Int. J. Appl. Math. Comput. Sci., 2020, Vol. 30, No. 2, 377–391
DOI: 10.34768/amcs-2020-0029

IMAGE CIPHER APPLICATIONS USING THE ELLIPTICAL CURVE AND CHAOS

VÍCTOR MANUEL SILVA-GARCÍA [a,*], ROLANDO FLORES-CARAPIA [a],
CARLOS RENTERÍA-MÁRQUEZ [b], BEJAMÍN LUNA-BENOSO [c],
JUAN CARLOS CHIMAL-EGUÍA [d]

[a]Center for Innovation and Technological Development
National Polytechnic Institute (IPN)
Av. Juan de Dios Bátiz S/N, Nueva Industrial Vallejo, 07738 Gustavo A. Madero, Ciudad de México, Mexico
e-mail: {vsilvag,rfloresca}@ipn.mx

[b]Higher School of Physics and Mathematics
National Polytechnic Institute (IPN)
Building 9, Av Instituto Politécnico Nacional, San Pedro Zacatenco, Nueva Industrial Vallejo
07738 Gustavo A. Madero, Ciudad de México, Mexico
e-mail: renteri@esfm.ipn.mx

[c]Higher School of Computing
National Polytechnic Institute (IPN)
Av. Juan de Dios Bátiz S/N, Nueva Industrial Vallejo, 07738 Ciudad de México, Mexico
e-mail: blunab@ipn.mx

[d]Computation Research Center
National Polytechnic Institute (IPN)
Av. Juan de Dios Bátiz Esq. Miguel Othón de Mendizábal S/N, Nueva Industrial Vallejo
07738 Gustavo A. Madero, Ciudad de México, Mexico
e-mail: jchimale@gmail.com

A novel symmetric cryptosystem of the substitution permutation network type is presented for image encryption in 14 rounds. An algorithm is developed to generate 15 keys to encrypt images where each key is the image size. These keys are calculated using an elliptic curve with a constant zero value. The proposed curve is non-singular, non-supersingular, nor trace one. Chaos is employed to find a generating element in a cyclic subgroup and it is produced using the logistic map equation. In addition, a 16×16 substitution box is constructed using both chaos and an algorithm that defines a bijective function. The following tools are used in order to measure the degree of randomness of the encrypted figures: entropy, correlation, the discrete Fourier transform and a goodness-of-fit test with the chi-square distribution. Furthermore, an image size variable permutation is applied in the first round, and its inverse in the fourteenth.

Keywords: elliptic curve, chaos, entropy, discrete Fourier transform, image ciphering.

1. Introduction

Images with important information must be encrypted with robust methods to prevent attacks. Hence, numerous methods of image encryption have been developed (Kumar *et al*., 2016; Li *et al*., 2012; Sam *et al*., 2012).

Six aspects should be considered in the image encryption process. The first one is system complexity. In this investigation a symmetric cryptosystem is constructed from an elliptical curve in such a way that an attack on this cryptosystem implies an attack on the elliptical curve. Thus, attacks on the proposed cryptosystem can be compared with those on an asymmetric cryptosystem, for

*Corresponding author

example, the Rivest, Shamir and Adleman cryptosystem (RSA). In this manner, the attack on the elliptical curve consists in finding the private key when the public key is known, which is called the discrete logarithm problem. In this research, a solution set consisting of more than 2^{200} elements is proposed. However, the number of elements can go up to 2^{512}, as shown in the flowchart of Fig. 1. This is equivalent to factoring a positive integer of $2^{15,000}$ in the RSA cryptosystem (Hemanth Chakravarthy and Kannan, 2015). As can be seen, this is a much higher value than what is currently known (Yarom *et al*., 2017; Thangavel *et al*., 2015).

A second aspect refers to the fact that there are investigations that do not perform randomness tests on encrypted images with instruments such as entropy and correlation (Chen *et al*., 2012), while in this investigation randomness evaluations are carried out using these tools. Besides, we propose a goodness-of-fit test that is not included in the National Institute of Standard and Technology 800-22 (NIST 800-22) standard.

The third point about the encryption process is the importance of substitution boxes, because they impart nonlinearity to the encryption procedure. Nevertheless, investigations have been carried out that do not apply substitution boxes (Chen and Chen, 2014).

The fourth point refers to results, and entropy in particular. This work reports results improving the entropy reported in other works (Huang and Ye, 2014; Zhu *et al*., 2013). A fifth issue to consider is the following: investigations have been conducted without applying the randomness measurements included in the NIST 800-22 standard to the encrypted image (Ye, 2010); however, in this work, the discrete Fourier transform is applied (Lang *et al*., 2010).

The sixth aspect refers to data loss in information encryption (Zhang, 2011). In this investigation, information encryption without loss is proposed, because there are countries, like Mexico, whose regulations do not permit lossy encryption (Nom-151, 2002).

An algorithm that defines a bijective function (Michael, 2006) is used to obtain boxes of 16×16 elements; i.e., a permutation over a "256–number" array is built. To generate this permutation, 256 constants are required. These constants are obtained using chaos, and the detailed procedure is described below.

The box used in this study has a high nonlinearity of 84.4%. Considering that the linear and differential attacks on the Data Encryption Standard (DES) cryptosystem were possible because it has a box with a very low nonlinearity, 43.7% (Silva García, 2007), then, with an 84.4% nonlinearity, those attacks cannot be carried out, at least in the way they were performed (Matsui, 1993; Biham and Shamir, 1992). On the other hand, the Triple Data Encryption Algorithm (Triple DEA) cryptosystem is still used (Barker *et al*., 2012).

In this research, four well-known images from the related literature are employed (Chen and Chen, 2013; Chen *et al*., 2014).

This article is structured as follows. The first part contains a review of the state of the art. Section 2 describes the tools used in the image encryption. Section 3 shows how the high-nonlinearity box is generated. In Section 4, the cipher algorithm is presented, and in Section 5, the images that will be encrypted are shown. In Section 6, the randomness results are presented. Section 7 focuses on the analysis and discussion of results, while Section 8 presents some conclusions.

2. Theoretical tools for image encryption

2.1. Elliptical curve. The elliptic curve used in this research is $y^2 \equiv x^3 - kx \mod p$. In addition, the following conditions must be fulfilled: $4((-k)^3) \not\equiv 0 \mod p$, $\#E(F_p) \not\equiv 1 \mod p$ and $\#E(F_p) \neq p$, where $\#E(F_p)$ is the number of solutions. The first condition assures that the curve is nonsingular (Washington, 2008); the second condition indicates that the curve is non-supersingular to avoid the Menezes, Okamoto and Vanstone attack (or the MOV attack) (Luca *et al*., 2004). The third condition assures that the curve is not of trace one (Luis and Encinas, 2004).

Two requirements will be shown below—the first demonstrates that $4 \mid \#E(F_p)$, and the second shows that k must satisfy the following condition: it must not be the fourth power $\mod p$ of some F_p field element. Chaos is used to propose solutions (x, y) from the curve with the intention of finding a generator element. It is required that the number of solutions $\#E(F_p)$ has a prime factor, say q, such that the discrete logarithm problem is infeasible to solve (Stinson, 2005).

A cyclic subgroup is constructed of size q in the solution set of the elliptic curve; also, a generating or primitive element α is sought such that $(q)\alpha = \infty$. (In other words, the null element (Stinson, 2005)). Besides, in the solution set, an addition operation + is defined that makes the solution set (E, +) an Abelian group (Gallian, 2012). The following theorem is applied to calculate the number of solutions.

