Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100407

Image Encryption using Chaos-Driven Elliptic Curve Pseudo-Random Number Generators

Omar Reyad[1,2,*], *Zbigniew Kotulski*[1] *and W. M. Abd-Elhafiez*[2]

[1] Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland
[2] Faculty of Science, Sohag University, Egypt

Received: 20 Jun. 2015, Revised: 6 May 2016, Accepted: 7 May 2016
Published online: 1 Jul. 2016

Abstract: Pseudo-random number sequences which using the form of elliptic curves can be generated efficiently in software or hardware by the same methods that are used for the implementation of elliptic curve (EC) public-key cryptosystems. In this paper, we proposed a secure image encryption scheme using key sequences generated from Chaos-Driven Elliptic Curve Pseudo-random Number Generator (C-D ECPRNG). This key sequences derived from random sequences based on EC points operations driven by a chaotic map. These constructions improve randomness properties of the generated sequences since it combines good statistical properties of an ECPRNG and a Chaotic Pseudo-random Number Generator (CPRNG). Entropy analysis of two test images shows that randomness of the ciphered images with the proposed key schemes are more random than in case of the ECPRNG without modulation by a chaotic map. Statistical and differential analysis demonstrate that the proposed schemes have adequate security for the confidentiality of digital images and the encryption is efficient compared to other competitive algorithms.

Keywords: Elliptic Curve Cryptography, Random Number Generator, Image Encryption, Chaotic Maps

1 Introduction

Cryptography is a practical means for protecting private and sensitive information. Cryptographic systems are divided between symmetric-key and public-key cryptosystems. The security of most known cryptographic systems depends upon generation of a long unpredictable key sequences that must be of sufficient size and randomness. For a sequence to be random, the period of the sequence must be large and various patterns of a given length must be uniformly distributed over the sequence. However, sources of truly random integers are hard to use in practice. Therefore, it is common to search for pseudo-random number generators (PRNGs).

Considerable research has been made in the design and analysis of PRNGs which are using the form of elliptic curves such as [1]. Since methods presented in [2], different approaches for extracting pseudo randomness from such elliptic curves have been proposed [3,4]. Elliptic curve cryptography (ECC) is a public-key cryptosystem introduced by Miller [5] and Koblitz [6]. Since then, many researchers tried to employ ECC on different data types and improve it's efficiency by proposing various techniques. In fact, the most attractive advantage that motivated cryptographers to use ECC was the suitability of it in the environments where processing power, storage, bandwidth or power consumption is constrained [7]. These characteristics of ECC motivated us to study the potential of using it for image encryption.

Inspired by the near similarity between chaos and cryptography, various techniques based on chaotic systems have been proposed to design a random bit generator called Chaotic Pseudo-random Number Generator (CPRNG) [8,9,10]. The CPRNG can be used in many applications requiring random binary sequences and also in the design of secure cryptosystems. The key sequence generators discussed in this paper is a variation of the last two schemes, where, the key sequence elements are random sequences based on Elliptic Curve Pseudo-random Number Generator (ECPRNG) with modulation by a chaotic map. Such a construction increases randomness of the generated sequence and makes its period (theoretically) infinite since it combines positive properties of both ECPRNG and CPRNG.

Images are widely used in various areas such as science, military, medical, engineering, art, entertainment,

[*] Corresponding author e-mail: ormak4@yahoo.com

advertising, education as well as training. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Image encryption is the process of realigning the plainimage into an incomprehensible one that is non-recognizable in appearance, disorderly and unsystematic. In recent years, various image encryption schemes have been proposed and widely used by several researchers to overcome image encryption problems [11,12,13].

In this paper, we propose a secure image encryption scheme using additive elliptic curve and chaotic switching mode. The proposed scheme utilizes key sequences generated from EC points operations driven by three chaotic maps. The simulation analysis demonstrated that the proposed scheme has large key space, low correlation among pixels in cipherimages and can satisfy the performance requirements for the confidentiality of digital images. Results of numerical analysis show that the proposed image encryption scheme outperforms the competitive image encryption algorithms.

The rest of the paper is organized as follows: In Section 2, we present preliminaries about some related works. Also the description of ECPRNG, CPRNG and the Chaos-Driven Elliptic Curve Pseudo-random Number Generator (C-D ECPRNG) constructions are discussed. The proposed schemes for image encryption and decryption are discussed in Section 3. In Section 4, we discuss the security and statistical analysis for the proposed schemes. Comparison of the proposed schemes with some existing schemes are made in Section 5 while conclusions are given in Section 6.

2 Preliminaries

In most cryptosystems, the cryptographic key is a crucial part. No matter how strong and how well designed the encryption algorithm might be, if the key is poorly chosen or the key space is too small, the cryptosystem will be easily broken. Due to this principle, EC points operations modulated by chaotic maps are chosen as a key stream generator because of their properties and easy implementation. In this paper we assume that the elliptic curve E is defined over a finite field $\mathbb{F}_p$ of prime order p which is represented by the elements of the set $[0,1,...,p-1]$.

2.1 Related Works

Several attempts for using ECC in image encryption has been proposed in literature. In [14], additive and affine encryption schemes using six schemes of key sequences obtained from random EC points were designed and investigated. An EC-based key generation based on combination of linear feedback shift register (LFSR) and cyclic EC over a finite prime field have been proposed in [15]. In [16,17], ECC was used only to encrypt the secret key that was used to encrypt images. The image encryption itself was done using permutation and diffusion [16] or code computing [17]. A new mapping method was introduced in [18] to convert a pixel's value to a point on an affine EC using a map table. A new scheme for image encryption based on a cyclic EC and generalized chaotic logistic map have been presented in [19]. Two ECC-based encryption algorithms: selective encryption of the quantised discrete cosine transform (DCT) coefficients and perceptual encryption based on selective bit-plane encryption have been presented in [20].

