International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 4 (2020) pp. 358-363
© Research India Publications. https://dx.doi.org/10.37622/IJAER/15.4.2020.358-363

Chaos-based Digital Image Encryption Using Unique Iris Features

Daniel F. Santos

Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Abstract

As the use of the Internet increases the exchange of private data as well, therefore the development of faster and novel algorithms is essential. This paper presents an algorithm for encrypting images based on the natural, unique and complex patterns present in the Iris and the use of Non-Linear Systems that present a chaotic behavior suitable for an encryption system. It has been proven that the developed algorithm produces optimal security values and can be used for encryption processes in real communications.

Keywords: Iris Features, Data Encryption, Security, Chaos

I. INTRODUCTION

With the rapid development and growth of communications and the social and economic scenarios that encourage the use of the internet, the number of data transmitted is increasing, consequently, it is necessary to develop efficient algorithms for encrypting data. In this article, it is proposed a symmetric-key algorithm to encrypt colour images with the possibility to be extended to other types of data such as text, audio and videos. Using a key exchange algorithm such as Diffie-Hellman it could used in public-key cryptography.

The iris recognition is a biometric technique to identify people capturing and analyzing unique patterns of the iris [1]. The iris recognition systems consists of 4 main stages [2], described as follows:

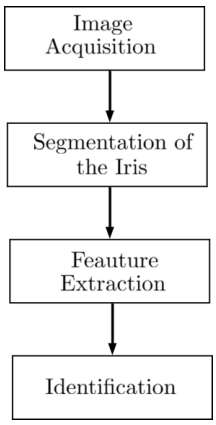

Fig 1. Stages to identify a person using the iris

Traditional encryption algorithms are based on prime numbers, for example, RSA, the proposed method uses Chaos theory to perform the encryption process. In the literature has been developed a variety of algorithms for image encryption, within them we have a project developed by Wei and Zhou in [3]in which they use unique features of the Iris and an AES algorithm to encrypt the information, the result of the study shows that the encrypted data has high security levels.

A. Segmentation of the Iris

Possibly the two most influential algorithms for locating the iris region are those proposed by Daugman [4] and Wildes [5]. Daugman's method uses the differential integral operator shown in (1) it is used to detect the iris and the limits of the pupil.

$$\max(r, x_0, y_0) = | G_{\sigma(r)} * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds | \quad (1)$$

where $I(x,y)$ is the image, r is the radius on which you are looking, $G_{\sigma(r)}$ is the Gaussian smoothing function with standard deviation σ, ds is a circular arc of radius r and (x_0, y_0) coordinates of the center. The integro-differential operator works as a detector of circular borders, changing the radius and the coordinates of the center where there is a maximum change of pixels at the edges. The Wildes method primary applies a Canny filter to the iris image and generates a binary edge map, the edge points are used to obtain the parameters of the circle using the circular Hough transform. However, these methods depend on particular parameters, such as standard deviation, threshold, etc., which makes it notably dependent on the specific characteristics of the iris. Consequently, these parameters can produce the algorithm to fail to locate the iris with different characteristics (for example, dark and light iris images) [6]. Therefore, the used method of segmentation of the present project uses a variation of Wildes algorithm presented in [7], this proposed algorithm of segmentation improves the efficiency and precision of the algorithm to perform the segmentation, therefore is suitable to the present scheme in which is necessary a high accuracy of segmentation.

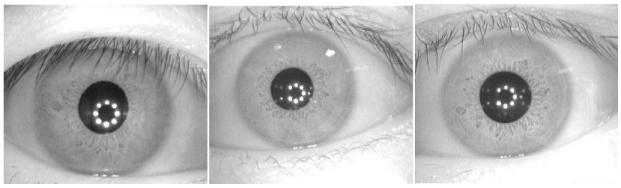

Fig 2. Three eyes, used for segmentation process

B. Arnold's Map

The Russian mathematician Vladimir Arnold used the more

general 2-dimensional chaotic map to encrypt an image [8]. Chaotic maps are completely sensible to initial conditions [9]. Arnold Map whose mapping in a three-dimensional plane describes a torus automorphism in which the mixture is much stronger than in the maps of Baker and Horeshoe [10]. The map of Arnold can be defined as the following transformation:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ N = \begin{bmatrix} 1 & t \\ q & tq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}\ mod\ N$$

Where q and t are the control parameters of matrix A. The characteristic coefficient of Lyapunov is given by (2):

$$\lambda = 1 + qt + \frac{\sqrt{t^2q^2 + 4qt}}{2} \quad (2)$$

If $q > 0$ and $t > 0$, Arnold's map is chaotic.