Theorem 1. *Let p be an odd prime number and also $k \not\equiv 0 \mod p$. Furthermore, let $\#E(F_p)$ be the number of solutions for the curve from the equation*

$$y^2 \equiv x^3 - kx \mod p. \tag{1}$$

Moreover, $p \equiv 1 \mod 4$, and p can be written as $p = a^2 + b^2$, where a, b are positive integers, and b is an even number; likewise, $a + b \equiv 1 \mod 4$. Then, the number of solutions is $\#E(F_p) = p + 1 + 2a$, if k is not the fourth power module p of some element in the F_p field, and it is

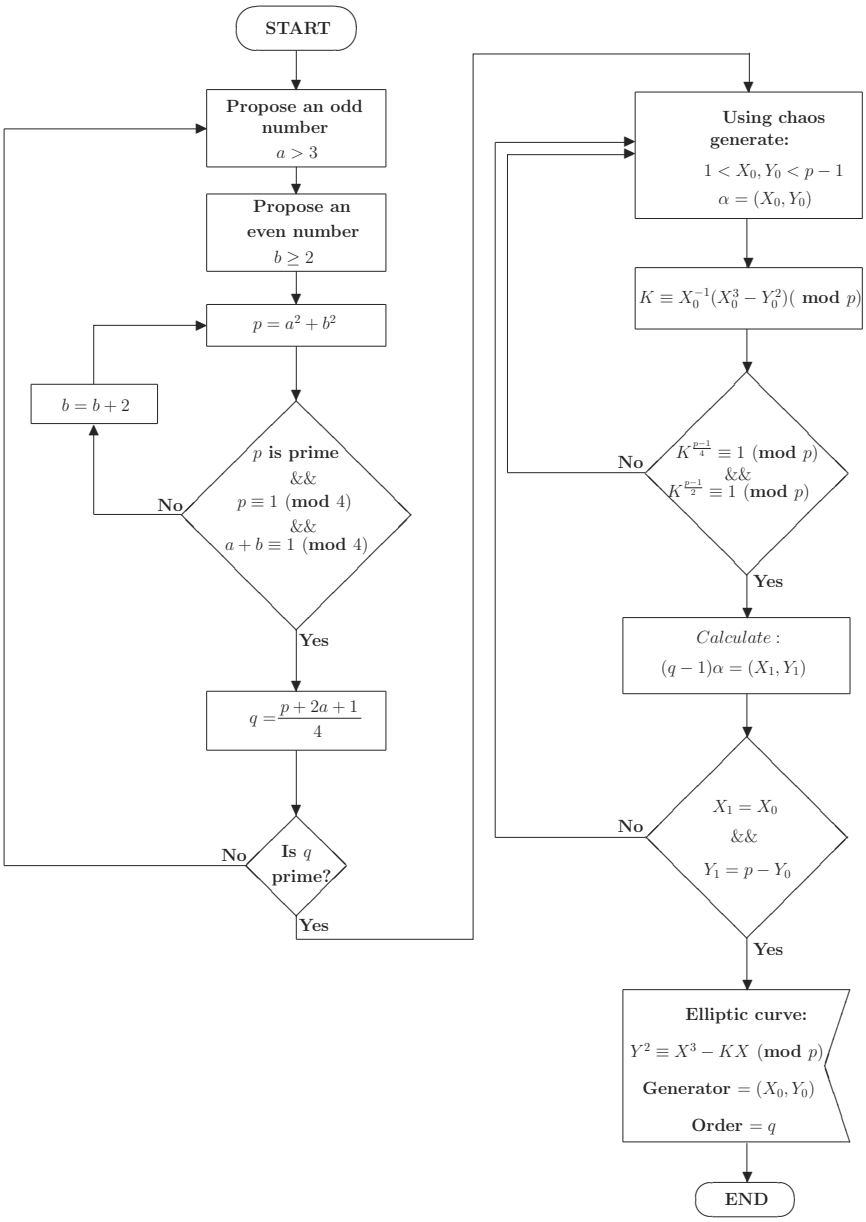


Fig. 1. Elliptic curve flowchart.

the square power module p of some element in the F_p field (Washington, 2008).

At this point, the next question may arise: How is it known that the integer k is not the fourth power module p of some element in the F_p field? To answer this, the following lemma is demonstrated.

Lemma 1. *Consider an elliptic curve of the form $y^2 \equiv x^3 - kx \mod p$ with $k \not\equiv 0 \mod p$. In addition, the condition $p \equiv 1 \mod 4$ is satisfied. Then, if k is the fourth power module p of some element in the F_p field, $k^{(p-1)/4} \mod p \equiv 1$ is implied.*

Proof. If k is the fourth power module p of some element in the field F_p, then there is a $z \in F_p$ such that $z^4 \equiv k \mod p$. However, it is true that $p \equiv 1 \mod 4 \Rightarrow 4 \mid (p-1)$. Then $(z^4)^{(p-1)/4} \equiv k^{(p-1)/4} \mod p$. Nevertheless, $(z^4)^{(p-1)/4} = (z)^{(p-1)}$. Using Fermat's little theorem, it follows that $(z)^{(p-1)} \equiv 1 \mod p$. Hence, this implies that $k^{(p-1)/4} \mod p \equiv 1$. ∎

Thus, we conclude that if $k^{(p-1)/4} \mod p \not\equiv 1$ it implies that k is not the fourth power module p of some element in the F_p field.

To find out if k is the square power module p of

some element in the F_p field, the Euler criterion is used (Stinson, 2005). To construct a cyclic subgroup in the solution set, first the following lemma is proved.

Lemma 2. *Suppose that the conditions stated in Theorem 1 are satisfied. Then* $4 \mid \#E(F_p)$.

Proof. According to the conditions of Theorem 1, it is known that $\#E(F_p) = p + 1 + 2a$. On the other hand, because the prime $p \neq 2$ and b is even, it follows that a is odd. Besides, $p + 1 + 2a = (a+1)^2 + b^2$, which implies that $a + 1$ is even. Thus, $4 \mid (a+1)^2$ and $4 \mid b^2 \Rightarrow 4 \mid \#E(F_p)$. ∎

The following theorem gives enough information to construct a cyclic subgroup in the solution set.

Theorem 2. *Consider an elliptic curve, E, defined on* Z_p*, where p is a prime number greater than 3. Then there are two positive integers* n_1, n_2 *such that there is an isomorphism from* $(E, +)$ *to* $Z_{n_1} \times Z_{n_2}$*. Further,* $n_2 \mid n_1$ *and* $n_2 \mid (p-1)$ *(Stinson, 2005).*

In our case, $n_2 = 1$ and $n_1 = q$, which is a prime factor of $\#E(F_p)$. This research proposes that $q = (p + 1 + 2a)/4$. Sometimes q is not prime; however, we look for other primes p such that the conditions of Theorem 1 are satisfied and $q = (p + 1 + 2a)/4$ is prime.

Another important question is: How do we find the first solution? In this research the problem is posed in a different way, namely, an initial point (x, y) is given, and a k is sought that enforces the expression (1). In fact, this k value must satisfy

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

An example with numerical values is used to illustrate the foregoing. Assign the following values: $a = 17$ and $b = 8$; it follows that p is 353. It can be seen that $p \equiv 1 \mod 4$ and that $a + b \equiv 1 \mod 4$. Furthermore, we suggest as a solution the point α = (231, 217), and with this information k is calculated according to expression (2) yielding, $k = 36$, with $(36)^{353-1/4} \not\equiv 1 \mod 353$ and $(36)^{353-1/2} \equiv 1 \mod 353$. Then, the curve is $y^2 \equiv x^3 - 36x \mod 353$.

Thus, according to Theorem 1 the number of solutions is $\#E(F_{353})$ = 388, and the prime q = 97. On the other hand, $97 \not\equiv 1 \mod 353$, $4(-36)^3 \not\equiv 0 \mod 353$ and $97 \neq 353$; then, the curve is non-singular, non-supersingular, and not even trace one. The non-singularity condition $4(-36)^3 \not\equiv 0 \mod 353$ is equivalent to $x^3 - y^2 \not\equiv 0 \mod p$, where x and y are the initial values in the expression (2).

The next thing to check is if $\alpha = (231, 217)$ is a 97 order element, so $(q-1)\alpha = (231, -217)$ must be satisfied. Therefore, $2\alpha = (336, 114)$; $4\alpha = (35, 291)$; $8\alpha = (191, 313)$; $16\alpha = (159, 261)$; $32\alpha = (146, 221)$; $64\alpha = (36, 330)$. Then, 96α is calculated as $64\alpha + 32\alpha = (231, 136)$. Note that $136 \equiv -217 \mod 353$, and it follows that $97\alpha = \infty$. Figure 1 illustrates the process for obtaining an elliptic curve.

2.2. Chaos. Our starting point is the logistic map equation:

$$\frac{\mathrm{d}P(y)}{\mathrm{d}y} = f(y, P(y)),$$

where $f(y, P(y)) = aP(y) - bP^2(y)$ and $a, b > 1$. On the other hand, the variable y is discretized; that is, it has the values $y_0, y_1, \ldots, y_n$. Then, for the previous numbers the function $P(y)$ has the following values: $P(y_0), P(y_1), \ldots, P(y_n)$.