2.2 Elliptic Curve Pseudo-Random Number Generator

Let E be an elliptic curve over $\mathbb{F}_p$, $p>3$, given by an affine Weierstrass equation of the form

$$E: y^2 = x^3 + ax + b \qquad (1)$$

with coefficients $a,b \in \mathbb{F}_p$, such that $4a^3 + 27b^2 \neq 0$. We recall that the set $E(\mathbb{F}_p)$ of points of any elliptic curve E in affine $\mathbb{F}_p$-valued coordinates form an Abelian group (with a point at infinity denoted by O as the neutral element).

Points addition and points doubling are the basic EC operations. Points multiplication on EC requires a scalar multiplication operation kP, defined for a point $P=(x,y)$ on EC and a positive integer k as k times addition of P to itself. This scalar multiplication can be done by a series of doubling and addition operations of P. Let us start with $P=(x_1,y_1)$ where $P \neq -P$. To determine $2P=(x_3,y_3)$, P is doubled, use the following equation:

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \;\; and \;\; y_3 = \left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3) - y_1.$$

To determine $3P$, addition of points P and $2P$ is used, treating $2P=Q$. Here, P has coordinates $P=(x_1,y_1)$ and $Q=2P$ has coordinates $Q=(x_2,y_2)$, where $P \neq \pm Q$. Then $P+Q=(x_3,y_3)$, where

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$$

and

$$y_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) - y_1.$$

Therefore, doubling and addition are applied depending on a sequence of operations determined for k. Every point (x_3, y_3) evaluated by doubling or addition is a point on the EC [21,22]. Let us now present constructions of generating sequences of pseudo-random points on elliptic curves:

2.2.1 Linear Congruential Generator on EC

The Linear Congruential Generator on EC (EC-LCG) for a given point $G \in E(\mathbb{F}_p)$ of high order ℓ is defined as the following sequence:

$$U_i = G \oplus U_{i-1} = [i]G \oplus U_0 \quad ,i = 1,2,..., \qquad (2)$$

where $U_0 \in E(\mathbb{F}_p)$ is the "initial value". The EC-LCG generator has been suggested in [23] and then studied in a number of papers such as [24,25,26].

2.2.2 Power Generator on EC

The Power Generator on EC (EC-PG) for a given point $G \in E(\mathbb{F}_p)$ of high order ℓ and an integer $e \geq 2$ provided that the greatest common divisor (gcd) of $(gcd(e,\ell) = 1)$ is defined as the sequence:

$$U_i = [e]U_{i-1} = [e^i]G \quad ,i = 1,2,..., \qquad (3)$$

where $U_0 \in E(\mathbb{F}_p)$ is the "initial value". The EC-PG generator has been introduced and studied in [27,28].

2.2.3 Dual-EC Generator

The Dual-EC generator is appeared in NIST recommendations [29], make use of two points G and Q on a non-super singular elliptic curve $E(\mathbb{F}_p)$ for generation of random numbers. The algorithm can be detailed as below:

$$\begin{aligned} U_i &= \varphi(x(U_{i-1} * G)) \quad ,i = 1,2,... \\ R_i &= \varphi(x(U_i * Q)) \quad ,i = 1,2,... \end{aligned}$$

where $U_0 \in E(\mathbb{F}_p)$ is the "initial value". The Dual-EC generator mechanism represents an EC scalar multiplication operation, followed by the extraction of the x coordinate for the resulting point U_i and for the random output R_i followed by truncation to produce the output sequence.

2.2.4 Other Constructions on EC

We note that after [2], there have been several other suggestions and approaches to extracting pseudo randomness from elliptic curves, see also [30,31,32]. However, these methods and results have a slightly different focus and we do not discuss them in this paper.

2.3 Chaotic Pseudo-Random Number Generator

Consider the following dynamical system defined as a pair (S, Φ), where S is the state space and $(\Phi : S \rightarrow S)$ is a measurable map [33]. The idea of construction of CPRNG is to divide the state space S, $\mu(S) = 1$, into two disjoint parts: S_0 corresponds to bit 0, S_1 to bit 1 such that $\mu(S_0) = \mu(S_1) = 1/2$. Assume that μ is a normalized invariant measure of the system, equivalent to a Lebesgue measure. To obtain a pseudo-random sequence of bits we observe the iterations of the system governed by the map Φ starting from an initial point $s \subseteq S$ and as a result of these iterations we obtain the infinite sequence of generated bits. Moreover, theoretically the period of such a CPRNG is infinite, since it is iterated over the infinite state space S.

In many practical applications for constructing CPRNG we assume that $S = [0, 1]$ is the interval, $S_0 = [0\ ,\ 0.5]\ ,\ S_1 = (0.5\ ,\ 1]$ are two subsets of the measure equal 0.5 and $\Phi\ :\ [0,\ 1] \rightarrow [0,\ 1]$ is a chaotic map with positive Lyapunov exponent λ. Such generators have good statistical properties under certain conditions [34]. In this paper, we consider three chaotic dynamical systems governed by the following maps to generate the binary sequences:

the Logistic Map [35]:

$$s_{i+1} = \Phi(s_i) = 4 \cdot s_i(1 - s_i)\,, \qquad (4)$$

the Tent Map [36]:

$$s_{i+1} = \Phi(s_i) = \begin{cases} 2s_i & if\ \ s_i < \frac{1}{2} \\ 2(1 - s_i) & if\ \ s_i \geq \frac{1}{2} \end{cases}, \qquad (5)$$

both for the state space $S = [0,1]$ and $S_0 = [0, 0.5]$, $S_1 = (0.5, 1]$, and the Chebyshev Map [37]:

$$s_{i+1} = \Phi(s_i) = \cos\left(4\cos^{-1}(s_i)\right), \qquad (6)$$

for the state space $S = [-1,1]$ and $S_0 = [-1,0]$, $S_1 = (0,1]$.

