3rd International Conference on Automation, Control, Engineering and Computer Science (ACECS'16)
Proceedings of Engineering & Technology (PET)
pp. 417-422
Copyright IPCO-2016

A Light Weight Method for Image Encryption Based on Chaos and Hopefield Neural Networks

Nabil Ben Slimane
Faculty of Sciences of Monastir
Electronics and Micro-Electronic
Laboratory Monastir, Tunisia
Email:nabilbenslimane88@gmail.com

Kais Bouallegue
Faculty of Sciences of Monastir
Electronics and Micro-Electronic
Laboratory Monastir, Tunisia
Email: kais_bouallegue@yahoo.fr

Mohsen Machhout
Faculty of Sciences of Monastir
Electronics and Micro-Electronic
Laboratory Monastir, Tunisia
Email: machhout@yahoo.fr

***Abstract*—Classical cryptographic algorithms has been widely studied by both scientists and hackers. Consequently, scientists are now trying to explore and find new algorithms to protect information against unauthorized access, security information and data becomes an important skills. Due to the increasing use of images in embedded systems and many domains such as industrial and medical.In this paper we propose a light weight method to encrypt and decrypt image using a combination between chaotic attractor of Henon and hopefield neural networks. Simulations show that the proposed encryption method is effective and has a high speed and level security.**

Keywords Image encryption . Chaotic Attractor . Hopefield Neural Network . Cryptosystem

I. Introduction

Encryption is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication [1]. The data of image could also be used by hackers that it may cause uncountable losses for the owner of images, to avoid these problems, it has become necessary and imperative to encrypt digital images before sending them. Traditional encryption algorithms such as DES (Data Encryption Standard), RSA (Rivest, Adi Shamir and Leonard Adleman) and AES(Advanced Encryption Standard) are not suitable design for image encryption due to some intrinsic features images such as the strong correlation between adjacent pixels, size, high redundancy. Moreover, these algorithms require more than the usual expected computation time and power while performing image encryption [2].To provide a better solution to image security problems, many methods for image encryption have been proposed such as which use chaotic systems that provide a good combination of speed performance and high security level. Many scientists have investigated and analyzed many chaos-based encryption algorithms in [3], [4], [5] and [6], all these works have been realized with the motivation of chaotic properties such as the sensitive on initial conditions and systems parameters, topological transitivity, nonperiodicity and pseudo-random property, other scientists has been going to use neural networks (NN), hopefield neural networks (HNN) [7], [8], [9], [10] for encryption algorithms seen an important role in information security for encryption/decryption of either text and Multimedia data, moreover (HNN) are the ability to generalize results obtained from known situations to unforeseen situations, the fast response time in operational phase, the high degree of structural parallelism, reliability, and efficiency [11], however the traditional cryptography methods and algorithms based on discrete mathematics which is very complex to implement and explore for image encryption. In this paper we propose a new cryptosystem using the combination between Henon attractor and hopefield neural networks to encrypt and decrypt image, the proposed algorithm is divided into two stages confusion and diffusion and respect classic Shannon requirement's[12]. In simulation the results illustrated show that our cryptosystem is efficient.

II. Models description

A. Henon map

The Henon map is a 2-D iterated map with chaotic solutions [13]. Its mathematical expression is given by Eq (1)

$$\begin{cases} x_{v+1} = y_v - ax_v^2 \\ y_{v+1} = bx_v \end{cases} \quad (1)$$

where x and y are the state variables, and the values of x and y at the v^{th} iteration are denoted by x_v and y_v respectively. To keep the map under chaotic state, the control parameters a=1.4 and b=0.3. In the proposed cryptosystem, Henon map is injected into neural model.

B. Neural model

A model describing the dynamics of the activity of neurons is described as follows [14] and he is given by Eq (2)

$$\begin{cases} \dot{w} = \frac{-w}{\tau} + f(qz)f(pw) + I \\ \dot{z} = \alpha z + \alpha f^2(pw) \end{cases} \quad (2)$$

where $\alpha = \frac{1}{B}$, p q are the positive constant, B is a time constant and I is an input signal.

$f(x) = 3xexp(\frac{-x^2}{2})$, $I(t) = \epsilon(sin\omega t)$

ISSN: 2356-5608

C. Neural-chaos model

The used model of chaotic sequence in our cryptosystem is given by Eqs (3) and (4)
(1) $\longrightarrow f_1(x,y)$, (2) $\longrightarrow f_2(w,z)$

$$\begin{cases} U = f_2 o f_1 = (f_1(x,y), f_2(w,z)) \\ \\ V = f_2 o f_1 = (f_1(x,y), f_2(w,z)) \end{cases} \quad (3)$$

$$\begin{cases} U = \frac{-f(x)}{\tau} + f(qf(y)) + f(pf(x)) + I \\ \\ V = \alpha f(y) + \alpha f^2(pf(x)) \end{cases} \quad (4)$$

III. Proposed image encryption/decryption algorithm

A. Image encryption process

In the proposed encryption algorithm, the image is encrypted using the combination of chaotic attractor of Henon and hopefield neural networks(HNN) as shown in Figure 1. Image $A_{N\times N}$ is loaded then we injected into confusion stage to permute the plainimage pixels without performing any change in their values while diffusion the scrambled image are XORED by chaotic matrix generated by chaos and hopefield neural networks to modify the values of each pixel to obtain ciphered image $ACR_{N\times N}$. Chaotic-neural sequence map can be defined by Eqs. (3) and (4) respectively.
Chaotic-neural sequence can be defined for an image $N \times N$.Its is given by Eq (5)

$$\begin{cases} U_{i+1} = (K.U_i) mod 256 \\ \\ V_{i+1} = (K.V_i) mod 256 \end{cases} \quad (5)$$

Where $1 \leqslant i \leqslant N$, K is an external integer key and U,V are the neural-chaotic state variables, and the values of U and V at the i^{th} iteration are denoted by U_i and V_i respectively.

1) Permutation pixels stage: The permutation pixels is the first stage of our encryption algorithm after the generation of two chaotic index sequence U_i and V_i to ensure permutation. Equation (5) is used to generate the index sequence of permutation which used for pixels permutation based on the ascending sorting of the chaotic-neural sequence, the initial condition of chaotic attractor is derived from parameters of chaotic neural sequence and input integer key.

2) Diffusion pixels stage: The modification gray-scale pixels values are the final stage to get a ciphered image, in this stage two chaotic sequences are generated using the same equation used in permutation stage except that we iterate each sequence $\frac{N\times N}{2}$ time.

Then we merge these two chaotic sequences into one vector named VS having $N \times N$ values to create a chaotic matrix $MI_{i,j}$ using Eq (6)

$$MI_{i,j} = reshape(VS, [N, N]) \quad (6)$$

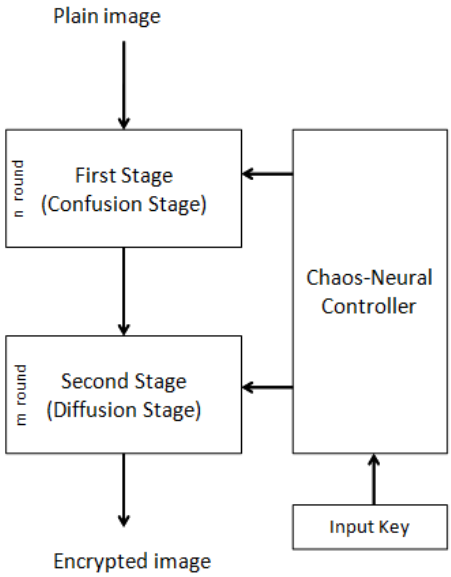

Fig. 1. Global architecture of proposed cryptosystem

Adapt matrix $MI_{i,j}$ by Eq (7) such that each element of level gray it ranges in [0,255].

$$MI_{i,j} = (round(10^5 MI_{(}i,j))) mod 256 \quad (7)$$

Finally compute the matrix $MI_{i,j}$ with permuted image $AP_{i,j}$ to obtain a ciphered image. the output of ciphered image is given by Eq (8)

$$ACR = AP \oplus MI \quad (8)$$

Where $\oplus$ denotes the exclusive OR operation bit-by-bit

B. Image decryption process

The decryption process is the reverse operation of the encryption process. Using the secret keys, we can generate two chaotic index sequences and the same chaotic matrix MI in encryption process .The decryption algorithm also consists of two stages. First, the cipherimage ACR is de-shuffled to produce permuted image AP by the chaotic matrix MI. Equation (9) is given to obtain the permuted image, then we permute pixels positions using two chaotic index sequences to obtain the plainimage.

$$AP = ACR \oplus MI \quad (9)$$

Where $\oplus$ denotes the exclusive OR operation bit-by-bit

IV. Simulation results and security statistical analysis

A. Statistical analysis

A good encryption cryptosystem should make the cipherimage confusing enough so that an attacker cannot explore any useful information from a statistical point of

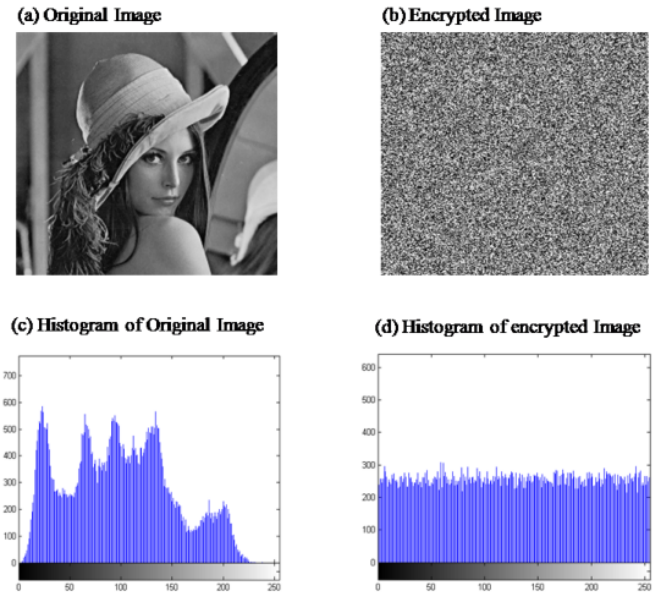

Fig. 2. Histograms of the plainimage and cipherimage

view. This requires of the cryptosystem has good randomness, and a chaotic sequence is very important to meet that. Here, we illustrate statistical analysis from four indicators: the histograms, correlations of two adjacent pixels, the information entropy and the differential attacks.

1) Histogram of ciphered image: The image histogram show how pixels in an image are spread by drawing the number of pixels at each color intensity level.The construction and computation of the histograms of the several cipherimages and their plainimages. We select several gray-scale images (256×256) having different contents, one example of Lena image is shown in Figure 2. In the histogram of the ciphered image we can remark that is uniform and is significantly different from that of the original image. Moreover, it does not exist any trace to employ any statistical attacks on the image under consideration.

2) Correlation of two adjacent pixels: We compute the correlation coefficients of adjacent pixels for both plainimage/cipherimage . This is done through estimating the correlation among two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in original and corresponding encrypted image. We select randomly 2000 pairs of two adjacent pixels from the image. Then, we compute correlation coefficients by the following Eq (10)

$$cov(x, y) = E(x - E(x))(y - E(y)) \tag{10}$$

Where x and y are gray-scale values of two adjacent pixels in the image. Figure 3 show the correlation distribution for 2000 pairs of horizontally adjacent pixels in one plainimage (Lena), and its corresponding cipherimage with the proposed algorithm for image encryption. A

TABLE I
CORRELATION COEFFICIENTS COMPARISON OF THE PROPOSED ALGORITHM FOR IMAGE ENCRYPTION WITH OTHERS, WE ADOPT THAT **(1)**:IMAGE NAME **(2)**:DIRECTION OF ADJACENT PIXELS **(3)**:CORRELATION PLAINIMAGE AND **(4)**:CORRELATION OF CIPHERIMAGE

(1)	(2)	(3)	(4)	[17]	[18]
Lena	Horizontal	0.9961	0.0021	0.0802	0.032
	Vertical	0.9928	0.0037	0.0706	0.027
	Diagonal	0.9841	0.0017	0.0738	0.038
Baboon	Horizontal	0.9090	0.0012	0.0773	NA
	Vertical	0.8250	0.0018	0.0770	NA
	Diagonal	0.7331	0.0011	0.0693	NA
Man	Horizontal	0.9878	0.0021	NA	NA
	Vertical	0.9783	0.0028	NA	NA
	Diagonal	0.9687	0.0019	NA	NA

comparison between correlation coefficients for horizontal, diagonal and vertical directions of both plainimages and cipherimages for three digital images (Lena, Baboon and plane) using the proposed image cryptosystem with chaotic attractor of Henon and neural networks is shown on Table I. Figure 3 show that the two adjacent pixels in the plainimages are strongly correlated however in the cipherimages, there is very low correlation between the two adjacent pixels for all images encrypted using our proposed algorithm for image encryption.
According to the values of correlation listed in Table I our proposed algorithm have a minimum absolute value of correlation coefficient in all used images for encryption test, it mean our cryptosystem is secure and efficient.

3) Entropy information: Entropy information is a mathematical theory for data communication and storage. Now, information theory is interested with correction of errors, compression of data and cryptography the entropy H(m) is computed by Eq (11)

$$H(m) = \sum_{i=0}^{2^N-1} P(m) \log_2 \frac{1}{P(m_i)} bits \tag{11}$$

where $P(m_i)$ is the probability of symbol m_i and the entropy is measured in bits. The entropy analysis test are executed on three images test, the Table II show the result it mean that the proposed cryptosystem for image encryption is nearly to proved theoretical entropy value which equals 8, to conclude that our cryptosystem respect to the entropy attack.
Table II show different values of entropies.

4) Differential attacks: Based on principles of cryptology, a good encryption algorithm should be sensitive to the plaintext sufficiently [15]. The sensitivity of the encryption algorithm can be quantified as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity

TABLE II
ENTROPIES ANALYSIS OF THE PROPOSED IMAGE CRYPTOSYSTEM

Image test	Lena	Baboon	Man
Entropy	7.9963	7.9848	7.9915

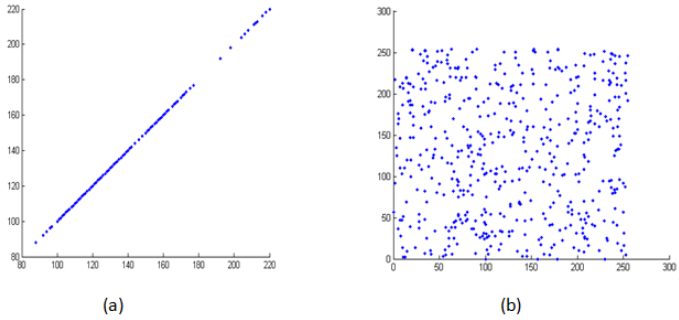

Fig. 3. Correlation of two horizontally adjacent pixels; (a) in the plainimage, and (b) in the cipherimage

(UACI).NPCR UACI are computed using Eqs (12) and (13) respectively.We can easily show different values of plaintext sensitivity on Table III.

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} G(i,j) \times 100\% \qquad (12)$$

$$UACI = \frac{1}{M \times N} \left(\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|Q_1(i,j) - Q_2(i,j)|}{255} \right) \times 100\% \qquad (13)$$

where M and N represent the width and height of the image respectively, Q_1 and Q_2 are cipherimage before and after one pixel is changed of one plainimage. According to values listed on Table III our cryptosystem is securely resistant against differential attacks.

B. Key space analysis

A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute force attacks infeasible [16]. The key space in our cryptosystem is estimated by the number of parameters used to drive chaotic hopefield neural network sequence.The initial condition and system parameters α, a, b and an integer Key K. If the precision is about10^{-16}, the key space is 10^{64}. So its enough to resist attack, moreover we have $K_t = \alpha, a, b, K$ is the key space in permutation stage with n round is K_t^n, the same in the second stage of encryption when using m round if K_t we have the key as K_t^m so in our scheme the key take the same space during encryption with key space $K_t^n K_t^m$.

TABLE III
VALUES OF PLAINTEXT SENSITIVITY

Image test	NPCR %	UACI %
Lena	99.6012	32.9426
Baboon	99.5996	30.0287
Man	99.6182	30.1248

TABLE IV
RUNNING TIME ENCRYPTION OF THE PROPOSED IMAGE CRYPTOSYSTEM

Image Test	256 × 256	512 × 512	1024 × 1024
Time(s)	0.0053	0.0112	0.038

C. Performance of the proposed cryptosystem

The implementation of our cryptosystem allows to estimate the performance of the reported image algorithms.an indexed image for"lena" is used as a plainimage.The specifications for utilized PC in all software implementation and tests were 3.06 GHz Pentium IV with 160 G hard-disk and 1024 MB of memory.To encrypt 256 × 256 gray-scale image is about 0.0053 s, our proposed chaotic-neural cryptosystem has a high speed and he is suitable for embedded systems.
Table IV compare the performance of the proposed image cryptosystem with different images size.

V. CONCLUSION

In this work, an efficient, secure and robust cryptosystem for image encryption is reported which is realized using two main process confusion and diffusion stage using chaotic neural key.The first stage of confusion is computed by permuting the pixel position by combination of chaotic attractor and neural networks, the second stage is the modification of pixels values controlled by the same chaotic sequence used in the fist process with a keystream and the number of iteration n and m respectively for confusion and diffusion process. Our experimental results show a good cryptographic features of level security and speed in image encryption.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology, 27, (2007).
[2] L.S. Chen, G.X. Zheng, Multimedia Security Handbook, CRC Press,2005.
[3] Chengqing Li, Tao Xie, Qi Liu, Ge Cheng, Cryptanalyzing image encryption using chaotic logistic map, Nonlinear Dyn, 78, 1545-1551, (2014).
[4] Fuh-Gwo Jenga, Wei-Lun Huangb, Tzung-Her Chen, Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes, Signal Processing: Image Communication, 34, 45-51, (2015).
[5] Lin, A. ; Jui-Cheng Yen, Design and realization of a new chaotic neural encryption/decryption network, Circuits and Systems, IEEE Asia-Pacific conf, 335-338, (2000).
[6] Ming Yang ; Trifas, M, Applied image processing to multimedia information security, Conf Image Analysis and Signal Processing,104-107,(2009).

[7] Jain, A.; Rajpal, N, A two layer chaotic network based image encryption technique,Conf Computing and Communication Systems (NCCCS),1-5, (2012).
[8] Wei Zheng; Zhiguang Zhao, Wavelet domain digital image hiding algorithm based on CNN encryption, conf Computer Application and System Modeling, 8, 386-390, (ICCASM), (2010).
[9] Leimin Wang, Yi Shen, Finite time stabilization of delayed neural networks,elsevier, 70, Pages 74-80, (2015).
[10] Joseph Chrol-Cannon, Yaochu Jin, Computational modeling of neural plasticity for self-organization of neural networks,elsevier, 125, Pages 43-54, (2014).
[11] I. Darkiran, K. Danisman, Artificial neural network based chaotic generator for cryptology, The Turkish Journal of Electrical Engineering Computer Sciences, 18, 744-753, 2010
[12] Shannon CE (1949) Communication theory of secrecy system. Bell Syst Technol J 28, 656-715
[13] Hénon M (1976) A two-dimensional mapping with a strange attractor. Commun Math Phys 50(1), 69-77
[14] Chunguang Li, Guanrong Chen, Coexisting chaotic attractors in a single neuron model with adapting feedback synapse, elsevier, 23, 1599-1604, (2005)
[15] Jianfeng Zhao, Shuying Wang, Yingxiang Chang, Xianfeng Li, A novel image encryption scheme based on an improper fractional-order chaotic system, Nonlinear Dyn, DOI 10.1007/s11071-015-1911-x, (2015).
[16] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D.Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, Proceedings of Fast Software Encryption - FSE 00, number 1978 in Lecture Notes in Computer Science, pages 213-230.Springer-Verlag, 2000.
[17] Ramzi Guesmi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, Mounir Samet, Hash key-based image encryption using crossover operator and chaos,Multimed Tools Appl, pp 1-17,(2015)
[18] Xingyuan W, Canqi J, Image encryption using game of life permutation and PWLCM chaotic system Opt Commun 285, 412-417,(2012)