Telecommand encryption for intercommunication of substation control centers

F Mesa¹, D M Devia¹, and R Ospina²
¹ Departamento de Matemáticas, Universidad Tecnológica de Pereira, Pereira, Colombia
² Escuela de Física, Universidad Industrial de Santander, Bucaramanga, Colombia

E-mail: femesa@utp.du.co

Abstract. New technologies are constantly generated and advanced every day and, with them, the need to use them to maintain constant communication with different people located anywhere in the world is also increasing. But this exponential growth also generates a very important security problem, since any information that is found in a device connected to the communications network or that travels through it, can be susceptible to being detected or intercepted by an unauthorized person that can be used improperly, causing large economic losses to companies or personal problems. For this reason, it is essential to use some mechanism that helps to protect the information from a malicious attack, one of the most used is cryptography that is responsible for writing in secret, providing confidentiality to the information through an encryption method.

1. Introduction

When we speak of chaos, we refer to the way a dynamic system acts that changes irregularly over time [1]. Based on chaotic discrete systems, various methods of secure communication have been developed in order to encrypt information [2]. The above is explained because chaos and cryptography are closely related, which allows a similarity to be established between the characteristics of dynamic systems such as sensitivity to parameters, mixing properties and even ergodicity with some characteristics seen in many cryptographic systems such as diffusion and confusion techniques.

Currently, communication between control centers and substations occurs through the sending and interpretation of telecommands which indicate specific orders to operators, there are reported cases in which people outside the control center have intercepted the signal and forwarded a False command, however, these reported cases were made as a test by the manufacturers to verify the security offered by the media and even more important the impact that could occur in case of receiving an improper remote control sent by a third party, due to this comes the need to develop a methodology for the encryption of telecommands for the intercommunication of control centers to substations (central) which helps to ensure greater security when sharing sensitive information [3,4].

This document proposes the use of an encryption technique based on logistic maps and its application to telecommands for the intercommunication of substation control centers [5]; and is structured as follows: basic concepts of intercommunication between control centers and substations and data encryption using logistics maps in section 2, encryption techniques based on logistics maps in section 3, results and conclusions in sections 4 and 5 respectively.
2. Fractal cryptography

Fractal or chaotic cryptography applies fractals and chaotic systems to obtain cryptographic methods. The cases of fractals that interest us for cryptography are those generated by a recursive or iterative process based on some mathematical function [6].

One of the characteristics of the chaotic dynamics is its extreme sensitivity to the initial conditions, for example, two relatively close initial values will differ as the system evolves. As we will see, it is possible to use a chaotic function that is initialized with a key to encrypt data. The safety of this type of cryptosystem is based on the hope that without knowing the secret key, chaotic behavior is difficult enough to predict using analytical methods. This would reduce possible attacks to a single category, force attacks, in which all possible keys against encrypted data are tested. Force attacks are rarely successful as they depend directly on the length of the key used [7].

2.1. Logistics maps

In the absence of linearity, chaos allows us to see that from very simple deterministic rules, complex behavior can occur. Stochastic signals, as well as applications based on chaotic systems are much simpler than those needed in stochastic systems, therefore, it is totally natural to propose the use of chaos as a noise manager in different applications. Starting from the fact that the logistic application is used to generate pseudocode numbers, some statistical tests have been carried out for series of numbers that were determined from discrete dynamical systems, and it was observed that these satisfy a large part of the characteristics of a pseudocode generator; when we vary the value of a parameter, it is observed that the logistic mapping presents a very broad behavior, causing chaotic or periodic trajectories to appear that have a fixed point; For this reason, in the study of population evolution in closed systems, the previous dynamic system is used more frequently since it is one of the simplest discrete models. In 1976 Robert May was the one who popularized logistic maps for the first time, which are in themselves a polynomial mapping and in particular correspond to a non-linear recursive algorithm which generates chaotic relationships [7]. We define in Equation (1) the chaotic relationship in one dimension, where $x_n \in (0,1)$. Through bifurcation diagrams it is possible to observe some characteristics corresponding to the asymptotic solution of a dynamic system depending on the control parameter

$$x_{n+1} = rx_n(1 - x_n), \quad n = 1,2,3,...$$

(1)

where $r$ is a constant parameter, $x_n \in (0,1)$ and $r \in (0,4)$. It is noteworthy that the value of $r$ is fundamental in the dynamics of the system this is evident when analyzing that for values of $r$ between 3.6 and 4 the logistic map has a chaotic behavior, as shown in the bifurcation diagram of Figure 1.

![Figure 1. Bifurcation diagram of a logistic map.](image)

2.1.1. Two-dimensional logistics maps

Starting from two one-dimensional logistic maps we can generate chaotic numbers, which will be used in the diffusion process. Using this technique, the image that is encrypted will have a much more uniform histogram, which can be used as a symmetric key when decrypting. A chaotic matrix with $m$ rows and
n columns is generated just like the original image matrix. Finally, we make the product of the chaotic matrix and the encrypted original image matrix [7,8].

2.2. Correlation analysis

The correlation image is composed from individual pixels, ensuring that there will always be a strong or weak correlation when the pixels are contiguous neighbors. Usually when the text image lacks format there will be a process of change between the pixels, and in this case the correlation between contiguous pixels is large and in the interest of rejecting possible statistical attacks this correlation should be decreased [6]. We can determine this correlation using Equation (2) and Equation (3).

\[
\rho(\tau) = \frac{\sum_{n=1}^{N} (x_{n+\tau} - \bar{x})(x_n - \bar{x})}{\sum_{n=1}^{N} (x_n - \bar{x})^2},
\]

(2)

\[
\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x(t_i).
\]

(3)

2.3. Telecontrol equipment and systems standard

International Electrotechnical Commission (IEC) standard, IEC 60870–5 [9] is the one that regulates all the different communication protocols between substations and control centers. The immense advantage of this protocol is that of establishing communication through a standard network, allowing simultaneous transmission between different devices. The IEC 60870-5-104 protocol [10] is widely used by supervisory control and data acquisition (SCADA) systems, at the substation and control center level, which have the IEC 60870-5-104 client driver to communicate with Gateway equipment or remote terminal unit (RTU) that contain the IEC 60870 protocol -5-104 server [10]. This protocol defines the use of a TCP / IP network as a means of communication, which offers the following advantages.

- In the end systems, there is no need for specific network software.
- No routing or network management functionalities are required in the end systems.
- The network management is not necessary in the end systems.
- The end systems and routers can be supplied by telecontrol and telecommunications specialists.

It is possible to guarantee total security of the information that is transmitted when using a network However, the use of a TCP / IP network

3. Encryption techniques based on logistics maps

In Figure 2 explains how the algorithms work in a practical case to encrypt images, but any type of information is encoded; where L is the length of the vector with the original information and LM the length of the vector with the encrypted information.

![Figure 2. Scheme of the encryption algorithm.](image-url)
An image is an array of numbers that represents the intensity of the color of the pixels and consists of 3 bytes or subpixels represented with a decimal value between 0 and 255, which correspond to the colors red (R), green (G) and blue (B), these are presented in a vector as follows in Equation (4) [2,11].

\[
\{P_1^R, P_1^G, P_1^B, \ldots, P_n^R, P_n^G, P_n^B\}.
\]

3.1. Image encryption

When we have an image, we can decompose it into its different red, green, and blue (RGB) planes. Using the iterated Gauss map [12], we can generate a succession of separate random numbers for the different planes, which we can quantify using Equation (5).

\[
S(i) = \begin{cases} 
0, & 0 \leq X(n) \leq 0.5 \\
1, & 0.5 \leq X(n) \leq 1
\end{cases}
\]

where \( S(i) \) is the quantized sequence, and \( X(n) \) is a random number. Finally, with the bits of the different image planes, we have the quantized sequence XOR [2,13].

3.2. Image decryption

Using an inverse procedure to the previous one corresponding to the coding of the image, and based on the same control parameters, the decryption process is carried out [2,14]; that is to say:

- It starts from an encrypted image and decomposes it into its RGB planes.
- The random sequence of each plane is generated by means of the iterated Gaussian map using the same control parameters.

4. Results

Before coding and decoding the typical telecommands (opening, closing) we proceed to perform the analysis with different images to check the effectiveness of the method (Figure 3). Figure 3(a) shows the image to encrypt Figure 3(b) shows the decomposition of the image on different planes (RGB).

![Figure 3. Original picture - image RGB decompose; (a) image to encrypt, (b) decomposition of the image on different planes (red, green and blue).](image)

Next, we show in Figure 4(a) the encryption of the image and, in Figure 4(b), the encryption of the corresponding RGB planes.
Figure 4. Image and RGB encrypted planes; (a) encryption of the image; (b) encryption of the RGB planes.

