Academic Journal of Nawroz University (AJNU), Vol.10, No.2, 2021

https://doi.org/10.25007/ajnu.v10n1a916

An Efficient Method of Image Encryption Using Rossler Chaotic System

Yasir Ahmed Hamza[1], Marwan Dahar Omer[2]
[1]Dept. of Computer Science, Nawroz University, Dohuk, Kurdistan-region, Iraq
[2]Dept. of Computer Science, Saint Leo University, Florida-Texas, USA

ABSTRACT

In this study, a new approach of image encryption has been proposed. This method is depends on the symmetric encryption algorithm RC4 and Rossler chaotic system. Firstly, the encryption key is employed to ciphering a plain image using RC4 and obtains a ciphered-image. Then, the same key is used to generate the initial conditions of the Rossler system. The system parameters and the initial conditions are used as the inputs for Rossler chaotic system to generate the 2-dimensional array of random values. The resulted array is XORed with the ciphered-image to obtain the final encrypted-image. Based on the experimental results, the proposed method has achieved high security and less computation time. Also, the proposed method can be resisted attacks like (statistical, brute-force, and differential).

Keywords: Encrypted-image; initial conditions; encryption key; RC4; Rossler chaotic system.

1. Introduction

Nowadays, people live in an era of connected world that convergence of computers and networks. In addition, a public network such as the internet becomes the most-used channel for transferring digital information. Using insecure channels like the internet may lead to several threats related to the confidentiality of transmitted digital information. Therefore, information security becomes an essential requirement to transferred digital information in a secure manner (Amalarethinam & Geetha, 2015). Digital Information may be in different formats such as (image, video, text, or sound). Digital images are the most used among other digital information. The security of digital images is not constrained for using an individual framework (Rehman, *et al.*, 2015). However, they have required confidentiality for their sensitive information according to using applications such as medical, military, satellite, unmanned aerial vehicle (UAV), and industry. These applications are required high security for digital images against the different attacks (Arab, *et al.*, 2019). In addition, the period of sending the encrypted image from the sender-party to the receiver is very striking. Because of irreparable corrupts may be occurs if the image encryption method took a long time. Image encryption approaches must take a minimum running time and high security (Arab, *et al.*, 2019).

For these reasons, image encryption plays a very effective factor in providing secrecy to the digital image. Image encryption is the approach that used to convert the contents of the plain image into unintelligible form or scrambled image to protect it from unauthorized persons (Dixit, *et al.*, 2018). In this case, just a receiver can retrieve the original image. Many image encryption methods are proposed depends on optics or chaos theories (Wen, *et al.*, 2015). Also, they can be divided into two categories: full-encryption and partial/selective-encryption. Full image encryption approaches are applied to the contents of the entire image, while selective image encryption methods are focused only on the meaningful part of the image (Belazi, *et al.*, 2015; Jawad and Sulong, 2015). Image encryptions are based on the chaotic systems have gained more attention (Mandal, *et al.*, 2014) after 1990 for their ability to increase the degree of security because the chaotic systems have

some significant features like the sensitive dependence to initial states and the parameters of system (Tang, *et al.*, 2019). The standard cryptography approaches are depending on theoretical or algebraic concepts. Digital images have several properties like the correlation between adjacent pixels, high volume, and the visual data redundancy. Therefore, the standard cryptography algorithms are inappropriate for image encryption; because of they have number of problems such as high encryption time and less security.

Chaos is another scheme that looks hopeful for designing good image encryption methods (Rehman, *et al.*, 2015). The chaotic system has implied a hidden behavior of a nonlinear system, which seems randomly. The randomness of the chaotic system is not has a stochastic origin. However, it is a pure result of the defined deterministic processes. The research community has comprehended chaotic cryptography and chaos depended communication will become a unique way for secure communication. The best approach for image encryption should consider the following criteria as the measures of evaluation (Kumari, *et al.*, 2017; Fu, *et al.*, 2018; Laiphrakpam & Khumanthem, 2017; Shan, *et al.*, 2018; Abundiz-Pérez, *et al.*, 2016; Belazi, *et al.*, 2015; Mondal, *et al.*, 2016):

- *Entropy*: it represents a measure of randomness and it must have a maximum value as possible. The ideal value of entropy is eight.
- *Correlation between Adjacent Pixels*: the correlation between the encrypted image and the original image must be a low as possible. The best correlation value is zero.
- *Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI)*: they stand for an average of the number of the encrypted image-pixels that have changed according to the changed pixel in the original-image. The NPCR and the UACI have values in an interval (0, 1). The ideal value is one and it refers to high security.
- *Large Key Space*: the key of the encryption method must have maximum size to make it resist for a brute-force attack.
- *Key Sensitivity*: the image encryption approach should have more sensitivity for changing in the size of the key and this change must reflect on the encrypted image.
- *Minimum Running-time*: the time complexity of the image encryption is significantly affected the practical applications. Therefore, this time must be a minimum as possible.
- *Histogram Analysis*: a histogram of the image is illustrated the distribution of its pixels at each gray-scale level. The histogram of the original image has a regular distribution while, a good image encryption method must make the encrypted image histogram is distributed uniformly to avoid the statistical analysis.

If the ideal values for the above criteria have been achieved, then the image encryption method can be resisted for attacks such as (statistical, differential, and brute-force).

In this paper, a new method of image encryption has been proposed. This approach is depends on symmetric stream cipher Rivest cipher (RC4) and chaotic system called Rossler system. Based on the experimental results, the proposed scheme has been achieved high security and minimum calculation time. Additionally, the suggested method can resist attacks such as (statistical, brute-force, and differential).

