Masking Digital Image using a Novel technique based on a Transmission Chaotic System and SPIHT Coding Algorithm

Masking Digital Image

[1]Hamiche Hamid
Laboratoire de Conception et Conduite des Systèmes
de Production, UMMTO, BP 17 RP, 15000,
Tizi-Ouzou, Algérie

[2]Lahdir Mourad
Laboratoire d'Analyse et Modélisation des Phénomènes
Aléatoires, UMMTO, BP 17 RP, 15000,
Tizi-Ouzou, Algérie

[3]Tahanout Mohammed
Laboratoire d'Analyse et Modélisation des Phénomènes
Aléatoires, UMMTO, BP 17 RP, 15000,
Tizi-Ouzou, Algérie

[4]Djennoune Said
Laboratoire de Conception et Conduite des Systèmes
de Production, UMMTO, BP 17 RP, 15000,
Tizi-Ouzou, Algérie

Abstract— **In this article, a new transmission system of encrypted image based on novel chaotic system and SPIHT technique is proposed. This chaotic system is made up of two chaotic systems already developed: the discrete-time modified Henon chaotic system and the continuous-time Colpitts one. The transmission system is designed to take profit of two advantages. The first is the use of a robust and standard algorithm (SPIHT) which is appropriate to the digital transmission. The second is to introduce farther complexity of the encryption using the chaotic system over secure channel. Through these two advantages, our purpose is to obtain a robust system against pirate attacks. Cryptanalysis and various experiments have been carried out and the results were reported in this paper, which demonstrate the feasibility and flexibility of the proposed scheme.**

Keywords- Chaos Modified Henon;Colpitts, SPIHT; Robustness.

I. INTRODUCTION

The fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. To meet this challenge, a variety of encryption schemes have been proposed [1-4]. Nevertheless, conventional image encryption algorithm such as data encryption standard (DES) is not suitable for image encryption. Because of the special storage characteristics of an image [5] and weakness of low-level efficiency when the image is large [6-7]. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions, system parameters, the density of the set of all periodic points and topological transitivity. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography [8]. Matthews proposed a chaotic encryption algorithm in 1989 [9]. Since then, researches of image encryption technology which are based on chaotic systems are increased [10-14]. These methods have high-level efficiency but also weakness, such as small key space, weak security and complexity to overcome these drawbacks. In this paper, a novel image encryption scheme incorporating a chaotic map is introduced. This scheme integrates chaotic encryption into the process of bit stream generation by an SPIHT (Set Partitioning In Hierarchical Tree) encoder. The proposed scheme only introduces few overheads to the image coder by using selective encryption, i.e., only sensitive bits in the compressed stream are encrypted.

Meanwhile, since a cipher-text feedback mechanism is employed, many powerful attacks such as the known-plain-text attack are not valid to break the designed cryptosystem. Furthermore, due to the use of chaotic pseudo-random bits, which efficiently masks the SPIHT coding bitstream, the ciphered stream can be truncated at any position while keeping the obtained bits decipherable. The rest of the paper is organized as follow. Section 2 discuses the proposed chaos-based image encryption scheme. Section 3 shows some numerical results. In section 4, we analyze the security of the new chaotic encryption scheme. Finally, section 5 concludes the paper.

II. THE PROPOSED CHAOS-BASED IMAGE ENCRYPTION SCHEME

In this work a communication system based on chaos encryption and SPIHT coding is realized. The global scheme of the proposed system for private communications is shown in Fig. 1. Note that the transmission channel is a public one. Consequently, any hacker has a free access to information passing through the channel which is considered perfect in our works.

