1. Noura OULMI[1], 2. Tewfik BEKKOUCHE[2], 3. Abdessalem BOULOUFA[1], 4. Habib BEY[1]

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

doi:10.15199/48.2023.10.10

An Efficient Nonlinear Post-Processing Applied to Image Encryption

Abstract. *In this paper, we propose an efficient non-linear post-processing placed downstream of an image encryption scheme. It consists firstly to encrypt the plaintext image by the confusion-diffusion technique using chaotic functions. Then, the resulting image is added to a chaotically generated image having the same dimensions. Obtained result passed through the arctangent function to give the encrypted image. Computer simulations have proven the support that a nonlinear function can give an image encryption scheme. In addition, the performance measurements carried out prove the superiority of the proposed method towards existing algorithms in the literature from the point of view of histogram analysis, correlation test and key space.*

Streszczenie. W *tym artykule proponujemy wydajne nieliniowe przetwarzanie końcowe umieszczone poniżej schematu szyfrowania obrazu. Polega ona po pierwsze na zaszyfrowaniu obrazu tekstu jawnego techniką zamieszania-dyfuzji z wykorzystaniem funkcji chaotycznych. Następnie powstały obraz jest dodawany do chaotycznie generowanego obrazu o tych samych wymiarach. Otrzymany wynik przeszedł przez funkcję arcus tangens dając zaszyfrowany obraz. Symulacje komputerowe dowiodły, że funkcja nieliniowa może zapewnić schemat szyfrowania obrazu. Ponadto przeprowadzone pomiary wydajności dowodzą wyższości proponowanej metody w stosunku do algorytmów istniejących w literaturze z punktu widzenia analizy histogramu, testu korelacji oraz przestrzeni klucza.* (***Wydajne nieliniowe przetwarzanie końcowe zastosowane do szyfrowania obrazu***)

Keywords: Nonlinear; Post-processing; Chaos; Inverse Tangent; Image encryption.
Słowa kluczowe: przetwarzanie obrazu, szyfrowaniw

Introduction

The progress that the world has seen in the field of exchange of information and communications, especially with the Internet tool, has favored a great fluidity of this information on the various transmission channels. On the other hand, this information, whatever its nature, sound, image, video, biometric database, is not immune to fraudulent attacks. To protect them, several techniques have emerged, including steganography [1, 3], watermarking [4, 6] and encryption [7, 11]. The image by its attractive specificity arouses the enthusiasm of researchers and scientists to develop other algorithms for its protection. Among the lines of research, we cite the encryption of images which is generally subdivided into two main parts: image encryption in the spatial domain and in the frequency domain [12, 14]. In this paper we are interested in the spatial domain which is essentially based on the architecture of confusion-diffusion, in which, we proceed to the change of the location of the pixels in the first place then to the change of their values using the operator XOR. The appearance of chaos [15] has boosted the research world to develop other coherent and robust image encryption algorithms [16] and despite this they will always remain vulnerable to some cryptographic attacks. This prompted us to find other ways to develop other more efficient and more robust algorithms [17]. The basic idea came to us by inserting nonlinear functions upstream or downstream of these encryption schemes.

It is in this context that we propose an image encryption scheme based on chaotic functions followed by the introduction of a nonlinear inverse tangent function downstream of this scheme. We will also demonstrate through simulation tests, the impact of nonlinearity on the robustness of image encryption through different performance measures. The manuscript is organized around four sections, in the first section we recall the definitions of some functions used, section two is interested in the proposed encryption and decryption schemes, section four concerns the experimental results and we end with a conclusion and prospects.

Preliminaries

In this section, we are interested in the definition of the chaotic logistic map function used in the confusion and diffusion phases as well as the inverse tangent function with which we created the nonlinearity in the proposed image encryption scheme.

A. Logistic map

The logistic map function is expressed iteratively as:

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

where x_0 is the initial condition parameter and $r \in [3.98,\ 4]$ is the control parameter.

