Image Encryption Based on Improved Rössler Hyperchaotic Map

Eduardo Rodríguez Orozco, E. Efren García Guerrero, Everardo Inzunza González, Oscar R. López Bonilla

Autonomous University of Baja California, Faculty of Engineering, Architecture and Design. Carretera Transpeninsular Ensenada-Tijuana 3917, Colonia Playitas. Ensenada, B.C., México, 22860.

{eduardo.rodriguez.orozco, eegarcia, einzunza, olopez}@uabc.edu.mx

2014 Published by $\mathcal{DIFU}_{100}ci@$ http://nautilus.uaz.edu.mx/difu100cia

Abstract

This article presents a cryptosystem encryption of digital images, efficient and secure. All the complexity of the encryption process rests on the improved chaotic dynamics of the Rössler hyperchaotic map. The algorithm implemented follows the principles of Kerckhoffs and Shannon of cryptography. From the results obtained experimentally and its security analysis, is shown that the proposed method is strong and safe. The proposed cryptographic scheme is simple, with high levels of security and of easy physical implementation, which together with the large key space that contains, makes it potentially attractive for applications in private communication systems.

Keywords: Chaotic encryption, hyperchaotic map, image encryption, security analysis

1. Introduction

In recent years, owing to frequent flow of digital images across the world over the public transmission media, it has become essential to secure them from leakages. During the last decade, numerous encryption algorithms have been proposed in the literature on different principles. Among them, chaos based encryption technique are considered good for practical use. Chaotic signals have apparently stochastic behavior and are characterized by a high bandwidth in the frequency spectrum. M.S. Baptista [1] has used chaotic signals to encrypt information, in order to transmit secret messages safely. Chaos and cryptography have some properties in common; the most important is the sensitivity to small changes in initial conditions. G. Giuseppe *et al.* [2] and L. Kocarev *et al.* [3] have used the chaos in the cryptosystem design. The common characteristic of secure communications schemes based on chaos is that they employ a chaotic signals to transmit confidential information.

The cryptographic schemes based on chaos that have been reported in recent years are many and varied [4]-[22]. Although many strategies and methods to develop efficient algorithms have been explored and despite the interest and effort in the subject, the security to transmit confidential information through a public channel remain the most important problem to solve.

This paper present a cryptosystem of digital images of simple structure. This is achieved thanks that the essence of the encryption process is based only on the improved chaotic dynamics of the Rössler hyperchaotic system [23]. Because of the complexity manifested by the improved chaotic system, it is not necessary any other operation or manipulation of information to be encrypted, which makes the proposed algorithm be simple and the same time efficient. The security and performance of the hyperchaotic encryption technique proposed is evaluated, using the most common methods of security analysis: *a*) *Statistical analysis*: it is obtained the image histograms of each stage of the encryption process, *b*) *Correlation analysis of pixels*: it is obtained the scatter plots between adjacent pixels (diagonal, vertical and horizontal), evaluating their correlation coefficients. *c*) *Differential attack*: it evaluates the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), and *d*) *Information entropy*: the value $H(s)$ is calculated. From the results obtained, it is suggested that this technique of the digital image hyperchaotic encryption is robust, safe and easy to implement, which together with a large key space that contains, make it highly viable to application over safe image communication systems.

The organization of this work is the following: **Section 2** presents a brief description of the improved hyperchaotic Rössler map and the proposed encryption algorithm. **Section 3** shows a description of the techniques of security analysis. **Section 4** presents the results obtained with the security and speed analysis. Finally, **Section 5** presents the conclusions of this work.

2. Proposed encryption algorithm

2.1. Improved Rössler hyperchaotic map

We propose the following improved hyperchaotic map described by Eqs. (1), and inspired by the Rössler hyperchaotic map [23].

