1. Fairouz Belilita[1], 2. Tewfik Bekkouche [2], 3. Nourredine Amardjia[3]

University of Setif-1, Algeria (1),
University of BBA, Algeria (2), University of Setif-1, Algeria (3)

doi:10.15199/48.2022.05.24

An Improved Chaotic System-based 1D Logistic Map Applied to Gray Scale Images Encryption

Abstract. *In this paper, we propose an improved chaotic system inspired from the classical 1D Logistic map. The main idea consists in enhancing the performance of the control parameter by extending its chaotic range. The improved Logistic map (ILM) is applied to gray scale encryption images using the confusion-diffusion architecture. The input image is first chaotically scrambled before performing an element by element recursive XOR on its successive chosen blocks of* (8×8) *or* (16×16). *Obtained result is reshaped to give the encrypted image. Computer simulations prove the performances of this method in terms of histogram analysis, correlation and sensitivity analysis.*

Streszczenie. *W tym artykule proponujemy ulepszony chaotyczny system inspirowany klasyczną mapą logistyczną 1D. Główną ideą jest zwiększenie wydajności parametru kontrolnego poprzez rozszerzenie jego chaotycznego zakresu. Ulepszona mapa logistyczna (ILM) jest stosowana do obrazów szyfrowania w skali szarości przy użyciu architektury pomyłek-rozproszenia. Obraz wejściowy jest najpierw chaotycznie zaszyfrowany przed wykonaniem element po elemencie rekurencyjnego XOR na jego kolejnych wybranych blokach (8×8) lub (16×16). Otrzymany wynik jest przekształcany w celu uzyskania zaszyfrowanego obrazu. Symulacje komputerowe potwierdzają wydajność tej metody w zakresie analizy histogramu, korelacji i analizy wrażliwości.* (***Ulepszona, oparta na systemie chaotycznym mapa logistyczna 1D stosowana do szyfrowania obrazów w skali szarości***)

Keywords: Improved Logistic map (ILM)– extending range- confusion _diffusion- image encryption.
Słowa kluczowe:mapa logistyczna, szyfrowanie, układ chaotyczny.

Introduction

With the technological progress in the field of telecommunications, the rate of information on the net continues to increase. As a result, this growing rise is not immune to malicious use and its protection becomes more than a necessity. Image by its remarkable attractiveness is part of this flow of information and image encryption is one of the most reliable and effective means of security and protection. The permutation-diffusion architecture [1] is the most adopted in image encryption which consists in moving the positioning of the pixels and then changing their values using the xor operator. In the literature, several image encryption algorithms [2-5] have been developed, in particular those based on this above mentioned architecture. However the appearance use of chaos for the first time in 1989 by Matthews [6] relying on its magnificent characteristics such as the high sensitivity to its initial parameters, ergodicity, and pseudo-randomness, made the big turning into image encryption whether in the spatial or the frequency domain [7-10] and has given rise to other very high performance algorithms.

These algorithms are mainly based on classical chaotic sequences of one dimension [11,12] such as the logistic map, the sin, the cubic map and others of two dimensions and more [13,14]. Despite the success experienced in the field of image encryption using these classic chaotic sequences, the algorithms developed in this direction remain vulnerable towards cryptographic attacks. This is due to the width of the control parameter of these chaotic sequences which presents a very narrow range that allows attackers to find the encryption key with the slightest effort. To remedy this problem, several algorithms, based on improved chaotic sequences aimed to widen the range of the control parameter, have been developed and then applied in color image encryption schemes.

These improved chaotic maps are based essentially in their structures either on the combination of two or more classical chaotic sequences [15], or on the result of their difference or their summation [16, 17]. In this context, we propose in this manuscript a new improved chaotic sequence inspired from the chaotic logistic map sequence, based on the composition of the latter and the exponential function. The results of the tests carried out as the Lyapunov diagram and bifurcation diagram have proved the validity of this map. When applied in a grayscale image encryption scheme, it has given better results and a lot of satisfaction once passing the various cryptographic tests. This paper is organized in this way. In section 2, we present the new chaotic sequence and the results of its validation. In section 3, we present the image encryption-decryption schemes based on this new chaotic map, in section 4, we relate the simulation and test results of the algorithm following the various cryptographic tests applied and we will end this work with a conclusion and an outlook.