2.4 Chaos-Driven Elliptic Curve Pseudo-Random Number Generator

The C-D ECPRNG is defined for the next two EC-sequences. Here, we will consider b_i as the random bits generated by the chaotic map Φ mentioned in 2.3

$$b_i = \begin{cases} 0 \ \text{ if } \ \Phi^i(s) \in S_0 \\ 1 \ \text{ if } \ \Phi^i(s) \in S_1 \end{cases}, i = 1,2,... \qquad (7)$$

2.4.1 Additive Elliptic Curve

This method is a modification of the EC-LCG proposed in 2.2.1. This generator takes high order point $G \in E(\mathbb{F}_p)$ as the seed point and is defined as the following sequence:

$$\begin{aligned} U_i &= [i(1+b_i)]G \oplus U_0 \\ &= \begin{cases} [i]G \oplus U_0 & if \;\; b_i = 0 \\ [2i]G \oplus U_0 & if \;\; b_i = 1 \end{cases} \quad, i = 1, 2, \ldots \end{aligned} \tag{8}$$

where $U_0 \in E(\mathbb{F}_p)$ is the ”initial value”.

2.4.2 Chaotic Switching Mode

This method works as the same method introduced in 2.4.1 above. The generator work on two curves $E_1(\mathbb{F}_{23})$ and $E_2(\mathbb{F}_{97})$ with small prime numbers 23 and 97 respectively. After applying the additive sequence in (8), we take one point from U_{E_1} and one point from U_{E_2} in a staggered manner in order to generate binary sequences from these two curves. For example, consider that after applying the additive sequence in (8) the resultant U_{E_1} points is A = $(a_1, a_2, ...)$ and U_{E_2} points is D = $(d_1, d_2, ...)$. We take this series of points (a_1 d_1 a_2 d_2 ....) to generate our sequence. In the case of chaotic switching, we randomly take points in unpredicted series based on chaotic map to generate pseudo-random sequence. For example, if b_1 = 0 we take a_1 and if b_1 = 1 we take d_1 and so on.

$$U_i = \begin{cases} a_i \in A & \text{if} \;\; b_i = 0 \\ d_i \in D & \text{if} \;\; b_i = 1 \end{cases}, i = 1, 2, \ldots \tag{9}$$

Using EC points sequence U_i result from the previous equations (8, 9) and by converting the x, y coordinates of each point $U_i(x, y)$ into binary format we can obtain the binary sequence B_i by applying the following map

$$B_i = U_i(x, y) = U_{RHB}(x, y). \tag{10}$$

This map takes the right-half bits (RHB) from x and y coordinates which is denoted by $U_{RHB}(x, y)$. If the number of bits is odd, we take the small right-half and we ignore the infinity points [38].

3 Image Encryption with the Proposed Key Schemes

The intended schemes for the generation of random sequences of EC points operations are discussed in Section 2.4. Its application for encrypting images is presented here. Ten key schemes for image encryption using various EC-sequences are designed and comparison of encrypted images is done using Histogram, Entropy and Correlation coefficient. The proposed schemes are applicable to other forms of data like text and video apart from images.

Both of additive elliptic curve method and chaotic switching mode for encrypting images are designed where the key sequences derived from EC points operations driven by three chaotic maps (Logistic, Chebyshev and Tent map) as described in Section 2.4(1, 2). The same key sequence is used for both encryption and decryption process. Here, ten schemes for image encryption using various key sequences are considered and they are given in Table 1.

Table 1: Various key schemes proposed for image encryption

Key	Scheme	Description
Key-1	$A-EC_{2x2}$	Additive $E(\mathbb{F}_{23})$
Key-2	$A-EC_{3x3}$	Additive $E(\mathbb{F}_{97})$
Key-3	$S-EC_{2x3}$	Switching of $E(\mathbb{F}_{23})$ and $E(\mathbb{F}_{97})$
Key-4	$L-EC_{2x3}$	Modulated with Logistic map
Key-5	$C-EC_{2x3}$	Modulated with Chebyshev map
Key-6	$T-EC_{2x3}$	Modulated with Tent map
Key-7	$A-EC_{7x7}$	Additive $E(\mathbb{F}_{12107})$
Key-8	$L-EC_{7x7}$	Modulated with Logistic map
Key-9	$C-EC_{7x7}$	Modulated with Chebyshev map
Key-10	$T-EC_{7x7}$	Modulated with Tent map

In this paper, we used equation (1) to generate three elliptic curves by choosing the parameters $(a = 2, b = 7)$ over two small primes 23 and 97 named $E(\mathbb{F}_{23})$ and $E(\mathbb{F}_{97})$ respectively and one large prime 12107 named $E(\mathbb{F}_{12107})$ to generate EC points. After applying the intended schemes in Section 2.4(1, 2) and then the map in equation (10), we obtain the binary sequences as indicated in Table 1. Here, the binary digit of $p = 23$ is equal 5 bits and for $p = 97$ is equal 7 bits, , so we take two RHB (EC_{2x2}) and three RHB (EC_{3x3}). Similarly the binary digit of $p = 12107$ is equal 14 bits, so we take seven RHB (EC_{7x7}) from the x, y coordinates of each point $U_i(x, y)$ of the resulted EC-sequences and we ignore the infinity points.

The first column in Table 1 represent the generated keys named $Key-1, \ldots, Key-10$ and the second column represent their related schemes. Schemes $A-EC_{2x2}$, $A-EC_{3x3}$ and $A-EC_{7x7}$ represent sequence generated from EC points addition operation without chaotic modulation as mentioned in Section 2.2.1 of $E(\mathbb{F}_{23})$, $E(\mathbb{F}_{97})$ and $E(\mathbb{F}_{12107})$ respectively. Sequence generated from chaotic switching mode of $E(\mathbb{F}_{23})$ and $E(\mathbb{F}_{97})$ is represented in scheme $S-EC_{2x3}$. Schemes $L-EC_{2x3}$, $C-EC_{2x3}$, $T-EC_{2x3}$, $L-EC_{7x7}$, $C-EC_{7x7}$ and $T-EC_{7x7}$ represent sequences generated from additive EC method modulated with Logistic, Chebyshev and Tent maps respectively. In the third column, description of each key scheme is given in brief according to it's generation method.