$$\begin{aligned}
x_1(k+1) &= C(\alpha x_1(k)(1-x_1(k)) - \beta(x_3+\gamma)(1-2x_2(k)))mod1,\\
x_2(k+1) &= C(\delta x_2(k)(1-x_2(k)) + \zeta x_3(k))mod1,\\
x_3(k+1) &= C(\eta((x_3(k)+\gamma)(1-2x_2(k))-1)(1-\theta x_1(k)))mod1,
\end{aligned} \tag{1}$$

where $\alpha = 5, \beta = 1, \gamma = 3, \delta = 7, \zeta = 8, \eta = 5, \theta = 6$ and $C = 1 \times 10^7$. The initial conditions used are: $x_1(0) = 0.1$, $x_2(0) = 0.15$ and $x_3(0) = 0.01$. Figs. 1a) (top) and 1b) (bottom) shows the frequencies spectrums of the states x_1, x_2 and x_3 of the original and improved Rössler system, respectively. For the original map Fig. 1a), shows that the states x_1 and x_2 have very similar spectral components and that frequencies above 30 KHz are wider, whereas the state x_3 contains small amplitude spectral components. Furthermore, as can be see in Fig. 1b) the improving effect of the spectral behavior of the three original states x_1, x_2 and x_3, which present uniform and continuous potency values [24]. Under these conditions the improved hyperchaotic system exhibits an almost random behavior, similar to noise signals, which is highly beneficial to the process of information encryption.

Fig. 2a) presents the strange attractor generated by the original Rössler hyperchaotic map, and Fig. 2b) presents the strange attractor produced by the improved Rössler hyperchaotic map proposed in this paper. It can be seen in the improved attractor that the points are scattered throughout the 3D space, which is very desirable in all cryptosystems, due to the wide scattering with random appearance.

A more global perspective of the original map behavior and the Rössler improved map defined by Eqs. (1), is evident from their bifurcation diagrams. For example, Fig. 3a) correspond to the bifurcation diagram of the Rössler hyperchaotic map [24] where $0 \leq \alpha \leq 4$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.2$, $\eta = 0.1$ and $\theta = 1.9$. It is noted that for $3.5 \leq \alpha \leq 3.9$ the map exhibits its hyperchaotic dynamics, however, when $\alpha > 3.9$ the map becomes unstable.

Fig. 3b) corresponds to the bifurcation diagram of the improved Rössler map defined by Eqs. (1), for $0 \leq \alpha \leq 50$, $\beta = 1$, $\gamma = 3$, $\delta = 7$, $\zeta = 8$, $\eta = 5$, $\theta = 6$ and $C = 1 \times 10^7$. It is observed that there are more areas where for different values of α, the map retains its hyperchaotic dynamics, without becoming unstable.

The corresponding values of the Lyapunov exponents of the system (1) evaluated are [24]: 0.008114, 0.006882 and 0.009371. This shown that the improved Rössler map is hyperchaotic [25].

2.2. Encryption algorithm

Given the properties manifested by the improved Rössler hyperchaotic map described by Eqs. (1), and which become evident in Figs. 1*b*), 2*b*) and 3*b*), it is proposed the cryptosystem shown in Fig. 4. The proposed cryptosystem is simple, fast and efficient, since the complexity of the encryption process lies in the hyperchaotic nature of the carrier signal, which is generated to encrypt the information. Furthermore, the Rössler hyperchaotic map comprises 7 parameters: $\alpha, \beta, \gamma, \delta, \zeta, \eta, \theta$, and 3 initial conditions: $x_1(k), x_2(k)$, $x_3(k)$, so that its key space is of 2^{524} [9, 10, 26], which makes it a robust enough cryptosystem against brute force attacks. Under these conditions, the proposed cryptosystem purses the Kerckhoffs and Shannon cryptography principles: *the security system must lie in the security of the key, supposing already known the rest of the parameters of the cryptosystem* [27]-[29].

Referring to Fig. 4, the cryptosystem requires two inputs, the first is the image to encrypt "Lena" and the