The parameters q and t will be part of the encryption key those parameters are extracted for the unique features of the iris. Using to the Arnold map, the image after X iterations cannot be understood, if the reverse process is done the image returns to its normal state.

C. Lorenz System

In 1963 Lorenz publish in [11], in this research he studied the models for describing the motion of the atmosphere, in terms of differential equations, obtaining the system:

$$\frac{dx}{dt} = -\sigma x + \sigma y$$

$$\frac{dy}{dt} = -xz + rx - y$$

$$\frac{dz}{dt} = xy - bz$$

where x represents the intensity of the convection, y represents the temperature difference between the ascending and descending currents, and z is proportional to the "distortion of the vertical temperature profile from linearity, a positive value indicating that the strongest gradients occur near the boundaries" [12].

The constant σ is the Prandtl number, guided by physical considerations Lorenz choose the numerical values $r = 28$ $\sigma = 10$ and b $= \frac{8}{3}$. With this configurations he observed that the systems presents high sensitivity to initial conditions [13].

D. SIFT

Scale-invariant feature transform (SIFT) [14] This algorithm seeks to detect and describe the characteristics of an image, it was patented by the University of British Columbia, and published by David Lowe in the year of 1999.

The process in general is to apply a Gaussian filter (smoothing) in varying levels varying σ

$$h(u,v) = \frac{1}{2\pi\sigma^2} e^{-\frac{u^2+v^2}{2\sigma^2}} \quad (3)$$

(3) is used to reduce the noise. Later, by Gaussian differences (as an approximation to the Laplacian-Gaussian) among consecutive images softening points of interest are sought, detected as local maxim and minim in both differential image and images before and after levels. The scaling of the object in the image and the comparison window could filter out points of higher interest, the process is repeated at multiple scales in the image, building a scale pyramid with their respective levels of sequence smoothing. As a result, points of interest corresponding to different scales and levels will be taken, therefore, as culminating steps, the points found in higher scales should be extrapolated to the original starting scale.

II. METHODOLOGY

To carry out the encryption the CASIA database was used, this provides a dataset of the iris, it was developed by the "Institute of Automation Chinese Academy of Sciences", and is one of the most known datasets in the literature for the recognition of iris. Different iris were used to encrypt the image.

The schema was implemented using OpenCV with a computer with 12 GB of RAM, Intel Core I7-4700MQ CPU 2.4GHz x 8 GEFORCE GT 740M / PCIe / SSE2 Graphic Card. The algorithm follows the next stages:

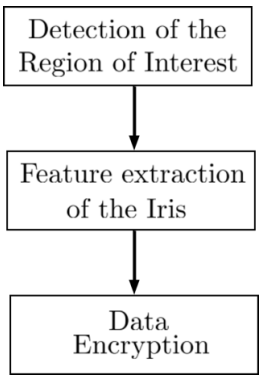

Fig. 3. General methodology proposed to encrypt data

1**. Detection of the Region of Interest:** In this stage, the image is processed in order to easily detect the region of interest using the segmentation algorithm proposed by

2. **Feature extraction:** In the present article we propose to use the descriptors of SIFT [14]. First, because the gradient information encoded in SIFT provides a generic description of the local regions of all IRIS regions. Secondly, the histogram derived from SIFT is distinctive for making iris classification. Third, SIFT is proven as one of the most robust descriptors for image analysis [15]

3. **Data Encryption**: For the encryption the key is generated from the SIFT descriptors that can reach a higher precision than Gabor and LBP [15], these descriptors will be the parameters for the permutation, the initial conditions for Lorenz map in diffusion process are fixed.

a. Permutation with Arnold's Chaotic Map

b. Diffusion with Lorenz' Chaotic System

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 4 (2020) pp. 358-363
© Research India Publications. https://dx.doi.org/10.37622/IJAER/15.4.2020.358-363

The Fig. 4 shows how this schema works.