The Euler algorithm is applied to solve this differential equation, and the expression (3) gives us the relationship between $P(y_{n+1})$ and $P(y_n)$ (Strogatz, 2014):

$$P(y_{n+1}) = P(y_n) + f(y_n, P(y_n)) \times \triangle y. \tag{3}$$

The magnitude of the increase $\triangle y$ is very small. The parameters r and s are specified in

$$r = 1 + a \times \triangle y, \quad s = b \times \triangle y. \tag{4}$$

Moreover, at the point y_n the function $P(y)$ has the value $P(y_n) = r/sy_n$ (David *et al.*, 2009). Incorporating this result into the expression (3), we get

$$y_{n+1} = ry_n(1 - y_n). \tag{5}$$

The limit of y_n can be calculated as $n \to \infty$ if this exists in the expression (5). This limit can be written as $\lim_{n\to\infty} y_{n+1} = \lim_{n\to\infty} ry_n(1 - y_n)$.

In practical situations, when n = 1000, the value y_n is stabilized if the limit exists. Table 1 shows the values of y_n for $n = 1000$, $y_0 = 0.6914152653$ and diverse r values. However, when $r = 3.79171828182845904\ldots$ 7319 (311 digits after the decimal point) the number of possible y_n values is enormous; that is, chaos occurs (Jiang *et al.*, 2006).

The expression (5) fulfills three aspects of chaos; namely,

(a) the quantities y_n are not random;

(b) the values y_n exhibit variations when small changes in r or y_0 values are made; i.e., they are sensitive to small variations;

(c) y_n cannot be predicted without carrying out the calculations in the expression (5).

Table 1. Diverse y_n values for $n = 1000$ and $y_0 = 0.691415265$.

r	1.3	1.6	1.75	1.82	1.95
y_n	0.23076923	0.375	0.42857142	0.45054945	0.48717948

2.3. Entropy. It is quantified according to (Shannon, 1948)

$$H(x) = -\sum_{x\varepsilon X} P(x)\log_2 P(x). \tag{6}$$

Besides, working with color images conforms with the RGB format, i.e., the basic colors: red, green or blue. In this research, each of these colors is described by one byte. Usually, 256 categories are sufficient to describe each color. In this sense, if each basic color has a uniform distribution, that is, all points have the same probability, then the value of the entropy is 8. In practical cases, values close to 8 are sought for the primary color distributions of an encrypted figure.

2.4. Correlation coefficient. Linear analysis between adjacent pixels using the correlation coefficient, or only correlation, is performed on the encrypted image. This analysis is carried out in three directions, namely, horizontal, vertical and diagonal. In this manner, an encrypted image complies with a good degree of randomness if the correlation between its adjacent pixels is a number close to zero. The calculation of the correlation between two random variables y, z is carried out as follows.

An encrypted image pixel is randomly chosen. This pixel has a value between 0 and 255 for each of the colors red, green, and blue, which is written as y_r, y_g, and y_b. Subsequently, an adjacent pixel is taken for each direction: horizontal, vertical, or diagonal according to the case, and just as before, the adjacent pixel has a value for red, green and blue. These are written as z_r, z_g and z_b.

Assume that N pairs of pixels y, z are chosen at random. Therefore, it is possible to calculate the correlations in the three directions for the three basic colors. The formula for calculating the correlation in the horizontal direction for the red color is

$$r_{h;y_r,z_r} = \frac{\frac{1}{N}\sum_{i=1}^{N}(y_{i,r}-\overline{y}_r)(z_{i,r}-\overline{z}_r)}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(y_{i,r}-\overline{y}_r)^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(z_{i,r}-\overline{z}_r)^2\right)}}, \tag{7}$$

where

$$\bar{y}_r = \frac{1}{N}\sum_{i=1}^{N} y_{i,r}, \quad \bar{z}_r = \frac{1}{N}\sum_{i=1}^{N} z_{i,r}. \tag{8}$$

The formulas for the vertical and diagonal directions are similar to the ones for the green and blue colors.

2.5. Discrete Fourier transform (DFT). This transform measures the degree of randomness of a chain of zeros and ones; that is, it checks that there are no repetitive patterns of zeros and ones.

In addition, the following parameters are involved in the calculation of the test statistic:

- $x_k = 2\varepsilon_k - 1$, where $\varepsilon_k = 0, 1$. It follows that $x_k = -1, 1$.
- N_0: It is an expected theoretical quantity; $(0.95) \times n/2$, where n is the string length.
- N_1: It is the number of times that $\|f_j\|$ is less than h, which is calculated as

$$h = \sqrt{\ln\frac{1}{0.05}(n)},$$

where n is the chain length.

- $f_j = \sum_{k=1}^{n} x_k e^{\frac{2\pi i(k-1)j}{n}}$, where $i = \sqrt{-1}$ and $j = 1, 2, \ldots, n/2 - 1$.

If n is odd, the last string bit is deleted, and f_j has a real and a complex part. The module $\|f_j\|$ is calculated and compared with h. If $\|f_j\| < h$, one is added to N_1. Otherwise, N_1 retains its previous value.

Then the quantity

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

and the test statistic p-value $=$ erfc$|\, d\,|/\sqrt{2}$ are calculated, where erfc$(|\, d\,|/\sqrt{2}) = 2(1-\Phi(|d|))$ (Rukhin *et al.*, 2010). The decision rule is: If the p-value is less than 0.01, we reject the hypothesis that the string is random, otherwise it is accepted. Note that the DFT test is included in the NIST 800-22 standard.

2.6. Goodness-of-fit test. This tool aims to find out if the distributions of the basic colors fit a uniform distribution (Kritzer *et al.*, 2014). If so, the distribution of primary colors is said to be random.

However, the above approach leads us to a statistical hypothesis test. In this test two elements are required, namely, a test statistic and a rejection region. The statistic $\chi^2 = \sum_{i=1}^{k}(o_i - \exp_i)^2/e_i$ is utilized for each primary

color, where o_i and $\exp_i$ are the observed and expected values. The χ^2 variable distribution is the chi-square distribution with $k-1$ degrees of freedom (Gaboardi and Rogers, 2017).

According to the central limit theorem, the statistic χ^2 approaches a normal distribution with mean μ = 255 and standard deviation $\sigma = (2 \times 255)^{0.5} = 22.58$ (Guionnet, 2002). With this information, it is easy to know which is the rejection region for the $\alpha = 0.01$ significance level, taking into account that the threshold is on the right-hand side of the normal distribution. Thus, the threshold for α = 0.01 is 307.61. Then, the decision rule is: If the χ^2 value is higher than 307.61, we reject the hypothesis that the string is random, otherwise it is accepted.

In the NIST 800-22 standard this type of test does not appear; that is, the randomness of the tones distribution for the basic colors in the encrypted image is not measured.

2.7. Algorithm for generating permutations. Given a non-negative integer $m \geq 2$ the sets

$$\mathbb{N}_m = \{n \in \mathbb{N} \mid 0 \leq n \leq m! - 1\}$$

and

$$\Pi_m = \{\pi \mid \pi \text{ is a permutation from array } 0, 1, \ldots m-1\}$$

are defined. According to the Euclid division algorithm (Gallian, 2012), any $n \in \mathbb{N}_m$ can be written in a unique way. Equation (9) illustrates this point:

$$\begin{aligned} n = {} & C_0(m-1)! + C_1(m-2)! + \ldots \\ & + C_{m-2}(1)! + C_{m-1}(0)!. \end{aligned} \tag{9}$$

When m is given, the numbers $(m-1)!, (m-2)!, \ldots, 1!, 0!$ are fixed, and it can be seen from the algorithm description that $C_{m-1} = 0$. Further, the following inequality easy to prove:

$$0 \leq C_i < (m-i) \text{ with } 0 \leq i \leq (m-2). \tag{10}$$

Once the values $C_0, C_1, \ldots, C_{m-2}$ are calculated, Algorithm 1 is constructed.

The set of positive integers $X[C_0], X[C_1], \ldots, X[C_{m-2}]$ and $X[C_{m-1}]$ is a permutation of the array $0, 1, \ldots, m-1$. This procedure is performed in $m-1$ steps. The complexity to carry out this algorithm is $O(m)$, because in each step a removal and substitution of an element is performed, with no change in the others.