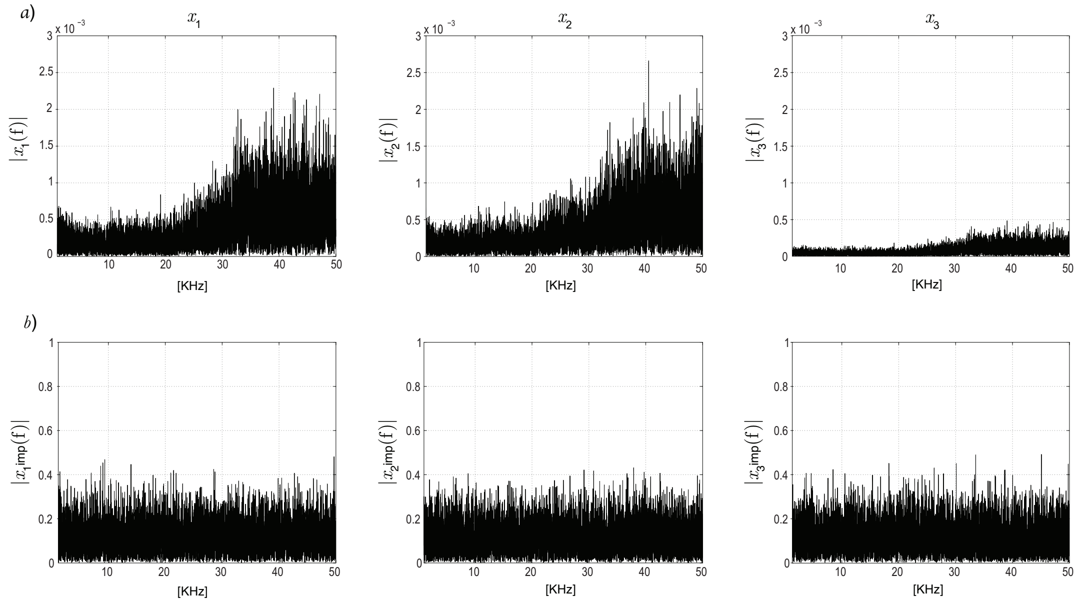

Figure 1. Frequencies spectrums of states x_1, x_2 and x_3. Top: *a*) original Rössler hyperchaotic map. Bottom: *b*) improved Rössler hyperchaotic map.

second is the encryption key ($\alpha, \beta, \gamma, \delta, \zeta, \eta, \theta, x_1, x_2$ and x_3). The original image is a matrix of numbers (a_{ij}), with $i = 1, ..., m$ and $j = 1, ..., n$, that is changed to a column vector (a_{l1}), with $l = m \times n$. Each number correspond to the gray level of each pixel image. Once the encryption key is known the hyperchaotic sequences are generated from the improved Rössler hyperchaotic map, Eqs. (1). An adjustment is made to the obtained hyperchaotic sequences, which involve a change of scale to obtain integers numbers of 8 bits. This is obtained from the operation $x_{im}(k) = Cx_i(k)\ mod\ 255$, with $C = 1 \times 10^7$ and $i = 1, 2, 3$, i.e., we can use any state how hypercaotic sequence. Finally the XOR operation is performed with the output $x_{im}(k)$ and each pixel of the image (a_{l1}), thereby obtained the cryptogram of the original image. Finally, the cryptogram can be send by public channel like internet.

2.3. Decryption algorithm

Fig. 5 shown the decryption diagram proposed. Basically it is the reverse of the encryption process (Fig. 4). The cryptogram is received by some channel public, for example the internet and the key used for encryption is typed (the same initial conditions and parameters), XOR operation is performed between the cryptogram and improved chaotic sequence. Finally we get the original image.

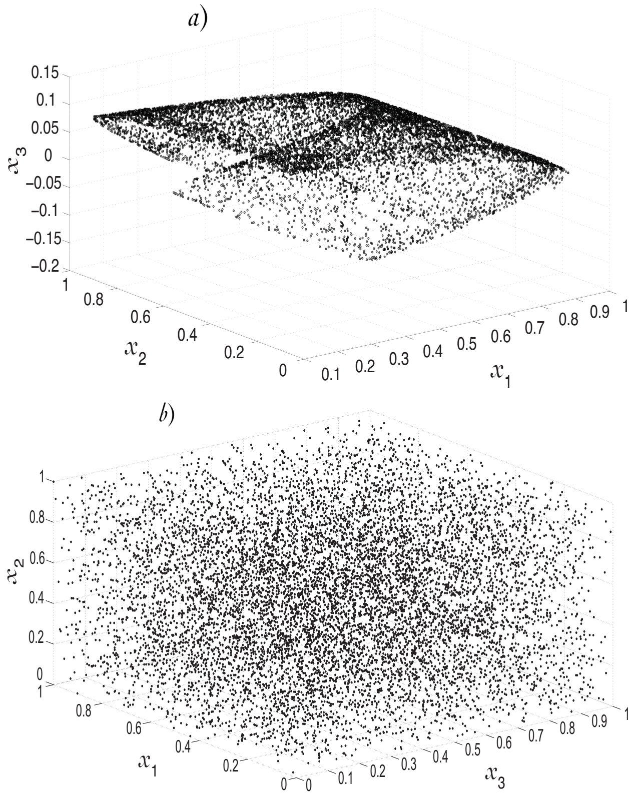

Figure 2. Strange attractor of the Rössler hyperchaotic map: *a*) original Rössler hyperchaotic map, *b*) improved Rössler hyperchaotic map.

