International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 2, April 2019, pp. 1399~1409
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i2.pp1399-1409

Pseudo-random bit generator using chaotic seed for cryptographic algorithm in data protection of electric power consumption

Francisca Elizalde-Canales, Iván Rivas-Cambero, Lucio Rebolledo-Herrera, Cesar Camacho-Bello
Faculty of Engineering Universidad Politécnica de Tulancingo, México

Article Info

Article history:

Received May 9, 2018
Revised Nov 2, 2018
Accepted Nov 20, 2018

Keywords:

Cryptography
Decryption
Encryption algorithm
Statistical tests

ABSTRACT

Cryptographic algorithms have played an important role in information security for protecting privacy. The literature provides evidence that many types of chaotic cryptosystems have been proposed. These chaotic systems encode information to obviate its orbital instability and ergodicity. In this work, a pseudo pseudo-random cryptographic generator algorithm with a symmetric key, based on chaotic functions, is proposed. Moreover, the algorithm exploits dynamic simplicity and synchronization to generate encryption sub-keys using unpredictable seeds, extracted from a chaotic zone, in order to increase their level of randomness. Also, it is applied to a simulated electrical energy consumption signal and implemented on a prototype, using low hardware resources, to measure physical variables; hence, the unpredictability degree was statistically analyzed using the resulting cryptogram. It is shown that the pseudo-random sequences produced by the cryptographic key generator have acceptable properties with respect to randomness, which are validated in this paper using National Institute of Standards and Technology (NIST) statistical tests. To complement the evaluation of the encrypted data, the Lena image is coded and its metrics are compared with those reported in the literature, yielding some useful results.

Corresponding Author:

Francisca Elizalde-Canales,
Department of Automation and Control,
Universidad Politecnica de Tulancingo,
Calle Ingenierías # 100. Col. Huapalcalco, Tulancingo, Hidalgo, C.P. 43629, México.
Email: francisca.elizalde@upt.edu.mx

1. INTRODUCTION

The electric power industry has become increasingly vulnerable because of smart grid growth used for interconnection of consumers with power generation, transmission, and distribution trought information technologies based on communication systems. In this sense, smart meters could inadvertently provide unauthorized access to consumer data, which is a concern in the management of information for the adoption of intelligent networks in the face of the increasing possibility of cyber-attacks, since security has not traditionally been considered a requirement in design of integrated systems and the application of security techniques specific to these devices is still incipient [1]-[4].

Cryptographic algorithms are the backbone of the protection of highly sensitive data. The selection of a suitable crypto-algorithm will dynamically affect the lifespan and performance of a device in terms of battery-life, hardware memory, computation latency, and communication bandwidth. In the current developments of resource-constrained environments, the trend is shifting towards lightweight algorithmic designs [5], [6].

To address the security problem, Badra *et al* in [7] presents a gradual distribution where homomorphic encryption is added to intelligent meters involved in data transferring from a source to the collector unit in such a way that intermediate results are not revealed to any device on the route. Also, there are privacy-preserving protocols based on additional homomorphic encryption [8] or masking [9] in the smart metering infrastructure that enable the calculation of the sum of all the household's load values at each time point without providing the individual values. However, Tonyali *et al*. [10] proposed a data obfuscation approach to preserve consumer privacy and simultaneously perform distribution state estimation. In this scheme, the Advanced metering infrastructure (AMI) network gateway computes the obfuscation vectors. The gateway multiplies the vector with a random number and distributes it to the smart meters using a shared key. On the other hand Rottondi [11], has proposed a friendly privacy infrastructure by means of a cryptographic algorithm that hides the pattern of energy consumption, based on Shamir's secret sharing scheme. Tan *et al*. [12] proposed a pseudonym-based privacy-preserving scheme reassuring privacy, integrity, and authenticity in AMI.

Recently, several research efforts have been introduced to overcome the challenges and find appropriate solutions associated with security, especially end-to-end security [6], [13]. Privacy-preserving schemes have advanced significantly in recent years, especially because of the need communication. Some research has focused on creating security mechanisms that are adequate for the context of intelligent measurement devices; however, the needs are varied and increasing. In addition, everyday privacy is exposed to intrusions from those who have malicious purposes and possess sufficient knowledge to find sensitive data.

In recent research, various cryptographic mechanisms have been presented to strengthen safety in measuring devices and intelligent power grids, as reviewed in [14]; however, the results obtained in [14] show the need for novel schemes to reduce the complexity and computational resources in the revised works. In this way, the present work has as strength the implementation of an algorithm of "data obfuscation" in an embedded system of low computational resources.

Therefore, in this work we propose a new algorithm based on a pseudo-random bit generator that uses chaotic seed. We tested the effectiveness of the implementation of the encryption algrorithm, combining two techniques; logistic map and congruential generator, to analyze the compensation between resources and security. The strengthening of security to preserve privacy against unauthorized attacks is the main objective that guides we design. However, for all practical applications, performance and the cost of implementation are also factors to consider security.

The remainder of this paper is organized as follow. Section 2 gives an overview of the encryption algorithm, which includes a logistic map and a linear congruential generator. Section 3 introduces our scheme cryptograohic, security parameters, and design goals. Section 4 gives security analysis; the results are compared with other methods in terms of security and performance. Finally, section 5 concludes this paper and suggests future research work.

2. THEORETICAL CONSIDERATION

Below we describe the combined methods used to design the encryption algorithm relevant to its computational characteristics, which includes a logistic map and a linear congruent generator with the purpose of strengthening the key, given that the strength of cryptography lies in the choice of the keys.