Theorem 3. *Algorithm 1 defines a function $I_m : \mathbb{N}_m \to \Pi_m$ that is bijective.*

Proof. First it is shown that I_m is a one-to-one function, by the *reductio ad absurdum* method (Kryachko, 2006). In this sense, suppose that for $n_1 \neq n_2 \in \mathbb{N}_m \Rightarrow I_m(n_1) = I_m(n_2)$. However, according to (9) the positive integers n_1, n_2 can be written as follows:

$$\begin{aligned} n_1 = {} & C_{0,1}(m-1)! + C_{1,1}(m-2)! + \ldots \\ & + C_{m-2,1}(1)!, \\ n_2 = {} & C_{0,2}(m-1)! + C_{1,2}(m-2)! + \ldots \\ & + C_{m-2,2}(1)!. \end{aligned}$$

By hypothesis, it is known that $I_m(n_1) = I_m(n_2)$ implies that the elements of both permutations were selected in the same way, so that $C_{0,1} = C_{0,2}, C_{1,1} = C_{1,2}, \ldots, C_{m-2,1} = C_{m-2,2}$. Nevertheless, if this is so, then $n_1 = n_2$.

The last result contradicts the hypothesis, so we conclude that $n_1 \neq n_2 \in \mathbb{N}_m \Rightarrow I_m(n_1) \neq I_m(n_2)$. This proves that I_m is a one-to-one function.

The function is surjective because the numbers of elements in sets $\mathbb{N}_m$ and Π_m are the same. ■

Algorithm 1. Generation of permutations.

Step 0. An array in increasing order is defined as follows: $X[0] = 0, X[1] = 1, \ldots, X[m-1] = m-1$.

Step 1. According to (10), we have $C_0 < m$. It follows that $X[C_0]$ is one element of the arrangement of Step 0. $X[C_0]$ is removed from the array and its place is taken by $X[m-1]$; that is, the last element arrangement and just two operations are performed: elimination and substitution. This means that the other array elements remain unchanged, and only the new position of $X[m-1]$ is assigned. In this sense, if the value of C_0 corresponds to the last element position, then $X[m-1]$ is removed from the array and its position is taken by the element $X[m-2]$.

Step 2. In the same way as in the previous step, $C_1 < (m-1)$, using (10), so that $X[C_1]$ is an element of the arrangement of Step 1. Likewise, as in the previous step, $X[C_1]$ is removed from the array and replaced with the last element. In case $X[C_1]$ is the last element of the array, proceed as in the previous step.

Step $m-1$. If this process is repeated, the result at the end will be the following: $X[C_{m-2}]$ and $X[C_{m-1}] = k$ with $0 \leq k \leq m-1$. The number $X[C_{m-1}]$ appears automatically as the last one, i.e., $C_{m-1} = 0$.

3. Box generation with high nonlinearity

From (5) it is possible to generate quantities of chaotic form using certain r values, such as r = 3.881 ... 7618 (311 digits after the decimal point). In fact, there is a great number of possible quantities that can be assigned to r to generate chaos (David *et al.*, 2009).

In this investigation we proceed as follows: An initial y_0 value is taken in the interval $0 < y_0 < 1$, with 499 digits. The range of n-values is from $n = 2000$ to 10,000

at most. The result is less than one, and the numbers to the right of the decimal point do not follow any pattern; that is, they appear pseudo-randomly. One thousand digits are taken after the decimal point in each iteration. In this manner, this article proposes to take blocks of one byte, one after another, to calculate the constants that are required in the expression (9), using the relation $C_i = b_i \mod (256 - i)$, where b_i is the non-negative integer value associated with the i-th byte. These bytes are taken from the right of the decimal point, for $i = 0, 1, \ldots, 254$.

Once the C_i constants are calculated for $i = 0, 1, \ldots, 254$, Algorithm 1 is applied to obtain a permutation of a 256-element array, taking into account that $C_{255} = 0$. A substitution box is a permutation of a 256-position arrangement. Once the box is obtained, its nonlinearity is calculated according to the expression $LN = \min NL_i$, where $NL_i = 2^7 - \frac{1}{2} \max_{a \in Z_{2^8}} |W_{f_i}(a)|$. In the nonlinearity calculation, the Walsh function is used (Carlet, 2005). We look for a box that has a 108 or 84.4% nonlinearity, considering that the maximum non-linearity is 128. Table 2 is a nonlinearity box of 108, and the y_0, r, and n values are shown below:

$y_0 =$
0.011252939361663712136408542963758
462423938085848604944654681613660 4
232668082619105963915700988161124 2
535062855346500248026738188463938 6
917372979749025311184114508791070 4
133410071268199448269028458397843 3
115384697908599350780424205725639 1
754085083047331188079488463360692 7
409744479391569734175740138641300 8
425165397690026129720664987366423 7
757332522528654668750322208551159 6
475740440449378841610190523203556 1
080131432229808878818773674554752 0
917757167622936023552105397856348 3
075414440423915077494 28,

$r =$ 3.881718281828459045235360287471 35
266249775724709369995957496696762 7
724076630353547594571382178525166 4
274274663919320030599218174135966 2
904357290033429526059563073813232 8
627943490763233829880753195251019 0
115738341879307021540891494884167 5
092447614606680822648001684774118 5
374234544243710753907774499206955 1
7027618,

$n =$ 4993.

4. Encryption procedure

The cryptosystem used in this research is a substitution-permutation network with 14 rounds because the highest security of the Advanced Encryption Standard has the same number of rounds. Moreover, the proposed algorithm defines a symmetric encryption process (Elminaam *et al.*, 2010). In this paper, Table 2 is used as the substitution box, which has a nonlinearity of 108, considering 128 as a maximum, which means 84.4% of the total nonlinearity. In Section 7, some reflections are given about the nonlinearity of the proposed box, DES boxes and linear attack (Silva García, 2007). A high-level description of Algorithm 2 is presented next:

(i) Round 1 starts with the XOR operation between the first scheduled key and the string to be encrypted. The procedure for generating the keys is described later; note that the size of each schedule key is the image size. After performing the XOR operation, the substitution procedure is utilized, according to Table 2, in accordance with the Federal Information Processing Standards Publication 197 (or FIPS 197) standard. A permutation of the image size denoted as P is applied to the output string. Afterward, the calculation of the permutation P is presented.

(ii) Rounds 2–13 proceed in the same way as in the previous paragraph, except that the permutation P is not used.

(iii) In Round 14, the XOR and substitution operations are applied, in that order. Later, the inverse permutation P^{-1} and the operation XOR with the last key of the key schedule are carried out to complete the encryption round.

Algorithm 2. Encryption procedure.

Define image chain $ICHO$ in bytes;
Define $k_1, \ldots, k_{15}$ the schedule keys of image size in bytes;
Require: $in \leftarrow ICHO$;
Require: $state \leftarrow in$;
Round 1;
Apply $state \oplus k_1$;
Apply Permutation $P(state)$; {The permutation over the image is applied as indicated in Section 2.7}
Apply operation $SubBytes(state)$; {Table 2 is used}
for $i \leftarrow 2$ to $i \leftarrow 13$ **do**
  Apply $state \oplus k_i$;
  Apply operation $SubBytes(state)$;
end for
Round 14;
Apply $state \oplus k_{14}$;
Apply operation $SubBytes(state)$;
Apply Permutation $P^{-1}(state)$;
Apply $state \oplus k_{15}$;
Require: $out \leftarrow state$;

Table 2. Substitution table with a nonlinearity of 108.

3d	19	25	45	0a	1d	0f	f1	b5	cf	ff	b9	54	36	07	d8
52	cd	20	8e	2d	d6	41	37	55	04	ca	62	7c	50	4b	46
97	e7	b3	64	63	24	f5	b2	17	5c	03	bb	ad	7a	3e	77
0b	67	8c	bd	f7	51	a9	7e	79	70	27	87	40	e6	b6	ac
c7	b0	73	1e	5f	05	9d	b1	fb	2b	e8	ae	30	42	fe	48
e9	4e	5d	0c	c0	9b	6e	44	14	9a	c9	7b	2f	78	c3	29
84	c8	85	6c	d2	08	f8	b4	26	7d	de	49	3f	1f	4d	74
d4	a6	86	83	90	21	32	ef	3a	02	13	bf	92	e2	89	c4
93	fc	d0	a4	98	72	39	82	fd	3b	da	a3	6d	80	06	16
ec	91	a2	e0	0e	76	1c	3c	8b	db	af	7f	a7	e5	18	f4
31	2c	88	df	e1	4a	a0	a8	a5	2a	5b	69	96	75	fa	9e
ed	1a	bc	9f	8a	33	ab	43	53	e4	38	4c	e3	68	d9	47
8f	6b	dc	34	9c	15	66	99	8d	0d	95	81	6a	01	57	56
d7	10	c6	cc	cb	23	94	ba	b7	6f	12	ee	f2	59	00	4f
09	5a	eb	1b	35	ce	65	71	28	61	f3	f0	c2	d3	a1	58
dd	22	b8	d1	5e	2e	11	aa	be	c5	d5	ea	f6	f9	60	c1

The permutation P is obtained using the algorithm developed in Section 2.7 as follows: Suppose the image has m pixels which are numbered from 0 to $m-1$. Then, the constants C_i are calculated to alter the order of the pixels. Note that it is not necessary to know the value of n in the expression (9), which is fortunate, because it is enormous.