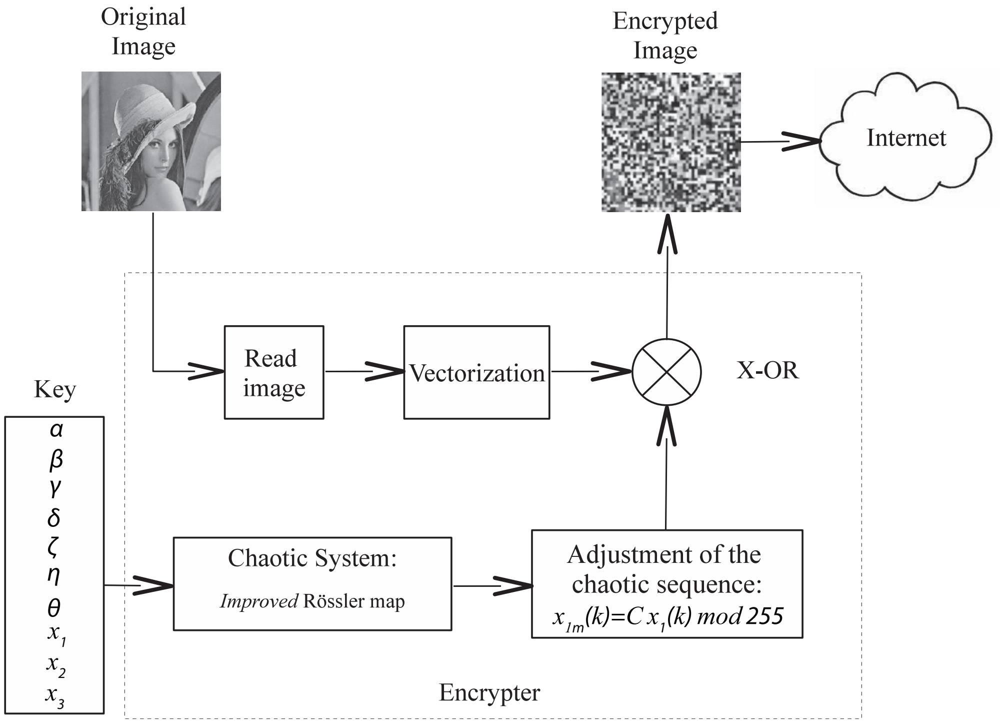

Figure 4. Block diagram of the hyperchaotic encrypter.

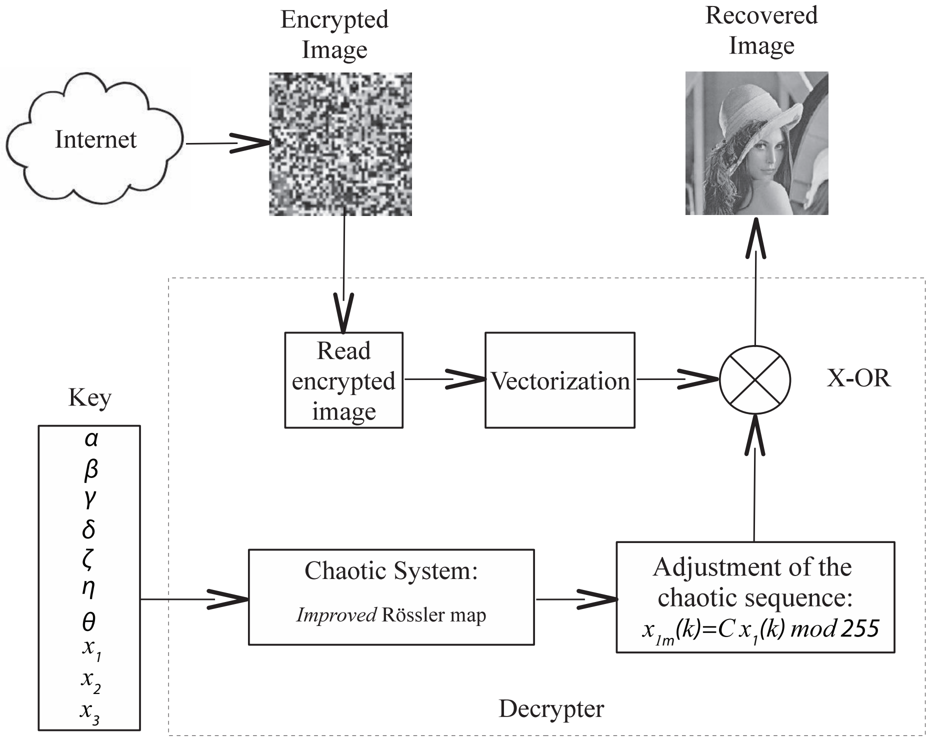

Figure 5. Block diagram of the hyperchaotic decrypter.