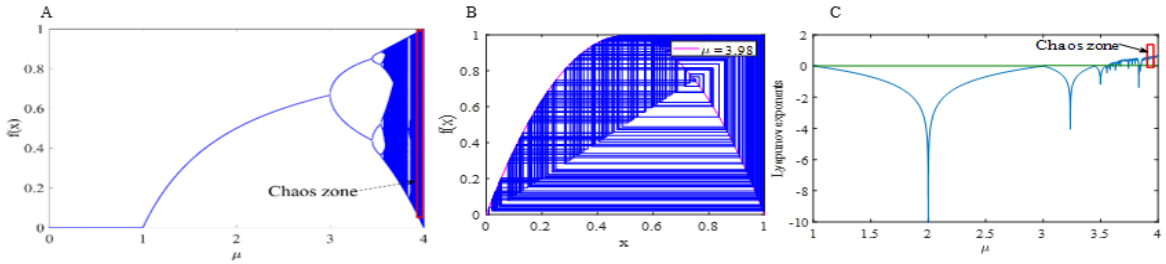
As chaos analysis and cryptography are related to this work, it is important to highlight how real numbers, used in chaos, are mapped into finite integer numbers used in cryptography. Thus, data from logistic maps are scaled and discretized into the integer interval (0-255) to keep the system consistent [15].

2.1. Logistic mapping

Among chaotic discrete systems, one of the most commonly used to encode information is the logistic map. This is because it is very simple, fast and sensitive to the initial conditions and control parameter. Logistic mapping exhibits very rich dynamics, depending on the value of a parameter. There may be trajectories, periodic or chaotic, approaching a fixed point. Logistic applications have been used as a generator of pseudo-random numbers. For this purpose, in [16], some statistical tests have been performed on the series of numbers obtained from this discrete dynamic system, and it has been found to possess many of the properties required by a pseudo-random number generator. This dynamic system is one of the simplest discrete models used for the study of population evolution in closed systems and is given by the following function [17]

$$x_{t+1} = \mu x_t (1 - x_t) \quad (1)$$

Where μ is a control parameter, which determines the degree of nonlinearity of the map and x_t is the state variable, which determines the sequence (x_0, x_1, x_2, ...) of the path or orbit corresponding to the initial condition x0. Here the constant μ takes values between (0, 4). The phase space of the system is in the interval (0, 1). Discrete dynamic systems evolve over time through the iteration process, in which the next state of the system is determined by its current state. As can be seen in Figure 1(a), the system presents period bifurcation with μ close to 3, which increases in frequency from this point and generates chaotic behavior. The figure indicates with a rectangle the area that can be exploited in a zone of chaos. Subsequently new bifurcations are generated that show chaotic behavior as in Figure 1, where the trajectory of the signal whose zone can be exploited to generate unpredictable sequences is shown. To guarantee unpredictable sequences, it is necessary to tune parameter μ within the chaotic system behavior. For this reason, dynamic analysis of chaotic generators with Lyapunov exponents is presented, as shown in the rectangle named "chaos zone" on the right of Figure 1(c).



(a) (b) (c)

Figure 1. (a) Logistic mapping bifurcation diagram, (b) Chaotic signal trajectory diagram with μ=3.98, (c) Diagram of Lyapunov exponents

The Lyapunov exponent quantifies the degree of sensitivity to initial conditions (local instability in a state space) by the following equation:

$$\lambda = (\lim_{n\to\infty} \{\frac{1}{2}\sum_{i=0}^{n-1} \ln |f'(x_i)|\} \quad (2)$$

Where λ can be defined as the mean natural logarithm applied to absolute values on first derivatives of the mapping function evaluated at the trajectory points [3]. In a single one-dimensional system, dependent on only one parameter, the logistic function brings together a range of different behaviors for the xt trajectories hence, when the value of μ and/or xt is changed, its dynamic characteristics are said to be universal. Examples of these characteristics are the initial conditions sensitivity, the route to chaos by period doubling or the phenomenon of intermittency.

2.2. Linear congruential generator

Pseudo-random numbers generation is defined as an algorithm that allows generating sequences of numbers with some randomness properties that play a relevant role in a large number of applications such as numerical simulations, communications or cryptography. The main advantages of these generators are the speed and repeatability of the produced pseudo-random sequences. In practice, pseudo-random number generation is not a trivial issue and the randomness quality in the produced sequence, may be essential in the application choice [16]. In a large quantity of cryptographic applications where keys and access codes are highly important, these generators have a major role. In fact, one of the oldest and simplest generators is the linear congruential generator, proposed by D.H. Lehmer [18] which, using an initial number called seed, can generate a sequence by recurrence under the relationship defined by the equation:

$$X_{n+1} = (aX_n + c) \bmod m \quad (3)$$

Where a, Xn and c must be greater than zero and the variable "m" must be a prime number larger than the first three values. This type of generator is computationally fast and easy to implement; however, some properties like generation of values in a sequence exhibit a maximum period of m-1. On the other hand,

the sequences produced by this generator are highly sensitive to changes in their parameters, which is a useful property in cryptography [19].

3. EXPERIMENTAL CONSIDERATION

The two methods described above are combined in the design of the proposed encryption algorithm, taking advantage of the main characteristics in each method. Such characteristics are the processing speed and the low cost, in terms of computational hardware resources required.