The rest of this paper organized as follows. Section 2 explains the previously image encryption methods. Section 3 clarifies the RC4 and Rossler system. Section 4 illustrates the proposed scheme in detail. Experimental results and discussion will be demonstrated in section 5. Section 6 summaries the conclusions of the suggested approach and indicates the future works followed by references

2. Literature Review

There are several methods of image encryption have

been proposed. These approaches can be classified into three categories: Standard Cryptography Algorithms (SCA), Chaotic Systems (CS) and Hybrid Methods (HM). Amalarethinam & Geetha (2015) have suggested a method of image encryption using SCA. This method based on the Magic Rectangle (MR). An image is divided into blocks of single bytes and each block is substituted with the value of MR. Then, the image is encrypted using public-key cryptosystems such as Rivest, Shamir, and Adleman (RSA) or ElGamal. The contribution of this method has increased the level of security while the limitation of it takes more running time. Rehman *et al.* (2015) have proposed an image encryption based on CS and DNA. The image is divided into blocks and DNA complementary rules are dynamically applied to each pixel of a block during an encoding and decoding process. Then, each block of the image is permuted using Piecewise Linear Chaotic Map (PWLCM) and logistic sequence is used to choose the rules of encoding and decoding for each pixel of the block. According to its experimental results, the proposed method is achieved high resistance against statistical and exhaustive attacks. The limitation of this method, it takes more running time when the size of image less than (512x512).

Arab *et al.* (2019) have suggested a novel image encryption based on HM. An encryption key is obtained by Arnold's chaos sequence. An image is ciphered using the modified Advanced Encryption Standard (AES) algorithm. Experimental results show the proposed method increases the running time while, it resists to the attacks such as differential, brute-force and statistical.

An infrared target encryption approach based on block-cross encryption and Logistic Sine System (LSS) have been proposed an HM by Wen *et al.* (2015). A Partial Differential Equation (PDE) is used to detect the infrared target regions. Then, block-cross encryption that depends on LSS is applied to encrypt the extracted pixels of infrared targets. According to the results, the suggested approach achieves high security and maximum payload capacity for the infrared image, while the time complexity for proposed method is not considered.

Belazi *et al.* (2015) have proposed an image encryption depends on HM. An image is divided into blocks and each block is permuted using Arnold's Cat Map (ACM). Then, a Discrete Wavelet Transform (DWT) is applied on each block to obtain the four sub-bands (Low-low (LL), Low-high (LH), High-low (HL), and High-high (HH)). Next, the LL sub-bands are just selected for encryption using AES. The results show the suggested approach is resistance against differential and statistical attacks, but it runs slowly when the size of the image is increased.

Mandal *et al.* (2014) have suggested the image encryption method using CS. This method is used (128) bits as a secret key and the key is used to generate initial states of Rossler Chaotic System (RCS). Then, the obtained chaotic sequences from RCS are converted into two-dimensional arrays and they XORed with the pixels of the original image. Experimental results illustrate a proposed approach is resisted to statistical attacks while this method has been exposed to cryptanalysis by Laiphrakpam & Khumanthem (2017). To recover the security problem of the encryption key for Mandal *et al.* (2014) method, Laiphrakpam and Khumanthem (2017) proposed the same method with just one modification of using a Secure Hash Algorithm (SHA) for the encryption key. A new method of CS based image encryption has suggested by Tang *et al.* (2019). This approach is based on using two chaotic maps (Henon and Lü). The results of this method show a good level of encryption for the image but it consumes more running time. Fu *et al.* (2018) have suggested a method of image encryption depends on CS. Lü chaotic and logistic map is applied to the plain image for scrambling and shuffling its contents. According to its results, the suggested

method presented more confidentiality for the encrypted image while it needs a lot of time for the encryption and the decryption processes.

Abundiz-Pérez *et al.* (2016) have proposed an approach of image encrypting using CS. The fingerprint image is scrambled using the hyperchaotic Rossler system. Depends on its results, the suggested method achieved high security and resistance against statistical attacks. However, it used a fixed key for the encrypting process. Mondal *et al.* (2016) have suggested a method of image encryption based on SCA. A Linear Feedback Shift Register (LFSR) is used to generate a pseudorandom number for an image permutation process. Then, the result of the permutation process is encrypted using the RC4 stream cipher. The results of the proposed approach show that it resists to brute-force, statistical, and differential attacks. Meanwhile, the limitation of this method is a weakness of RC4 (Jindal & Singh, 2015). Also, LFSR has two problems periodic and predictable (Han & Kim, 2017).

3. Preliminaries:

3.1 Rossler Chaotic System

Some characteristics of a chaotic system have significant importance for the image encryption methods (Abundiz-Pérez, *et al.*, 2016): (i) a simple process able to generate complicated dynamics that produces a pseudorandom string where the secret data can be concealed. (ii) Small changes in the initial states of a chaotic system produces high variations in the output dynamic that can be used for increasing the number of encryption keys.(iii) the encryption histogram maintains the identical distribution for any chaotic string that makes the encryption method resist against statistical attacks.

In 1976, Otto E. Rossler proposed a system of three differential equations with one of them has non-linear term that has a dynamic behavior able to produce chaos. Rossler system can be defined as (Laiphrakpam and Khumanthem, 2017):

$$\frac{dx}{dt} = -y - z \qquad (1)$$

$$\frac{dy}{dt} = x + ay \qquad (2)$$

$$\frac{dz}{dt} = b + z(x - c) \qquad (3)$$

where $(x, y, z) \in \mathbb{R}^3$ are the dynamical variables that defined the phase space, t is a time, and $(a, b, c) \in \mathbb{R}^3$ are the parameters for controlling Rossler system. Also, $(x0, y0, z0) \in \mathbb{R}^3$ are initial states or initial conditions of Rossler system. The Rossler attractor is achieved the chaotic system when the values of (a=0.2, b=0.2, and c= 5.7) (Mandal, *et al.*, 2014). Figure 1 illustrates the Rossler attractor with the initial states (x0=1.9895, y0= 0.6878, and z0= 0.3741).