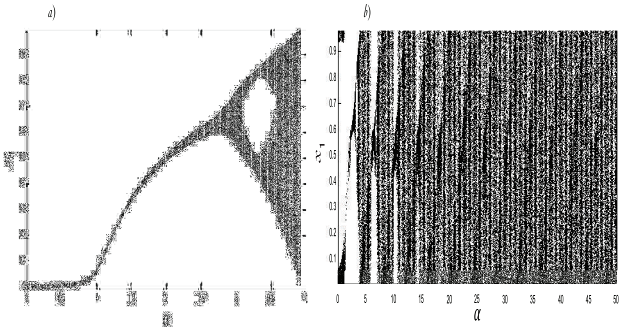

Figure 3. Graph of bifurcation in α of the Rössler hyperchaotic map: *a*) original Rössler hyperchaotic map, *b*) improved Rössler hyperchaotic map .

3. Security analysis

From the image to analyze, either the original image or the cryptogram, at least 1000 pairs of adjacent pixels are taken (horizontally, vertically or diagonally) and their correlation coefficients [4] respectively are calculate, using the following equations:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{2}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{3}$$

where $cov(x,y)$ is the covariance, $D(x)$ is the variance, x and y denotes the values in the gray scale of the image under analysis. For our calculations based on numerical computation, we use the following equation in discrete form:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{4}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{5}$$

where $E(x)$ is the average value of gray levels of the pixels.

3.1. Differential attacks

To perform differential analysis attacks [4] and understand the differences between the encrypted images using two common measures NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). These measures are used to test the influence of change of a pixel in the whole encrypted image.

Number of pixels change rate (NPCR) [4, 19, 22] Measures the percentage of the number of pixels between two different images and it can be calculated using the following expression:

$$NPCR = \frac{\sum_{i,j} \varDelta(i,j)}{W \times H} \times 100\%, \tag{6}$$

where $\varDelta(i,j)$ is a binary arrangement: $\varDelta(i,j) = 0$, if $C_1(i,j) = C_2(i,j)$, or $\varDelta(i,j) = 1$, when $C_1(i,j) \neq C_2(i,j)$. C_1 and C_2 are encrypted images obtained with very similar keys (initial conditions). W and H define the size of the image under analysis.

Unified average changing intensity (UACI) [4, 19, 22]
Measures the average intensity of the difference between the two encrypted images (C_1 and C_2), using the expression:

$$UACI = \frac{1}{W \times H}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{7}$$

where C_1, C_2, W and H have the same meaning as in Eq. (6).

3.2. Information entropy

In 1949, Claude E. Shannon [28, 29] introduced the mathematical foundations of Theory of the Information applied to communication and data storage. The information entropy is an approach that shows the randomness of the data. It can be used to assess the security of the encryption [22]. To calculate the entropy $H(s)$ [6, 7, 16], of a source (s), we have that

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \cdot Log_2(\frac{1}{P(s_i)}), \tag{8}$$

where $P(s_i)$ represents the probability of the symbol s_i. For a purely random source that emitting 2^N symbols with equal probability, after evaluating the Eq. (8), we have an entropy $H(s) = N$, in this case, for images with pixels completely random in the scale of 8-bit gray, its entropy $H(s) = 8$ bits. When the images are encrypted, their entropy should ideally be 8. When a cryptosystem emits symbols (cryptograms) with entropy less than 8, this encrypter has certain degree of predictability, so that its security is at risk [7].