B. Inverse Tangent

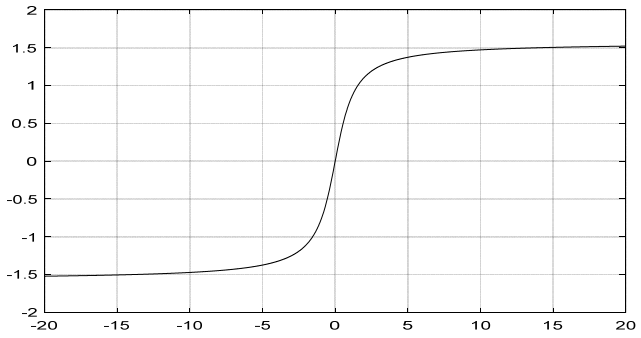


Fig.1. The plot of inverse tangent function

Fig. 1. illustrates the Inverse Tangent (tan-1) function plot over the interval $-20 < x < +20$. As shown in this figure, for real elements of x, $tan^{-1}(x)$ returns values in the interval $[-\pi/2, \pi/2]$. We exploit the nonlinearity of this function by inserting it into our proposed image encryption scheme. This will give this scheme a robustness and immunity against possible attacks. We also recall that during decryption we use the Tangent function and we have reversed the roles to avoid the infinite case when x takes the value 0.

Proposed encryption / decryption scheme

The proposed image encryption scheme as shown in Fig. 2 is summarized in the following steps:

- Let P be the plaintext image of size $N \times N$.
- Reshape this input image into a vector v of length $1 \times N \times N$.
- Generate a chaotic sequence using the logistic map function (x_0, r_0) having the same dimensions as the vector v , with x_0 the initial condition parameter and $r_0 \in [3.98,\ 4]$ is the control parameter.
- Reorder the vector v according to an increasing order given by the chaotic sequence (x_0, r_0) to obtain the permuted vector v_1 . This step is called the permutation phase.
- Generate another chaotic sequence based on the logistic map function having as parameters (x_1, r_1) of the same size as the vector v_1 .
- Convert the obtained sequence from [0 1] values to [0 255] to give another sequence named s .
- Perform the bit-wise XOR operation between v_1 and s to form a vector y as follow:

$$y_k = \begin{cases} v_{1k} \oplus s_{k'} & k = 1 \\ v_{1k} \oplus s_k \oplus y_{k-1}, k = 2,3,4,...N \times N \end{cases} \quad (2)$$

- Generate another chaotic sequence v_2 based on the logistic map function having as parameters (x_2, r_2) of the same size as the vector v_1 .
- Calculate the inverse tangent of the sum of the sequences v_2 and y to form the vector v_3 .

$$v_3 = \tan^{-1}(v_2 + y) \quad (3)$$

- Finally, the encrypted image is obtained by reshaping v_3 into an $N \times N$ matrix.

The decryption system takes the above steps of the encryption system in a reverse manner.

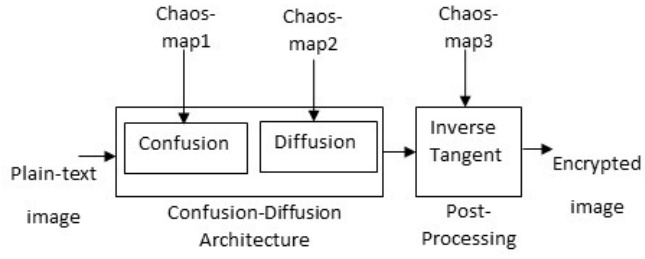


Fig. 2. The proposal encryption scheme

Results and discussion

In this section, we will present the different simulations made to prove the impact of nonlinearity in the proposed image encryption scheme. To do so, we have used a personal laptop in a MATLAB 2018 environment. The test images used having different sizes, are that of Lena (256X256), Barbara (512X512) and Living- room (512X512). Fig. 2 illustrates the test images used as well as their histograms, while Fig .3 presents the encryption result of these images and their corresponding histograms. The initial value and the control parameter (x_1, r_1) of the logistic chaotic maps are given respectively as follows:

$(x_0 = 0.25, r_0 = 3.99)$; $(x_1 = 0.35, r_1 = 3.99)$;