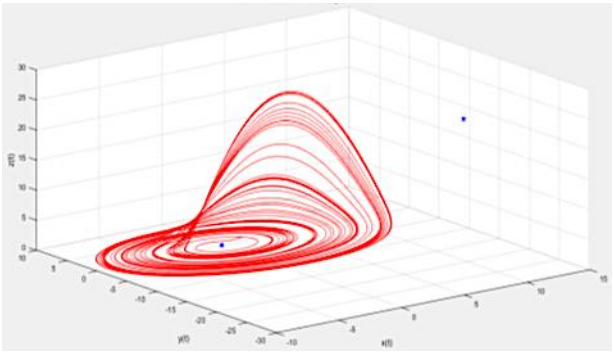


FIG. 1. THE ROSSLER ATTRACTOR

3.2 RC4

RC4 is very simple to implement and fast algorithm of stream cipher that based on symmetric key (Jindal & Singh, 2015). Ron Rivest designed this algorithm in 1987. It is used a variable key from (1-256) bytes. The key generation of RC4 is partitioned into two stages. The first stage is Key Scheduling Algorithm (KSA) and the second stage is Pseudorandom Generation Algorithm (PRGA). Using the key, the KSA is initialized a substitution box (S-box) and then, the PRGA is used to permuted the values of S-box. The values of S-box are XORed with the values of the input image to generate a ciphered image. During the decryption process, the same key is used to generate the S-box and the values of the S-box are XORed with the values of the ciphered image to obtain the original

image as shown in Figure 2.

3.3 The Proposed Scheme

In this section of the paper, the proposed method for image encryption and decryption will be explained in detail. Therefore, the suggested approach is divided into six stages:

- ***The Encryption Key (EK):*** The key has a variable length from (1-256) bytes. This key is used during RC4 encryption process and it used for generating the initial conditions to Rossler Attractor (RA).

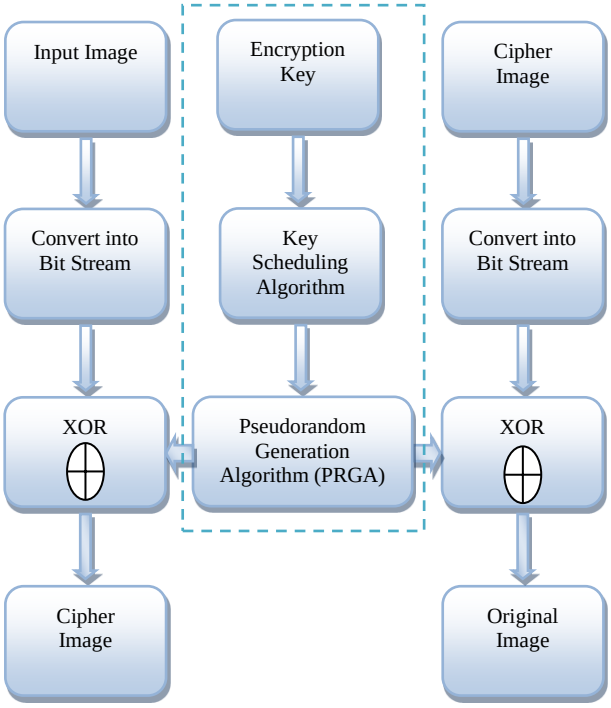


Fig. 2. RC4 Encryption and Decryption

- ***The Initial Conditions:*** The EK is converted from the symbolic representation into American standard code for information interchange (ASCII) values and then these ASCII values are added together to find their summation. Next, the natural logarithm is applied twice to the result of summation to find the value of (x0). The value of (x0) is used to compute the value of (y0) by taking the logarithm for it. Also, the value of (z0) is calculated according to logarithm of (y0). The result of this process is the initial conditions (x0, y0, z0) for RA. For example, if the user is used EK= *%An@[Efficient#+_)2020+e2*. The result of conversion will become as shown in Table 1 and the summation is (1880).

TABLE 1. ASCII VALUES OF EK

37	65	110	64	91
69	102	102	105	99
105	101	110	116	35
43	95	41	50	48
50	48	43	101	50

The value of (x0) is *2.020093136004661*, the value of (y0) is *0.703143617283222*, and the value of (z0) = *0.352194116025971*. In order to avoid the negative values, the absolute function is applied to each result of the logarithm.

The proposed method uses this process for the initial conditions to generate a different value of (x0, y0, and z0) that based on the EK. As mentioned before, the chaotic system has sensitively dependency to initial conditions.

- ***Image Encryption Using RC4***: During this stage, a plain image is encrypted according to the EK and RC4 stream cipher. The result of this stage is a ciphered-image.
- ***Image Ciphering Using RCS***: The ciphered image is used as an input for the RCS. Initially, the parameters of system (a, b, and c) and the initial conditions (x0, y0, and z0) are employed as the inputs for the Rossler system to produce an array of random-values. As mentioned before, the Rossler system has three differential equations. Therefore, the Runge-Kutta method is used to solve it by applying the following equations (Fu, *et al.*, 2018):

$$K1 = h * f(t, x) \quad (4)$$

$$K2 = h * f\left(t + \frac{h}{2}, x + \frac{k1}{2}\right) \quad (5)$$

$$K3 = h * f\left(t + \frac{h}{2}, x + \frac{k2}{2}\right) \quad (6)$$

$$K4 = h * f(t + h, x + k3) \quad (7)$$

$$x = x + \frac{(k1 + 2 * k2 + 2 * k3 + k4)}{6} \quad (8)$$

where a step-size is $h = 0.05$ and f is a function that

has two parameters (t, x), t is a time and x is unknown value that is approximately calculated by each iteration of the Runge-Kutta method. Additionally, $K1$ stands for the increment that uses x and it depends on the slope at the starting of the period. $K2$ refers to the increment which is based on the slope at the mid-point of the interval and it employs $K1$ and x. $K3$ is also the increase that depends on the tendency at the mid-point and it uses $K2$ and x. Finally, $K4$ is the increment which is based on the slope at the end of the interval using $K3$ and x. The final value of x is computed by equation (8). After solving the Rossler system using the Runge-Kutta method and by initializing the other parameters of it, the result is a 2-dimensional array that has three rows and multi columns. The first row represents the values of x, the second row holds the values of y, and the last row contains the values of z.