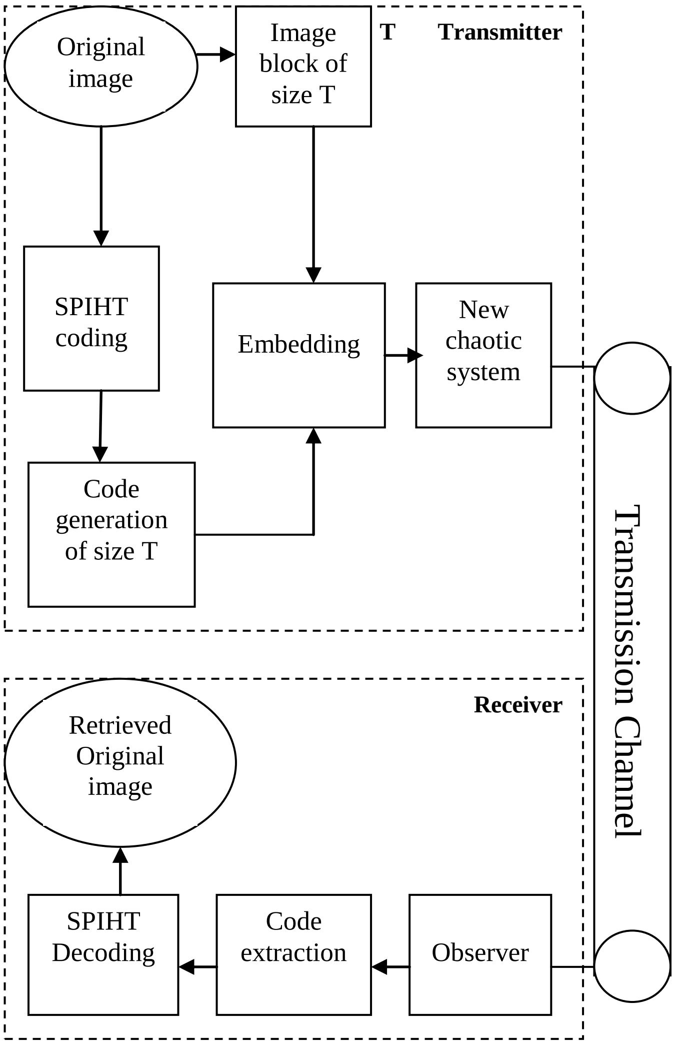

Figure 1. Transmission chain based on a chaotic dynamical system and SPIHT coding

III. TRANSMITTER PRESENTATION

The transmitter is composed of two main blocks (see Fig. 1): a SPIHT coding block and chaotic system block.

A. *SPIHT Coding*

Progressive coding (also called embedding coding) refers to the way that the most significant bits representing an image are placed at the beginning of the code. The code bits are arranged according to their importance relative to the representation of the image. A decoder can truncate the code at any position and obtain an estimate of the image based on the information up to that particular point. There are two well-known progressive coding schemes which are EZW (Embedded Zerotree Wavelet coding) [15] and SPIHT algorithms [16-19]. Note that SPIHT algorithm is more efficient than EZW. After the subband decomposition is applied to the concerned image, the SPIHT algorithm works by partitioning the subband-decomposed image into significant and insignificant partitions by using the following function:

$$S_n(T) = \left.\begin{array}{c} 1 \max\limits_{i,j\in T}\left\{\left|C_{i,j}\right|\right\} \geq 2^n \\ 0 \text{ otherwise} \end{array}\right\} \qquad (1)$$

Where $S_n(T)$ represents the significance of a set of coordinates T and $C_{\{i, j\}}$ is the coefficient value at coordinate (i, j).

There are two passes in the algorithm: the sorting pass and the refinement pass. Three lists are defined, which are the list of insignificant sets (LIS), list of insignificant pixels (LIP), and list of significant pixels (LSP), respectively. The LIP and LSP consist of nodes that contain single pixels, while the LIS contains nodes that have descendants. The sorting pass is performed on these three lists and finally makes pixels in LSP, which is arranged in an order according to the information importance. The maximum number of bits required to represent the largest coefficient in the spatially oriented tree is designated as n_{max}, computed by the following formula:

$$n_{\max} = \left\lfloor \log_2\left(\max_{i,j}\left\{\left|C_{i,j}\right|\right\}\right)\right\rfloor \qquad (2)$$

During the sorting pass, those coordinates of the pixels that remain in LIP are tested for the significance. The result $S_n(T)$ is then sent to the output. Those that are significant will be moved to LSP, along with their sign bits output. Sets in LIS will also have their significance tested and, if they are found to be significant, they will be removed. Consequently the result will be partitioned into subsets. Subsets with a single coefficient, if found to be significant, will be added to LSP, or else they will be added to LIP.

During the refinement pass, the *nth* most significant bit of the coefficients in LSP is an output. The value of n is then decreased by 1 and the sorting and refinement passes are repeated.

This process continues until either the desired rate is reached, or $n = 0$, and all the nodes in LSP have their bits output. The latter case will result in an almost perfect reconstruction since all the coefficients have been processed completely.