$(x_2 = 0.45, r_2 = 3.99)$;

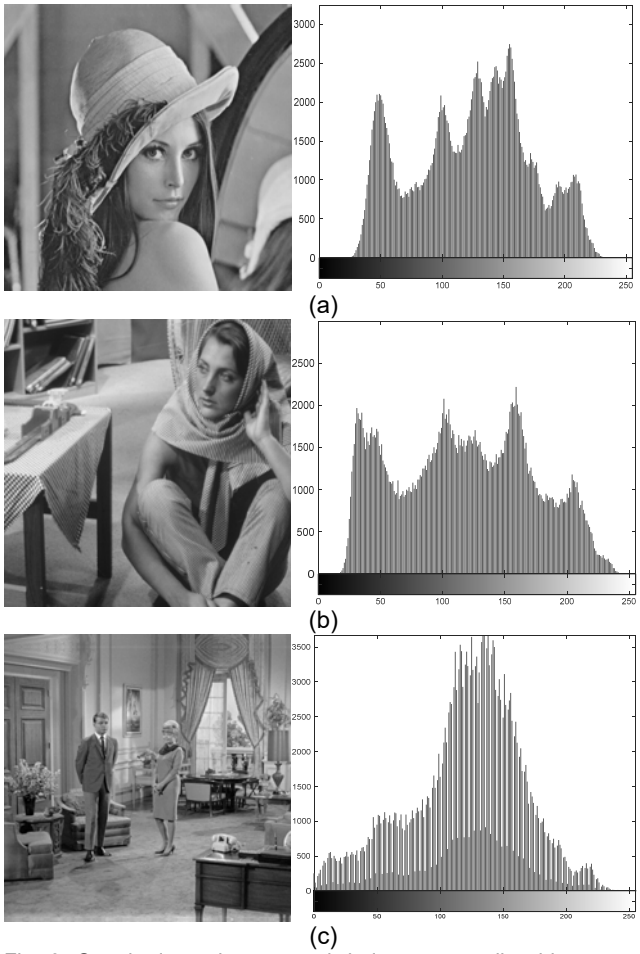


Fig. 3. Standard test images and their corresponding histograms (a) Lena (b) Barbara (c) Living-room

A. Histogram analysis

As shown in Fig. 3, the three test images of Lena, Barbara and Living-room have different histograms; each of them has its own histogram. On the other hand, the encrypted images as illustrated in Fig. 4 have the same appearance of their histograms; therefore, an unspecified attacker cannot extract any specific information to find the original image. This proves the robustness of the proposed encryption scheme with respect to the histogram analysis test.

The loss data test consists in assuming that part of the information is lost during the path connecting the transmitter and the receiver. Fig. 5 illustrates the simulation results of this test, Fig. 5 a gives respectively the encrypted images with a loss of 25% , 50% and 75%. On the other hand, Fig. 5 b illustrates the corresponding decrypted images. We clearly notice that despite a loss of up to 75%, the decrypted image remains identifiable and decipherable, which qualifies the proposed algorithm as robust with respect to the loss data test.