For C_i calculation, the first key of the key k_1 is utilized. It is divided into 8-bit blocks. The first three blocks of eight bits from k_1 are taken, i.e., 1, 2, and 3, to form a 24-bit string. The non-negative integer value of this string is denoted as a_0.

Then, the calculation of the first constant is proposed as $C_0 = a_0 \mod (m-0)$, where m is the number of pixels in the image. To compute the second constant, C_1, a byte is shifted to the right; in other words, bytes 2, 3 and 4 are taken from the string k_1 which is again a 24-bit block. Following the same process, the calculation of C_1 is carried out as $C_1 = a_1 \mod (m-1)$.

Thus, employing the previous procedure, all the constants can be calculated. This research uses 24-bit blocks, because the resolution level in many images is 2^{24}. Further, remember that the last constant $C_{m-1} = 0$.

Once the constants C_i have been calculated, Algorithm 1 is applied to obtain the permutation P. The pseudocode of the cipher system is written below.

4.1. Generating the keys of the schedule. The keys that participate in each round are called the keys of the schedule. The curve points are used for the key generation, which is $y^2 \equiv x^3 - kx \mod p$. The values k, p and $\#E(F_p)$ comply with conditions mentioned in Section 2.1.

The solution points (x, y) of the elliptic curve appear in a pseudo-random way. In addition, the elliptic curve has the following characteristics: The prime p is greater than 2^{200}, and the prime $q = \#E(F_p)/4$ is approximately the same size. An example is shown below:

$p =$ 34432346E82BE3BDC457ACCA180066AA10D8490921073CE1D2EF5D,
$q =$ 10C8D1BA0AF8EF7115EB328603B703097C633E9002E113B4B0D5,
$k =$ C3BAFA05D4ABE4C690B1A7871D4004C282C743D3F4D5EBE099074,
$l =$ 72BEE5E993AA9CE05AE5EC7FA843930A784D2807E45E151BAD5,
$a =$ 73AB10A8CA1F88F8223B67FE9FB,
$b =$ F6E,
$x_0 =$ 15F2624F4395FC95F8EDBDDD393D1CA9B85A84DE8506EC64799021,
$y_0 =$ 164D0B7582AC23408094612C1BF122BAA10572BDB732E5955628F2,
$\alpha = (x_0, y_0)$,
$x_1 =$ 288082CA102FAD4FBD00057C26A70674558E8E84B085130242E64C,
$y_1 =$ 2C9E205DFB96AD32F6F8F6498EE2B5A27CFB7B6032DCF26FD5F9F,
$(l)\alpha = (x_1, y_1)$.

We propose the first key, k_1, of the key program to be obtained as follows: Calculate the point $(l)\alpha = P_0$ and compute the points $P_0 + \alpha, P_0 + 2\alpha, \ldots$ such that the concatenation of these points is the shortest string, but greater than or equal to the image size. If it is greater, the remaining bits are removed to make the string equal to the image size. Let us denote this chain as D. Subsequently, a one-bit circular shift to the left is proposed to be performed on the D-chain.

The resulting string after the shift is divided into 8-bit blocks, and the substitution box of Table 2 is applied in the same way as in FIPS 197. Let us call D_0 the previous

result. In this manner, we continue with another circular shift of one bit to the left and then use the substitution box of Table 2 in the same way as above. The result is denoted as D_1.

If we follow this process, the chain D_6 will be obtained, which is proposed as the first key of the key schedule, i.e., k_1. In Section 7 it is explained why D_6 is taken as the first key. To obtain the remaining 14 keys, that is, the keys up to k_{15}, the same procedure is continued as follows:

(i) A one-bit rotation is applied to the left of the string k_1, and the result is divided into 8-bit blocks. Then, the substitution operation is performed on each block using the box of Table 2, in accordance with FIPS 197, resulting in k_2.

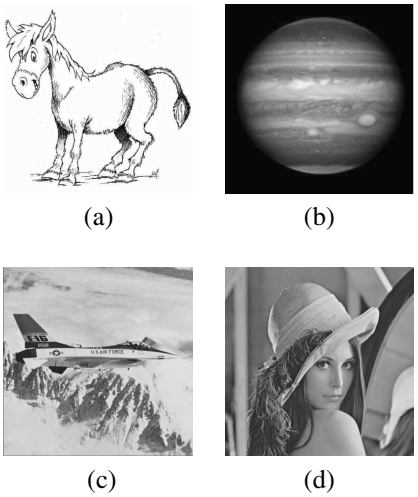
(ii) The k_2 string is rotated one bit to the left and the result is again divided into blocks of one byte. In the same manner as in the previous section, the substitution operation is carried out in each block using Table 2 and the same procedure, resulting in the k_3 key. To obtain the key k_i, with $i = 4, \ldots, 15$, the first step is a rotation of one bit to the chain k_{i-1} left, and then the substitution is performed as noted above. In Section 6, the entropies of the 15 keys of the key schedule are shown.

It can be observed that the point (x_1, y_1) is the key to developing the symmetric cryptosystem. Then, the sender uses the public key of the receiver, say "Q", to encrypt the point (x_1, y_1), and later the receiver, using their private key, say "m", decrypts the sent point (Stinson, 2005).

4.2. Size of the key set. Assume that the point set where the schedule keys are built has $q = (p + 2a + 1)/4$ elements, which is approximately $|p/4|$, and the $||$ symbols mean that only the integer part is taken. Additionally, all points are different from each other because q is a prime number. If the size p is 2^{256} and the solution set of q elements is called Q, it follows that the number of elements in Q is approximately 2^{254}. Then, the key set denominated as K has 2^{254} keys, approximately. The null element is excluded from concatenation since it has no integer coordinates. On the other hand, the number of solutions could be increased using curves with a higher p prime. The following is an example where the number of keys is 2^{516}:

$p =$ 2F1BD60FF5F55449B5D2765DA1DE14383FF
56BCD6F3CAEF2AD5E65E4AACFBA0958A7CC
69AAE4D557609EAD24F87B00B6F0AF20CE9
D31328A34B5F1C8B57AA99781,

$q =$ BC6F583FD7D55126D749D976877850E0FFD
5AF35BCF2BBCAB5799792AB3EE8259987CE
75D61F5E454BDAAAC9C9491387073D69C53
26612E2D1706AD39ABE30EC1,



(a) (b) (c) (d)

Fig. 2. Images test: Donkey (a), Jupiter (b), Jet (c) and Lena (d).

$k =$ 284A486422077C13FBC9104BEC90D429142
F7C1449A811BA8137C4FBD94B9DD6E29300
5F8B7D1CE499ABF333511CD8A62AF4AF35F
9AD42478742B3968A65F11D91,

$x_0 =$
1A1BB41D1504B67385EF47D542F4DD7A045
8B80940F64AE5621B75FA72777AD79912B7
1157E19F9F933C84B43F22FB1BA3D12C033
79C9D3E9623E583C6BAA6807B,

$y_0 =$
7101D47696F6ABBBB991796F4EE88174727
9180820B94B8D57F8E69A897E390EB96AAD
1CBE0466795F66E3556A2DF5BD2090059FF
ED0EA0212AEC9C13A0701134,

$\alpha = (x_0, y_0)$.

5. Images to be encrypted

The test images used to illustrate the encryption processes are presented in Fig. 2. They consist of 512×512 pixels. Some of these figures have been employed in previous developments in this field.

The Donkey image is used to test the proposed cryptosystem, because if a symmetric system is used in its encryption, there is a risk that the encrypted figure will not pass the randomness tests proposed in this work. In fact, in the case of the Advanced Encryption Standard (AES) the cipher block chaining (CBC) mode is used to encrypt images. However, this algorithm offers a maximum security of 2^{256} (Daemen and Rijmen, 1999).