Logistic map defined in (1) exhibits high sensitivity to initial conditions, which is applied for parameter tuning and to generate two sequences with highly random properties. In the current work, parameter values are quoted in the intervals xt ∈ (0, 1) and μ ∈ (3.85, 4) to force operation within the chaos zone [20]. Within these intervals, along with the initial conditions, the logistic (1) presents and maintains chaotic behavior; thus, series of numbers are generated and used as chaotic seeds to complement the encryption key by applying a "confusion technique". This technique hides the relationships between the original information, the encrypted one and the generated key. In order to obtain two pseudo-random sequence generators, the logistic function is iterated with the following parameters and initial values: μ=3.89 and x0=0.00499 for the first sequence and μ=3.86 and x0=0.01999 for the second sequence. These values are chosen, due to their simulated chaotic behavior, filling the entire generated map with 125,000 iterations. Moreover, these two sequence generators behave as parameters of the linear congruential generator; therefore, the mixture generated is useful for encrypting electric power consumption signals.

In Figure 2, the block diagram containing the pseudo-random generator algorithm is shown, illustrating the sequence generating functions and how they feed the Congruential generator. This diagram represents the procedure followed to generate two sequences (GNPR1 and GNPR2), used as seeds with unpredictable numbers, and generated through a one-dimensional logistic map, located in a chaotic zone, evaluated by Lyapunov exponents, keeping the unstable behavior. These sequences are coupled to the congruential generator through its parameters to increase the randomness level in the generated sequences [21]; thus, an electrical energy consumption signal was encrypted through the exclusive disjunction logical operator XOR; the signal was both simulated and physically implemented. Subsequently, the information is fully encrypted and ready to be sent wirelessly through a likely unsafe channel.

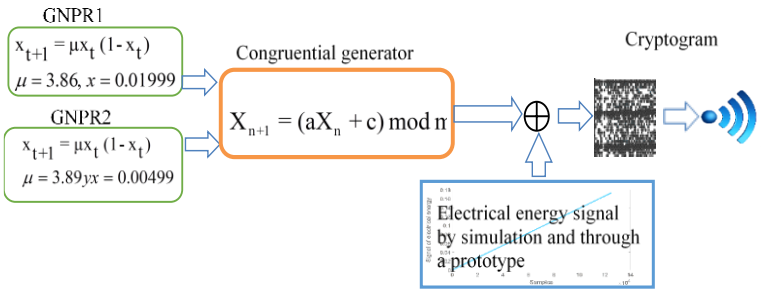
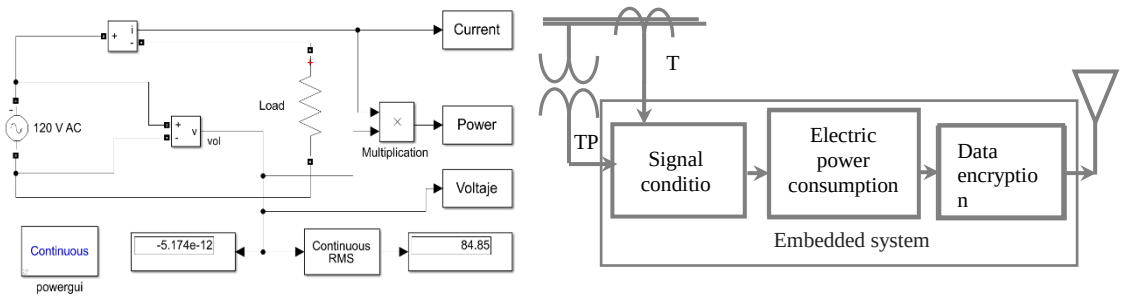


Figure 2. Block diagram: pseudo-random generator algorithm



(a) (b)

Figure 3. The scheme of the signal of consumption of electric energy, (a) Signal outline of electric energy consumption by simulation, (b) Physical implementation scheme

In Figure 3, the signal measurement scheme for electric power consumption is shown with a simulated resistive load in Matlab/Simulink. Correspondingly, the physical implementation scheme is shown in Figure 3(b), represented as an embedded system. The prototype developed in this work is used to acquire physical variables, signal conditioning, energy consumption calculation, data transmission and mainly, the pseudo-random generator algorithm embedded in real-time.

Once the data sent is received in the central system (PC), it must be deciphered with the originally generated key and a recovery algorithm. The receiver performs the inverse operation from the original algorithm to reconstruct the message from the received signal. Thus the merged data can be reconstructed; the decryption process is very similar to that of encryption except that methods are applied in an inverse manner.

The general model of the proposed algorithm, a combination of two techniques, is shown in Figure 4. The first technique is the logistic mapping and implies high sensitivity to slight change. The second corresponds to the congruential generator which is fed by the first one. Later, the flowing electric energy consumption data are encrypted while the data is flowing, by an XOR operation bewteen the pseudo-random sequence and electric consumption data.