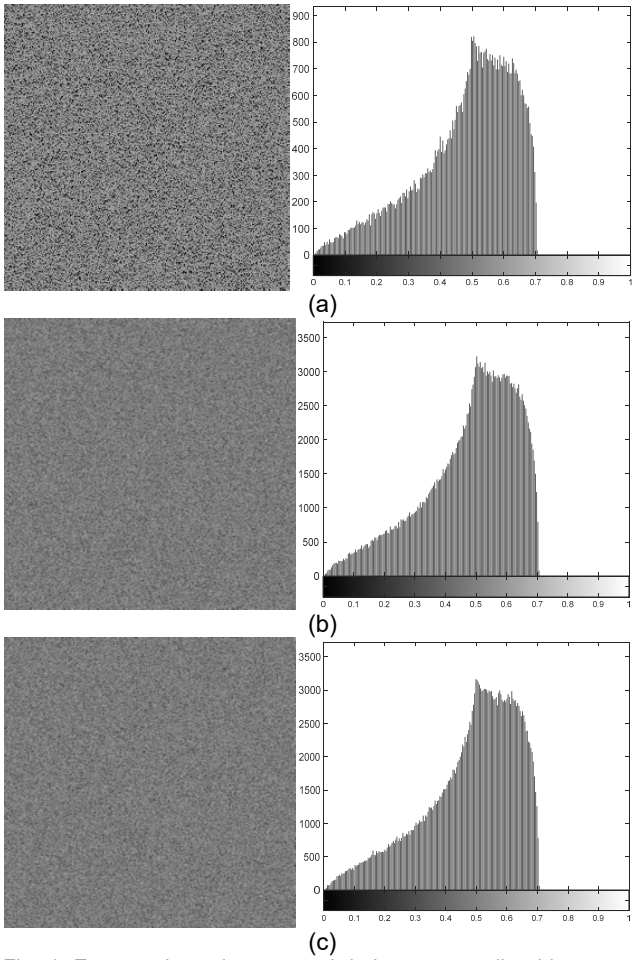


Fig. 4. Encrypted test images and their corresponding histograms (a) Lena (b) Barbara (c) Living-room

B. Data loss

C. Correlation analysis

During the correlation analysis, we randomly take 1000 pixels from the original image and the same number from the encrypted image, then we calculate the inter-pixels correlation rate in the three directions namely in the horizontal, vertical and diagonal direction. Table 1 summarizes the results obtained carried out on the Lena test image. We clearly notice that the correlation rate for the encrypted image borders on the value 0 and for the original image approaches unity, we note also the impact of nonlinearity on the decorrelation between pixels, in fact the results obtained from the correlation rate in the proposed algorithm are better than those obtained without the application of nonlinearity and even exceed those of the reference [7].

Table 1. Correlation analysis

	Original Lena	The proposed	The proposed without non-linearity	[7]
Horizontal	0.9195	0.0032	0.0059	0.0065
Vertical	0.9548	-0.0029	0.0030	0.0035
Diagonal	0.9201	0.0007	0.0013	0.0018