In this paper, the proposed method uses the values of x and it takes the number of x values that equal to the size of the ciphered image *CI*. For example, if the size of *CI* is (512x512). That means, the number of the x values that will be taken is $512 * 512 = 262144$. The ciphered image has values in range [0-255] while the values of x are floating-point values. Therefore, these values must be modulated in range [0-255] and the following equation is applied for each value of x:

$$x'(i,j) = mod(x(k) * 100000,256) \qquad (9)$$

where x' is a new 2-dim array that has size similar to the size of *CI*, $1 \le i \le 512$, $1 \le j \le 512$, $1 \le k \le 262144$ and mod is a modulo operator. Finally, the following formula is applied to ciphering *CI* using the Rossler chaotic system:

$$CI'(i,j) = CI(i,j) \oplus x'(i,j) \qquad (10)$$

where CI' is the final ciphered-image. The block diagram for the image encryption is demonstrated in Figure 3.

- ***Image Deciphering Using RCS***: The same values of the system parameters (a, b, and c) and the initial conditions (x0, y0, and z0) that are generated from the EK are employed to the RCS to generate x'. Then, the equation (10) is used to deciphered the image.
- ***Image Decryption Using RC4***: The same encryption key is used for the decryption process because of the RC4 is symmetric encryption method. The resulted image of RCS is decrypted using RC4 to obtain the original image as shown in Figure 4.

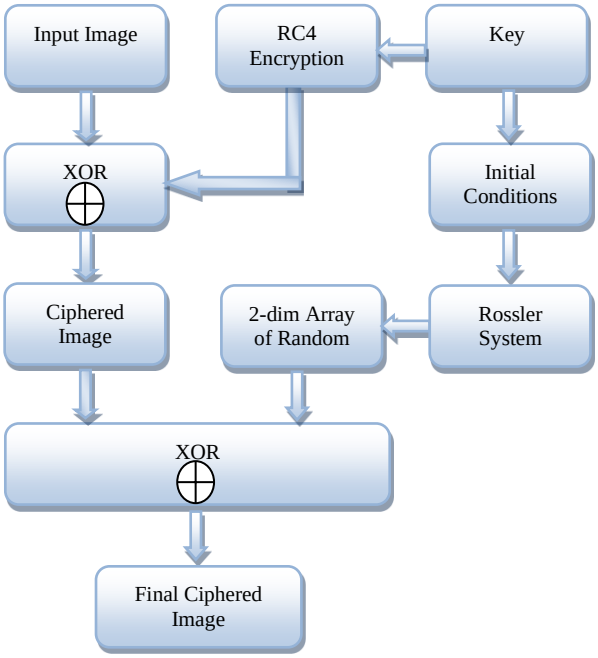


FIG. 3. THE BLOCK DIAGRAM OF IMAGE

4. Experimental Results and Discussions

In this section of the paper, the proposed method has been implemented using MatlabR2019b that is installed on Sony Vaio laptop, Intel Core (i3) CPU 1.9 GHz, 4 GB RAM, and Microsoft Windows 10 Home 64-bit operating system. Therefore, the suggested method has been evaluated its performance according to different attacks like (brute-force, differential, and statistical) and other criteria that are used to evaluate the image encryption methods. The set of grayscale images of size (512x512) that are frequently employed for testing the image encryption approaches are shown in Figure 5. Using EK= *%An@[Efficient#+_)2020+e2*

and the values of the initial conditions [*x0, y0, z0*] = [*2.020093136004661, 0.703143617283222, 0.352194116025971*] respectively, the set of the images have been encrypted by applying the proposed scheme and the results of the encryption process have been shown in the Figure 6. According to Figure 6, all encrypted-images are randomly scrambled and they are converted into illegible form.

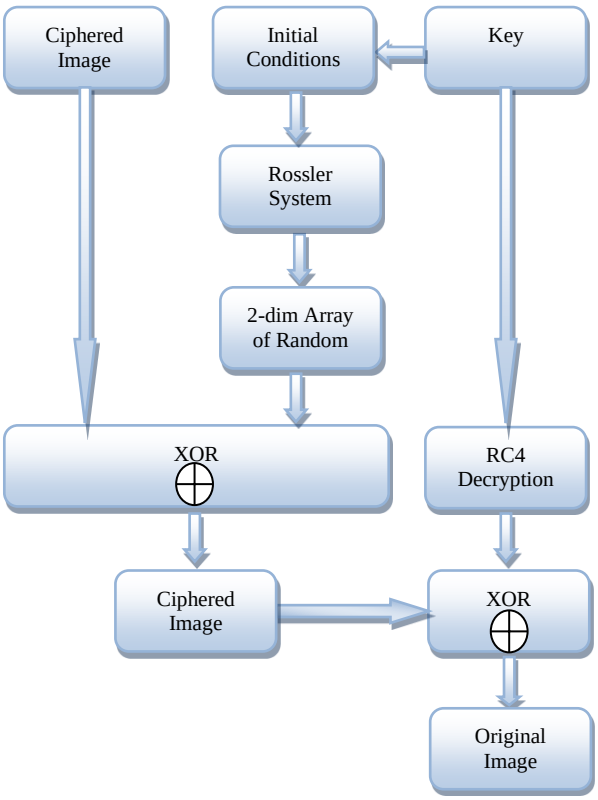


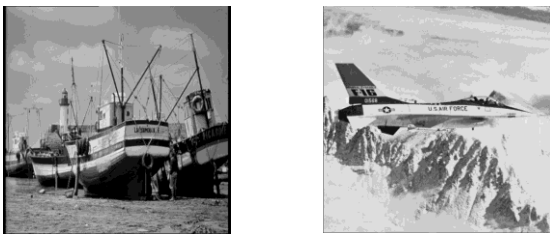
FIG. 4. THE BLOCK DIAGRAM OF IMAGE

Generally, the evaluation of image encryption methods must pass from the following analyses.

