efficient Chaos-Based Substitution-Box and Its Application to Image Encryption, Electronics, Vol. 10, Multidisciplinary Digital Publishing Institute, (2021), pp. 1392.

[40] Zhang, Yong, Statistical test criteria for sensitivity indexes of image cryptosystems, Information Sciences, Vol. 550, Elsevier, (2021). pp. 313–328.

[41] Eder, Christian and Pfister, Gerhard and Popescu, Adrian, Standard bases over Euclidean domains, Journal of Symbolic Computation, Vol. 102, Elsevier, (2021), pp. 21–36.

[42] Silva-García V.M., González-Ramírez M.D., Flores-Carapia R., Vega-Alvarado E., Rodríguez-Escobar E., A Novel Method for Image Encryption Based on Chaos and Transcendental Numbers, Vol. 7, IEEE Access, IEEE, (2019), pp: 163729–163739.

[43] Aragona, Riccardo and Civino, Roberto, On Invariant Subspaces in the Lai–Massey Scheme and a Primitivity Reduction, Mediterranean Journal of Mathematics, Vol. 102, Elsevier, (2021), pp. 1–14.

[44] Asharov, Gilad and Segev, Gil and Shahaf, Ido, Tight tradeoffs in searchable symmetric encryption, Journal of Cryptology, Vol. 34, Springer, (2021), pp. 1–37.

[45] Khan, Naqash Azeem and Altaf, Muhammad and Khan, Farman Ali, Selective encryption of JPEG images with chaotic based novel S-box, Multimedia Tools and Applications, Vol. 80, Springer, (2021), pp. 9639–9656.

[46] Lin, Chih-Hsueh and Hu, Guo-Hsin and Chan, Che-Yu and Yan, Jun-Juh, Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm, Applied Sciences, Vol. 11, Multidisciplinary Digital Publishing Institute, (2021), pp. 1329.

[47] Zhang, Mingyue and Zhou, Junlong and Zhang, Gongxuan and Zou, Minhui and Chen, Mingsong, EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles, Journal of Systems Architecture, Vol. 117, Elsevier, (2021), pp: 102161.

[48] Shakiba, Ali, A novel 2D cascade modulation couple hyperchaotic mapping for randomized image encryption, Multimedia Tools and Applications, Vol. 80, Springer, (2021), pp. 17983–18006.

[49] Bhat, Krishnaraj and Mahto, Dindayal and Yadav, Dilip Kumar and Azad, Chandrashekhar, Image Security Using Hyperchaos and Multidimensional Playfair Cipher, Security and Privacy: Select Proceedings of ICSP 2020, Vol. 744, Springer, (2021), pp. 93.

[50] Liu, Yanan and Cui, Yijun and Harn, Lein and Zhang, Zheng and Yan, Hao and Cheng, Yuan and Qiu, Shuo, PUF-Based Mutual-Authenticated Key Distribution for Dynamic Sensor Networks, Security and Communication Networks, Vol. 2021, Hindawi, pp. 1–13.

[51] Masood, Fawad and Boulila, Wadii and Ahmad, Jawad and Sankar, Syam and Rubaiee, Saeed and Buchanan, William J, A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos, Remote Sensing, Vol. 12, 2020, Multidisciplinary Digital Publishing Institute, pp. 1893.