There are two features reside in the SPIHT, which makes the design to be introduced in the next section. First, the SPIHT is not noise tolerant, i.e., the method is sensitive to small modification of bits in their bitstreams. Secondly, from the above discussion, it is clear that there are two kinds of data contained in a SPIHT-coded bitstream: they are named structure bits and data bits, respectively. Structure bits refer to those used for synchronizing the encoding end and the decoding end in the construction of spatially oriented tree. These bits are extremely sensitive to noise, especially the first few bits in the bitstream. Data bits refer to those coding signs of image coefficients or coding values of coefficients generated in the refinement pass. Change of data bits does not seriously affect the reconstruction of the image, but only introduces a small amount of noise to the result.

Thus, to protect an image, an efficient method is to encrypt only those structure bits.

B. New Chaotic System

The new chaotic system is the discrete-time modified Henon chaotic system which is coupled with the sampled continuous-time Colpitts chaotic system. The new chaotic system block is detailed as follows:

1) Discrete-time chaotic system

The discrete-time chaotic system is the modified Henon's map (see for example [20-21]). A simplified version of our proposed discrete scheme is:

$$\left.\begin{aligned} x_1(k+1) &= a - x_2^2\ (k) - bx_3(k) \\ x_2(k+1) &= x_1(k) \\ x_3(k+1) &= x_2(k) \\ y(k) &= x_2(k) \end{aligned}\right\} \qquad (3)$$

where $x = [x_1\ x_2\ x_3]^T \in R^3$ denote the state vector and y(k) the output. Chaotic behavior of system (3) as shown by Fig. 2 is obtained by setting its parameters a=1.76 and b=0.1. These parameters are chosen such that system (3) exhibits chaotic behavior. Initial conditions $x_1(0)=1$, $x_2(0)=0.1$ and $x_3(0)=0.1$ are chosen inside the strange attractor basin.

In private communication, one of the main purposes is to increase the security. It is interesting to modify the system (3) by introducing in its dynamic, the sampled states of a continuous-time chaotic system. The continuous-time chaotic system used in our work is given as follow:

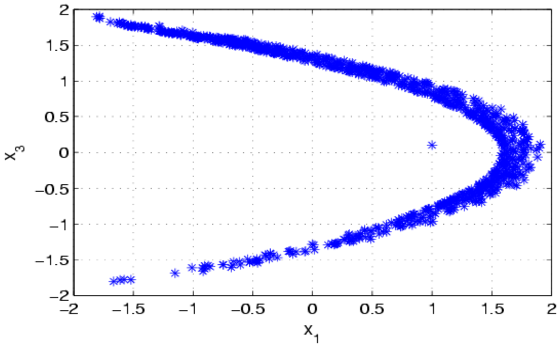

Figure 2. Chaotic attractor of modified Henon system

2) Continuous-time chaotic system

This system has been widely studied in the literature [22-23]. The state equations of the normalized Colpitts's oscillator in a continuous time are given as:

$$\left.\begin{aligned} \dot{z}_1 &= a_1(-\exp(-z_2)+1+z_3) \\ \dot{z}_2 &= a_2 z_3 \\ \dot{z}_3 &= -a_3(z_1+z_2) - a_4 z_3 \end{aligned}\right\} \qquad (4)$$

Where $z = [z_1\ z_2\ z_3]^T \in R^3$ is the state vector and $a_1 = \frac{g}{q(1-k)}, a_2 = \frac{g}{qk}, a_3 = \frac{qk(1-k)}{g}, a_4 = \frac{1}{q}$.

To have a chaotic behavior as shown by Fig. 3, the parameters of system (4) are given as follows: g=4.46; q=1.38 and k=0.5. Initial conditions $z_1(0)=1.6$, $z_2(0)=8$ and $z_3(0)=0.1$ are chosen inside the strange attractor basin.

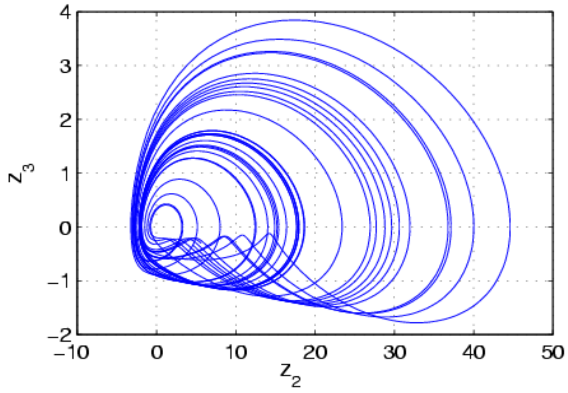

Figure 3. Chaotic attractor of Colpitts system

In order to make the transmitter more complex thus more robust (see Section 4), we have chosen to add the three states (z_1, z_2, z_3) and the message m to the third dynamic of the system (3). Then, the new obtained coupled system is:

$$\left.\begin{aligned} x_1(k+1) &= a - x_2^2\ (k) - bx_3(k) \\ x_2(k+1) &= x_1(k) \\ x_3(k+1) &= x_2(k) + A_1 z_1(nT) \\ &\quad + A_2 z_2(nT) + A_3 z_3(nT) + cm(k) \\ y(k) &= x_2(k) \end{aligned}\right\} \qquad (5)$$

Where A_1, A_2, A_3 and c are the new parameters of the new discrete-time chaotic system, $n \in N$ and T is the sampling period of the system (4). To preserve the chaotic behavior of the system defined by (5), these parameters are chosen with precaution. In our case, we must respect the following values:

$A_1 \leq 0.01, A_2 \leq 0.01, A_3 \leq 0.1$ and $c \leq 1$. The strange attractor oh the new chaotic discrete-time is shown by the Fig. 5.

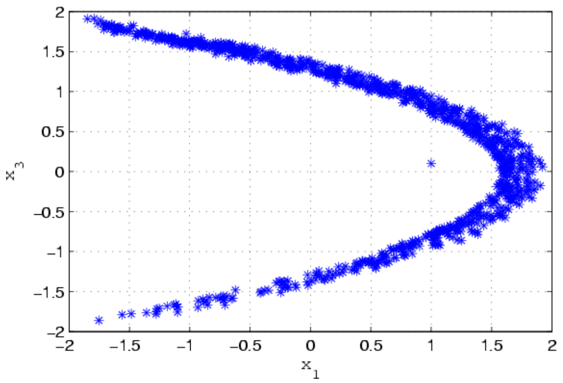

Figure 4. Chaotic attractor of new chaotic system

IV. Receiver Presentation

The receiver is also composed of two main blocks (see Fig. 1): a chaotic observer and SPIHT decoding block. The receiver blocks are detailed as follows:

A. *Chaotic Observer*

In this part, the system (5) with the output y(k)=x_2(k) is considered. For the reception, based on the works of [24-25], we have designed a delayed discrete observer that works with a sampling time T and which allows to reconstruct all states and the transmitted message m of (5). The design of the observer is detailed in the work [26], it is given as follow:

$$\left.\begin{aligned} \hat{x}_1(k-1) &= y(k) \\ \hat{x}_3(k-2) &= \frac{a-y(k)-y^2(k-2)}{b} \\ \hat{m}(k-3) &= \frac{a-y\ (k)-y^2(k-2)}{bc} \\ &\quad - \frac{y(k-3)+A_1 z_1(nT-3)+A_2 z_3(nT\ \ -3)}{c} \\ &\quad - \frac{A_3 z_3(nT-3)}{c} \end{aligned}\right\} \qquad (6)$$

B. *SPIHT Decoding*

The SPIHT decoding is the inverse process of SPIHT coding. So we may refer to the concrete procedures of the encryption algorithm as explained in the subsection 2.1.1. In the following section, the numerical results are given.

V. Numerical Results

Numerical results and performance analysis of the proposed image encryption scheme are provided in this section. Fig. 5 depicts the original image which is a 256×256 size 8 bits Lena image.

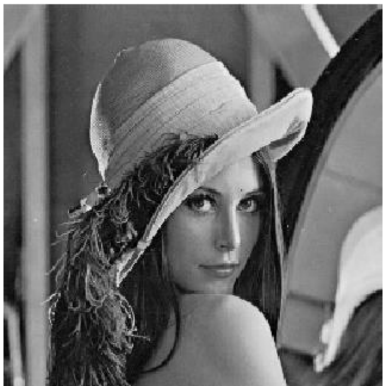

Figure 5. Original image

Figs. 6 and 7 show results of encrypting image and decrypting image, respectively. It can be seen that the decrypted image is clear and correct without any distortion with PSNR (Peak Signal to Noise Ratio) equal to 28.51 dB. This result shows clearly the performance of the used method.