6. Results

The tools for randomness measurement are divided in two groups, namely, those that present a result, such as entropy and correlation, and those that perform a

hypothesis test, which are the discrete Fourier transform and the goodness-of-fit test.

6.1. Entropy and correlation. In Table 3, the results of entropy for the encrypted images of Fig. 2 are presented. Similarly, the entropies of the 15 keys of the key schedule are shown in this part. As pointed out in Section 4, the first key of the schedule is obtained from l and (x_1, y_1). These entropies are shown in Table 4.

The correlation results of the encrypted images are presented in Table 5, taking into account that $N = 3000$. Figure 3 presents the $(x_{c,d}, y_{c,d})$ point graph of Lena encrypted with the l value. The subscript c indicates the color and d the direction. In fact, it is a graph that shows the scatter of the points $(x_{c,d}, y_{c,d})$. Figure 4 presents the histogram of its basic colors distribution encrypted with l.

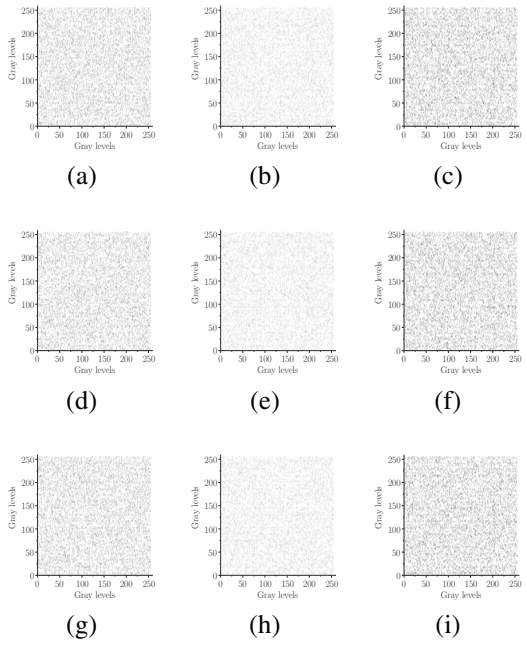


Fig. 3. Points $(x_{c,d}, y_{c,d})$ for the horizontal direction for the red (a), green (b) and blue (c) colors, for vertical direction (d), (e) and (f), and diagonal direction (g), (h) and (i), using the Lena test image encrypted with the l value.

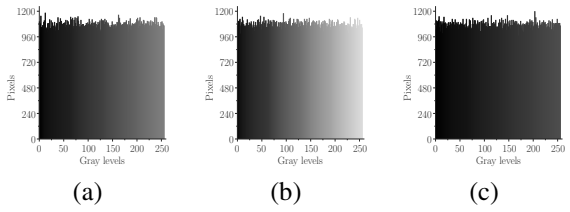


Fig. 4. Basic color distribution of Lena encrypted with the l value for the red (a), green (b) and blue (c) colors.

Fig. 5. Original (a) and ciphered (b) Lena picture with the l value.

6.2. Discrete Fourier transform and the proposed test. Randomness measurements using the DFT in the ciphered images are presented in Table 6. The proposed test for randomness measurement is the goodness-of-fit test using the χ^2 distribution. Table 7 shows the results for the four encrypted test images.

6.3. Entropy of 10,000 values. In this subsection, the following experiments are reported: Given the elliptic curve of Section 4, 10,000 values were proposed for l at random and later the next entropies were calculated, the maximum, average and minimum, using the encrypted image of Lena. The results are presented in Table 8, and Fig. 5 shows the encrypted image to illustrate how the proposed process encrypts with the l value.

6.4. Sensibility. To conclude this section, it would be instructive to present the sensitivity results; that is, the correlation between two encrypted images with different and close keys. In this paper, the keys l and $l + 1$ are proposed. Table 9 shows those results.

7. Analysis and discussion of results

We begin with the proposed symmetric cryptosystem security. The construction of this cryptosystem is based on the elliptic curve, because the key-generation of the schedule depends on the Curve parameters, i.e., p, q, k and α, where α is the generating element. In this sense, we calculate the point $(x_1, y_1) = l \times \alpha$ where l is a random positive integer, such that $1 \leq l \leq q - 1$. Then, 15 keys of the schedule can be calculated, as seen in Section 4.1. The sender only has to mail the point (x_1, y_1) using the elliptic curve. Recall that the curve only encrypts points of itself.

Thus, an attack on the proposed cryptosystem implies an attack on the elliptic curve, because it is desired to know (x_1, y_1). However, the above implies that the private key must be found when the public key is known, which implies solving the discrete logarithm problem (Washington, 2008). In fact, it is considered that solving the discrete logarithm problem for an elliptic curve having a q of size 2^{512} is equivalent to factorizing n

Table 3. Entropies of the encrypted images of Fig. 2 using the value l.

Entropy	Donkey	Jupiter	Jet	Lena
Red	7.99921	7.99931	7.99932	7.99925
Green	7.99920	7.99938	7.99931	7.99935
Blue	7.99936	7.99920	7.99934	7.99928

Table 4. Entropies of the 15 keys using l for the test images.

Key	Entropy	Key	Entropy
1	7.99970	9	7.99977
2	7.99974	10	7.99976
3	7.99976	11	7.99976
4	7.99976	12	7.99979
5	7.99977	13	7.99979
6	7.99975	14	7.99976
7	7.99974	15	7.99975
8	7.99979		

of 2^{15000} size in an RSA scheme (Hemanth Chakravarthy and Kannan, 2015). Besides, it is not complicated to generate curves following the flowchart of Fig. 1 such that the number of solutions has a prime factor of 2^{512}. In addition, if a brute force attack is carried out by constructing the first key of the keys schedule, it would imply solving a 2^n problem where n is the image size.

Moreover, it is important to mention that for calculating the elliptic curve several values of a are randomly proposed, and the program runs in parallel for each a (Sakthivel and Nedunchezhian, 2014). This is because there are some values of a where the computation program takes a long time to find a generator element. Nevertheless, if the program runs in parallel using 16 threads, this possibility is significantly reduced because of the following reasoning.

According to Theorem 1, the total number of solutions is given by $\#E(F_p) = p + 2a + 1$. Furthermore, it is known that the number of solutions q is given by $q = (p + 2a + 1)/4$. Then, the probability of finding a generating element α is $1/4$, and it follows that the probability of failure is $3/4$ for each thread. Taking into account that α is chosen randomly, the events are independent. Thus, using the binomial model with $p = 3/4$ and $n = 16$, it is possible to calculate the probability that none of the threads obtain the generator element, that is, the probability of error. This calculation is made as follows (Feller, 2015):

$$P(X = 16) = \binom{16}{16}\left(\frac{3}{4}\right)^{16}\left(\frac{1}{4}\right)^{16-16}. \qquad (11)$$

Hence, the error probability is $(3/4)^{16}$, approximately 1%. It is clear that the error can be further reduced if desired.

The proposed box has a nonlinearity of 108, the maximum being 128; this implies that the percentage of nonlinearity is 84.4%. Furthermore, it is mentioned that the linear attack was applied to the DES cryptosystem, because the seventh substitution box has a nonlinearity of 14. Since in this case the maximum nonlinearity is 32, it follows that the percentage of nonlinearity is 43.7%.

It can then be observed that the linear attack would not be successful in the presented cryptosystem, because the proposed box nonlinearity is higher than 40%. In fact, its nonlinearity is higher than that of any of DES boxes (Silva García, 2007). In addition, the use of a particular box with the aforementioned nonlinearity has the advantage of generating an original and secure encryption system, which can be used exclusively by a specific corporation or institution.

There are areas of human activity in which the images must not be compressed with loss of information, e.g., national defence, astronomy, and cinema; moreover, the rules for information handling in some countries do not allow compression. For this reason our proposal does not compress the images. As indicated above, the elliptical curve encrypts points of itself. In fact, when it is desired to encrypt symmetric cryptosystem keys, a protocol is required for encryption (Zhang, 2011). In this sense, the proposed cryptosystem encrypts only one point, and it is not necessary to elaborate an additional protocol for the distribution of symmetric cryptosystem keys.

Furthermore, in secure communication schemes, two cryptosystems are used, one symmetric and one asymmetric, for sending the keys, for example, AES and the elliptic curve. In this sense, our case is simpler because it requires only the latter. Besides, with the elliptic curve it is possible to use the Diffie–Hellman protocol (Koziel *et al.*, 2016).