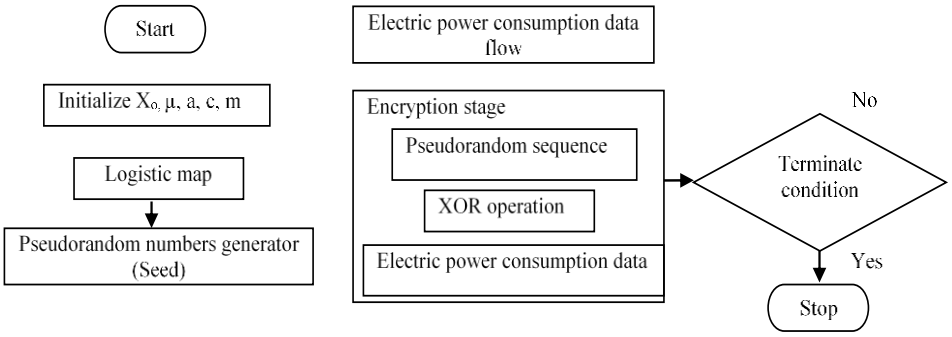


Figure 4. Algorithm flow diagram

4. RESULTS

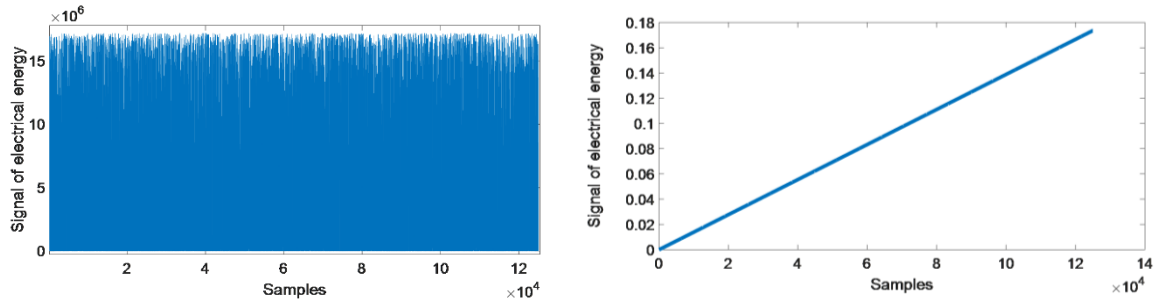
In this section, we perform an analysis with different statistical tools to evaluate four characteristics: independence, uniformity, distribution and correlation between succession cipher data.

4.1. Pseudo-random generator

A pseudo-random generator to strengthen the data security is reported, based on the logistic map and the linear congruential generator reviewed in Sections 2.1, 2.2 and 3. Furthermore, in order to maintain the balance between security and performance for the cost effective usage of computational resources, embedded algorithm implementation is also presented.

To evaluate the encryption algorithm just proposed, set for processing electrical energy and data signals from digital electric meters in smart grids, a 60 Hz alternating-current test circuit is designed in which the voltage and current are measured to calculate the power as well as the energy consumed by a resistive load. The electric power consumption signal obtained is shown in Figure 2(b), where the resistive load is 144Ω. For this demonstrative case, only the energy consumption is presented over the course of 10 seconds.

One of the most common attacks is the brute-force attack, in which all possible combinations of the encryption key are tried. As encryption key of length 128 bits or more is considered secure against brute force attacks [3], [22], in the proposed cryptographic algorithm, the key space is 2*n*, where *n* is the key length in bits. In the present work, *n*=128, with two pseudo-random number generators where each chaotic map uses two variables of 64-bit length. Figure 5(b) shows the behavior of the energy consumption while Figure 5(a) shows its encrypted equivalent. The latter presents behavior with variation in the signal, as affected by the encryption algorithm, in its basic properties (frequency and amplitude) and signal noise approximation.



(a) (b)

Figure 5. Representation of energy consumption signal, (a) Encrypted signal with the proposed algorithm, (b) Original signal

4.2. Analysis of the cryptogram

Histograms allow graphical representation of data distribution. Figure 6 shows the encrypted signal distribution, exhibiting a mean of 1.8173^{03} and variance metrics of 1.0860^{06} for the original signal, while for the encrypted signal, mean, and variance were calculated as 4.4981^{05} and 6.7240^{10} respectively.

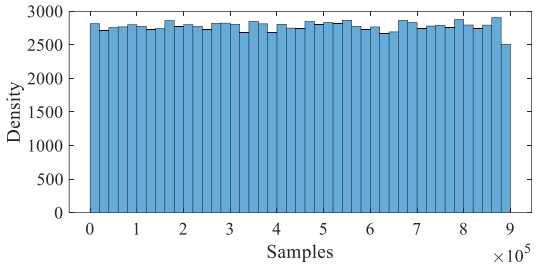


Figure 6. Histogram encrypted data

4.3. Criterion for evaluating encryption

This criterion can be divided into two main categories. The first group includes statistical tests: data correlation coefficients and entropy values [23]. The second group includes sensitivity tests: a bit change in the encryption key and the mean squared error [24].

4.3.1. Correlation coefficient

A correlation analysis is performed to measure the linear association between the original data and the encrypted data. Then, the correlation with encrypted and decrypted data is analyzed in order to determine if there is any loss of information when using the algorithm. Since the values are widely scattered with respect to what could be a linear pattern plot, a low degree of association is expected. It can be affirmed that there is no or very little correlation, as can be seen numerically through the correlation coefficient. In order to obtain numerical measures, the correlation coefficient is calculated using the following equation:

$$c = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad (4)$$

In this case n is the number of elements in the two adjacent vectors x and y. For strongly encrypted data, the correlation coefficients should approximate zero [24]. The reported value for correlation coefficient is 0.0016.

4.3.2. Entropy measure

Entropy measures the uncertainty of an information source by calculating the randomness of the data, which precludes any predictability.