Measures of assessment

1) *NPCR* and *UACI*

A biometric system should comply with accuracy, speed and resource requirements, be strong and robust against various attacks [1]. For that reason this part is focus on present some of them.

The number of changing pixels ($NPCR$) and Unified averaged changed intensity (UACI) are the most common measures to evaluate the strength for image encryption respect to differential attacks. Frequently a high ($NPCR$) and (UACI) is interpreted as a high resistance to differential attacks.

$$D(i,j) = \begin{cases} 1 \; if \; C^1(i,j) = C^2(i,j) \\ 0 \; if \; C^1(i,j) \neq C^2(i,j) \end{cases} \quad (1)$$

(1) defines the comparison function between the pixel of the original image and the pixel after the encryption process.

$$NPCR = N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{MN}$$

$$UACI(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{MN}$$

where C^1 represents the pixel of the original image and C^2 representing the pixel after the encryption process, M and N represents the number of rows and cols of the image.

The range of $NPCR$ and $UACI$ is [0,1]. An $NPCR$ of 0 represents that the image did not change after encryption and 1 represents that the image changes completely.

According to [16] the optimal values of $NPCR$ and $UACI$ are 99.61% and 33.46% respectively.

2) Correlation

The encryption of the image must have as a purpose a low correlation of adjacent pixels, which can be calculated using the correlation coefficient r_{xy} is given as follows:

$$r_{x,y} = \frac{(\frac{1}{N}\sum_{i=1}^{N}(x_i - x')(y_i - x'))}{(\frac{1}{N}\sum_{i=1}^{N}(x_i - x')^2)(\frac{1}{N}\sum_{i=1}^{N}(y_i - y')^2)}$$

The parameter N denotes the total number of pairs of pixels, while x_i, y_i are values of each pair of adjacent pixels.

3) Entropy

$$H = \sum_{j=0}^{2^L-1} p(m_i) \log_2 \frac{1}{p(m_j)}$$

Let $L = 8$ the number of gray levels, red, blue and green colors are in a [0,255] range and $p(m_j)$ represents the possibility that this value appear. The maximum value of entropy is 8, so the closer the entropy is to 8, the more secure the algorithm is against attacks

4) Scrambling Degree

$$\mu_{iris} = \frac{\sigma_c^2}{\sigma_i^2}$$

Where μ_{iris} denotes the degree of randomization, σ_c denotes the standard deviation of the encrypted image, $\sigma_i$denotes the standard deviation of the original image.

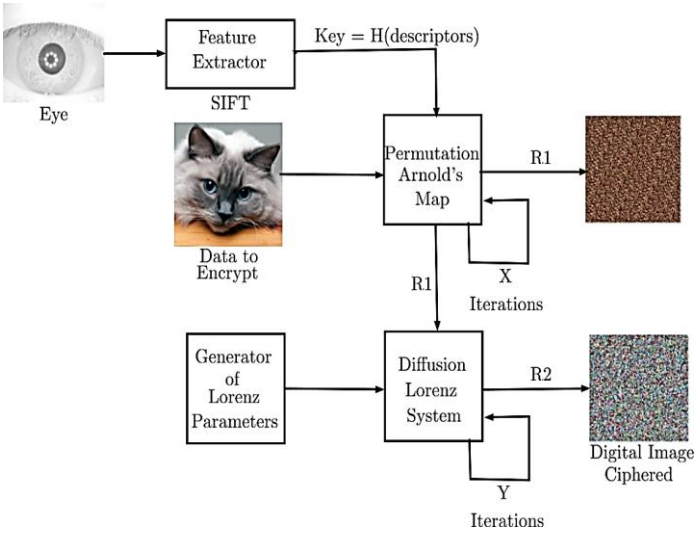

Fig. 4. Methodology proposed to cipher data using the unique features of the Iris and Chaos Theory

III. ALGORITHM DS-CHAOTIC

The algorithm proposed is shown in Fig. 4. Results were obtained from 158 iris images, some iris after the segmentation process can be seen in Fig. 5.