After the encrypted RGB planes have been obtained as seen in Figure 5(a), the decryption process is carried out using the methodology proposed above, as shown in Figure 5(b).

Figure 5. Decryption process; (a) encrypted RGB planes, (b) decrypted planes.

Once the drawings are decrypted, the images are concatenated to reproduce the original image as shown in the Figure 6. As can be seen the decryption process was successful in large percentage, however, at the time of rebuilding the image there is some variation when performing the reconstruction of the color blue, this is due to, when the images are processed deciphered and concatenated the layer of this color is multiplied by a scale factor that alters its hue slightly, therefore by dividing by that scale factor it is possible to obtain the image shows in the Figure 7.

Figure 6. Original picture decrypted. Figure 7. Image decrypted and processed.

Following the application service data units (ASDU) standard, the sending of telecommands is carried out under the following structure Figure 8. In Figure 8 the Type ID corresponds to the type of
interface standard for connecting devices, VSQ is the vocaloid sequence, COT is the acronym for central office terminal, the common address corresponds to the common address protocol, and the other elements that appear correspond to the information of each of the objects that were encrypted. Using the proposed technique will proceed to encrypt and decrypt as shown in Figure 9.

In this way it is possible to interpret the command as an image and perform the encryption and decryption process, in this way you can guarantee an even higher security index when transmitting sensitive data such as the operating maneuvers carried out to carried out in substations.

![Figure 8. ASDU standard.](image)

![Figure 9. Telecommand picture encryption and decryption process.](image)

5. Conclusions
The coding of sensitive information such as closing and opening orders of disconnectors is essential to maintain the correct operation of the power electrical system. The use of data encryption techniques and their application to telecommands guarantees a high security index, avoiding information leaks and possible external manipulations of the transmitted information, resulting from the operations carried out in the electric substations.

References
[1] Singh S, Parida R, Pradhan C 2018 Comparative analysis of image encryption using 2D and 3D variations of duffing map International Conference on Communication and Signal Processing (ICCSP) (Chennai: IEEE)

[2] Sahay A, Pradhan C 2017 Multidimensional comparative analysis of image encryption using gauss iterated and logistic maps International Conference on Communication and Signal Processing (ICCSP) (Chennai: IEEE)

[3] Hazarika N, Borah S, Saikia M 2014 A wavelet based partial image encryption using chaotic logistic map IEEE International Conference on Advanced Communications, Control and Computing Technologies (Ramanathapuram: IEEE)

[4] Shahna K, Mohamed A 2018 An image encryption technique using logistic map and z-order curve International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR) (Ernakulam: IEEE)

[5] Li-Hong L, Feng-Ming B, Xue-Hui H 2013 New image encryption algorithm based on logistic map and hyper-chaos International Conference on Computational and Information Sciences (Shiyang: IEEE)

[6] Zhu A, Li L, Chen M 2010 An improved BMP image encryption algorithm based on logistic map International Conference on Computer and Communication Technologies in Agriculture Engineering (Chengdu: IEEE)

[7] Saffari R M, Mirzakuchaki S 2016 A novel image encryption algorithm based on discrete wavelet transform using two-dimensional logistic map 24th Iranian Conference on Electrical Engineering (ICEE) (Shiraz: IEEE)

[8] Jha Y, Kaur K, Pradhan C 2016 Improving image encryption using two-dimensional logistic map and AES International Conference on Communication and Signal Processing (ICCSP) (Melmaruvathur: IEEE)
[9] International Electrotechnical Commission (IEC) 2020 Telecontrol Equipment and Systems - Part 5: Transmission Protocols - All Parts, IEC 60870-5 (Switzerland: International Electrotechnical Commission)

[10] International Electrotechnical Commission (IEC) 2006 Telecontrol Equipment and Systems - Part 5-104: Transmission Protocols –Network access for IEC 60870-5-101 using standard transport profiles, IEC 60870-5-104 (Switzerland: International Electrotechnical Commission)

[11] Jiang Y, Li B 2016 A novel image encryption algorithm based on logistic and henon map 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) (Chengdu: IEEE)

[12] Hammond M M, Yoshiro K, Sigher A 2013 Inf. Technol. Convergence 253 407-415

[13] Ramasamy K, Siddiqi M U, Alias M Y 2006 Performance of JPEG image transmission using proposed asymmetric turbo code EURASIP Journal on Advances in Signal Processing 2007 075757:1

[14] Mishra A, Sharma K, De A 2014 Int. J. Comput. Sci. Telecommun. 5(1) 8-16