The entropy is given by:

$$H = \sum_{i=1}^{2^8} P(S_i) \log_2 P(S_i) \quad (5)$$

where H represents Shannon's entropy, the surprise of an event or its level of uncertainty, S is a symbol and P gives the probability of occurrence. It is considered that the higher the value of H, the more unexpected the event. In other words, there will be greater randomness and higher unpredictability [25]. In this sense, entropy measured was 7.9936.

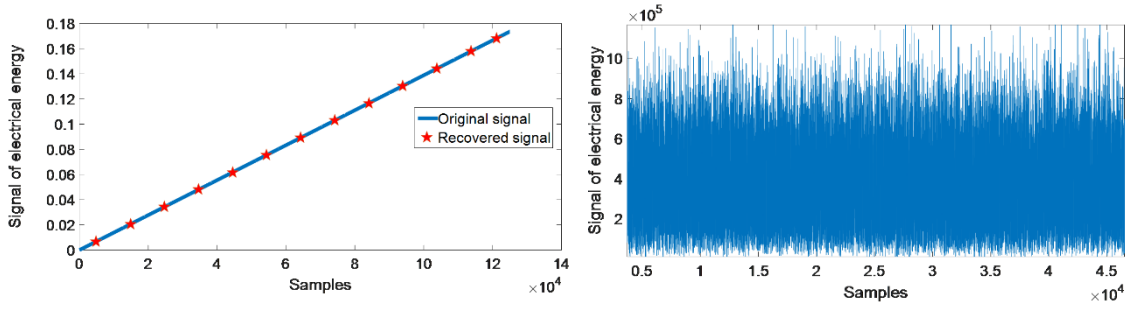
4.3.3. Sensitivity tests

Strongly encrypted algorithms must be sensitive to any small change in input values and produce a totally different output. Quantitatively, the different measures are defined for the assessment of levels of protection against differential attacks [22]. The decrypted signal is shown in Figure 7(a), and deciphering is considered adequate, since the signal obtained is equal to the original signal as will be proved by using the MSE. Conversely, when the decryption is applied after changing a single value of a key parameter, it can be seen that the result is completely different from what would be expected in Figure 7(b). It can be noted that a good encryption process proves to be sensitive to slight changes in any of its parameters. Therefore, a slight change in the key or in some of the parameters of the sub-key generator leads to completely different behavior during the decryption process.

The error measures the variation between the encrypted signal and the original signal, yielding a value of zero when no variation exists in the parameters. This sensitivity was evaluated using the mean square error, which quantifies how the decrypted data differs from the original one. The mean square error is calculated using the following equation:

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2 \quad (6)$$

In this case, $\hat{Y}$ is a vector of n predictions and Y is the vector of the original values. For verification of encryption and decryption by appropriate use of the algorithm and key, the equation yields a value of zero.



(a) (b)

Figure 7. Signal recovered with and without change in key encryption key, (a) Recovered signal superimposed on the original signal, (b) Decoded signal with bit change

4.4. Physical implementation

The pseudo-random algorithm presented in this paper is implemented in a prototype to experiment with real data and evaluate the randomness properties for the proposed cryptogram. This way, proper behavior is empirically confirmed. The embedded system scheme for the prototype is shown in Figures 9A and 9B. Where, current and voltage are measured by current sensor (1122-30Amp.) and AC transformer. Signal conditioning was applied on these signals for signal scaling to Arduino platform (UNO). Inside an Arduino system, analog to digital (A/D) conversion was developed by using a sampling each 50 milliseconds. After acquisition, signal processing for energy signal is done before encryption application. Once data is encrypted, communication via Bluetooth (HC-05 transmitter) is established with another embedded device with the same characteristics as the one described. On this device, the algorithm was

embedded and re-transmitted to a personal computer for analysis, via USB channel. Figure 9C shows the resulting signal. The data acquisition stage can be subdivided into two sub-stages; one for signal conditioning and the other for data acquisition, based on the Atmega328 microcontroller.

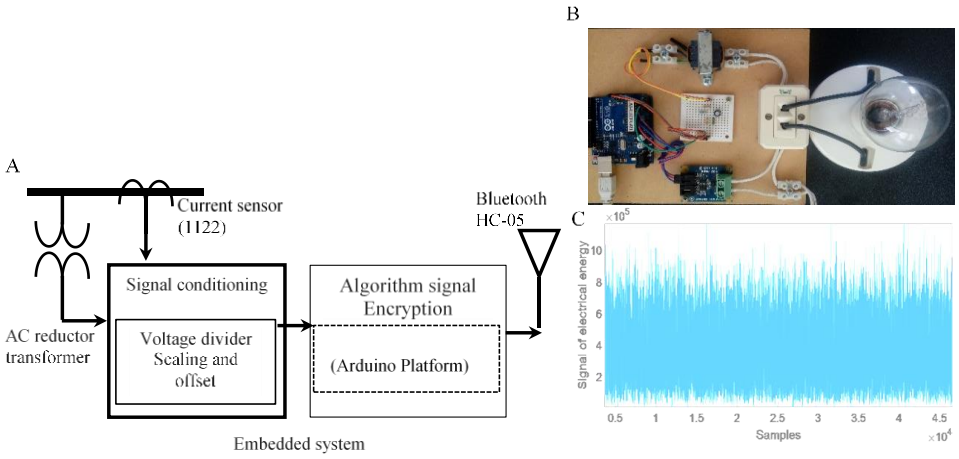


Figure 9. Prototype of acquisition (a) Scheme embedded system (b) Image of processing and encryption of electric power consumption data (c) Resulting signal