- ***Entropy-based Analysis:***

  Information entropy can be defined as the grade of uncertainty that is concerned with a random occurrence (Mondal, *et al.,* 2016). It used as a measurement to amount of information that exists in the occurrence. The entropy value is increment according to randomness or uncertainty. Consequently, it uses in different domains like statistical inference, cryptography, and data compression.

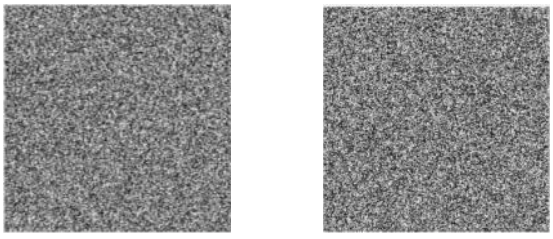
(a) Lena (b) Baboon



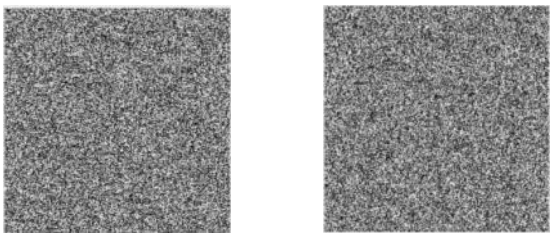
(c) Boats (d) Airplane

(e) Penguin (f) Koalas

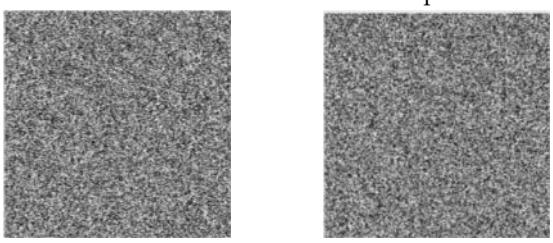
FIG. 5. THE SET OF TEST IMAGES



(a) Encrypted-image Lena (b) Encrypted-image Baboon



(c) Encrypted-image Boats (d)Encrypted-image Airplane



(e) Encrypted-image Penguin (f) Encrypted-image Koalas

FIG. 6. THE SET OF ENCRYPTED-IMAGES

If the encrypted-image has a high value of entropy, that means it will be resist to the entropy-based attack. The information entropy is computed by equation:

$$H(S) = -\sum_{i=0}^{N-1} P(s_i).\,\mathrm{Log}_2\, P(s_i) \qquad (11)$$

where $H(S)$ is a value of entropy for the encrypted-image, N is the overall number of symbols, $s_i \in S$ and $P(s_i)$ is the probability of the symbol s_i. The grayscale image has values in range [0-255], the maximum value of entropy is eight. The set of test images have been separately encrypted and the entropy for each encrypted-image has been calculated. Additionally, the total time that is needed to encrypted each image and the total time which is required to decrypted each image are computed using (*Seconds*) as a unit of the time, as shown in Table 2.

TABLE 2. THE ENTROPY, ENCRYPTION TIME, AND DECRYPTION TIME VALUES OF THE CIPHERED-IMAGES

Image	Entropy	Encryption Time (Second)	Decryption Time (Second)
Lena	7.9993	2.44	2.95
Airplane	7.9993	2.43	3.19
Baboon	7.9993	2.39	3.02
Boats	7.9993	2.39	3.15
Penguin	7.9992	2.41	2.82
Koalas	7.9993	2.35	2.90

According to the values of Table (2), the proposed scheme achieves high values of entropy for all encrypted-images that are approximately (≈8) and it resists to entropy-based attack. Also, the suggested method needs a little calculation time.

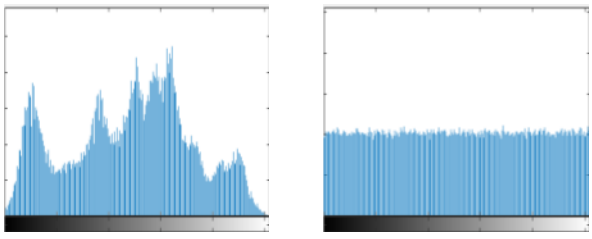
- ***Histogram Analysis:***

  Image encryption methods must have uniformly distributed histogram for the encrypted-image to be resistance against the statistical attack (Abundiz-Pérez, *et al.*, 2016). Figure 7 is demonstrated the histogram for each test image (before the encryption process and after the encryption).

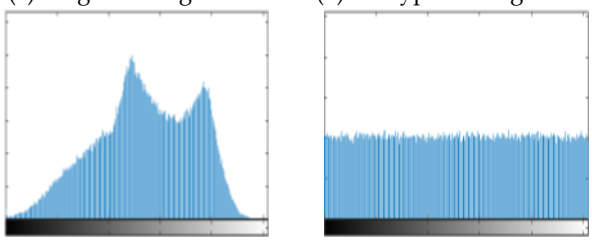
  Based on results of Figure 7, the proposed scheme presents a uniform-distributed histogram for all encrypted-images and it is able to resist against the statistical attack. In addition, the uniformity-distributed histogram is used to avoid any statistical information about the encrypted-image to the adversary (Laiphrakpam & Khumanthem, 2017).