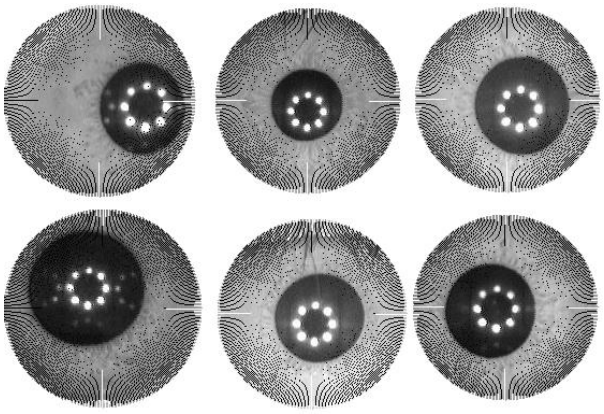

Fig. 5. Some iris after segmentation algorithm proposed in [7] used to encrypt images

After segmentation of the iris, the vector of characteristics was obtained using the SIFT algorithm, some key points of the iris can be shown in Fig. 6.

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 4 (2020) pp. 358-363
© Research India Publications. https://dx.doi.org/10.37622/IJAER/15.4.2020.358-363

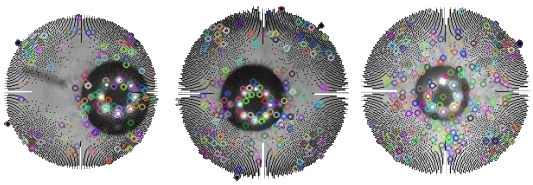

Fig. 6. Key points drawn in some regions of interest

The proposed encryption algorithm uses color images, this bases its operation through Arnold's chaotic map and it is described by the **Algorithm 1**.

Algorithm 1 Encryption Algorithm

1: **procedure** $Cipher(Img, IrisDescriptors)$
2: **for each** $descriptor$ **in** $IrisDescriptors$ **do**
3: $t \leftarrow \varphi_1(descriptor)$
4: $q \leftarrow \varphi_2(descriptor)$
5: $Img \leftarrow \mathcal{F}_A(Img, t, q)$
6: **return** Img

where $\varphi_1$and φ_2 are functions that receives a descriptor and generate a value that is used as a parameter for the Function of Arnold $\mathcal{F}_A$.

In this phase the process of permutation of the pixels of the image is carried out, in which each pixel is changed position with one-to-one correspondence, that is to say that all the pixels that make up the permuted image correspond to the group of pixels of the original image, so that it is possible to recover the real image without any distortion. Different techniques can be applied to perform the permutation of an image, for example, the Chaotic Map of Arnold is simple and efficient in its implementation, and shows good results in terms of the metric to establish how much the pixels have moved from their original position [17].

Now for each of the 158 irises the same image was encrypted, for this encryption process the Figure of Lena was used, some results after permutation can be seen in Fig. 7.

Fig 7. Some results after permutation process, using Arnold's map, the image encrypted is the same using different iris.

After Apply Arnold process, Runge-Kutta 4 method was used to generate the values of Lorenz System and then apply the diffusion process.

IV. RESULTS

Now to test the security of the encryption, the $UACI$, $NPCR$, Entropy, Scrambling degree, correlation measurements on the 158 encrypted images are calculated. Finally is shown a table with results and a comparison with a method of encryption.