4.5. Cryptosystem validation using the NIST 800-22rev1a

The NIST Test Suite was developed to test the randomness of the binary sequences produced and incorporates a set of statistical tests for the validation of random number generators and random sequence generators for cryptographic applications [26]. The NIST Test Suite has statistical tests that evaluate the presence of a pattern, which, if detected, indicates that the sequence is not random. In each test, a P-value is calculated with a significance level of α=1%. A P-value greater than α means that the sequence is random with a confidence level of 99%. The statistical performance of the cryptosystem was evaluated using a set of statistical tests, by using 125000 samples of 1Mbit data and setting the parameter interval μ in (3.86-4), the initial condition interval of xt is (0,1). Each P-value corresponding to a particular test is presented in Table 1 and indicates the 1-Mbit sequences produced by the proposed algorithm that passes a specific test for both the simulated signal and the prototype implementation. The results of the 15 NIST tests [26] performance on proposed algorithm are shown in Table 1. It is clear from these results that the methods, congruential generator and logistic map, are not enough to pass all the tests; nevertheless, the mixed methods succeed in all tests.

Table 1. NIST Test

Test	Used Methods				Proposed Algorithm			
	Generator Congruential		Logistic Map		Simulated		Implemented	
	P-value	Status	P-value	Status	P-value	Status	P-value	Status
Approximate entropy	0	×	0	×	0.8097	✓	0.3679	✓
Block frequency	0.0190	✓	0	×	0.4917	✓	0.8712	✓
Cumulative sums(Forward)	.0024	✓	0	×	0.4128	✓	0.2456	✓
Cumulative sums(Reverse)	.0028	✓	0	×	0.3129	✓	0.5297	✓
FFT	0	×	.0259	✓	0.8043	✓	0.0067	×
Frequency	0	×	.0379	✓	0.4065	✓	0.3200	✓
Linear complexity	.6282	✓	0	×	0.7503	✓	0.3372	✓
Longest run	.3041	✓	0	×	0.5048	✓	0.0470	✓
Non overlapping template	.3026	✓	.1060	✓	0.5094	✓	0.3896	✓
Overlapping template	.2157	✓	0	×	0.3136	✓	0.1526	✓
Rank	.9352	✓	.4691	✓	0.8851	✓	0.0712	✓
Runs	0	×	0	×	0.4369	✓	0.6248	✓
Non periodic templates	0	×	0	×	0.5094	✓	0.7154	✓
serial	0	×	0	×	0.3816	✓	0.9645	✓
Universal	.3954	✓	0	×	0.8772	✓	0.2589	✓

The results obtained in Table 1 demonstrate that all NIST metrics were achieved under simulation using the proposed encryption algorithm; whereas in the prototype, the FFT test shows a low P-value, which is assumed to be a result of electrical interference in the circuit

4.6. Cryptosystem tests on image lena processing

In this section, the proposed algorithm strength was evaluated by encrypting the color version of the Lena image and comparing the correlation coefficient with [3], [27], and [28]. The selected size of Lena image was 512×512 pixels and, to keep the described procedure in Section 4.6, the degree of entropy and distortion on the encrypted image was determined. The correlation coefficient was analyzed since the security analysis of a cryptographic process is essential to ensure the strength of the cryptographic technique. A histogram of an image depicts the frequency of each pixel. A good cipher image has a uniform frequency distribution of the pixel values [29]. Figure 10(a) shows the original image, and Figure 10(c) shows the ciphered image. Likewise, Figures 10(c) and 10 show the original image histograms and the ciphered image respectively.

From Figure 10, we can also see how the frequency distribution of pixels in the ciphered image histogram is uniformly distributed, as expected by the proposed algorithm. In order to determine the level of entropy and disorder of the ciphered image, the correlation of 1,000 randomly selected points was analyzed. Table 2 presents the results of the horizontal, vertical and diagonal correlation of adjacent pixels. This table also shows that the proposed algorithm generates a correlation coefficient closer to zero than the other two references.

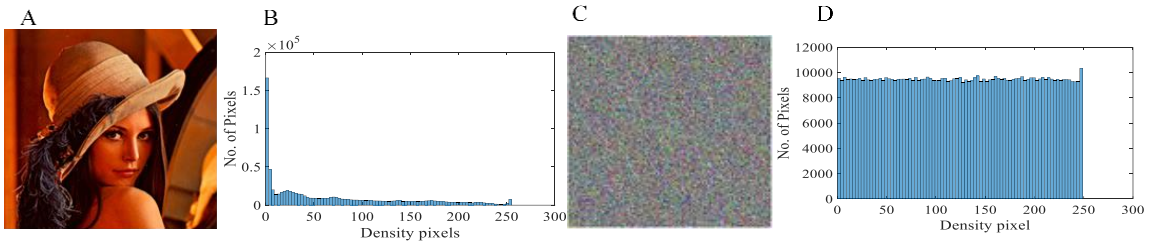


Figure 10. Shows Lena image, (a) Original image, (b) Histogram original image, (c) Cipher image, (d) Histogram cipher image

Table 2. Comparison of the Correlation Coefficient of the Algorithm Proposed with Other References

	Encrypted image(Correlation coefficient)			
Direction	Algorithm proposed	Hossam *et al*., [27]	Chong *et al*., [28]	Jiménez *et al*., [3]
Horizontal	0.0074	0.0308	0.0368	0.0270
Vertical	-0.0089	0.0304	-0.0392	-0.0009
Diagonal	-0.0032	0.0317	0.0068	0.0020

As implementation was a main objective, comparison of processing time was first tested in a personal computer under Matlab R2015a, with an Intel(R) Celeron 2 Core processor at 2.16 GHz of frequency, 4GB in RAM, under Windows 10 Home O.S. was used. The resulting processing time were 0.5263 seconds, encrypting 125,000 samples of electric power consumption data. As the encryption with chaotic seed was the main target, execution time was neglected during prototyping; however, real time communication was achieved.