Regarding the concatenation of the coordinates of the curve point, from a given point (x_1, y_1), it is necessary to clarify the following: Each coordinate is written without zeros to the left. That is, it starts with the most significant hexadecimal number other than zero, so that there will be at most three zeros to the left; in fact, this happens when number 1 is expressed in hexadecimal as 0001. Another relevant point to note is that the integer l is utilized to obtain the point $l \times \alpha = (x_1, y_1)$ and only masks the information. In other words, the receiver does not need to know the value of l, because the keys of the schedule can be calculated by knowing only the point (x_1, y_1).

Table 5. Correlation of the encrypted test images using the l value and calculated in three directions: horizontal, vertical and diagonal, for the three basic colors.

Color	Correlation coefficient	Donkey	Jupiter	Jet	Lena
Red	*Horizontal*	0.0016	0.0072	0.0413	0.0102
	Vertical	0.0089	0.0026	0.0846	0.0108
	Diagonal	0.0341	0.0344	0.0132	0.0318
Green	*Horizontal*	0.0251	0.0007	0.0218	0.0300
	Vertical	0.0453	0.0078	0.0271	0.0426
	Diagonal	0.0274	0.0012	0.0014	0.0312
Blue	*Horizontal*	0.0205	0.0441	0.0270	0.0390
	Vertical	0.0294	0.0081	0.0184	0.0061
	Diagonal	0.0178	0.0081	0.0181	0.0222

Table 6. Randomness measurements of the encrypted test images with the l value using the discrete Fourier transform (✓: accepted, x: rejected).

	$\alpha = 0.01$	Donkey	Jupiter	Jet	Lena
DFT	Red	0.81/✓	0.68/✓	0.95/✓	0.99/✓
Test	Green	0.21/✓	0.35/✓	0.71/✓	0.37/✓
	Blue	0.86/✓	0.96/✓	0.88/✓	0.35/✓

The analysis of the results starts with the entropy of the keys program. It was mentioned that the process "shift, substitution" is applied six times before generating the first key because the first strings have a low entropy, that is, 7.9... But from the seventh step onward the chains have an entropy of 7.999...

All the encrypted images of Fig. 2 have an entropy of 7.999... Thus, it is concluded that the randomness is adequate; in fact, it is better than the values reported in other well-known works (Huang and Ye, 2014; Zhu *et al.*, 2013). Table 10 compares the entropy values of other investigations with ours.

With respect to the correlation calculation, the following is pointed out: in Section 2.4 it was mentioned that N pairs of adjacent points are taken in each direction. Our proposal is $N = 3000$, and the pairs are chosen in a random way. On the other hand, it is known that, when the correlation between two variables is close to zero, this means that there is no linear relation between them, which confirms that the color distribution is random.

In this sense, the highest value of correlation in Table 5 is less than 0.085, which confirms that the color distribution in the encrypted figures is random. The results of Table 6 confirm that the encrypted figures do not have repetitive patterns, so it is concluded that the basic color distribution of the encrypted test images is random.

In relation to the results of the proposed test, in Table 7, they also indicate that the null hypothesis is accepted. Recall that the null hypothesis states that the color distribution is random. Therefore, we conclude that the distribution of the three basic colors is random.

The Lena image was encrypted using 10,000 different values of l that were chosen at random. Table 8 reports the minimum, average, and maximum entropies for each basic color, namely, red, green, and blue. As can be seen, the values of the entropy for each of these colors correspond to random distributions.

In regard to sensibility, Table 9 shows the results of the Lena image encrypted with values of l and $l + 1$. As can be seen, there is no relationship between the images when they are encrypted with two different and close keys.

7.1. Our contribution. In this work, a novel symmetrical cryptosystem for color-image encryption in 14 rounds is proposed. The cryptosystem has two parts: the first one is asymmetric due to the elliptical curve, and the other is symmetric because an algorithm of 14 rounds is constructed. Thus, two types of attacks can be expected: those that are applied to the curve and those applied to the symmetric system. Regarding the attacks on the curve, the following may be mentioned: supersingular curves, curves of trace one, or solving the discrete logarithm problem. In our case, none of these attacks can be carried out, since our curves are non-supersingular, they are not trace one, and also the solution set size is such that the discrete logarithm problem cannot be solved (Stinson, 2005).

On the other hand, a high non-linearity substitution box is constructed to avoid both linear and differential attacks to the proposed symmetric cryptosystem (Matsui, 1993; Biham and Shamir, 1992). Additionally, a brute force attack on the symmetric system involves solving a problem of 2^n, where n is equal to the image size in bits.

Table 7. Results of the proposed test for the encrypted test images with the l value (✓: accepted, x: rejected).

	$\alpha = 0.01$	Donkey	Jupiter	Jet	Lena
Proposal	Red	$0.08/\checkmark$	$0.60/\checkmark$	$0.69/\checkmark$	$0.22/\checkmark$
Test	Green	$0.07/\checkmark$	$0.90/\checkmark$	$0.63/\checkmark$	$0.81/\checkmark$
	Blue	$0.85/\checkmark$	$0.74/\checkmark$	$0.78/\checkmark$	$0.40/\checkmark$

Table 8. Entropies results of the encrypted Lena image using 10.000 random values of l. Minimum, average and maximum entropies are reported for each basic color.

Entropy	Minimum	Average	Maximum
Red	7.99900	7.999293	7.99950
Green	7.99902	7.999293	7.99950
Blue	7.99907	7.999292	7.99951

In addition, the resulting encrypted images present a good randomization to avoid possible attacks on them by using chaotic systems. In this sense, an instrument based on the distribution χ^2 is proposed to measure the randomness of the encrypted images, which is not included in the NIST 800-22 standard. This proposal for image encryption can be used for developing secure communication schemes using only one cryptosystem, the elliptic curve, and not two systems like in the PKI scheme (Lozupone, 2018). Considering all of the above, it can be affirmed that the proposed image encryption cryptosystem is highly secure and efficient.

7.2. Limitations and scope. Two limitations are described in this paper. The first one refers to the following point: the algorithm of Fig. 1 is not convenient to run with a single value of a, because sometimes it takes a considerable time to find the generator element, so it must be run in parallel using several values of a.

The second is about the calculation of the first schedule key, which is the start for generating the others. However, in the computation of this first schedule key the operation of multiplicative inverse of b modulo p is performed sequentially, where $b \in \mathbb{Z}_p^*$. Moreover, this operation is carried out for each point that is concatenated. Therefore, it takes more time to generate the schedule keys for the proposed system than to generate the schedule keys of a symmetric system as AES, FIPS 197.

The application field of this development is so broad that it includes applications such as sending encrypted images on mobile devices.

8. Conclusions

This research presented a novel symmetric cryptosystem that encrypts color images with a high degree of security and high quality. The cryptosystem is a 14-round substitution-permutation-network-type system. The keys of the schedule are of image size and they are constructed using a zero constant elliptic curve. Chaos is used to calculate the curve generator and a 256 $\times$ 256 box. An algorithm was proposed to generated permutations, and we define a scheme of communication that needs only the elliptical curve; i.e., it is simpler than the PKI scheme with two different cryptosystems. The results corresponding to entropy and correlation show a good degree of randomness of the encrypted figures and in the entropy case the results surpass those of other previous developments. On the other hand, the discrete Fourier transform results and the goodness-of-fit test proposed always indicate that the randomness null hypothesis is accepted; besides, the time to encrypt an image of 512 $\times$ 512 is lower than a second. Finally, the software was developed in Java and Visual Studio.

Acknowledgment

The authors would like to thank Instituto Politécnico Nacional (Secretaría Académica, COFAA, SIP, CIDETEC, and ESFM), CONACyT, and SNI for their economical support to develop this work.

References

Barker, W.C., Barker, E. and Mouha, N. (2012). Recommendation for the Triple Data Encryption Algorithm (TDEA) block cipher, Revision 2, *NIST Special Publication* 800-67, National Institute of Standards and Technology, Gaithersburg, MD.

Biham, E. and Shamir, A. (1992). Differential cryptanalysis of the full 16-round DES, *in* E.F. Brickell (Ed.), *Advances in Cryptology—CRYPTO'92*, Lecture Notes in Computer Science, Vol. 740, Springer, Berlin/Heidelberg, pp. 79–88.

Carlet, C. (2005). On highly nonlinear S-boxes and their inability to thwart DPA attacks, *INDOCRYPT, Bangalore, India*, pp. 49–62.