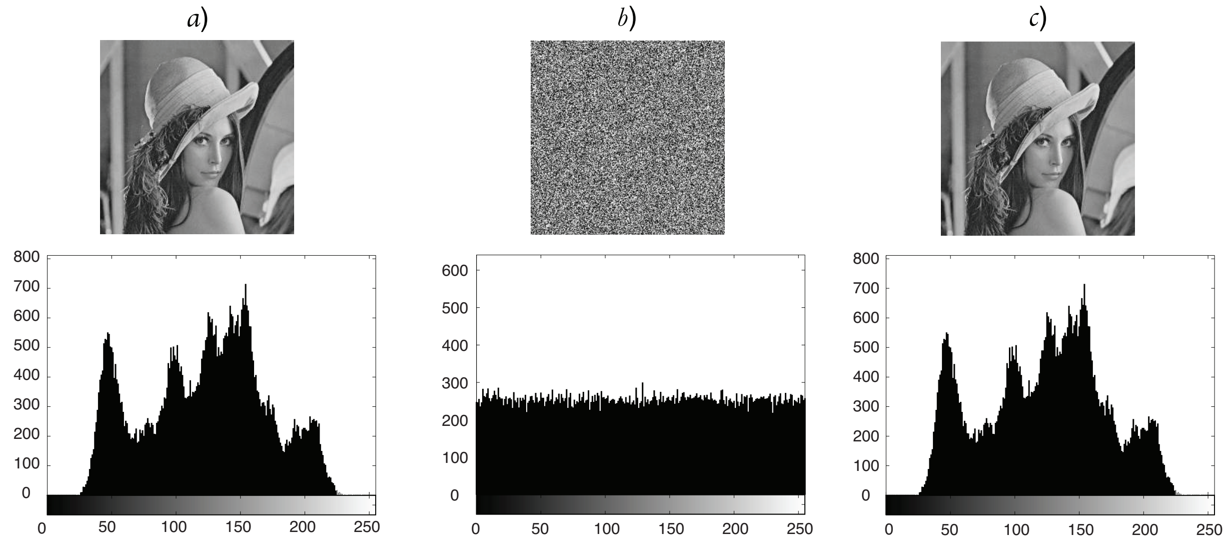

Figure 6. Top: *a*) original image, *b*) cryptogram, *c*) recovered image. Bottom: *a*) histogram of the original image, *b*) histogram of the cryptogram, *c*) histogram of the retrieved image.

4. Results of the security analysis

4.1. Statistical analysis

4.1.1. Statistical histogram

Fig. 6*a*) shows the original image "Lena" and at the bottom shows the corresponding histogram. Fig. 6*b*) shows the encrypted image using the initial conditions as encryption key: $x_1(0) = 0.10$, $x_2(0) = 0.15$, $x_3(0) = 0.01$, in the lower part of Fig. 6*b*) is shown its corresponding histogram. It can be observed how the information is spread evenly among all shades of 0 to 255 in the gray scale. Under these conditions, we can say that the system is robust against attacks of statistical type. Fig. 6*c*) shows the recovered image in the receiver and its corresponding histogram in the bottom. It is observed that both, the recovered image and its histogram are equal to the original image.

4.1.2. Correlation analysis of adjacent pixels

In this section, we examine the correlation between two horizontally, vertically and diagonally adjacent pixels. We randomly select 2400 pairs of pixels (x_i, y_i) of the image under analysis (original or encrypted) and with these pairs of adjacent pixels, the scatter plot is generated, i.e., the pixel x_i vs y_i is plotted. Then, the corresponding correlation coefficients r_{xy} are calculate, from the Eq. (2). By way of example, Figs. 7*a*) and 7*b*) show the distribution of correlation of two horizontally adjacent pixels of the original image "Lena" and the encrypted image, respectively. From Eq. (2), we obtain the corresponding correlation coefficients: 0.9249 and -0.0100.

Proceeding similarly, we obtain the correlation coefficients of two vertically and diagonally adjacent pixels for the original image "Lena" and its corresponding encrypted image. Table 1 shows the values obtained.

Table 1. Correlation coefficients of two adjacent pixels in the original image of "Lena" and its corresponding encrypted image, from $x_1(0) = 0.10$, $x_2(0) = 0.15$ and $x_3(0) = 0.01$.