Finalli, in Table 3, the comparative average encryption time taken from some Lena images of different sizes is shown. The execution time of the cryptographic algorithm increases at a lower rate than observed in Li *et al*. [30]. The time analysis was performed on a 2.26 GHz Core 2 Duo CPU with a 4 GB RAM notebook running on using Matlab; the same characteristics as Li *et al*. [30].

Table 3. Comparative Ciphering Time

Image	Ciphered time(s)	
sizes (pixels)	Algorithm proposed	(Li *et al*., 2016)[30]
256 x 256	0.84	0.90
512 x 512	1.79	1.82
1024 x 1024	8.46	13.08
2048 x 2048	33.45	76.38

5. CONCLUSION

A pseudo-random bit generator algorithm with chaotic encryption, based on dynamic sequences, is presented in this paper. These sequences are generated from one-dimensional functions of a logistic mapping coupled to a linear congruential generator whose parameters constitute the secret key for the coding system. Also, the encryption algorithm is proposed for implementation in embedded, low cost hardware focused on security features improvement, with computational resources to obtain the appropriate execution speed.

The generator is applied to encrypt information of electric power consumption, obtained by simulation and by a prototype of energy measurement, and then tests of encryption and deciphering are carried out in an ideal environment, thus recovering the original signal. The algorithm is evaluated with the main statistical functions and validated with the NIST tests and with the application on the Lena image as base of comparison. Hence, all NIST metrics were achieved under simulation except under FFT test in prototyping. This is assumed to be a consequence of electrical interference on prototyping circuit, therefore, PCB circuit enhancement will be done in future work.

The statistical evaluation shows a significantly decreasing correlation between the encrypted and original values of the order of 10^{-3}. It is confirmed that the cryptogram that shows a high degree of unpredictability also evidences an entropy very close to 8, which means that the cryptogram offers the confidentiality expected for the information and thereby decreases the vulnerability to cyber-attacks. In addition, tests are performed to measure the processing time, entropy and degree of disorder using the Lena image, obtaining metrics comparable to those reported in the literature reviewed. In future investigations, it will be necesary to optimize the algorithm, so it can be applied for flow encryption.

The algorithm presented in this research offers a high degree of confidentiality, since the information can only be used with the same key used to generate the cryptographic system. In this case it has a mean squared error of 3.469111 in sensitivity tests, which indicates how far the wrong decrypted data is from the original data. A processing time of 0.5263 seconds was observed on a 2.16 GHz Intel Celeron.

ACKNOWLEDGEMENT

The paper was supported by the Consejo Nacional de Ciencia y Tecnología (CONACyT Beca 408093).

REFERENCES

[1] M. Mylrea, "Smart Energy-internet-of-things Opportunities Require Smart Treatment of Legal, Privacy and Cybersecurity Challenges," *The Journal of World Energy Law & Business*, vol. 10,(2), pp. 147-158, 2017.
[2] Z. Guan, G. Si, J. Wu, L. Zhu, Z. Zhang and Y. Ma, "Utility-Privacy Tradeoff Based on Random Data Obfuscation in Internet of Energy," *IEEE Access*, vol. 5, pp. 3250-3262, 2017.
[3] M. Jiménez-Rodríguez, *et al.*, "Sistema Para Codificar Información Implementando Varias Órbitas Caóticas," *Ingeniería, Investigación y Tecnología,* vol 16(3), pp. 335-343, 2015.
[4] M. N. Dazahra, F. Elmariami, A. Belfqih, J. Boukherouaa, "A Defense-in-depth Cybersecurity for Smart Substations," *International Journal of Electrical and Computer Engineering*, vol. 8(6), pp. 4423-4431, 2018.
[5] J. Kong, L. Ang and K. Seng, "A Comprehensive Survey of Modern Symmetric Cryptographic Solutions for Resource Constrained Environments," *Journal of Network and Computer Applications*, vol. 49, pp. 15-50, 2015.
[6] Z. Mrabet, N. Kaabouch, H. Ghazi and H. Ghazi, "Cyber-security in Smart Grid: Survey and Challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469-482, 2018.
[7] M.Badra and S. Zeadally, "Lightweigt and Efficient Privacy-Precerving Data Agrgregation Approach for the Smart Grid," *Ad Hoc Networks*, vol.64, pp.32-40, 2017.
[8] F. Borges de Oliveira, "On Privacy-Preserving Protocols for Smart Metering Systems," 2017.
[9] F. Knirsch, G. Eibl and D. Engel, "Error-Resilient Masking Approaches for Privacy Preserving Data Aggregation", *IEEE Transactions on Smart Grid*, vol. 9(4), pp. 3351-3361, 2018.
[10] S. Tonyali, O. Cakmak, K. Akkaya, M. Mahmoud and I. Guvenc, "Secure Data Obfuscation Scheme to Enable Privacy-Preserving State Estimation in Smart Grid AMI Networks," *IEEE Internet of Things Journal*, vol. 3(5), pp. 709-719, 2016.
[11] C. Rottondi and G. Verticale, "Privacy-friendly Load Scheduling of Deferrable and Interruptible Domestic Appliances in Smart Grids," *Computer Communications*, vol. 58, pp. 29-39, 2015.
[12] X. Tan, J. Zheng, C. Zou and Y. Niu, "Pseudonym-based Privacy-preserving Scheme for Data Collection in Smart Grid," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 22(2), p. 120, 2016.
[13] Y. Benslimane and K. Ahmed "Efficient End-to-End Secure Key Management Protocol for Internet of Things," *International Journal of Electrical and Computer Engineering*, vol.7(6), pp. 3622-3631, 2017
[14] S. Desai, R. Alhadad, N. Chilamkurti and A. Mahmood, "A survey of Privacy Preserving Schemes in IoE enabled Smart Grid Advanced Metering Infrastructure," *Cluster Computing*, 2018
[15] P. Shukla, *et al.*, "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing," *Entropy*, vol. 17(12), pp. 1387-1410, 2015.