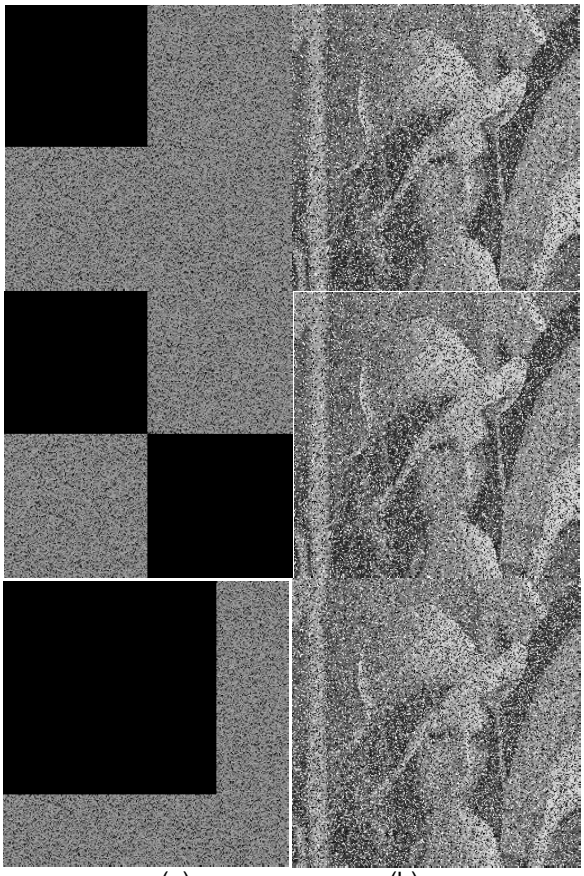


Fig. 5. Loss data test (a) Encrypted Lena (b) Corresponding decrypted Lena

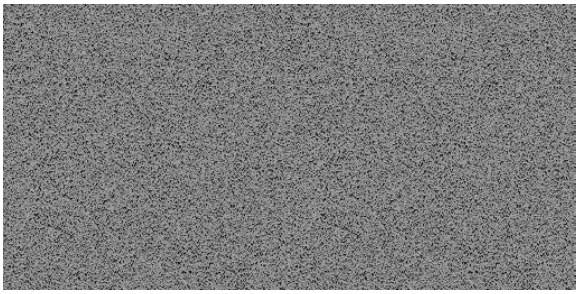
D. Key space and sensitivity analyses

Concerning the sensitivity test, we assume that the encryption key is composed of the parameters of the chaotic functions used in this encryption algorithm $k(x_0, r_0, x_1, r_1, x_2, r_2)$ and the corresponding decryption key is $k'(x_0', r_0', x_1', r_1', x_2', r_2')$. Each time we make a small change in one of these parameters and we keep the others as they are. We will then follow the impact of this change on the decrypted image of Lena. Fig. 6 illustrates the different cases mentioned and we note that the accuracy of the parameters r_i is of the order of 10^{15} on the other hand that of the parameters x_i is of the order of 10^{16}. From there, we conclude that the key space is evaluated at:

$$0.25 \times 0.25 \times 0.25 \times 10^{15} \times 10^{15} \times 10^{15} \times$$

$$10^{16} \times 10^{16} \times 10^{16} \cong 0.015 \times 2^{279} \cong 2^{273}$$

which is largely sufficient compared to that required in cryptography 2^{100}.



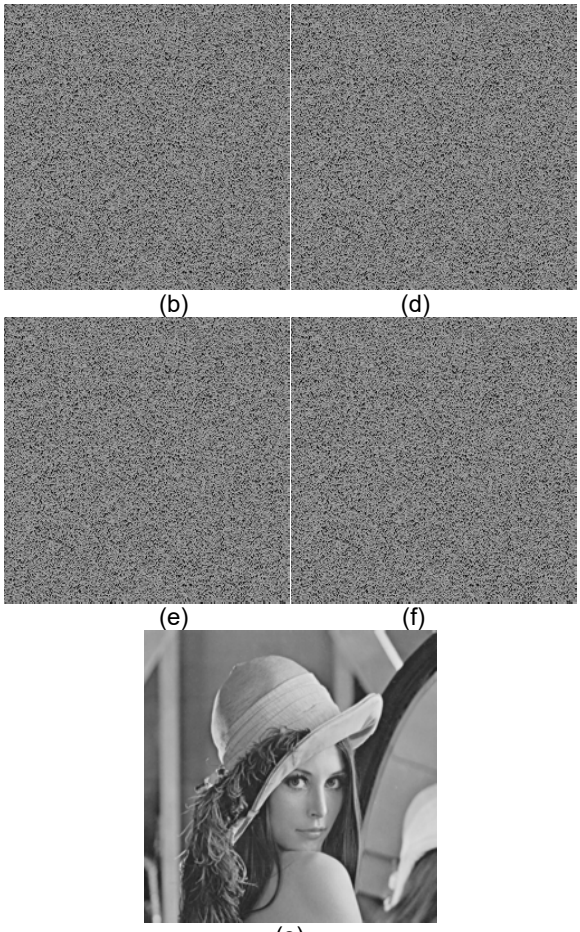


Fig. 6. Test of sensitivity: Decrypted Lena with a minor variation in chaotic parameters (a) $x_0' = r_0 \times 10^{-16}$ (b) $r_0' = r_0 \times 10^{-15}$ (c) $x_1' = r_1 \times 10^{-16}$ (d) $r_1' = r_1 \times 10^{-15}$ (e) $r_2' = x_2 \times 10^{-16}$ (f) $r_2' = r_2 \times 10^{-15}$ (g) Correct key

Conclusion

In this paper, we have introduced a nonlinear function which is the inverse tangent placed downstream of an image encryption scheme based on the confusion-diffusion architecture. Performance measures such as PSNR and correlation rate used in the evaluation of this proposed algorithm have proven the effectiveness of nonlinearity in encryption schemes. Furthermore, cryptographic attacks applied on this algorithm have also demonstrated its superiority compared to other works existing in the literature. This encouraged us to think about designing other more efficient nonlinear functions that we will use in our next work.