Pixels	**Original image**	**Encrypted image**
Horizontal	0.9249	-0.0100
Vertical	0.9550	0.0305
Diagonal	0.9058	0.0278

4.2. Differential attacks

To perform the analysis against differential attacks, we use very similar keys similar to encrypt the original image of "Lena". We use as a first encryption key the values of: $x_1(0) = 0.10$, $x_2(0) = 0.15$ and $x_3(0) = 0.01$, obtaining the cryptogram C_1. The following key used is: $x_1(0) = 0.10{+}1{\times}10^{-10}$, $x_2(0) = 0.15$ and $x_3(0) = 0.01$, obtaining the cryptogram C_2. The difference between the keys used is 1×10^{-10} for $x_1(0)$. Using Eqs. (6) and (7), we obtain: $NPCR = 99.5758\%$ and $UACI = 33.4820\%$. These result show that the algorithm is strong against differential attacks, because the NPCR is approximate to the ideal value of 100%. All our numerical calculus is based in to standard IEEE std 754 [26].

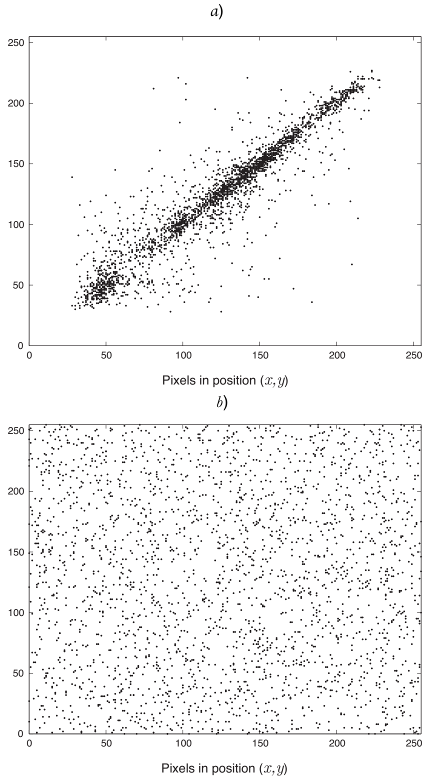

Figure 7. Correlation of two horizontally adjacent pixels: *a*) original image, *b*) encrypted image.

4.3. Information entropy

To evaluate the information entropy of the hyperchaotic encryption algorithm used in this paper, we use the Eq. (8). First, we calculated the probability of occurrence of each symbol (pixel), this is with the aid of the histogram of the cryptogram (Fig. 6). In the case of the cryptogram obtained with the encryption key $x_1(0) = 0.10$, $x_2(0) = 0.15$ and $x_3(0) = 0.01$, the calculated entropy is $H(s_i) = 7.9984$ very close to the ideal value to $H(s) = 8.0$ bits.

4.4. Speed performance

In this section, we present the analysis processing velocity of proposed encryption algorithm. The encryption speed of images (Lena) with different sizes by using the proposed scheme is shows in Table 2, that are obtained by specific commands of programming. The computer used in this test is 2.8 GHz Intel Core 2 Duo and 4 Gb 667 MHz. With such a speed, this cryptosystem encryption of digital images is efficient to be used for transmission through a public communication channel, where the encryption time should be short relative to the transmission time, like internet.

Table 2. Encryption/Decryption speed test result.

Image size (pixels)	Encryption/Decryption (s)
256 x 256	0.11
512 x 512	0..469
1024 x 1024	1.8365

5. Conclusions

Based on the improvement of the hyperchaotic dynamics of the Rössler map posed in this paper, we proposed a cryptosystem with the following characteristics: *i*) it has a simple logical structure, *ii*) it is efficient in terms of the demanded computational resources, *iii*) results of very competitive security levels are obtained, *iv*) physical implementation is easy, and *v*) it has a large key space, so the algorithm implemented follows the principles of *Kerckhoffs* and *Shannon* of cryptography. Under these conditions, we can suggest the application of the proposed cryptosystem, in applications of digital images encryption to be transmitted through a public communication channel like internet, or more so, in private communications systems through the use of embedded devices.

Acknowledgments

This work was supported by CONACyT, Mexico under Research Grant No. 119168. It was also supported by the Internal Research Project of the Autonomous University of Baja California (UABC), through the 16th convocation of the Internal Research Projects, with the program number 1379 to practice in the years 2012-2014. The E.R.O. research is supported in his PhD studies by CONACyT.

References

[1] M.S. Baptista, “Cryptography with chaos,” *Physics Letters A*, Vol. 240, pp. 50-54, March 1998.

[2] G. Grassi and S. Mascolo, “A System Theory Approach for Designing Cryptosystems Based on Hiperchaos,” *IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Applications*, Vol. 46, No. 9, pp. 1135-1138, September 1999.

[3] L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*. Studies in Computacional Intelligence, Vol. 354. Springer, 2011, p. 27.