[16] M. François, *et al.*, "Pseudo-random Number Generator Based on Mixing of Three Chaotic Maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19(4), pp. 887-895, 2014.
[17] R. May, "Simple Mathematical Models with Very Complicated Dynamics," *Nature*, vol. 261(5560), pp. 459-467, 1976.
[18] D. H. Lehmer, "Mathematical Methods in Large-Scale Computing Units," *2nd symposium on large-scale digital calculating machinery*, Cambridge, massachussets, pp.141-146, 1949.
[19] A. Rezk, A. Madian, A. Radwan and A. Soliman, "Reconfigurable Chaotic Pseudo Random Number Generator based on FPGA," *AEU - International Journal of Electronics and Communications*, 2018.
[20] C. Robinson, "Dynamical Systems," *Boca Raton, Fla.CRC Press*, 2009.
[21] T. Ahmed and M. Rahman, "The Hybrid Pseudo Random Number Generator," *International Journal of Hybrid Information Technology*, vol. 9(7), pp. 299-312, 2016.
[22] A. Radwan, *et al.*, "Symmetric Encryption Algorithms Using Chaotic and Non-Chaotic Generators: A review," *Journal of Advanced Research*, vol. 7(2), pp. 193-208, 2016.
[23] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol.28, pp. 656-715, 1949.
[24] A. Kerckhoffs, "La Cryptographie Militaire," *Journal des sciences militaires*, vol 9, pp. 161-191, 1883
[25] D. Pavanello, *et al.*, "Statistical Functions and Relevant Correlation Coefficients of Clearness Index," *Journal of Atmospheric and Solar-Terrestrial Physics*, vol. 130-131, pp. 142-150, 2015.
[26] L. Bassham, *et al*.,"A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST, 2018. [Online]. Available: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic. [Accessed: 25- Jan- 2016].
[27] E.A. Hossam, *et al.*, "An efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," *Informatica*, vol 31, pp. 121–129, 2007.
[28] C. Fu, *et al.*, "A Novel Chaos-Based Bit-level Permutation Scheme for Digital Image Encryption," *Optics Communications*, vol. 284(23), pp. 5415-5423, 2011.
[29] R. Parvaz and M. Zarebnia,"A Combination Chaotic System and Application in Color Image Encryption," *Optics & Laser Technology*, vol. 101, pp. 30-41, 2018.
[30] C. Li, G. Luo, K. Qin and C. Li, "An Image Encryption Scheme Based on Chaotic Tent Map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127-133, 2016.

BIOGRAPHIES OF AUTHORS

Francisca Elizalde-Canales, received a B.S. degree in computing in 1997 from Universidad Autonoma del Estado de Hidalgo (UAEH) and an M.Sc. information and knowledge management from the Instituto Tecnologico y de Estudios Superiores de Monterrey (ITESM) in 2010. She is currently completing a Ph. D. program in optomecatronica from Universidad Politecnica de Tulancingo. Her interest areas are security information, cryptography and smart grid.

Ivan Rivas-Cambero, received a B.S. Eng in electrical engineering from Instituto Tecnológico de Tepic, México in 1998, an M.S.. Degree in electrical engineering from CINVESTAV Guadalajara in 2002, and a Ph. D. in industrial engineering from UAEH, Pachuca, México in 2012. He is now working as Full-time Professor at Universidad Politécnica de Tulancingo, México. His main areas of interest are dynamical systems and operation and control of non-linear systems using fuzzy logic.

Lucio Fidel Rebolledo-Herrera, received his B.S. degree in electronics science from Autonomous University of Puebla, México in 1995 an M.Sc. degree from National Institute of Astrophysics, Optics and Electronics (INAOE) in 2000. He developed some projects on industry and became a full-time professor at Polytechnic University of Tulancingo, México in 2009. In 2017 he received his Ph.D. from INAOE. Currently, he is a researcher at Polytechnic University of Tulancingo, México. His research interests are biomedical signal processing, non-linear dynamic systems, stochastic dynamics, pattern classification, statistical signal processing and embedded systems.

César Camacho-Bello, received his B.S. degree in industrial engineering from UAEH in 2006, his M.S. degree in optical computing from the Polytechnic University of Tulancingo in 2011, and his PhD in optics from INAOE in 2014. He is now a researcher in the Polytechnic University of Tulancingo, Mexico. His research interests include pattern recognition, biometric analysis, computer vision, and digital image processing.