- ***Key Sensitivity Analysis:***

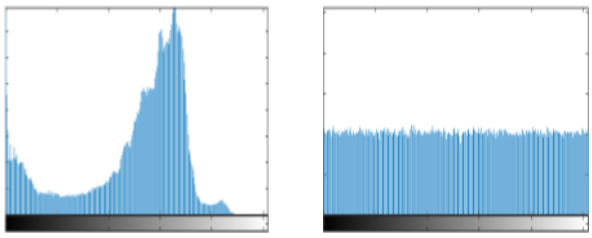
  The proposed method is mainly depends on the encryption key due to this key is used by RC4 for encrypting the image and it employed to generate the initial conditions of Rossler chaotic system. Additionally, any image encryption method must be sensitive to the alteration in the encryption key in order to be able resist against brute-force attack (Mandal, *et al.*, 2014). Consequently, any change (even slightly change) in the encryption key must be affected the entire image and it should generate a different encrypted-image.



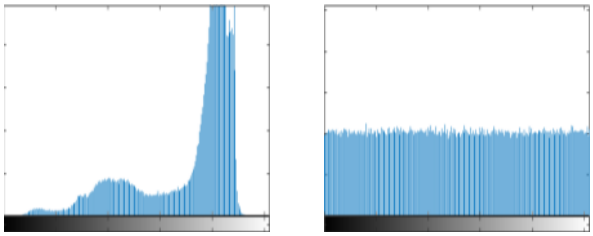
(a) Original-image Lena (b) Encrypted-image Lena



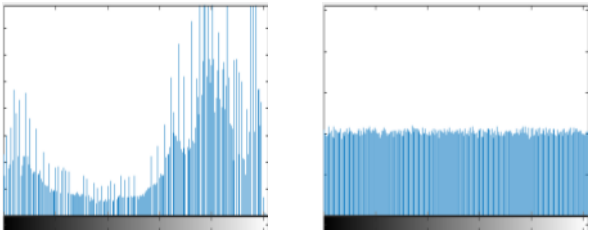
(c) Original-image Baboon (d) Encrypted-image Baboon



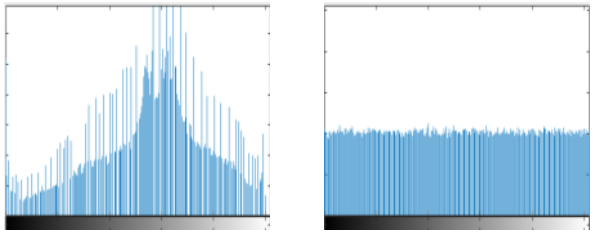
(e) Original-image Boats (f) Encrypted-image Boats



(g) Original-image Airplane (h) Encrypted-image Airplane



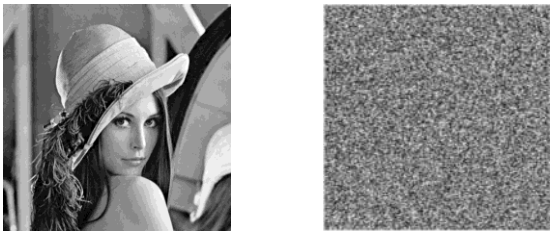
(i) Original-image Penguin (j) Encrypted-image Penguin



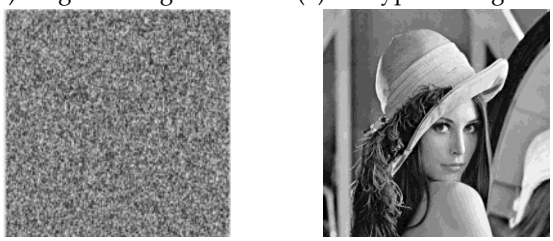
(k) Original-image Koalas (l) Encrypted-image Koalas

FIG. 8. THE HISTOGRAM FOR EACH ORIGINAL IMAGE AND ITS ENCRYPTED-IMAGE

In order to evaluate the performance of proposed method against this type of attack, the plain image (Lena) has been encrypted using the EK= *%An@[Efficient#+_)2020+e2* and the values of the initial conditions [*x0, y0, z0*] = [*2.020093136004661*, *0.703143617283222*, *0.352194116025971*] respectively. Then, during the image decryption process, the encryption key has been changed into EK = *%An@[Efficient#+_)2020+e* by removing the last number (2) from it and the initial conditions also have been changed into [*x0, y0, z0*] = [*2.012966694810439*, *0.699609601468841*, *0.357232811705393*]. The result of this change in the encryption key, it leads to generate a different encrypted-image as shown in Figure 8.



(a) Original-image Lena (b) Encrypted-image Lena



(c) Decrypted-image Lena with changed EK (d) Decrypted-image Lena with unchanged EK

FIG. 8. THE RESULTS OF KEY SENSITIVITY

Depends on the results of Figure 7, the proposed method has ability to resistance against the brute-force attacks. Additionally, it ensures the protection versus known plain-text attacks.

- ***Key Space Analysis:***

  An essential requirement of all types of cryptography algorithms is the key. According to Kerckhoffs' principle (Alvarez & Li, 2006), the security of a cryptographic system must completely depends on its key only, even if it is well designed or strong. When the key is weakly selected or the key size is very small, the cryptographic system can be simply broken.

  The proposed scheme depends on the encryption key of RC4. This key is a variable key from (1-256) byte, typically between (5) bytes and (16) bytes. Therefore, the suggested approach can be used (16) bytes that is equal to (2^{128}) bits. In addition, RC4 key is employed to produce the initial conditions for RCS. Each variable of the initial conditions [x0, y0, and z0] has size 10^{16}. The key space for the suggested method can be computed as follows: $10^{16}\times10^{16}\times10^{16}=10^{48}$ and 2^{128}, that means, the total size of key is ($10^{48}\times2^{128}$). According to (Alvarez & Li, 2006) the key size must be greater than (2^{100}) for image encryption method in order to be resisted

brute-force attack. Consequently, the proposed approach is able to resist the exhaustive attack.

- ***Differential Analysis:***

  This analysis is applied to test the resistance of suggested approach versus the differential attack. The adversary can use this attack to determine the relation between same plain images and find the encryption key in case of the encryption algorithm is weak (Abundiz-Pérez, *et al.,* 2016). The differential analysis can be implemented between two same images by changing only one pixel. Then, these two images are encrypted by employing the same encryption key. Finally, the encrypted-images are compared according to two parameters. The first parameter is NPCR that is used to compute a precision of the number of changed pixels during the image encryption process. The second parameter is UACI, which is employed to find intensity for the unified average of the changed pixels. The NPCR and UACI values can be calculated by equations:

$$Diff(x,y) = \begin{cases} 0, & CI_1(x,y) = CI_2(x,y) \\ 1, & CI_1(x,y) \neq CI_2(x,y) \end{cases} \quad (12)$$

$$NPCR = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} Diff(x,y)}{M \times N} \times 100\% \quad (13)$$

$$UACI = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} |CI_1(x,y) - CI_2(x,y)|}{L \times M \times N} \times 100\% \quad (14)$$

where $Diff$ is 2-dim array of the difference that has size equal to the size of the encrypted-image, CI_1 is the original encrypted-image, CI_2 is the modified encrypted-image, $1 \leq x \leq M, 1 \leq y \leq N$, and $L = 255$ is the maximum value of the grayscale image. Therefore, the differential analysis has been applied for all test-images. Each original test-image has been changed just one-pixel value at different position of it and the modified version of the test-image has been saved in another name. Then, these two images have been individually encrypted for computing the NPCR and UACI values. Table 3 is tabulated the values of NPCR and UACI for all test images.

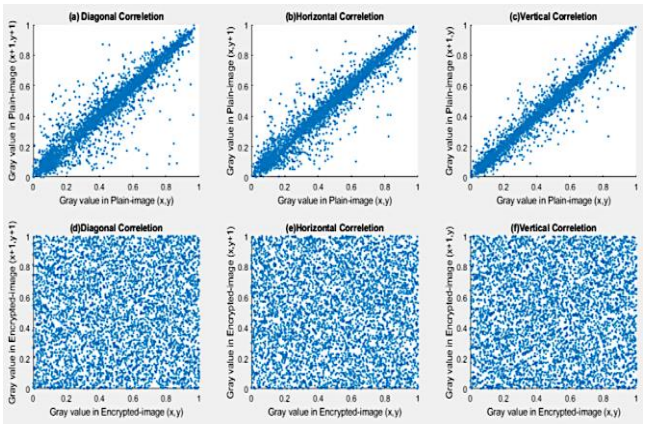


FIG. 9. DIAGONAL, HORIZONTAL, AND VERTICAL CORRELATION DISTRIBUTION OF THE PLAIN IMAGE, DIAGONAL, HORIZONTAL, AND VERTICAL CORRELATION DISTRIBUTION OF THE ENCRYPTED-IMAGE,

Generally, the plain image has a high correlation between adjacent pixels. Consequently, the image encryption method must decrease the correlation to increase the resistance versus the statistical attacks (Abundiz-Pérez, *et al.,* 2016). Figure 9 is illustrated diagonal, horizontal, and vertical correlation distribution of the plain image and diagonal, horizontal, and vertical correlation distribution for the encrypted-image. Correlation coefficient can be calculated by equations:

$$M(a) = \frac{1}{N}\sum_{i=1}^{N} a_i \, , M(b) = \frac{1}{N}\sum_{i=1}^{N} b_i \quad (15)$$

$$V(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i - M(a))^2 \quad (16)$$

$$V(b) = \frac{1}{N}\sum_{i=1}^{N}(b_i - M(b))^2 \quad (17)$$

$$cov(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i - M(a))\big(b_i - M(b)\big) \quad (18)$$

$$R_{ab} = \frac{cov(a,b)}{\sqrt{V(a)} \times \sqrt{V(b)}} \quad (19)$$

where a and b are the values of two-adjacent pixels. M is the mean, V is the variance, cov is the covariance, and R_{ab} is the correlation coefficient.

Table 4 is listed the values of correlation of (5000) pixels that are randomly chosen from the plain image and encrypted-image (Lena). Based on the values of Table 4, the correlation of plain image is

close to one, which means there is a high correlation. However, the encrypted-image has a correlation near to zero, which is indicated to low correlation. Consequently, the proposed approach can be resisted versus the statistical attack.

- ***Comparison with Other Works:***

  Finally, the proposed method has been compared with other similar methods in order to evaluate its performance. Therefore, the comparison has been applied among the proposed method, method of Laiphrakpam and Khumanthem, (2017), and approach of Mondal, et al., (2016) due to following criteria (key space, entropy, NPCR, and UACI). Table 5 is listed the values of performance comparison. Based on the results of Table 5, the suggested approach has been achieved best values over the other methods.

TABLE 3. THE NPCR AND UACI VALUES FOR ALL TEST IMAGES

Image Name	Position (x,y)	Pixel Value		NPCR (%)	UACI (%)
		Original	Modified		
Lena	(128,128)	204	205	99.61	33.46
Baboon	(128,128)	160	161	99.61	33.46
Airplane	(128,128)	198	199	99.61	33.46
Boats	(256,256)	91	92	99.61	33.46
Penguin	(256,256)	25	26	99.61	33.46
Koalas	(256,256)	80	81	99.61	33.46

TABLE 4. THE CORRELATION COEFFICIENT VALUES FOR PLAIN IMAGE AND ENCRYPTED-IMAGE

Image	Diagonal Correlation	Horizontal Correlation	Vertical Correlation
Plain	0.9580	0.9736	0.9848
Encrypted	-0.0016	0.0249	0.0042

5. Conclusions

In this paper, a new approach of image encryption has been proposed. This method combines RC4 with RCS. According to experimental results, the suggested method has been achieved high resistance versus different attacks. Also, it has been increased the size of the encryption key. Finally, RC4 has been disposed from its weakness

Table 5. The performance comparison among the suggested approach, method of Laiphrakpam and Khumanthem, (2017), and approach of Mondal, et al., (2016)

Image	Proposed Scheme				Method of Laiphrakpam and Khumanthem, (2017)				Method of Mondal, et al., (2016)			
	Key Space	Entropy	NPCR	UACI	Key Space	Entropy	NPCR	UACI	Key Space	Entropy	NPCR	UACI
Boats	$10^{48} \times 2^{128}$	7.9993	99.61	33.46	10^{48}	7.9993	99.61	33.47	2^{92}	N/A	N/A	N/A
Airplane		7.9993	99.61	33.46		7.9993	99.63	33.48		N/A	N/A	N/A
Penguin		7.9992	99.61	33.46		N/A	N/A	N/A		7.9536	99.58	27.42
Koalas		7.9993	99.61	33.46		N/A	N/A	N/A		7.9569	99.56	19.57

6. References

Abundiz-Pérez, F., Cruz-Hernández, C., Murillo-Escobar, M., López-Gutiérrez, R. and A. Arellano-Delgado, A. (2016). A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map. Hindawi:Mathematical Problems in Engineering, 2016:1-15.

1. Alvarez, G. and Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, 16(8): 2129-2151.
2. Amalarethinam, D. and Geetha J. (2015). Image Encryption and Decryption in Public Key Cryptography Based on MR. Proceedings of 2015 IEEE International Conference on Computing and Communications Technologies (ICCCT'15), Chennai, India.
3. Arab, A., Rostami, M. and Ghavami, B. (2019). An Image Encryption Method Based on Chaos System

and AES Algorithm. Springer, The Journal of Supercomputing, 75(10):6663–6682.

4. Belazi, A., El-Latif, A., Rhouma, R. and Belghith, S. (2015). Selective Image Encryption Scheme Based on DWT, AES S-Box and Chaotic Permutation. Proceedings 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, Dubrovnik, Croatia.
5. Belazi, A., Rhouma, R. and Belghith, S. (2015). A Novel Approach to Construct S-Box Based on Rossler System. IEEE, Proceedings 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), 611-615, Dubrovnik, Croatia.
6. Dixit P., Gupta A., Trivedi M. and Yadav V. (2018) Traditional and Hybrid Encryption Techniques: A Survey. In: Perez G., Mishra K., Tiwari S. and Trivedi M. (Ed.) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, 4: 239-248, Springer, Singapore.
7. Fu, C., Zhang, G., Zhu, M., Chen, Z. and Lei, W. (2018). A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy. Hindawi: Security and Communication Networks, 2018:1-13.
8. Han, M. and Kim, Y. (2017). Unpredictable 16 bits LFSR-based True Random Number Generator. IEEE: Proceedings 2017 International SoC Design Conference (ISOCC) 284-285, Seoul, South Korea.
9. Jawad, L. and Sulong, G. (2015). A Survey on Emerging Challenges in Selective Color Image Encryption Techniques. Indian Journal of Science and Technology, 8(27):1-12.
10. Jindal, P. and Singh, B. (2015). RC4 Encryption-A Literature Survey. Elsevier: Procedia Computer Science, 46(2015): 697-705.
11. Kumari, M., Gupta, S. and Sardana, P. (2017). A Survey of Image Encryption Algorithms. Springer: 3D Display Research Center, 8(37):1-35.
12. Laiphrakpam, D. and Khumanthem, M. (2017). Cryptanalysis of Symmetric Key Image Encryption Using Chaotic Rossler System. Elsevier: Optik, 135(2017): 200–209.
13. Mandal, M., Kar, M., Singh, S. and Barnwal, V. (2014). Symmetric Key Image Encryption Using Chaotic Rossler System. Wiley: Security and Communication Networks, 7(11): 2145–2152.
14. Mondal, B. Sinha, N. and Mandal, T. (2016). A Secure Image Encryption Algorithm Using LFSR and RC4 Key Stream Generator. In: Nagar A., Mohapatra D. and Chaki N. (Ed.) Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. Smart Innovation, Systems and Technologies, 43: 227-237, Springer, New Delhi.
15. Rehman, A., Liao, X., Kulsoom, A., and Abbas, S. (2015). Selective Encryption For Gray Images Based on Chaos and DNA Complementary Rules. Springer, Multimedia Tools Application, 74(13): 4655–4677.
16. Shan, Y., He, M., Yu, Z. and Wu, H. (2018). Pixel level Image Encryption Based on Semantic Segmentation. IEEE, Proceedings 2018 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), 147-153, Prague, Czech Republic.
17. Tang, Z., Yang, Y., Xu, S., Yu, C. and Zhang, X. (2019). Image Encryption with Double Spiral Scans and Chaotic Maps, Hindawi: Security and Communication Networks, 2019:1-15.
18. Wen, W., Zhang, Y., Fang, Z. and Chen, J. (2015). Infrared Target-based Selective Encryption by Chaotic Maps. Elsevier, Optics Communications, 341: 131–139.