[4] G.Chen, Y. Mao and C.K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, Vol. 21, pp. 749-761, 2004.

[5] H. Gao, Y. Zhang, S. Liang and D. Li, “A new chaotic algorithm for image encryption,” *Chaos, Solitons and Fractals*, Vol. 29, pp. 393-399, 2006.

[6] S.Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A*, 240, pp. 50-54, March 1998.

[7] S.Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons and Fractals*, Vol. 35, pp. 408-419, 2008.

[8] Q. Zhang, L. Guo and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, Vol. 52, pp. 2028-2035, 2010.

[9] V. Patidar, N.K. Pareek, G.Purohit and K.K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, Vol. 284, pp. 4331-4339, 2011.

[10] F. Chong, L. Bin-bin, M. Yu-sheng, L. Xiao and C. Jun-jie, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, Vol. 284, pp. 5415-5423, 2011.

[11] L. Zhengjun, G. Min, D. Yongkang, L. Feng, L. Shen, A.A. Muhammad, D. Jingmin and L. Shutian, "Double image encryption by using Arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering*, Vol. 50, pp. 248-255, 2012.

[12] A. Awad and D Awad, "Efficient Image Chaotic Encryption Algorithm with No Propagation Error," *ETRI Journal*, Vol. 32, No. 5, pp. 774-782, October 2010.

[13] D. Moon, Y. Chung, S.B. Pan, K. Moon and K.II. Chung, "An Efficient Selective Encryption of Fingerprint Images for Embeded Processors," *ETRI Journal*, Vol. 28, No. 4, pp. 444-452, August 2006.

[14] X. Wang and L. Yang, "A novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models," *Optics Communications*, Vol. 285, pp. 4033-4042, 2012.

[15] A.H. Abdullah, R. Enayatifar and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *International Journal of Electronics and Communications AEÜ*, Vol. 66, pp. 806-816, 2012.

[16] A. Akhshani, S. Behnia, A. Akhavan, H.A. Hassan and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *Optics Communications*, Vol. 283, pp. 3259-3266, 2010.

[17] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, Vol. 372, pp. 394-400, 2008.

[18] R. Rhouma, S. Meherzi and S. Belghith, "OCML-based colour image encryption," *Chaos, Solitons and Fractals*, Vol. 40, pp. 309-318, 2009.

[19] J. Peng, D. Zhang and L. Xiaofeng, "A Digital Image Encryption Algorithm Based on Hyper-chaotic Cellular Neural Network," *Fundamenta Informaticae*, Vol. 90, pp. 269-282, 2009.

[20] S. Mazloom and A.M Eftekhari-Moghadam, "Color image encryption based on Coupled Nonlinear Chaotic Map," *Chaos, Solitons and Fractals*, Vol. 42, pp. 1745-1754, 2009.

[21] L. Shubo, S. Jing and X. Zhengquan, "An Improved Image Encryption Algorithm based on Chaotic System," *Journal of Computers*, Vol. 44, No. 11, pp. 1091-1100, 2009.

[22] M. Yongyi and D. Zichao, "A New Image Encryption Algorithm of Input-Output Feedback Based on Multi-chaotic System," *Applied Mechanics and Materials*, Vol. 40-41, pp. 924-929, 2011.

[23] O.E. Rössler, "An equation for hyperchaos," *Physics Letters*, Vol. 71A, No. 2, 3, pp. 155-157, April 1979.

[24] E. Inzunza González, "Encriptado caótico en sistemas biométricos," Tesis de Doctorado, Facultad de Ingeniería, Arquitectura y Diseño (FIAD), Universidad Autónoma de Baja California (UABC), Ensenada, B.C., México, Enero 2013.

[25] Z. Hegui, Z. Cheng and Z. Xiangde, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," Signal Processing: *Image Communication*, Vol. 28, pp. 670-680, 2013.

[26] IEEE Computer Society "IEEE Standard for Floating-Point Arithmetic," *IEEE Std* 754^{TM}, pp. 1-58, 2008.

[27] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, Vol. IX, pp. 5-38, Janvier 1883.

[28] C.E. Shannon, "Communication Theory of Secrecy Systems," *The Bell System Technical Journal*,Vol. 28, No. 4, pp. 656-715, 1949.

[29] C.E. Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal*, Vol. 27, pp. 379-424, July 1948, pp. 623-656, October 1948.