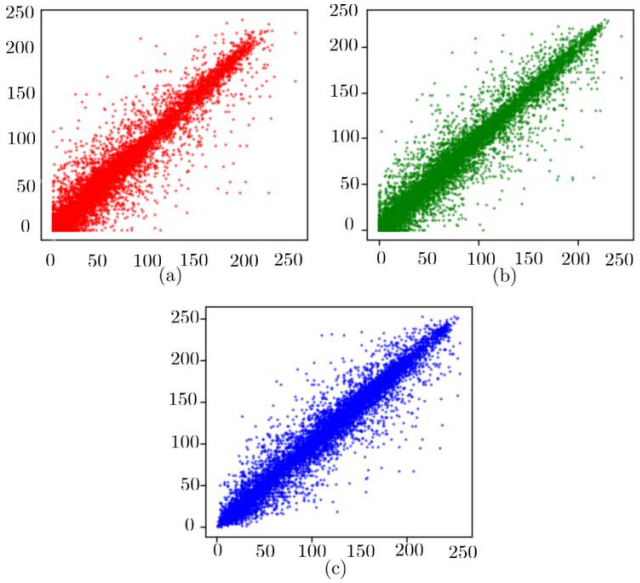

Fig. 8. Correlation plots for the real image (image to cipher), (a) Red, (b) Green, (c) Blue

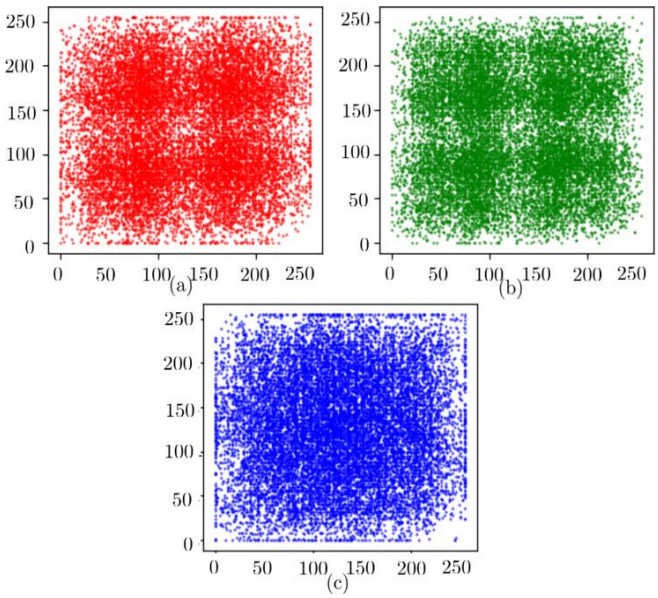

Fig. 9. Correlation plots for the ciphered image, (a) Red, (b) Green, (c) Blue

In [16] they propose another algorithm in which they compute entropy, $UACI$, $NPCR$ and correlation coefficients for gray images, in the Table I are shown the results

Table I: Comparison $UACI$, $NPCR$, Entropy, Correlation and scrambling degree for each one of the channels (R,G,B) for

the 158 iris, against results in [16]

Measure	Red	Green	Blue	Results in [16]
NPCR	0.996	0. 996	0. 995	0.996
UACI	0.544	0.529	0.504	0.335
Entropy	7.837	7.861	7.840	7.998
Correlation	0.03	0.03	0.02	0.03
Scrambling Degree	1.818	1.491	1.153	-

Based on the results, it is possible to see that the measures achieved using Chaos Theory and the iris descriptors produce optimal results, although is difficult to establish a comparison with the article [16] the present article improve the UACI and the correlation measures and reduce the entropy for the channels, finally this work extend the encryption of images for one or more channels.

V. CONCLUSIONS AND FUTURE WORK

The proposed encryption scheme produces adequate results, with high security, and therefore may suggest that it can be used in environments where there is trust between agents. Due to the nature and characteristics shown by non-linear systems and the uniqueness of the iris.

Although the algorithm successfully encrypts the image, it is not guaranteed that the iris is real. For that reason, it is proposed to develop a module that integrates some of the options from the literature [18] and [19] as a liveness detection system before the present algorithm is used.

VI. ACKNOWLEDGMENTS

Institute of Automation Chinese Academy of Science for providing the CASIA Dataset [20] and Universidad Distrital Francisco José de Caldas.