4 Security and Statistical Analysis

A good encryption scheme should be robust against all kinds of possible attacks. The attacks are varying in nature such as statistical attack, brute-force attack, etc. Hence, analysis of encryption schemes such as key space analysis, statistical analysis, correlation analysis and key sensitivity analysis ensures right development of the security system. What follows are the security aspects of the proposed key schemes using the available techniques of analysis.

4.1 Key Space Analysis

The key space that is being used for encryption must be large enough to make the brute-force attack infeasible [39]. The proposed chaos-driven elliptic curve pseudo-random key sequence generator has a flexible, moderately large key space, which comprises of a number of initial points and control parameters for chaotic maps, possible ECs and the base point. Hence, this large key space is sufficient which is immune to all kinds of brute-force attacks. Results of applying the XOR operation in encryption of images with the ten proposed key sequences are shown in Figs. 1(a – j) for Lena image and Figs. 2(a – j) for Fingerprint image.

4.2 Statistical Analysis

Statistical analysis on cipherimages is of crucial importance for any encryption algorithm. Actually, a perfect cipher should be vigorous against any statistical attack. Statistical analysis has been performed to show the resistance of the proposed encryption schemes against the possible statistical attacks. The following aspects related to statistical attack are considered in this paper.

4.2.1 Histogram Analysis

To prevent the leakage of information to an adversary, it is important to ensure that cipherimage does not have any statistical resemblance to the plainimage. A good image encryption scheme should always generate a cipherimage of the uniform histogram for any plainimage. In this work, the histograms are plotted for two encrypted images (Lena and Fingerprint). The histogram of Lena plainimage contains large spikes while the histograms of it's cipherimages are almost flat and uniform which indicates equal probability of occurrence of each pixel as shown in Figs. 3(a – c) for Key-1, Key-2 and Key-3 as examples. They are significantly different from the respective histogram of the Lena plainimage and hence does not provide any clue to employ any statistical attack on the proposed image encryption schemes. For the histogram of Fingerprint plainimage, it is clear that it is almost non-flat and nonuniform which indicates that all pixels occur with nonequivalent probability and the histograms of it's encrypted images using Keay-1, Key-2 and Key-3 in Fig. 4 are not very flat. However, histograms of it's encrypted images using Key-4 to Key-10 are flat and uniform which provides security against cipher-text only attack by statistical analysis.

4.2.2 Entropy analysis

Entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = -\sum_{i=0}^{255} P(m_i) log_2 P(m_i) \tag{11}$$

where $P(m_i)$ represents the probability of symbol m_i. For all the considered cipherimages, the number of occurrence of each gray level is recorded and the probability of occurrence is computed. Tables 2 and 3 indicates the various values of the entropies for the plain and encrypted images. Except for Key-1, Key-2 and Key-3 in Table 3, it can be noted that the entropy of the encrypted images are very near to the theoretical value of 8 indicating that all the pixels in the encrypted images occur with almost equal probability. Therefore, the information leakage in the proposed cipher schemes is negligible, and it is secure against the entropy-based attack.

4.2.3 Randomness Tests

The proposed key sequences generator is based on the arithmetic operation of ECC and the properties of chaotic maps. The random sequences are unpredictable and the period of the sequences is analyzed theoretically. In addition, sequences produced by this generator have passed tests from the NIST's SP 800-22 ”Statistical Test Suite for Random and Pseudo-random Number Generators for Cryptographic Applications” as introduced in [38]. As a result, statistical attacks are difficult to perform in the proposed key sequences generator.

4.3 Correlation Analysis

It is known that two adjacent pixels in a plainimage are strongly correlated vertically, horizontally and diagonally. This is the property of any ordinary image. The maximum value of correlation coefficient is 1 and the minimum is 0.

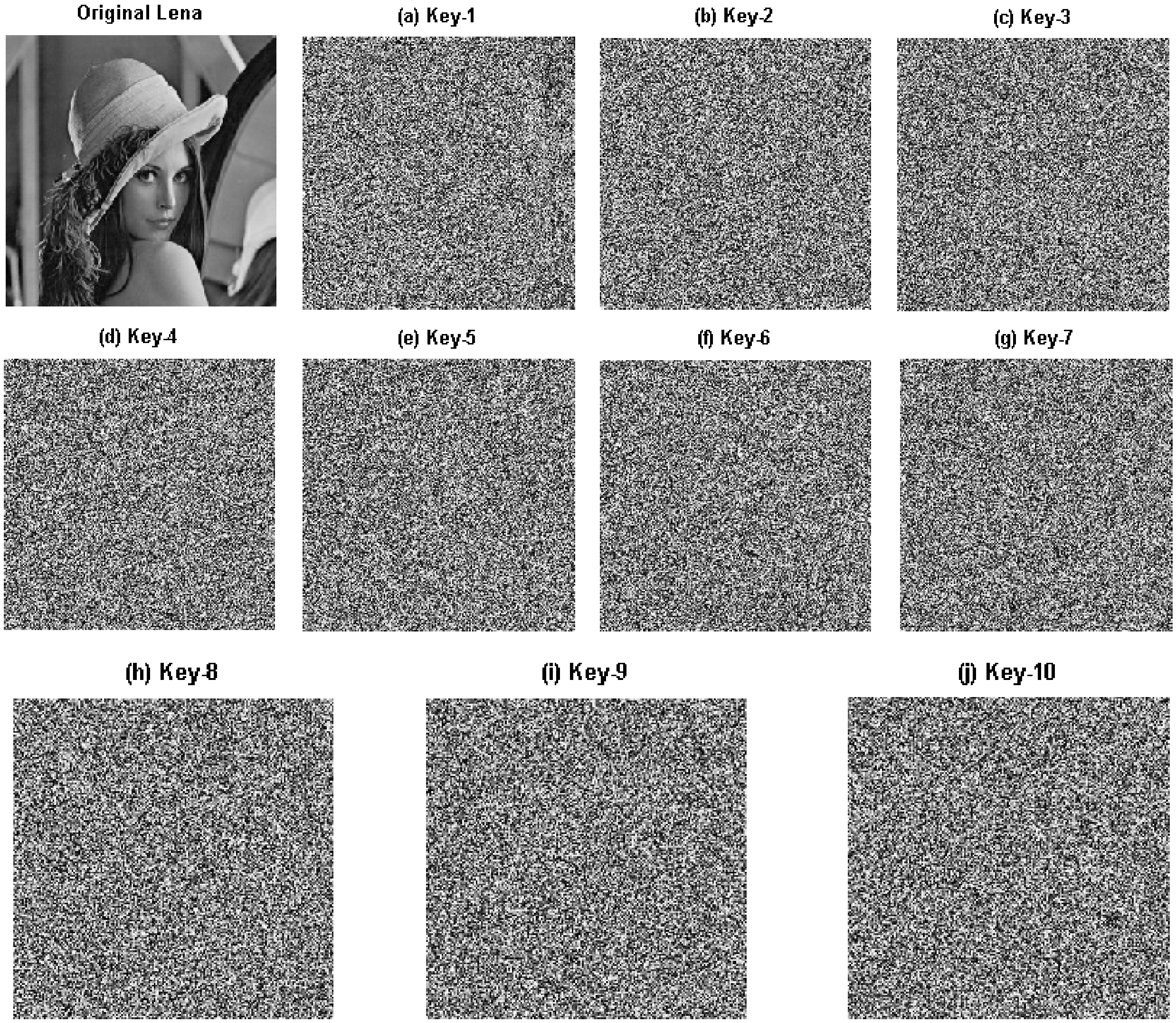

Fig. 1: Lena image encrypted with the ten proposed keys

A robust encrypted image to statistical attack should have a correlation coefficient value of ˜0. Results of horizontal, diagonal and vertical directions are obtained as shown in Tables 2 and 3 for Lena and Fingerprint plain and cipher images respectively. These tables demonstrate that there is negligible correlation between the two adjacent pixels in the encrypted images, even when the two adjacent pixels in the plainimage are highly correlated.

4.4 Differential Analysis

In order to avoid the known-plaintext attack, the changes in the cipherimage should be significant even with a small change in the plainimage. If one small change in the plainimage can cause a significant change in the cipherimage, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. To quantify this requirement, two common measures are used: number of pixels change rate (NPCR) and unified average changing intensity (UACI) [40]. We have tested the NPCR and UACI with the proposed key schemes to assess the influence of changing a single pixel in the plainimages on the encrypted images. From the results, we have found that the average values of the percentage of pixels changed in encrypted image is greater than 99.68% for NPCR and 30.54% for UACI in case of Lena. In the case of Fingerprint, the percentage of pixels changed in encrypted image is greater than 99.68% for NPCR and 38.53% for UACI. This implies that the proposed key schemes is very sensitive with respect to small changes in the plainimage.

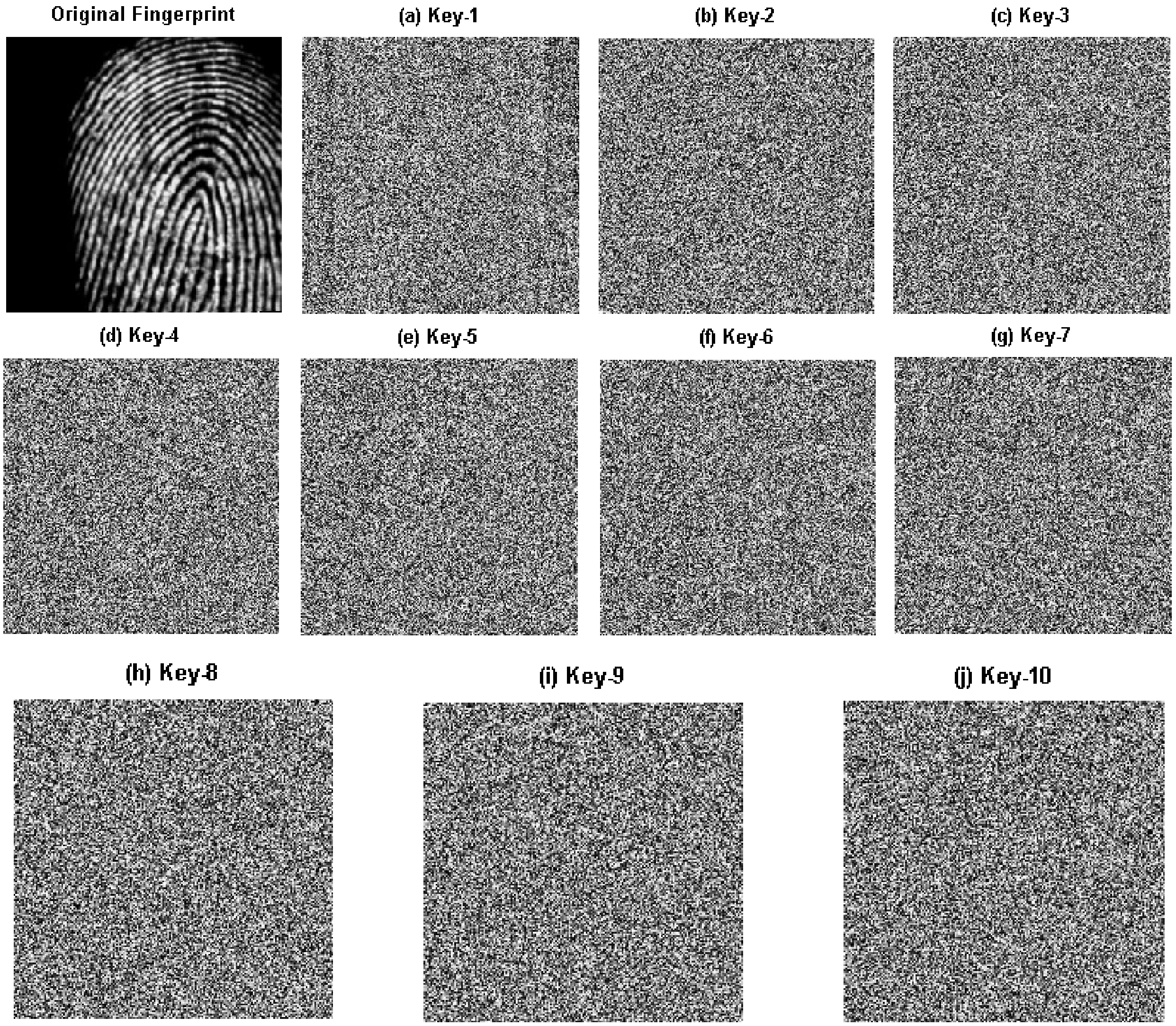

Fig. 2: Fingerprint image encrypted with the ten proposed keys

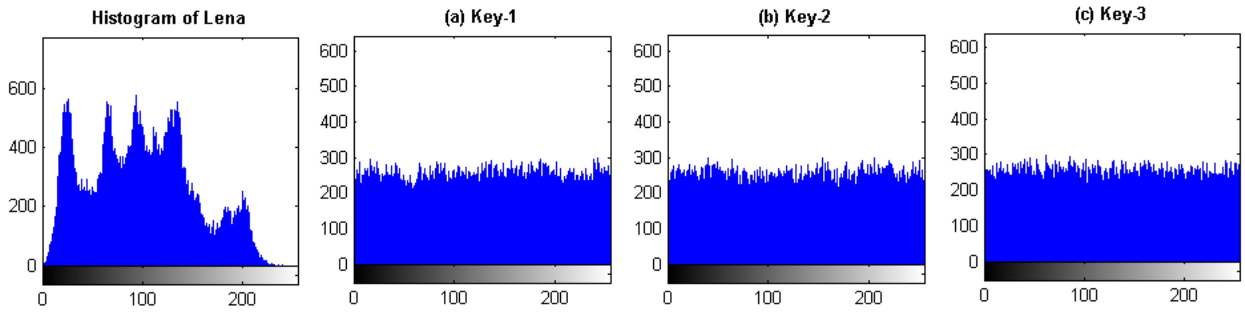

Fig. 3: Histogram of Lena image and encrypted images with the ten proposed keys

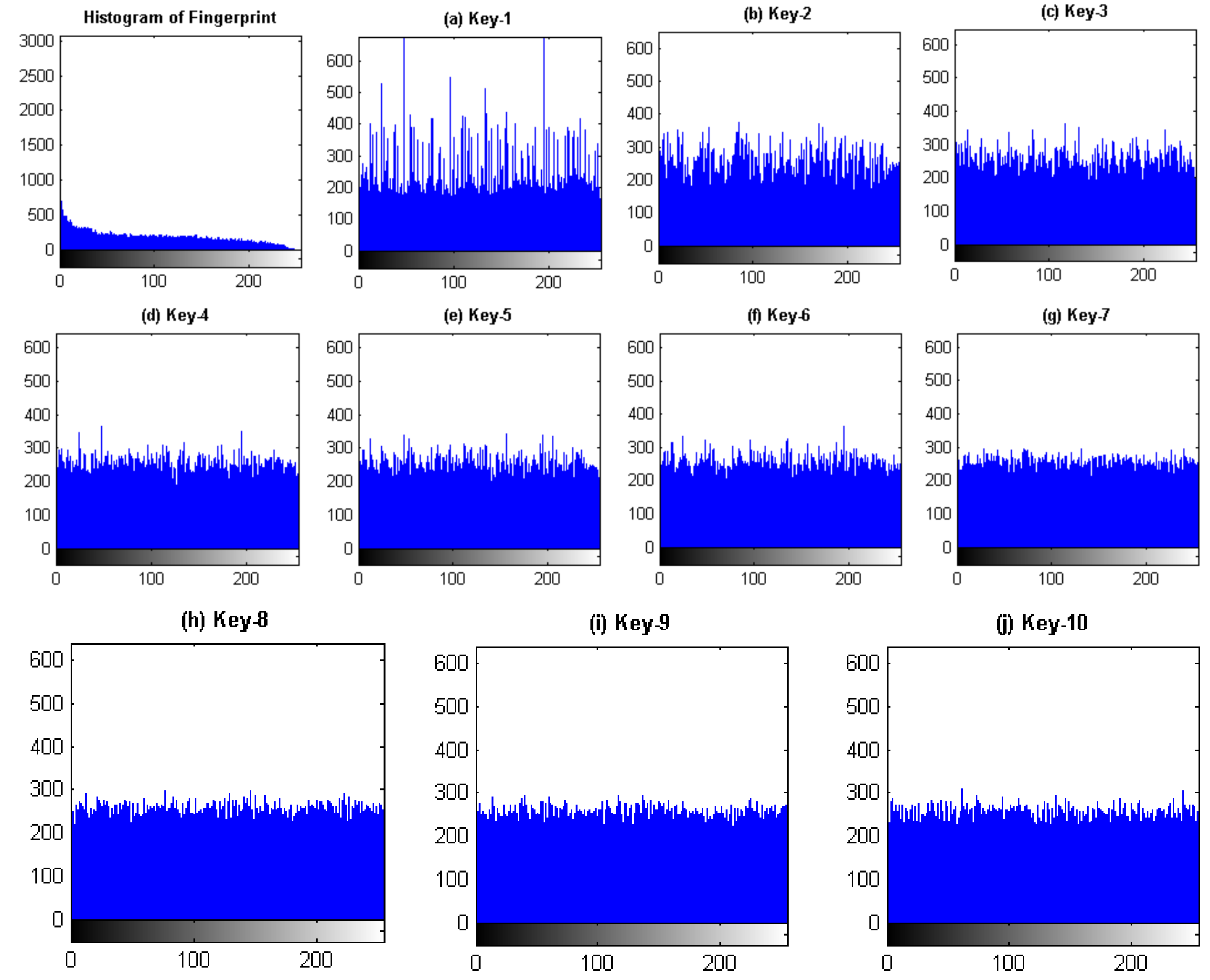

Fig. 4: Histogram of Fingerprint image and encrypted images with the ten proposed keys

5 Comparison of The Proposed Schemes with Existing Schemes

By comparing the entropy and correlation analysis with other schemes, the proposed schemes shows significant results as in Tables 2 and 3. It is shown that the entropy and correlation coefficient values of Lena image are performing better for all the proposed keys compared to the other schemes as shown in Table 2. In Table 3, due to the lowest entropy value for the Fingerprint plainimage, only the proposed Key-4 to Key-10 are performing better compared to the other schemes mentioned in Table 3.

6 Conclusions

In this paper, we have presented a new scheme for image encryption based on the Chaos-Driven Elliptic Curve Pseudo-random Number Generators. In the presented algorithm, we have modulated the random sequences generated from additive operation of elliptic curve points and three chaotic maps in order to obtain efficient keystream sequences for encryption. All the simulation and experimental analysis show that the proposed encryption schemes has high sensitivity to secret keys and almost ideal entropy of the cipherimages. In addition, it has large key space, which is by far very safe for image encryption applications, and outperforms the competitive image encryption algorithms in terms of efficiency comparing to other encryption schemes.

Acknowledgement

This work has been supported by the European Union in the framework of European Social Fund through the

Table 2: Comparison of entropy and correlation coefficients of the proposed schemes and other schemes for Lena image

Scheme	Entropy	Horizontal	Vertical	Diagonal
Lena	7.5807	0.93915	0.96890	0.91686
Key-1	7.9963	0.00936	-0.08948	0.00877
Key-2	7.9966	0.00056	-0.03608	0.00144
Key-3	7.9974	0.00069	-0.00450	-0.00295
Key-4	7.9972	-0.00018	-0.01739	0.00001
Key-5	7.9969	0.00108	-0.02107	0.00340
Key-6	7.9974	0.00446	-0.01491	-0.00513
Key-7	7.9969	-0.00174	-0.00407	-0.00341
Key-8	7.9971	0.00018	-0.00876	-0.00109
Key-9	7.9971	-0.00102	0.00382	-0.00280
Key-10	7.9973	0.00581	-0.00730	0.00192
Ref.[16]	7.9990	0.001	0.006	0.091
Ref.[15]	7.9952	0.0072	0.000158	-0.0428
Ref.[18]	7.9981	0.004971	0.003803	0.003519
Ref.[19]	7.9973	0.0010	0.0017	0.0125
Ref.[14]	7.9964	-0.000798	-0.0013	-0.0046
Ref.[41]	NA	0.0005938	0.0041	0.0048

Table 3: Comparison of entropy and correlation coefficients of the proposed schemes and other schemes for Fingerprint image

Scheme	Entropy	Horizontal	Vertical	Diagonal
Finger	6.3367	0.91398	0.94519	0.82989
Key-1	7.9279	0.01043	-0.05708	0.01918
Key-2	7.9789	-0.00735	-0.00013	-0.01388
Key-3	7.9881	0.00022	-0.03475	0.00539
Key-4	7.9931	0.00017	-0.02025	0.00349
Key-5	7.9918	0.00026	-0.02444	0.00056
Key-6	7.9928	0.00757	-0.01305	-0.00403
Key-7	7.9970	-0.00358	0.00170	0.00228
Key-8	7.9975	0.00115	-0.00763	0.00519
Key-9	7.9974	0.00608	-0.00116	-0.00344
Key-10	7.9972	0.00062	-0.00383	-0.00114
Ref.[16]	7.9990	0.001	0.006	0.091
Ref.[15]	7.9952	0.0072	0.000158	-0.0428
Ref.[18]	7.9981	0.004971	0.003803	0.003519
Ref.[19]	7.9973	0.0010	0.0017	0.0125
Ref.[14]	7.9964	-0.000798	-0.0013	-0.0046
Ref.[41]	NA	0.0005938	0.0041	0.0048

project: Supporting Educational Initiatives of the Warsaw University of Technology in Teaching and Skill Improvement Training in the Area of Teleinformatics.

References

[1] D. Jao, D. Jetchev, R. Venkatesan, On the bits of elliptic curve Diffie-Hellman keys, INDOCRYPT 2007, vol. 4859, Springer, Heidelberg, 2007.

[2] B.S. Kaliski, One-way permutations on elliptic curves, Journal of Cryptology 3, 187–199 (1991).

[3] M. Caragiu, R.A. Johns, J. Gieseler, Quasi-random structures from elliptic curves, J. Algebra, Number Theory Appl. 6, 561–571 (2006).

[4] L.P. Lee, K.W. Wong, A random number generator based elliptic curve operations, Computers and Mathematics with Appl. 47, 217–226 (2004).

[5] V. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology-CRYPTO'85, vol. 218, Springer, Heidelberg, 1986.

[6] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation 48, 203–208 (1987).

[7] N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, Comparing elliptic curve cryptography and RSA on 8-bit CPUs, Cryptographic Hardware and Embedded Systems (CHES), vol. 3156, Springer, Heidelberg, 2004.

[8] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, Advances in Cryptology-EUROCRYPT'91, vol. 547, Springer, Heidelberg, 1991.

[9] Z. Kotulski, J. Szczepanski, Discrete chaotic cryptography, Annalen der Physik 6, 381–394 (1997).

[10] Z. Kotulski, J. Szczepanski, K. Gorski, A. Paszkiewicz, A. Gorska, On constructive approach to chaotic pseudorandom number generators, Proceedings RCMIS 1, 191–203 (2000).

[11] T. Gao, Z. Chen, Image encryption based on a new total shuffling algorithm, J. Chaos, Solitons and Fractals 38, 213–220 (2008).

[12] V. Patidar, N.K. Pareek, K.K. Sud, Modified substitution-diffusion image cipher using chaotic standard and logistic maps, J. Comm. in Nonlinear Sci. and Numerical Simul. 15, 2755–2765 (2010).

[13] S.P. Indrakanti, P.S. Avadhani, Permutation based image encryption technique, Int. J. of Computer Appl. 28, 45–47 (2011).

[14] S.V. Sathyanarayana, M. Aswatha Kumar, K.N. Hari Bhat, Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points, Int. J. Netw. Secur. 12, 137-150 (2011).

[15] S. Maria, K. Muneeswaran, Key generation based on elliptic curve over finite prime field, Int. J. Elect. Sec. and Digital Forensics 4, 65–81 (2012).

[16] K. Gupta, S. Silakari, Efficient hybrid image cryptosystem using ECC and chaotic map, Int. J. Comput. Appl. 29, 1-13 (2011).

[17] Z. Zhao, X. Zhang, ECC-based image encryption using code computing, Advances in Intelligent Sys. and Comp., vol. 181, Springer, Heidelberg, 2013.

[18] A. Soleymani, M.J. Nordin, A.N. Hoshyar, M.A. Zulkarnain, E. Sundararajan, An Image Encryption Scheme Based on Elliptic Curve and a Novel Mapping Method, Int. J. of Digital Content Tech. and its Appl. 7, 85–94 (2013).

[19] A.A. Abd El-Latif, X. Niua, A hybrid chaotic system and cyclic elliptic curve for image encryption, Int. J. Electron. Commun. 67, 136-143 (2013).

[20] L. Tawalbeh, M. Mowafi, W. Aljoby, Use of elliptic curve cryptography for multimedia encryption, IET Inf. Secur. 7, 67-74 (2013).

[21] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic, Dordrecht, 1993.

[22] J.H Silverman, The arithmetic of elliptic curves, Springer-Verlag, Berlin, 1995.

[23] S. Hallgren, Linear congruential generators over elliptic curves, Preprint CS94-143, Dept. of Comp. Sci., Cornegie Mellon Univ., 1994.

[24] G. Gong, T.A. Berson, D.R. Stinson, Elliptic curve pseudorandom sequence generators, Selected areas in cryptography, vol. 1758, Springer, Berlin, 2000.

[25] O. Reyad, Z. Kotulski, On Pseudo-random Number Generators Using Elliptic Curves and Chaotic Systems, J. Appl. Math. Inf. Sci. 9, 31-38 (2015).

[26] P. Beelen, J. Doumen, Pseudorandom sequences from elliptic curves, Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 2002.

[27] T. Lange, I.E. Shparlinski, Certain exponential sums and random walks on elliptic curves, Canad. J. Math. 57, 338-350 (2005).

[28] E. El Mahassni and I.E. Shparlinski, On the distribution of the elliptic curve power generator, Proc. 8th Conf. on Finite Fields and Appl., Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 111-119 (2008).

[29] E. Barker, J. Kelsey, Recommendation for random number generation using deterministic random bit generators, Special Publication 800-90, NIST, 2005.

[30] R.R. Farashahi, B. Schoenmakers, A. Sidorenko, Efficient pseudorandom generators based on the DDH assumption, PKC 2007, vol. 4450, Springer, Heidelberg, 2007.

[31] M. Caragiu, R.A. Johns, J. Gieseler, Quasi-random structures from elliptic curves, J.Algebra, Number Theory Appl. 6, 561-571, (2006).

[32] I.E. Shparlinski, Pseudorandom number generators from elliptic curves, Affine Algebraic Geometry, Amer. Math. Soc. 477, 121-142 (2009).

[33] L.P. Cornfeld, S.V. Fomin, Ya.G. Sinai, Ergodic Theory, Springer-Verlag, Berlin, 1982.

[34] J. Szczepanski, Z. Kotulski, Pseudorandom number generators based on chaotic dynamical systems, Open Systems and Information Dynamics 8, 137–146 (2001).

[35] S.C. Phatak, S.S. Rao, Logistic map: A possible random-number generator, Physical Review E 51, 3670–3678 (1995).

[36] J.M. Amigo, L. Kocarev, J. Szczepanski, Theory and Practice of Chaotic Cryptography, Physics Letters A 366, 211–216 (2007).

[37] X.F. Liao, X.M. Li, J. Peng, et al, A digital secure image communication scheme based on the chaotic Chebyshev map, Int. J. Commun. Syst. 17, 437–445 (2004).

[38] O. Reyad, Z. Kotulski, Statistical Analysis of the Chaos-Driven Elliptic Curve Pseudo-random Number Generators, CCIS, vol. 448, Springer, Heidelberg, 2014.

[39] P. Christof, Applied cryptography and data security, http://www.crypto.ruhr-uni-bochum.de/en_lectures.html

[40] S.E. Borujeni, M. Eshghi, Chaotic image encryption design using Tompkins-Paige algorithm, Hindawi Pub. Cor., Math. Prob. in Eng. 2009, 1–22 (2009).

[41] H. Khanzadi, M. Eshghi, S.E. Borujeni, Image Encryption Using Random Bit Sequence Based on Chaotic Maps, Arab J. Sci. Eng. 39, 1039-1047 (2014).

Omar Reyad is a PhD student at the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland. He received his MSc in computer science from Sohag University, Egypt. His main research interests are in elliptic curve cryptography, cryptographic protocols and random number generators.

Zbigniew Kotulski is a Professor and Head of the Security Research Group at the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland. He received his MSc in Applied Mathematics from Warsaw University of Technology and PhD and DSc degrees from the Institute of Fundamental Technological Research of the Polish Academy of Sciences. He is the author and co-author of five books and over 160 research papers on applied probability, cryptography, cryptographic protocols and network security.

Walaa Abd-Elhafiez received her B.Sc. and M.Sc. degrees from south valley university, Sohag branch, Sohag, Egypt in 2002 and from Sohag University, Sohag, Egypt, Jan 2007, respectively, and her Ph.D. degree from Sohag University, Sohag, Egypt. Her research interests include image segmentation, image enhancement, image recognition, image coding, video coding, and their applications in image processing.