The new chaotic map

In this section, we briefly review the classical 1D Logistic map which is necessary for the construction of the new chaotic improved 1 D Logistic map called here ILM.

The classical1 D Logistic map

The classical 1 D Logistic map is expressed iteratively as:

(1) $$x_{i+1} = f_r(x_i) = r \times x_i \times (1 - x_i)$$

where x_0 is the initial condition parameter ∈ [0 1] and r □ [3, 95 4] is the control parameter.

.

ILM map

The ILM is the result of the composition of two functions, which are the exponential function and 1D Logistic map, the modular improved map is expressed iteratively as follows:

(2) $$x_{i+1} = g_r(x_i) = mod(r \times e^{x_i} \times (1 - e^{x_i}), 1)$$

where x_0 is the initial condition parameter ∈ [0 1] and r □ [0 ∞] is the control parameter.

Lyapunov exponent

The Lyapunov exponent is used to measure the degree of stability of a system. A system sensitive to very small variations of the initial condition will have a positive exponent (chaotic system). On the other hand, the exponent is negative if the system is not sensitive to small variations of the initial conditions, the trajectories approach

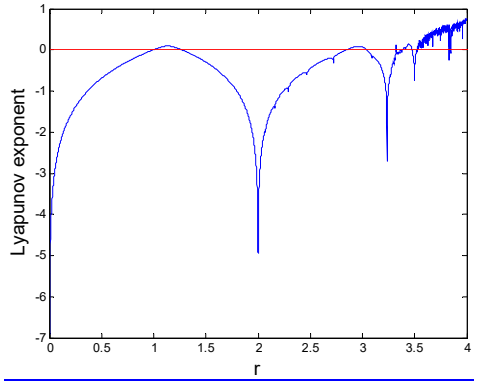
and we therefore lose information on the initial conditions. For a discrete time system, Lyapunov exponent for an orbit starting with x_0 is defined as follows:

$$(3) \quad LE\left(x_{0,}r\right) = \lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} ln\left|g'_r(x_i)\right|$$

Diagram of bifurcation

The bifurcation diagram is a plot, which makes it possible to quickly evaluate all the possible solutions of a system as well as their stability according to the variations of one of its parameters. It also makes it possible to identify the particular values of the parameter which induce bifurcations. It presents intervals over which the asymptotic solutions evolve continuously with the parameter, and it ranks the values of the parameter on the x-axis and the values of one of the state variables on the y-axis.

a)



b)

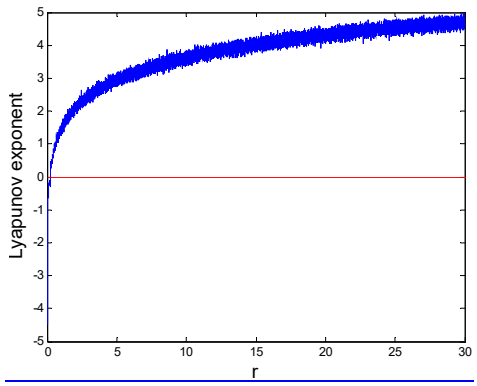
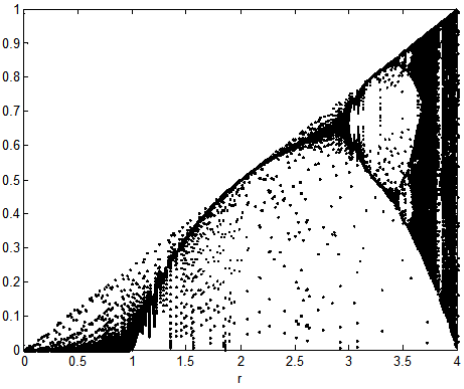


Fig.1. Lyapunov exponent for (a) 1D Logistic map (b) ILM

a)



b)