Chen, W. and Chen, X. (2013). Ghost imaging for three-dimensional optical security, *Applied Physics Letters* **103**(22): 221106.

Table 9. Correlation between encrypted figures of Lena for the l and $l+1$ keys.

Correlation	Sensitivity analysis for the Lena image using the l, $l+1$ keys
Red	0.021
Green	0.033
Blue	0.005

Table 10. Entropy compared using three standard images according to 256 grey levels.

Image	Other algorithms (Huang and Ye, 2014)	Our algorithm with the l value
Lena	7.989579	7.999285
Barbara	7.991714	7.999321
Peppers	7.991507	7.999316

Chen, W. and Chen, X. (2014). Double random phase encoding using phase reservation and compression, *Journal of Optics* **16**(2): 025402.

Chen, W., Chen, X. and Sheppard, C.J. (2012). Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain, *Optics Express* **20**(4): 3853–3865.

Chen, W., Javidi, B. and Chen, X. (2014). Advances in optical security systems, *Advances in Optics and Photonics* **6**(2): 120–155.

Daemen, J. and Rijmen, V. (1999). AES proposal: Rijndael, *FIPS 197*, National Institute of Standards and Technology, Gaithersburg, MD.

David, E., Penney, C. and Edwards, H. (2009). *Ecuaciones diferenciales y problemas con valores en la frontera, cómputo y modelado*, Pearson Educación, México, pp. 429–440.

Elminaam, D.S.A., Abdual-Kader, H.M. and Hadhoud, M.M. (2010). Evaluating the performance of symmetric encryption algorithms., *IJ Network Security* **10**(3): 216–222.

Feller, W. (2015). On the normal approximation to the binomial distribution, *in* R. Schiling *et al.* (Eds.), *Selected Papers I*, Springer, Cham, pp. 655–665.

Gaboardi, M. and Rogers, R. (2017). Local private hypothesis testing: Chi-square tests, *arXiv* 1709.07155.

Gallian, J. (2012). *Contemporary Abstract Algebra*, 8th Edn, Cengage Learning, Boston, MA.

Guionnet, A. (2002). Large deviations upper bounds and central limit theorems for non-commutative functionals of Gaussian large random matrices, *Annales de l'Institut Henri Poincare B: Probability and Statistics* **38**(3): 341–384.

Hemanth Chakravarthy, M. and Kannan, E. (2015). Hybrid elliptic curve cryptography using ant colony based authentication system for cloud computing, *Journal of Engineering and Applied Sciences* **10**(16): 7273–7279.

Huang, X. and Ye, G. (2014). An image encryption algorithm based on hyper-chaos and DNA sequence, *Multimedia Tools and Applications* **72**(1): 57–70.

Jiang, M., Shen, Y., Jian, J. and Liao, X. (2006). Stability, bifurcation and a new chaos in the logistic differential equation with delay, *Physics Letters A* **350**(3): 221–227.

Koziel, B., Jalali, A., Azarderakhsh, R., Jao, D. and Mozaffari-Kermani, M. (2016). NEON-SIDH: Efficient implementation of supersingular isogeny Diffie–Hellman key exchange protocol on arm, *International Conference on Cryptology and Network Security, Milan, Italy*, pp. 88–103.

Kritzer, P., Pillichshammer, F., Niederreiter, H. and Winterhof, A. (2014). *Uniform Distribution and Quasi-Monte Carlo Methods: Discrepancy, Integration and Applications*, De Gruyter, Boston, MA.

Kryachko, E.S. (2006). On the proof by reductio ad absurdum of the Hohenberg–Kohn theorem for ensembles of fractionally occupied states of coulomb systems, *International Journal of Quantum Chemistry* **106**(8): 1795–1798.

Kumar, M., Iqbal, A. and Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, *Signal Processing* **125**: 187–202.

Lang, J., Tao, R. and Wang, Y. (2010). Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function, *Optics Communications* **283**(10): 2092–2096.

Li, L., El-Latif, A.A.A. and Niu, X. (2012). Elliptic curve Elgamal based homomorphic image encryption scheme for sharing secret images, *Signal Processing* **92**(4): 1069–1078.

Lozupone, V. (2018). Analyze encryption and public key infrastructure (PKI), *International Journal of Information Management* **38**(1): 42–44.

Luca, F., Mireles, D.J. and Shparlinski, I.E. (2004). MOV attack in various subgroups on elliptic curves, *Illinois Journal of Mathematics* **48**(3): 1041–1052.

Luis, F.J.E.G.y. and Encinas, H. (2004). Una revisión de los criptosistemas de clave pública sobre curvas elípticas e hiperelípticas, *in* B. Ramos Álvarez and A. Ribagorda Garnacho (Eds), *Avances en criptología y seguridad de la información*, Ediciones Díaz de Santos, Madrid, pp. 149.

Matsui, M. (1993). Linear cryptanalysis method for DES cipher, *Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway*, pp. 386–397.

Michael, S. (2006). *Calculus, Third Edition*, Cambridge University Press, Cambridge.

Nom-151 (2002). *Norma Oficial Mexicana NOM-151-SCFI-Prácticas comerciales, Requisitos que deben observarse para la conservación de mensajes de datos*, Diario Oficial de la Federación, México.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M. and Barker, E. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications, *Technical report*, Booz-Allen and Hamilton Inc, Mclean, VA.

Sakthivel, A. and Nedunchezhian, R. (2014). Analyzing the point multiplication operation of elliptic curve cryptosystem over prime field for parallel processing, *International Arab Journal of Information Technology* **11**(4): 322–328.

Sam, I.S., Devaraj, P. and Bhuvaneswaran, R.S. (2012). A novel image cipher based on mixed transformed logistic maps, *Multimedia Tools and Applications* **56**(2): 315–330.

Shannon, E. (1948). A mathematical theory of communication, *Bell System Technical Journal* **27**(3): 379–423.

Silva García, V.M. (2007). Criptoanálisis para la modificación de los estándares des y triple des, *DSc thesis*, Instituto Politécnico Nacional, México, pp. 24–29.

Stinson, D.R. (2005). *Cryptography: Theory and Practice*, CRC Press, Boca Raton, FL.

Strogatz, S. H. (2014). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, Westview Press, New York, NY.

Thangavel, M., Varalakshmi, P., Murrali, M. and Nithya, K. (2015). An enhanced and secured RSA key generation scheme (ESRKGS), *Journal of Information Security and Applications* **20**: 3–10.

Washington, L.C. (2008). *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, FL.

Yarom, Y., Genkin, D. and Heninger, N. (2017). CacheBleed: A timing attack on OpenSSL constant-time RSA, *Journal of Cryptographic Engineering* **7**(2): 99–112.

Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map, *Pattern Recognition Letters* **31**(5): 347–354.

Zhang, X. (2011). Lossy compression and iterative reconstruction for encrypted image, *IEEE Transactions on Information Forensics and Security* **6**(1): 53–58.

Zhu, H., Zhao, C. and Zhang, X. (2013). A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem, *Signal Processing: Image Communication* **28**(6): 670–680.

Víctor Manuel Silva-García is a research professor of the Center for Innovation and Technological Development in Computing at IPN, a doctor of computer science, the coordinator of the Security and Network Laboratory, a member of the Mexican Mathematical Society.

Rolando Flores-Carapia is a professor at CIDETEC-IPN and belongs to the Researchers National System. He received his doctorate degree from National Polytechnic Institute in 2011. His research interests include image processing and cryptography.

Carlos Rentería-Márquez is a research professor of ESFM at IPN. His research topics are applications of number theory and algebraic geometry to the construction of codes for information transmission and construction of cryptographic systems. He is a member of the Mexican Mathematical Society.

Bejamín Luna-Benoso holds a Bachelor's degree in physics and mathematics (2002) from ESFM-IPN. He obtained a degree in science (2007) and a doctorate (2011) in CIC at IPN. Currently he is a professor-researcher of ESCOM-IPN. His research areas are image analysis, cryptography, and pattern recognition.

Juan Carlos Chimal-Eguía obtained his PhD in sciences at ESFM of IPN in 2003. He is currently a professor at the Computation Center of Research of IPN. He is the author of more than 80 articles in journals as well as national and international conferences. He has also been a visiting professor at the University of Alberta, Canada. The areas of interest of Dr. Chimal are the modeling and simulation of physical systems using differential equations, as well as complex systems and non-linear dynamics.

Received: 10 September 2018
Revised: 2 May 2019
Re-revised: 22 August 2019
Accepted: 6 November 2019