Acknowledgment

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

***Authors**:*

Dr OULMI Noura, Department of Electronics, Faculty of Technology, LEM Laboratory, University of Setif-1, Algeria, E-mail: oulnor@yahoo.fr;

Dr BEKKOUCHE Tewfik, Department of electro-mechanics, Faculty of Technology, ETA Laboratory, University of BBA, Algeria E-mail: bekkou66@hotmail.com;

Prof BOULOUFA Abdessalem, Department of Electronics, Faculty of Technology, LEM Laboratory, University of Setif-1, Algeria, E-mail: a_bouloufa@yahoo.fr

Mr. BEY Habib, Department of Electronics, Faculty of Technology, LEPCI Laboratory, University of Setif-1, Algeria, E-mail: bey_habib@univ-setif.dz.

REFERENCES

[1] PC. Mandal, I. Mukherjee, G. Paul, BN. Chatterji. Digital image steganography: A literature survey. Information Sciences. 609, (2022), pp. 1451–88.

[2] DRIM. Setiadi, S. Rustad, PN. Andono, GF. Shidik, Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing. 206, (2023), pp. 108908.

[3] H. Xie, Y. Gao, H. Zhang, J. Sun, A novel color image steganography algorithm based on bit counting and multiple-base system. 269, Optik (2022), pp. 169893.

[4] S. Belilita, N. Amardjia, T. Bekkouche, I. Nouioua, Combining SVD-DCT Image Watermarking Scheme Based on Perona-Malik Diffusion. Elektronika Ir Elektrotechnika. 25, (2019), pp. 68–74.

[5] S. Mokhnache, T. Bekkouche, D. Chikouche, A robust watermarking scheme based on DWT and DCT using image gradient. Int J Appl Eng Res. 13, (2018), pp. 1900–7.

[6] A. Bose, SP. Maity, Secure sparse watermarking on DWT-SVD for digital images. Journal of Information Security and Applications. 68, (2022), 103255.

[7] A. Yahi, T. Bekkouche, M. El Hossine Daachi, N. Diffellah, A color image encryption scheme based on 1D cubic map. Optik. 249, (2022), pp. 168290.

[8] F. Belilita, T. Bekkouche, N. Amardjia, An Improved Chaotic System-based 1D Logistic Map Applied to Gray Scale Images Encryption. PRZEGLĄD ELEKTROTECHNICZNY. (2022), pp. 130–2.

[9] D. Herbadji, N. Derouiche, A. Belmeguenai, T. Bekkouche, A. Labiad, M. Lashab, et al. A New Image Encryption Scheme Using an Enhanced Logistic Map. 2018 International Conference on Applied Smart Systems (ICASS), (2018), p. 1–6.

[10] Y. Zhou, L. Bao, CLP. Chen, A new 1D chaotic system for image encryption. Signal Processing. 97, (2014), 172–82.

[11] C. Pak, L. Huang. A new color image encryption using combination of the 1D chaotic map. Signal Processing. 138, (2017), pp. 129–37.

[12] T. Bekkouche, S. Bouguezel. A recursive non-linear pre-encryption for opto-digital double random phase encoding, Optik. 158, (2018), pp. 940–50.

[13] SE. Azoug, S. Bouguezel, A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform. Optics Communications. 359, (2016), pp. 85–94.

[14] T. Bekkouche, N. Diffellah, L. Ziet, Hybrid image encryption based on digital pre-encryption and optical single random phase encoding. Optica Applicata (2019), pp. 559–69.

[15] L. Xu, X.Gou, Z. Li, J.Li, A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Optics and Lasers in Engineering. 91, (2017), pp. 41–52.

[16] FEA. El-Samie, HEH. Ahmed, IF. Elashry, MH. Shahieen, OS. Faragallah, E-SM. El-Rabaie, et al, Image Encryption : A Communication Perspective. CRC Press, (2013).

[17] C. Han. An image encryption algorithm based on modified logistic chaotic map. Optik. 181, (2019), pp. 779–85.