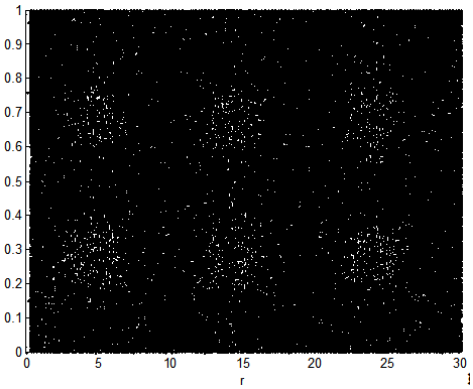


Fig.2. Bifurcation diagram for (a) 1D Logistic map (b) ILM

Figure. 1 illustrates a comparison of the Lyapunov exponent (LE) as a function of the control parameter r jointly for the 1D classic logistic map (Fig. 1. a) and the ILM (Fig. 1. b). It is very clear that the width of the range r where LE is greater than zero is restricted to a very short interval [3.8 4] (chaotic zone), however, the one of the improved sequence ranges from 0.2 to 30 and can even extend to infinity. This reasoning is furthermore reinforced by using another important tool which is the bifurcation diagram illustrated in Fig. 2. It consists in representing the distribution of the values x_i of such a chaotic sequence as a function of r, which clearly shows that this distribution is completely uniform (Fig. 2. b) for the ILM, whereas that of the classical sequence presents discontinuity and windowing in its chaotic distribution (Fig. 2. a).

Proposed image encryption process

The following steps describe the proposed image encryption algorithm:

1. Let P be the original image of size $(N \times N)$. First we calculate the normalized pixels average value M expressed by the following equation:

$$(4) \quad M = \frac{1}{255}\sum_{ij}^{N} \frac{P_{ij}}{N \times N}$$

then, we introduce a dependency between the calculate value and the parameters of chaotic maps by injecting it therein those parameters jointly in diffusion and permutation.

2. Let BN be the chosen block's size per line (e.g. 8 or 16 per line). First, we generate a vector having the same size as BN, containing positive integers that are less than or equal to BN ordered chaotically. (x_0, r_0) are the parameters of the used ILM.

3. Divide the image into BN rows and BN columns. So we obtain $(BN \times BN)$ smaller sub-images (or blocs) of size $(m \times m)$, with $m = N/BN$.

4. Reorder each row and each column blocs according to the previous generated chaotic vector.

5. Reshape the scrambled image to be of size $(m \times \frac{N \times N}{m})$ which is a sequence of $N \times N/m$ blocs.

6. Generate another ILM chaotic map(x_1, r_1) of size $(N \times N)$ and reshape it to be same as the scrambled image (of size $(m \times \frac{N \times N}{m})$).

7. Generate a third ILM map(x_2, r_2) of size $(N \times N)$ and reshape it to be same as the scrambled image (of size $(m \times \frac{N \times N}{m})$).

8. Perform 2 bit-XOR operations, the first is between each image bloc and the corresponding bloc from the

chaotic map and the second is between each image bloc and its previous bloc.
9. Reshape both the obtained image and the generated chaotic map into $(1 \times N \times N)$ vectors,
and then reorder the image pixels again according to the chaotic map permutation vector.
10. Finally, put the image into its original shape $(N \times N)$ to obtain the encrypted image.

To get the plain image out of the encrypted one we just need to reverse the encryption steps above.

Results and discussion

Computer simulations are done under MATLAB software (2014a) environment, the test images are Lena (256×256) and Barbara (256×256), we have using also three ILM chaotic parameters namely $(\mathrm{x}_0 = 0.32, \mathrm{r}_0 = 10.04)$, $(\mathrm{x}_1 = 0.42, \mathrm{r}_1 = 20.06)$ and $(\mathrm{x}_2 = 0.52, \mathrm{r}_2 = 25.22)$. Fig. 3 illustrates test images and the corresponding histogram of each image using blocks of size (16×16). It shows also the corresponding encrypted images with their histograms.

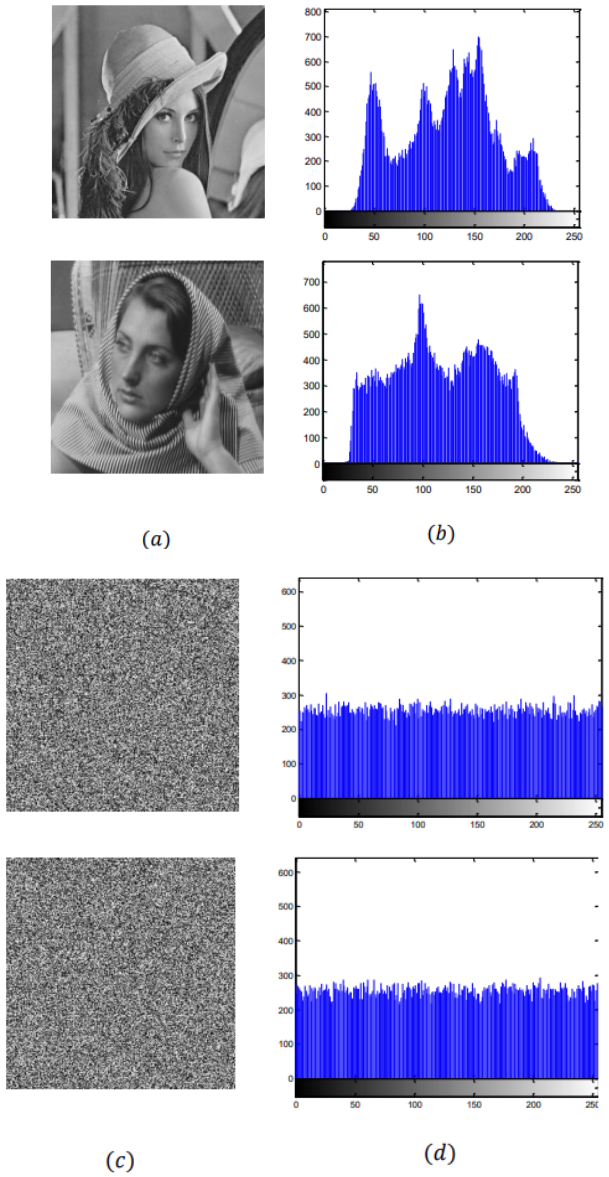


Fig.3. Results of encryption process (a) Original images (b) their Histograms (c) the corresponding encrypted images (d) histograms of encrypted images

Histogram anaysis

By observing Fig. 3, we notice that the histograms of the two encrypted images of Lena and Barbara are similar to a white noise histogram where all pixel values have the same probability of occurrence. So an attacker is not able to derive any useful information about the original image from just analyzing the encrypted image histogram. This proves that the proposed encryption method resists attacks by histogram analysis.

Correlation coefficient

It is well known that there is a high redundancy and a strong correlation between neighboring pixels of a natural image. A creditable encryption algorithm will always try to defuse the existing resemblance between these neighboring pixels in order to deprive attackers of any information that can reveal the encryption system used. The correlation test between adjacent pixels involves randomly selecting 1000 pairs of adjacent pixels from the original image and 1000 pairs from the resultant encrypted image and analyzing the correlations in the horizontal, vertical and diagonal directions of the two original and encrypted images.

Table 1. The Correlation coefficient for the two test images and their corresponding encrypted images

	Lena	Barbara
	Original image/Encrypted image	Original image/Encrypted image
Vertical	0.9593/0.004	0.9548/-0.0003
Horizontal	0.9258/0.0026	0.8156/0.008
Diagonal	0.9295/0.0019	0.8549/-0.0005

Table 1 recapitulates the results obtained for the measurement of the correlation coefficients of the two test images Lena and Barbara and their corresponding encrypted images using the proposed encryption algorithm. The correlation coefficients of the original images in all three directions approach 1, while those of their encrypted images approach 0. In this case, we say that the encryption significantly weakened the pixel correlation of the encrypted image.

Sensitivity analysis

To test the sensitivity of the proposed encryption scheme, let k_1 be the encryption key which is composed of the parameters of the second and the third ILM map $k_1(x_1, r_1, x_2, r_2)$, the corresponding decryption key is designed by $k_2(x_1', r_1', x_2', r_2')$. If the encryption key is exactly the decryption one i.e., $k_1 = k_2$, the decrypted image is identical to the original. We make then a minor variation of 10^{-15} on one of the parameters $(x_1, r_1, x_2 \; or \; r_2)$, and we set the remaining parameters at their fixed values. The results of simulations obtained show that the limit of the appearance of the image decrypted in the clear is of 10^{-16}, this confirms the high sensitivity of the proposed method which is of the order of 10^{+15} for the different parameters of the encryption key.

Key space analysis

According to the previous results obtained in the test of sensitivity, we have reached a precision of 10^{15} for each parameter of the encryption key, therefore, we conclude that the key space is evaluated at $10^{15+15+15+15} = 10^{60} \cong 2^{192}$, which is widely sufficient compared to the value required in cryptosystems [18].

Conclusion

In this paper, we have presented a new chaotic sequence based on the 1D logistic map, we have demonstrated the validity of this sequence through a set of tests like the Lyapunov exponent and the bifurcation diagram. Furthermore, we have applied this new improved chaotic sequence in an image encryption scheme and the simulation results towards various cryptographic tests are very satisfactory. Also, In the near future, we intend to implement this scheme on an FPGA support to give a clearer practical aspect.

Acknowledgments

The authors would like to thank the General Directorate for Scientific Research and Technological Development of the Algerian Republic in general, the ETA laboratory of Bordj Bou Arreridj university and the LIS laboratory of Setif-1 university.

Authors

***Authors**: Dr Fairouz Belilita, Department of Physics, Faculty of Sciences, LIS Laboratory, University of Setif-1, Algeria, E-mail: fairouz.amardjia@univ-setif.dz; Dr Tewfik Bekkouche, Department of electro-mechanics, Faculty of Technology, ETA Laboratory, University of BBA, Algeria E-mail: bekkou66@hotmail.com; Pr. Nourredine Amardjia, Department of Electronics, Faculty of Technology, LIS Laboratory, University of Setif-1, Algeria, E-mail: amardjianour@univ-setif.dz*

REFERENCES

[1] J. E. Shannon, Communication Theory of Secrecy Systems, System Technical Journal, 28 (1949), pp. 656–715.

[2] N.K. Pareek, V. Patidar, K.K. Sud, Diffusion-substitution based gray image encryption, Digital Signal Processing, vol. 23 (2013), pp. 894–901.

[3] A. Beloucif, O. Noui, Design of a tweakable image encryption algorithm using chaotic based schema, Int. J. Information and computer security, 8 (2016), pp. 205–220.

[4] J.N.M. Bezerra, V.V.A. Camargo, A. Molter, A new efficient permutation-diffusion encryption algorithm based on a *chaotic map*, Chaos. Solitons & Fractals, 151 (2021) 111235.

[5] A. Hasheminejad, M.J. Rostami, A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map, Optik, 184 (2019), pp. 205–213.

[6] J. Matthews, On the derivation of a chaotic encryption algorithm, Cryptologia 4 (1989) 29–42.

[7] J. Lang, R. Tao, Y. Wang, Image encryption based on the multiple parameter discrete fractional Fourier transform and chaos function, Opt. Commun.283 (2010) 2092–2096.

[8] S.E. Azoug, S. Bouguezel, A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform, Opt. Commun. 359 (2016) 85–94.

[9] T. Bekkouche, S. Bouguezel, A recursive non-linear pre-encryption for opto-digital double random phase encoding, Optik. 158, (2018), pp. 940–950.

[10] E. Swiercz, Image encryption algorithms based on wavelet decomposition and encryption of compressed data in wavelet domain, Przeglad Elektrotechniczny. 2 (2018) 79–83.

[11] Y. Zhou, L. Bao, C.L. Philip Chen, A new 1D chaotic system for image encryption, Signal Processing. 97 (2014) 172–182.

[12] X. Wu, H. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, Applied Soft Computing, 37 (2015), pp. 24–39.

[13] A. Broumandnia, Designing digital image encryption using 2D and 3D reversible modular chaotic maps, Journal of Information Security and Applications, 47 (2019) 188–198.

[14] X. Gao, Image encryption based on 2D hyper chaotic map, Optics and Laser Technology, 142 (2021) 107252.

[15] J.R. Parvaz, M. Zarebnia, A combination chaotic system and application in color image, Optics and Laser Technology, 101 (2018) 30–41.

[16] D. Herbadji, A. Belmeguenai, N. Derouiche, H. Liu, Colour image encryption scheme based on enhanced quadratic chaotic map, IET Image Processing, 14 (2020) 40–52.

[17] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic, Signal Processing, 138 (2017), pp. 129–137.

[18] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos based cryptosystems, Int. J. Bifurcation Chaos, 16 (2006), pp. 2129–2151.