ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

Compression algorithm and encryption of information through a chaotic discrete system

Maricela Jiménez Rodríguez[1], María Guadalupe González Novoa[1], José Aarón Rodríguez Cadena[2], César Ascencio Sánchez[1], Octavio Flores Siordia[1]
[1]Universidad de Guadalajara, Centro Universitario de la Ciénega
[2]Universidad de Guadalajara, Centro Universitario de los Altos

Abstract*— Currently ICT facilitate communication and data transmission through the network, but it is necessary to implement a compressing and encrypting method to prevent malicious users can get information. This work proposes a system to encrypt text files, which provides two techniques: one for compressing and another gives the possibility of converting the coded information in an image, in order to make it safer. In the system, an encoding technique was implemented, based on a chaotic logistic map to generate two orbits apparently shown as misinformation, one of which was used to blend with the original information and another allows changing the location of data to be encode.

***Index Terms*— Compression, chaos, encryption, logistic, security.**

I. INTRODUCTION

Now a days, the new communication technologies are used to keep in touch with customers, suppliers, friends, teachers or family and most of the time information is transmitted without using any technique to shield from an attacker as hackers, crackers, man-in-the-middle, etc. When transmitting information is advisable to apply a compression technique to convert a string of input data (original data) in another string of data (compressed string) with a smaller size to make it faster to transmit [1]. It is also necessary to implement cryptography, which allows you to write in secret, and provides confidentiality to information using an encryption method [2], [3]. The systems are divided into symmetric encryption using the same key to encode and decode and the asymmetric systems, where a public key to encrypt is used and a private key to decode [2]. Chaotic systems have been used in several studies to develop information coding methods [4]-[14]. The properties of ergodicity of chaos and its high sensitivity to conditions and parameters allow design of encrypt algorithms with good confusion (hides the relationship between the plaintext, the cipher text and the key) and dissemination (consisting of transposition or Site change of individual elements from the original information) [15]. Also the Master-Slave Synchronized Chaotic System is implemented to encode information [13]. Because it represents a great way to code, since they can take advantage of cryptographic properties of chaotic systems to encrypt information on a device, transmitting and decoding another.

Ranjan Bose and Saumitr Pathak implemented a technique for coding and compressing information using adaptive arithmetic. They combine the unpredictable behavior of the logistic function with an adaptive arithmetic code and use it to encrypt text. The initial condition and the chaotic map parameter is used as a key to encrypt [4]. In another research they developed a symmetric key algorithm to encrypt, where implemented several one-dimensional chaotic maps and an external key of 128 bits, using chaotic maps randomly to encode the plaintext [5]. They also conducted an algorithm based on chaotic maps networks to encrypt color images, in this logistic chaotic map is implemented a number of iterations and cycles to make the image indistinguishable [6]. In another study they developed a cryptosystem to encrypt color images or videos; combining diffusion and confusion techniques using coupled chaotic maps [15]. In another research a system was developed to encrypt images by a discrete logistic map system. They use an encrypted blocks of 8 bits and a external secret alphanumeric key or ASCII of 256 bits in length [7].

They have also developed systems for encoding by chaotic synchronization which also use a discrete system to apply the diffusion technique and a continuous one for confusion [13].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

The algorithm proposed in this research combines the information with a chaotic orbit that makes it harder for an attacker to detect which is the plain text, increasing security by converting cipher text in an image; because when transmitting alone, only the ones who have the encryption keys will know that the image is actually encoded information.

The remainder of this paper is organized as follows, Section 2 explains the implemented mathematical model and the proposed algorithms; some tests developed with the system are located in Section 3; Section 4 explains the conclusions and finally Section 5 mentions the future scope.

II. METHODOLOGY

A. *Logistic Map*

This logistic map is one of the simplest known discrete chaotic system and is expressed in Equation (1).

$$x_{n+1} = bx_n(1 - x_n) \qquad (1)$$

In Equation (1) n is an integer which takes the values $\{0,1,2, ..., n\}$ and indicates the iteration number, x_n is the variable and can take values $0 \leq x_n \leq 1$, the system parameter is b, which should be a positive real number $1 < b < 4$. By solving the logistic map system equations, the sequence x_n values generated by an iteration process produces an orbit whose behavior is governed by the parameter b and the initial condition x_0. For this system is chaotic parameter $3.57 < b < 4$.

B. *Algorithm for encoding*

The logistic equation used in this algorithm to generate two chaotic orbits:

- The first is generated in step 2, and the keys used b and x_0.
- The other is calculated in step 5, where 2 different values are used for the keys b and x_0.

Step 1.- Convert to its ASCII $0 < c < 255$ value and is stored in the $plain\_text[c_1,c_2,c_3,...,c_n]$ vector whose length is n.

Step 2.- Use the first values of b and x_0 keys to solve Equation (1) n times and generate $v\_log1[x_1,x_2,x_3,...,x_n]$ with values between 0 and 1.

Step 3.- Multiply each term v_log1 by 255 to generate values that easily mix with the plain text.

$$filled = round(v\_log1 * 255)$$

Step 4.- Generate the *cipher* vector of $l = 2*n$ length. Where *plain_text* information and *filled* vector values are mixed.

$$cipher = [cif_1, cif_2, cif_3, ..., cif_l]$$

Step 5.- Use other values of b and x_0 to solve Equation (1) and generate a new chaotic orbit of length n:

$$v\_log2 = [x_1, x_2, x_3, ..., x_n]$$

Step 6.- Multiply by l each term of v_log2 and round to generate the *loc* vector with values between 0 and l, which are used to indicate which location the *cipher* vector will store the *plain_text* information :

$$loc[u] = round(v\_log2 * l)$$
$$loc = [u_1, u_2, u_3, ..., u_n]$$

Step 7.- Take a position of the *loc* vector and if it is not occupied in the *cipher* vector, store the following value of *plain_text* vector. Repeat until you have settled in all positions *plain_text* information. See Figure 1.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

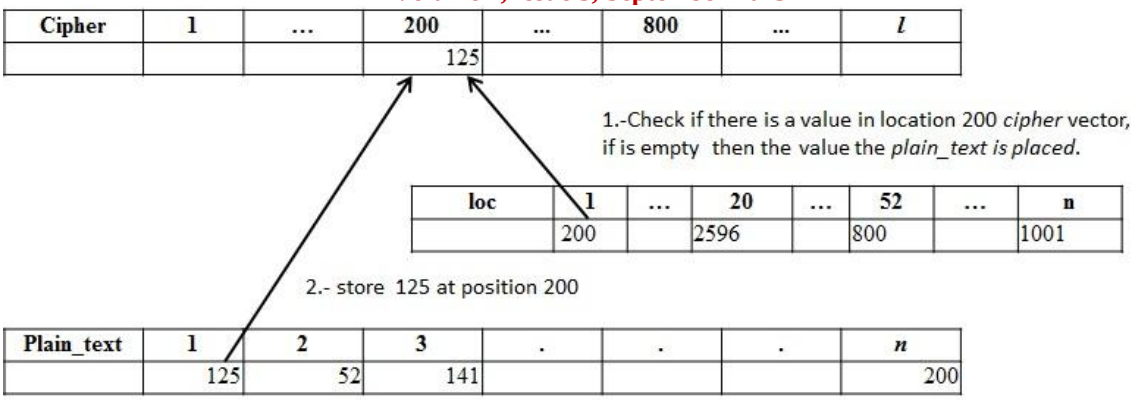

Fig 1: Process to mix information of the encrypted vector.

Step 8. Take the following value that is not stored in the cipher vector of *plain_text* and place it on the next empty position of the *cipher* vector. Repeat until all *plain_text* values are stored in *cipher*.

Step 9. Use the values of the *filled* vector to place numbers between *0* and *255* on all vacant positions *cipher* vector, consecutively.

C. Compression Method

Once the encoded information is in the *cipher* vector, to compress the information we must checked it as many times as the value is repeated.
Step 1. Take a value of the *cipher* vector, and check it as many times it is repeated consecutively:

a. It is not repeated, and then the value is stored in *comp* vector.

$$comp=[val,....]$$

b . It is repeated once; it must be stored twice in *comp* vector.

$$comp=[val,val,...]$$

c . It is repeated two or more times, a *rep=255+repetition number* is calculated.

$$comp=[val,rep,...]$$

D. Convert the encoded information into an image.

Step 1. Each image is composed of pixels which in turn are integrated by three subpixels : P^R (red) , P^G (green) and P^B (blue) with a value between *0* and *255* , like the *cipher* vector .

1. Three terms of the *cipher* vector are taken, which are used as P^R, P^G and P^B respectively, and are stored as pixels in one image.

E. Algorithm to decrypt

Step 1.- Perform Steps 5 and 6 from the algorithm to encrypt.
Step 2.- Generate *plain_text* vector of length *n*.
Step 3.- Take a position of *loc* vector and if the position is not empty in the *cipher* vector, the value is taken and stored in the following empty location of *plain_text* vector. Repeat it until you have settled all the values of the positions indicated in location *loc* vector in the *plain_text*. See Figure 2.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

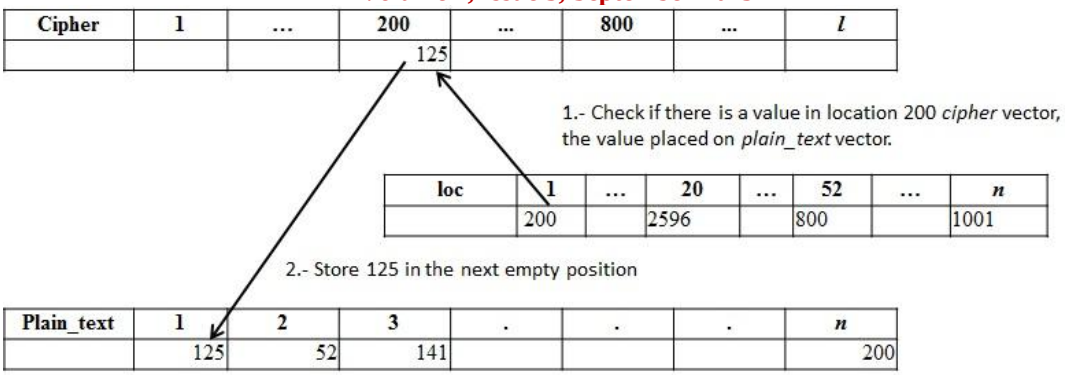

Fig 2: Process to return the values of the cipher vector to plain_text.

Step 4.- Browse the *cipher* vector from the start and in a consecutive way, take values to place them in the next empty location of *plain_text* up to recover the *n* values of *plain_text*.

III. RESULTS

The algorithms proposed in Section B and C used for coding and compressing a text file of 2905 characters. Subsequently decompressed and decoded for correlation analysis and linear association measure between the file before using algorithms and the file after using them.

The results are presented in the correlation diagram of Figure 3, where a correlation coefficient of 1 is shown, indicating that the linear association between the two files is very strong. Thus it can be seen that there is no loss of information after the algorithms are used.

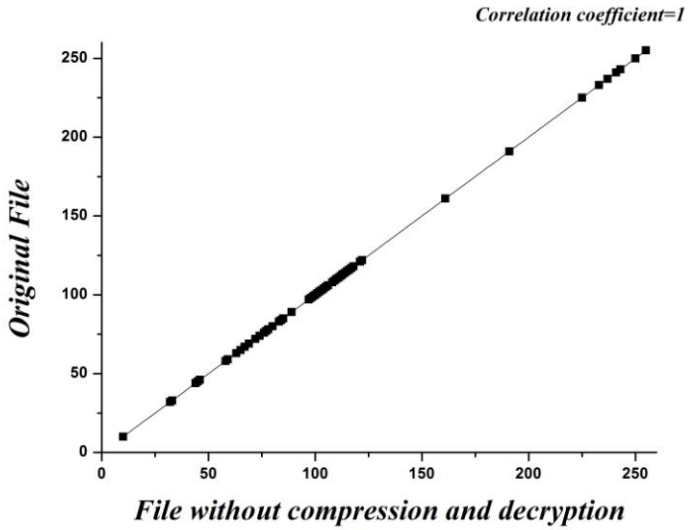

Fig 3: Correlation original file Diagram *vs* file without compression and decryption.

Algorithms Sections B and D were also used to encode and then stored the encrypted file in to an image, as shown in Figure 4.

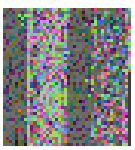

Fig 4: Image with encode information.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

IV. CONCLUSIONS

In this research a system was proposed to encode and compress wherein the mathematical logistic map model is implemented. According to the results it was observed through a correlation diagram of the system respects the integrity of the encoding information, that is, there is no loss at the time of decoding. It also provides added security when converting the coded information in an image as it is more difficult for the attacker to determine the contents of the encrypted information. In the system a very simple mathematical model was used in order to increase speed, because it is computationally solved faster and easier.

V. FUTURE SCOPE

Perform a system where the compression and encryption technique proposed is implemented in this investigation to encode and compress multiple files into one. Besides developing a method to apply steganography in order to hide the information in images and sound files.

ACKNOWLEDGMENT

The authors acknowledge the support from PRODEP-SEP (Convocatoria de Fortalecimiento de Cuerpos academics) (Mexico).

REFERENCES

[1] D. Salomón, "Compresión de datos," [date of reference September 16 of 2015] Available at: http://www.davidsalomon.name/DC4advertis/dataCompression4thesp.pdf

[2] A. Gómez, "Enciclopedia de la seguridad informática," México: Editorial Ra-Ma, 2011.

[3] M. López, "Criptografía y seguridad en computadores," [date of reference September 2 of 2015] Available at: http://wwwdi.ujaen.es/_mlucena/lcripto.html.

[4] B. Ranjan, and P. Saumitr, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," IEEE Transactions on Circuits and System-I, vol. 53, no.4, pp. 848-857, 2006.

[5] N. K. Pareek, V. Patidar, and K. K. Sud,"Cryptography using multiple one-dimensional chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 10, pp. 715-723, 2005.

[6] A. Pisarchik, and N. J. Flores, "Computer algorithms for direct encryption and decryption of digital images for secure communication," Proceedings of the 6th WSEAS International Conference on Applied Computer Science, pp. 29-34. (2006).

[7] E. Hossam, H. Ahmed, K. Haamdy, and F. Osama, "An Efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," Informatics, vol. 31, pp. 121-129, 2007.

[8] U. Parlitz, L. Kocarev, T. Stonjanovski, and H. Preckel, "Encoding messages using chaotic synchronization," Physical Review E, vol 53, no.5,pp. 4351-4361, 1996.

[9] U. Parlitz, L. Chua, L.J. Kocarev, K. Halle,. and A. Shang, "Transmission of digital signals by chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, no. 4, pp. 973-977, 1992.

[10] V. Annovazzi, S. Donati, and A. Sciré, "Synchronization of chaotic lasers by optical feedback for cryptographic applications," IEEE Journal of Quantum Electronics, vol. 33, no. 9, pp. 1449-1454, 1997.

[11] Y. Tao, and C. Leon, "Secure communication via chaotic parameter modulation," IEEE Transactions on Circuits and Systems - I: Fundamental Theory and Applications, vol 43, no. 9,pp. 817-819, 1996.

[12] J. Zhang, and Y. Zhang, "An Image Encryption Algorithm Based on Balanced Pixel and Chaotic Map," Hindawi Publishing Corporation: Mathematical Problems in Engineering, pp. 1-7, 2014.

[13] M. Jiménez, J. Rider, and A. Pisarchik, "Secure communication based on chaotic cipher and chaos synchronization," Discontinuity, Nonlinearity and Complexity, vol 1, no. 1, pp. 57-68, 2012.

[14] M. Jiménez, O. Flores, and M.G. González, "System for Information Encryption Implementing Several Chaotic Orbits," Ingeniería, Investigación y Tecnología, vol. 16, no. 3, pp. 335-343, 2015.

[15] A. N. Pisarchik, and M. Zanin, "Imagen encryption witch chaotically coupled chaotic maps," Elsevier Physica D, vol. 237, no. 20, pp. 2638-2648, 2008.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 5, September 2015

AUTHOR BIOGRAPHY

Maricela Jiménez Rodríguez, undergraduate degree in Computation Engineering, (UdeG 1999), Master degree in Applied Computation in 2003, Universidad Central Martha Abreu; in 2005, obtained Cisco Certified Network Associate certification, and in 2007 Cisco Certified Academy Instructor certification. Was awarded a Doctoral degree in Science and Technology at the Centro Universitario de los Lagos (CULagos) (U de G) in 2012. Currently is a professor in the Department of Technological Sciences at the Centro Universitario de la Ciénega (CUCIénega) and conducts investigation in the areas of Security Systems and Communications and Systems Elaboration, in addition to Applied Mathematics in Systems Development.

María Guadalupe González Novoa, full-time professor, works at the Department of Basic Sciences of the UdeG, Ciénega. Has a Master degree in Applied Computation with a specialty in databases, awarded from 2005. Her area of specialization is object-oriented programming and software development, distributed systems, the application of algorithms, and data structure. Participates in diverse investigation projects, is the author of various international and national publications, books and peer-review articles, all with reference to the line of investigation with which she collaborates: Elaboration of Security Systems and Communications. Currently works in the development of applications with technology for networks and security.

José Aarón Rodríguez Cadena, Undergraduate degree in Law (UIA 1998), Master degree in Law (UdeG 2013). Currently professor at Centro Universitario de los Altos (CUALTOS) in the Organizational Studies Department and conducts investigation related with e-governance, e-commerce, Digital Society, Security Systems and Communication, Legal informatics.

César Ascencio Sánchez, full-time professor affiliated with the Department of Basic Sciences, CUCiénega (U de G). Undergraduate degree in Electromechanical Engineering, Master degree in the Sciences of the Teaching of Mathematics, has published books and peer-reviewed articles focusing on the teaching and learning of mathematics through Communications and Information Technology (CIT).

Octavio Flores Siordia, full-time professor in the Department of Technological Sciences at CUCiénega, (U de G). Undergraduate degree in Chemical Engineering, Master degree in Chemical Engineering, Doctoral degree in The Teaching Methodology. Specialization area: Applied Mathematics. Participates in the following line of investigation: Elaboration of Security Systems and Communications, collaborates in diverse investigation projects, has various international and national publications, books and peer-reviewed articles, in reference to the development of applications with technology for networks and security.