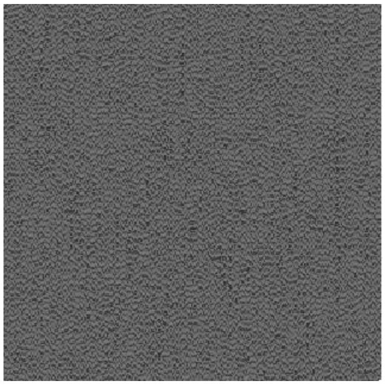

Figure 6. Encrypted image

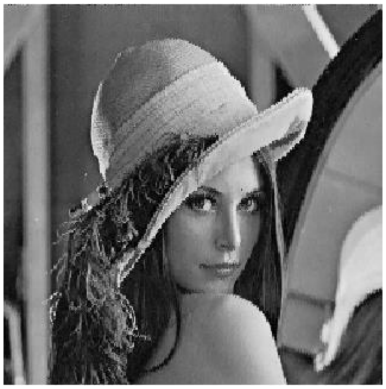

Figure 7. Decrypted image

Figs. 8 and 9 show some results of decrypting with 0.05 bpp (bits per pixel) and 1 bpp, respectively. In the following section, the robustness of the proposed scheme is studied.

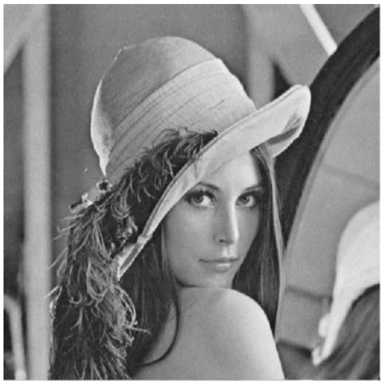

Figure 8. Decrypted image with 0.5 bpp

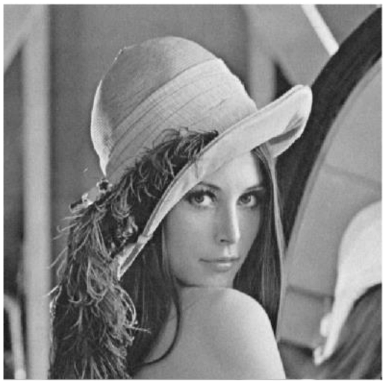

Figure 9. Decrypted image with 1 bpp

VI. SECURITY ANALYSIS

The security of the above-described chaos-based encryption scheme is now analyzed by studying two tests: histogram analysis and key space analysis.

A. *Histogram Analysis*

As expected, the test results show that the histogram of encipher-image is quasi uniform, which makes statistical attacks difficult.

This result is in accordance with the result given by Fig. 6, Figs. 10 and 11 show the histograms of plain and encrypted image, respectively.

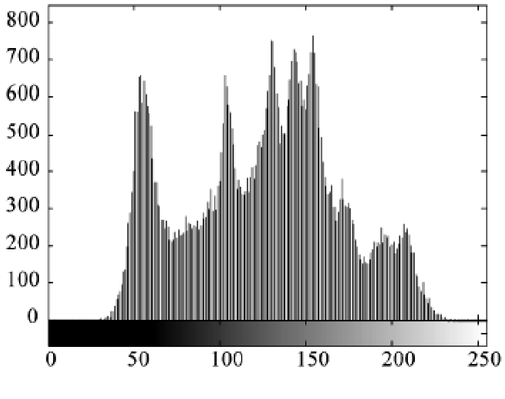

Figure 10. Histogram of plain image

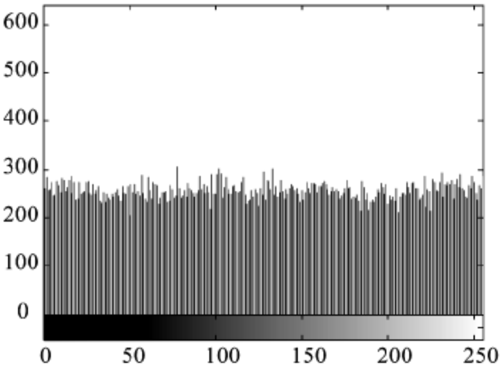

Figure 11. Histogram of encrypted image

B. *Key Space Analysis*

One of the most important properties of cryptographic systems is the existence of a secret key which defines the level of security of the cryptosystem [27-28]. The better secret key is designed, the larger is the key space hence and the more secure is the cryptosystem. Chaotic systems are well-known for their high sensitivity to initial conditions and parameters variations. From a cryptographical viewpoint, the initial conditions and the parameters of chaotic systems may be used to define a secret key for the chaos-based communication systems.

In the present case-study, in which we have used two chaotic systems in the transmitter (continuous and discrete systems), let us assume that the initial conditions are exactly known by a non-authorized intruder. We consider the parameters of the two systems to construct a secret key for our communication scheme. Firstly, we suppose that a non-authorized intruder knows the structure of the two chaotic systems without knowing exactly the true values of their parameters.

Let P_i:=(p_1=g, p_2=q, p_3=k, p_4=a, p_5=b, p_6=A_1, p_7=A_2, p_8=A_3) be the secret key. Our aim is to determine the size *r* of the key space K_s={P_1, P_2,..., P_r} which represents the finite set of all possible keys in order to evaluate the level of security produced by the secret key. To that end, we have to define the range of variation and the sensitivity of each parameter p_i, for i=1,...,8.

Without much loss of generality, we assume that the size s of the interval of variation of each parameter pi that leads to chaotic behaviors of the two systems is equal to 10^{-1}. Simulation experiments are carried out to evaluate the sensitivity S_i of each parameter P_i by determining the smallest parameter mismatch that gives us two different chaotic behaviors (i.e., two different attractors) when the rest of parameters p_j, for $j \in 1,2,...8/\, i$ are fixed.

Figs. 12 and 13 illustrate the sensitivity of the two systems to small changes of parameters g and a, respectively. The sensitivity to parameters is illustrated in TABLE I.

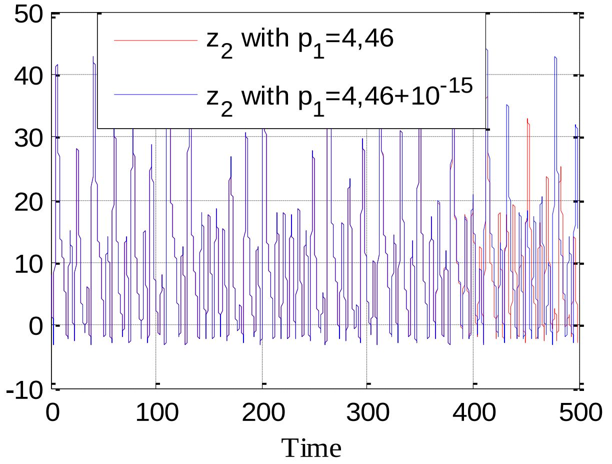

Figure 12. State z_2 of the continuous chaotic system for small changes (10^{-15}) of parameter g

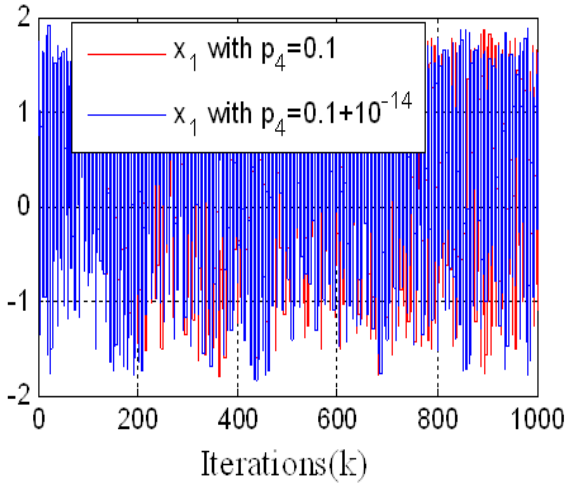

Figure 13. State z_3 of the new discrete chaotic system for small changes (10^{-14}) of parameter a

TABLE I. SENSITIVITY TO PARAMETERS

Chaotic system	**Parameters**	**Sensivity**	**Nb. of possibilities** $(N_i = s \times S_i^{-1})$
Colpitts chaotic system	p_1=g=4.46 p_2=q=1.38 p_3=k=0.5	S_1=10^{-15} S_2=10^{-15} S_3=10^{-15}	N_1=10^{14} N_2=10^{14} N_3=10^{14}
New chaotic system	p_4=a=1.76 p_5=b=0.1 p_6=A_1=0.01 p_7=A_2=0.01 p_8=A_3=0.1	S_4=10^{-14} S_5=10^{-14} S_6=10^{-15} S_7=10^{-15} S_8=10^{-15}	N_4=10^{13} N_5=10^{13} N_6=10^{14} N_7=10^{14} N_8=10^{14}

The size of the key space is:

$$r = \Pi_{i=1}^{8}\left(N_i\right) = 10^{14\times6+13\times2} = 10^{110}.$$

Relying on nowadays available computational power, a key space of size $O(2^{100})$ is generally required. In our case $r=10^{110} >> 2^{100}$ which means that the key space produced enhances a largely satisfactory level of security from a cryptographical viewpoint. The same reasoning may be applied to define and characterize a secret key for the first case-study.

Compared with other similar encryption schemes [10, 13-14, 17], our algorithm described above has higher security and can resist all kinds of known attacks, such as the known-plaintext attack and so on. Here, some security analysis results on the scheme are described, including the most important ones like keyspace analysis, statistical analysis, and differential analysis.

VII. CONCLUSION

In this paper, a novel chaotic image encryption scheme integrated with SPIHT wavelet image coding has been introduced. To overcome the drawbacks of small key space and weak obscure in the current chaotic encryption methods, its structural parameters are used as encryption key in chaotic. Experimental analysis demonstrates that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed. Finally, numerical simulations results illustrate the effectiveness of the proposed method. To demonstrate the robustness of our system, further works are needed, particularly, the test of the system with transmission to channel noise, the correlations of adjacent pixels in the encipher image, wider gray scale image database and its behavior in real time.

From an engineer's perspective, chaos-based image encryption technology is very promising for real-time secure image and video communications in biomedical, military and commercial applications.

REFERENCES

[1] G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps". IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. Vol. 48, No. 2, 2001, pp. 163-169.

[2] C.C. Chang, M.S. Hwang and T.S. Chen, "A New Encryption Algorithm for Image Cryptosystems," Journal System Software, Vol. 58, 2001, pp. 83-91.

[3] H. Cheng and X. B. Li, "Partial Encryption of Compressed Images and Videos," IEEE Transactions Signal and Process, Vol. 48, No. 8, 2000, pp. 2439-2451.

[4] N. Bourbakis and C. Alexopoulos, "Picture Data Encryption Using SCAN Patterns," Pattern Recognition, Vol. 25, No. 6, 2007, pp. 567-581.

[5] H. H. Nien, C. K. Huang, S. K. Changchien, H. W. Shieh, T. Chen and Y. Y. Tuan, "Digital C and Decoding Using a Novel Chaotic Random Generator," Chaos Solitons and Fractals, Vol. 32, No. 3, 2005, pp. 1070-1080.

[6] Q. Alsafasfeh and A. Alshabatat, "Image Encryption Based on Synchronized Communication Chaotic Circuit," Journal of Applied Sciences Research, Vol. 7, No. 4, 2011, pp. 392-399.

[7] Q. Alsafasfeh and A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems," Journal of Signal and Information Processing, Vol. 2, 2011, pp. 238-244.

[8] H. Gao, Y. Zhang, S. Liang and D. Li, "A New Chaotic Algorithm for Image Encryption," Chaos, Solitons and Fractals, Vol. 29, No. 2, 2006, pp. 393-399.

[9] C. Fu, Z. Zhang and Y. Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps," Third International Conference on Natural Computation, Vol. 3, Washington, 2007, pp. 24-27.

[10] L. Zhang, X. Liao and X. Wang, "An Image Encryption Approach Based on Chaotic Maps," Chaos, Solitons and Fractals, Vol. 24, No. 3, 2005, pp. 759-765.

[11] S. Bu and B. Wang, “Improving the Security Encryption by Using a Simple Modulating Method,” Chaos, Solitons and Fractals, Vol. 19, No. 4, 2003, pp. 919-924.

[12] L. Shubo, S. Jing and X. Zhengquan, “An Improved Image Encryption Algorithm based on chaotic system”, Journal of Computers, vol. 4, No. 11, November 2009, pp. 1091-1100.

[13] L. Wang, Q. Ye, Y. Xiao, Y. Zou and B. Zhang, “An Image Encryption Scheme Based on Cross Chaotic Map,” Congress on Image and Signal Processing, Sanya, 27-30 May 2008, pp. 26-27.

[14] I. A. Ismail, M. Amin, H. Diab, “An Efficient Image Encryption Scheme Based on Chaotic Logistic Maps,” International Journal of Soft Compution, Vol. 2, 2007, pp. 285-229.

[15] M. Shapiro, “Embedded Image Coding Using Zerotrees of Wavelet Coefficients,” IEEE Transactions on Signal Processing, Vol. 41, No. 12, 1993, pp. 3445-3462.

[16] T. Brahimi, A. Melit and F. Khelifi, “Fast Encryption Methods for Audiovisual Data Confidentiality,” Digital Signal Processing, Vol. 19, 2009, pp. 220-228.

[17] R. Lin, Y. Mao and Z. Wang, “Chaotic Secure Image Coding Based on SPIHT,” Third International Conference on Communications and Networking, China, 2008.

[18] M. Lahdir, A. Nait-Ali and S. Ameur, “Fast Encoding-Decoding of 3D Hyperspectral Images Using a Non-Supervised Multimodal Compression Scheme,” Journal of Signal and Information Processing, Vol. 2, No. 4, 2011, pp. 316-321.

[19] S. Lian, J. Sun and Z. Wang, “A Secure 3D-SPIHT Codec,” European Signal Processing Conference, Vi enna, Austria, 2004.

[20] A. S. Dmitriev, G.A Kassian and A.D Khilinsky, “Chaotic Synchronization of Henon Mappings: The Information Approach,” Technical Physics Letters, Vol. 28, 2002.

[21] K. Vesely and J. Podolsky, “Chaos in a Modified Henon-Heiles System Describing Geodesics in Gravitational Waves,” Technical Physics Letters A, Vol, pp. 271, 2000, pp.368-371.

[22] G. M. Maggio and O.D. Feo, “Nonlinear Analysis of the Colpitts Oscillator and Application to Design,” IEEE Transactions on Circuits and Systems: Fundamantal Theory and Applications, Vol. 49, 1999.

[23] G. M. Maggio and M.P. Kennedy, “Experimental Manifestations of Chaos in the Colpitts Oscillator,” in: Proc ICECS, Seville, Spain, 1997, pp. 194-204.

[24] I. Belmouhoub, M. Djemaï and J.P. Barbot, “Observability Quadtatic Normal Form for Discrete-Time Systems”, IEEE Transactions on Automatic Control, Vol. 50, 2005.

[25] M. Djemaï, J.P. Barbot and I. Belmouhoub, “Discrete-Time Normal Form for Left Invertibility Problem”, European Journal of Control, Vol. 15, pp. 194-204, 2009.

[26] H. Hamiche, M. Ghanes, J.P. Barbot and S. Djennoune, “Secure Digital Communication based on Hybrid Dynamical Systems,” Communication Systems, Networks and Digital Processing, CSNDSP'10, Newcastle, U.K, 2010.

[27] F. Anstett, G. Millerioux and G. Bloch, “Chaotic Cryptosystems: Cryptanalysis and Identifiability”, IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications, Vol.53, 2006.

[28] H. Dimassi, A. Lori'a and S. Belghith, “A new secured scheme based on chaotic synchronization via smooth adaptive unknown-input observer,” Communications in Nonlinear Science and Numerical Simulations, Vol. 17, No. 9, 2012, pp. 3727-3739.

AUTHORS PROFILE

Hamid Hamiche was born in Algeria in 1974. He received his Magister degree in Electronic from the Mouloud MAMMERI University of Tizi-Ouzou (Algeria) in 2002 and Ph.D. degree in Automatic Control from the Mouloud MAMMERI University of Tizi-Ouzou and National School of Electronics and Applications of Cergy-Pontoise (France) in 2011. His research activities deal with sliding-mode control, observation of chaotic systems and synchronization of chaotic systems. His main application domain is cryptography.

Mourad Lahdir was born in Algeria in 1969. He received his Magister degree in Electronic from the Mouloud MAMMERI University of Tizi-Ouzou (Algeria) in 1999 and Ph.D. degree in Electronics Remote Sensing from the Mouloud MAMMERI University of Tizi-Ouzou in 2007. His research activities are image processing, Meteosat and hyperspectral image compression, wavelet and fractal image application, progressive data transmission and watermarking.

Mohammed Tahanout was born in Algeria in 1975. He received his engineering degree in 1998 in Electronic telecommunications from the Mouloud MAMMERI University of Tizi-Ouzou (Algeria) and his Magister degree in Electronic radar system in 2003 from USTHB university of Algiers (Algeria). His research activities are radar image processing, telecommunications, radar system and signal processing.

Saïd Djennoune was born in Algeria in 1956. He received his Magister degree in Electronic from the High Commission for Research of Algiers (Algeria) and Ph.D. degree in Automatic Control from the Mouloud MAMMERI University of Tizi-Ouzou (Algeria). Since 2005, he is a Professor. His research activities deal with fractional derivative, synchronization of chaotic systems, control and observation of electric machines, which are applied to industrial problems.