REFERENCES

[1] K. Delac and M. Grgic, “A survey of biometric recognition methods,”46th International Symposium Electronics in Marine, pp. 16–18, 2004.

[2] K. Bowyer, K. Hollingsworth, , and P. Flynn, “Image understanding foriris biometrics” Computer Vision and Understanding, vol. 110, no. 2,pp. 281–307, 2008.

[3] W. Wei and Z. Jun, “Image encryption algorithm based on the keyextracted from iris characteristics” IEEE International Symposiumon Computational Intelligence and Informatics, Budapest Hungary, November 2013.

[4] J. Daugman, “High confidence visual recognition of persons by a testof statistical independence” Pattern Analysis and Machine Intelligence IEEE Transactions, vol. 15, pp. 1148–1161, 1993.

[5] R. P. Wildes, “Iris recognition: an emergin biometric technology,”Procedings of the IEEE,, vol. 85, pp. 1348–1363, 1997.

[6] M. Erbilek and M. Fauirhurst, “Evaluating iris segmentation for scenariooptimisation,”University of Engineering and Digital Arts, University ofKent, Canterbury, Kent CT2 7NT ,UK.

[7] D. F. Santos and H. E. Espitia, “Detection of Uveal Melanoma using Fuzzy and Neural Networks classifiers,” TELKOMNIKA Telecommunication,Computing, Electronics and Control, vol. 18, no. 4, 1963.

[8] J. Peng, S. Jin, and Y. Liu, “Design and analysis of an image encryptionscheme based on chaotic maps” 2010 International Conference onIntelligent Computation Technology and Automation (ICICTA), vol. 1,pp. 1115–1118, 2010.

[9] A. H. Abdullahb, I. F. Isninb, and M. L. Ayman Altameemc, “Image encryption using a synchronous permutation-diffusion technique” Opticsand Lasers in Engineering, vol. 90, pp. 146–154, March 2017.

[10] G. Makris and I. Antoniou, “Cryptography with chaos, chaotic modelingand simulation (cmsim),” vol. 1, no. 2241–0503, pp. 169–178, 2013.

[11] E. Lorenz, “Deterministic non periodic flow. j. atmosph. sci. 20,” pp.130–141, 1963.

[12] E. Ghys, “The lorenz attractor, a paradigm for chaos,”Poincar´e Seminar, Springer Basel AG, pp. 1–54, 2010.

[13] U. of Oxford, “Three dimensional systems, the lorenz equations.”

[14] A. T. J. S. C. Liu, J. Yuen and W. Freeman, in Proc. ECCV Marseille,France, pp. 28–42, 2008.

[15] M. I. Zhenan Sun, M. I. Hui Zhang, F. I. Tieniu Tan, and J. Wang,“Iris image classification based on hierarchical visual codebook,”IEEETransactions on Pattern Analysis and Machine Intelligence, vol. 36, June2014.

[16] S. Z. X. Zhang, C. Wang and Q. Yao, “Image encryption scheme basedon balanced two-dimensional cellular automata,”Math. Problems Eng.,vol. 9, pp. 1–10, 2013.

[17] S. K. Abd-El-Hafiz, S. H. AbdElHaleem, and A. G. Radwan, “Per-mutation techniques based on discrete chaos and their utilization inimage encryption,”13th International Conference on Electrical En-gineering/Electronics, Computer, Telecommunications and InformationTechnology (ECTI-CON), 2016.

[18] E. L. K. Park and J. Kim, “Fake iris detection by using purkingj image,”Procedings ICB and Hong Kong China, pp. 397–403, 2006.

[19] S. Lee, K. Park, , and J.Kim, “Robust fake iris detection based onvariation of the refelectance ratio between the iris and the sclera, ”Proc. Biometric

Consortium Conf, Baltimore, USA, 2006.

[20] Center for Biometrics and Security Research, "Institute of AutomationChinese Academy of Sciences," online, accessed 20 Sep, 2018, Sep2005, http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp