# Design, Implementing, and Testing a Novel Chaotic Random Generator CRN

**Amr Sayed Abdel Fattah Youssef**

***Abstract*: Nowadays, the importance of implementing a secure communication system that protects the privacy and confidential information from cyber-attacks and eavesdroppers is widely recognized. This requires developing solutions that not only address security issues but should not affect the speed of our system also. To achieve secure communication, most security systems rely on randomness generators, which play a vital role in the encryption process, with more randomness equaling greater security. In this paper, we propose a methodology for designing and implementing a novel random generator by using Lorenz chaotic signals. The proposed chaotic random generator CRN has been tested using NIST's Statistical Test Suite for Random and Pseudorandom Generators for Cryptographic Applications and results have been discussed.***

***Keywords*: Chaotic, Random, security, wireless**

## I. INTRODUCTION

A chaotic signal has numerous features that make it attractive for communication systems. To begin with, the wideband nature of chaotic signals makes them resistant to the adverse effects of multipath fading. Consequently, when these signals are utilized for encoding information, they produce spread-spectrum signals that have wider bandwidth and lower power spectral densities. In addition, chaotic signals can generate a multitude of spreading waveforms with ease because of their sensitivity to initial conditions. Furthermore, their non-periodic nature in the time domain results in a relatively uniform frequency spectrum. Finally, their noise-like signal structure offers a high level of confidentiality as they have a low probability of detection and interception, making them suitable for secure communication purposes. Moreover, the synchronization of chaotic systems can be achieved both theoretically and practically [6,7,8].

The most important characteristic of this type of signal is that it can be easily generated by simple circuits, these simple circuits lead to the low-cost implementation of the product. For all aforementioned properties, the chaotic signals provide a new class of signals which can be used in secure communication systems [9,10,11]. The security aspects of chaos-based cryptosystems have been studied in several works [1,8].

In [12, 13], it was shown that unmasking some chaos-based secure communication systems is possible by modeling and predicting the transmitter. Additionally, a recent examination of the parameters of a chaos-based cryptosystem's receiver that utilized chaotic synchronization revealed that the security of the cryptosystem is susceptible to certain attacks if the dynamic model of the chaos system is known. [14].

Our main objective is to create a chaotic cryptosystem that is "provably secure," which means that mathematical proofs show that the cryptosystem can withstand certain types of attacks. Pioneering work in this field was done by C.E. Shannon [15]. In his information theory, he developed measures for information associated with a message and the notion of perfect secrecy: a perfectly secret cipher perfectly resists all ciphertext-only attacks. An adversary gets no information about the plaintext, even if his computing power and time resources are unlimited.

Shannon's perfect secrecy can be summarized in the following statement [15]: "An encryption is perfectly secret if and only if an adversary cannot distinguish between two plaintexts, even if his computing resources are unlimited". For example, if the adversary knows that a ciphertext c is the encryption of either "1" or "0", he has no better chance than 1/2 of choosing the right one. This probability can be obtained even without knowing the ciphertext. In other words, the reception of ciphertext doesn't improve the vision of the adversary or increase the probability of any specific plaintext over others. Consequently, randomness and the security of cryptographic schemes are closely related; There is no security without randomness. An encryption method provides secrecy only if the ciphertexts appear random to the adversary [1,2,3,4].

Vernam's one-time pad, which encrypts a message m by XORing it bitwise with a truly random bit string, is the most famous perfectly secret cipher. It even resists all the passive attacks mentioned previously. This can be mathematically proven by Shannon's theory. Vernam's one-time pad is perfectly secret, because, due to the truly random key string k(t), the encrypted message m(t) XOR k(t) is a truly random bit sequence c(t) for the adversary [16]. Figure 1 shows Vernam's one-time pad or XORing encryption technique.

Random number generators are used in many areas including [17,18]

- Cryptography and watermarking for image authentication.
- message keys for ciphers.
- random challenges for authentication purposes.
- password generation
- Security communication
- Simulation such as Monto-Carlo simulation

**Manuscript received on 07 March 2023 | Revised Manuscript received on 29 April 2023 | Manuscript Accepted on 15 May 2023 | Manuscript published on 30 May 2023.**
***Correspondence Author(s)**
**Amr Sayed Abdel Fattah Youssef***, Aviation Science, Higher Colleges of Technology, Alain, UAE. Email: ayoussef@hct.ac.ae, ORCID ID: https://orcid.org/0009-0002-5059-2457

- Initialization vectors for neural networks and genetic algorithm
- Emulate of noise in the evaluation of communication systems.

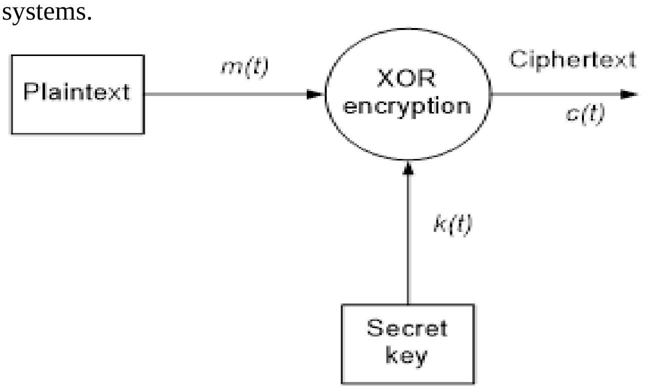


**Figure 1. Vernam's One-Time Pad Or XORing Encryption Technique**

A random number generator (often abbreviated as RNG) is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random. Computer-based systems for random number generation are widely used but often fall short of this goal, though they may meet some statistical tests for randomness intended to ensure that they do not have any easily discernible patterns. [15]

Let us suppose that the set of possible messages is finite in number $m_1, \ldots, m_n$ that these have a priori probabilities $P(m_1), \ldots, P(m_n)$, and that messages are enciphered into possible cryptograms $E_1, \ldots, E_m$ by

$$E = \text{kim} \quad (1)$$

The cryptanalyst intercepts a particular *E* and can then calculate, the posteriori probabilities for the various messages, $P_E(m)$. It is natural to define perfect secrecy by the condition that, for all *E*, the posteriori probabilities are equal to the priori probabilities. In this case, intercepting the message has given the cryptanalyst no information.

A necessary and sufficient condition for perfect secrecy can be found as follows in the Bayes' theorem [19]

$$P_E(m) = \frac{P(m)P_m(E)}{P(E)} \quad (2)$$

where

*P(m)* is the a priori probability of message m.

$P_m(E)$ is the conditional probability of cryptogram *E* if message *m* is chosen, i.e. the sum of the probabilities of all the keys which produce cryptogram *E* from message *m*.

*P(E)* is the probability of obtaining cryptogram E from any cause.

*P_E(m)* a posteriori probability of message m if cryptogram *E* is intercepted.

For perfect secrecy, $P_E(m)$ must equal *P(m)* for all *E* and for all *m*. For our proposed system, the data to be transmitted is binary "0" or "1" with equal probability, $P(0)=P(1)=P(m)=1/2$. Because this data is encrypted by a random key to produce E, the randomness leads us to say that $P_m(E)=P(E)=1/2$. Therefore, it is obvious that the condition of perfect security is satisfied in our system, where $P_E(m)$ equals *P(m)*.

The main challenge here is to generate and handle truly random bit sequences of sufficient length as required for perfect secrecy, which is impractical in most situations. To overcome this problem, our proposal is to use a chaotic random number generator to produce the secret key. The randomness of the key used has been proven by the NIST test [5]. This means that the XORing technique will satisfy perfect security by using the proven randomness key.

## II. RANDOMNESS CHARACTERISTICS OF THE CHAOTIC SIGNAL

In the proposed CRNG, the parameters of the chaotic signal serve as random seeds, and the sequence of binary variables generated from the chaotic dynamics can be used as the running-key sequence. The randomness of the running-key sequence is vital for the security of such chaos-based cryptosystems. In this work, a new approach to the design of CRNG is proposed. The new approach relies on frequency-domain aliasing to improve the randomness of the running-key sequence and improve the security of the key seeds. Frequency-domain aliasing is obtained through a sampling of the chaotic signal with a sampling frequency that is within the bandwidth of the chaotic signal. The frequency spectrum of the sampled discrete-time sequence is flatter, and therefore whiter, leading to improved randomness. Moreover, the running-key sequence provided by the sampled chaotic signal is highly sensitive to the sampling frequency. The randomness of the running-key sequence and the nonanalytical nature of the sampling frequency can considerably enhance the security of the cryptosystem. The randomness of the running-key sequence and its sensitivity to the sampling frequency are quantitatively evaluated by the correlation functions. In stream cipher cryptography, the critical problem is to generate a long running-key sequence efficiently from short and random keys [20, 21] which are also called key seeds. In a chaos-based cryptosystem, the parameters and initial conditions of the chaos systems play the role as random seeds and the sampled state variables of the system generated from the chaotic dynamics are the running-key sequences. Since chaotic systems are sensitive to initial conditions as well as parameter variations, the parameter space of some chaotic systems is large enough for the random key seeds. The running-key sequence can be recovered from the receiver side by synchronization of the chaotic systems [6,7]. To achieve a high level of cryptosystem security, it is preferable that the running-key sequence have a high degree of randomness. To improve the randomness of the running-key sequence, a sampling scheme for the continuous time chaotic signal is demonstrated, whose sampling frequency is considerably below the bandwidth of the chaotic signal. Since the spectrum of the sampled discrete-time sequence can be flattened due to frequency-domain aliasing, its degree of randomness can be increased by slowing down the sampling frequency. Thus, the sampled discrete time sequence as the running-key sequence and the sampling frequency can be used together with the chaotic system parameters as the key seeds.

Retrieval Number: 100.1/ijrte.A75240512123
DOI: 10.35940/ijrte.A7524.0512123
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

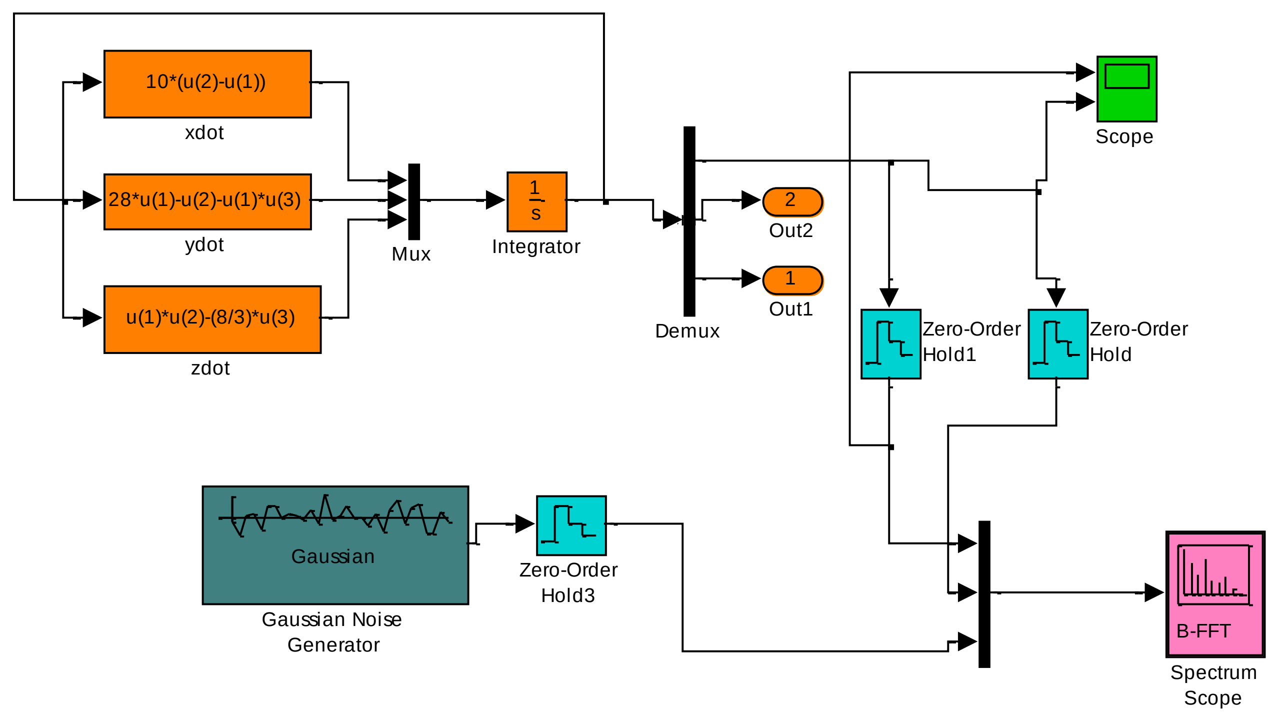


**Figure 2. Simulink model for sampling Lorenz chaotic signal**

Fig. 2 shows the Simulink model for sample Lorenz chaotic signal where Lorenz system consists of three coupled first-order ordinary differential equations as described in equations 4-6.

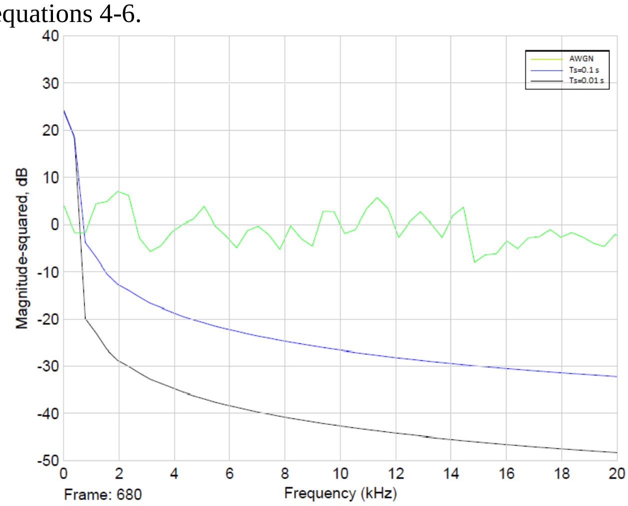


**Figure 3 Frequency spectra of xs with different sampling periods.**

$$\frac{du}{dt} = K(c_1 v - c_1 u) \tag{4}$$

$$\frac{dv}{dt} = K(c_2 u - v - uw) \tag{5}$$

$$\frac{dw}{dt} = K(uv - c_3 w) \tag{6}$$

where $c_1$ , $c_2$ and $c_3$ are arbitrary constants with the values 10, 28, and 2.666 respectively. $K$ represents the time scaling factor of the Lorenz system [22]. The frequency spectra of the sampling periods are shown in Fig. 3, where $Ts$=0.1, 0.01 sec and the spectra of AWGN is added for comparison purpose.

Several reasons can be stated to indicate why the use of sampled chaotic sequences with aliasing in the frequency domain can greatly strengthen the secure protection of the cryptosystem from attacks. First, the sampled running-key sequence is highly sensitive to the sampling frequency which has a non-analytical nature. This can greatly improve the security of the key seeds when the sampling frequency is included in the key seeds. Hence, there is no information about the original sampling rate of the running-key sequence contained in the encrypted data sequence transmitted through the communication channel. Next, frequency aliasing makes it impossible to reconstruct the original continuous time chaotic signal from the running-key sequence. Finally, the running-key sequence with aliasing in the frequency domain provides little information for directly estimating the parameters of the continuous time chaotic systems. By contrast, in the case where only the continuous time chaotic signal is used, recent work showed that the cryptosystem security is vulnerable under some attacks [14,23,24].

## III. CHAOTIC RANDOM NUMBER GENERATOR (CRNG)

The schematic diagram for the proposed chaotic random number generator (CRNG) is shown in Fig. 4. As shown in the Figure, a chaotic signal generator is the core of randomness. The chaotic signal is sampled at regular intervals using a sample and hold circuit. The sampled signal is mapped into either "0" or "1" by a decision circuit and then the output is fed to a buffer register. Finally, the randomness of the generated sequences is tested by the NIST test suites.

*Retrieval Number: 100.1/ijrte.A75240512123*
*DOI: 10.35940/ijrte.A7524.0512123*
*Journal Website: www.ijrte.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

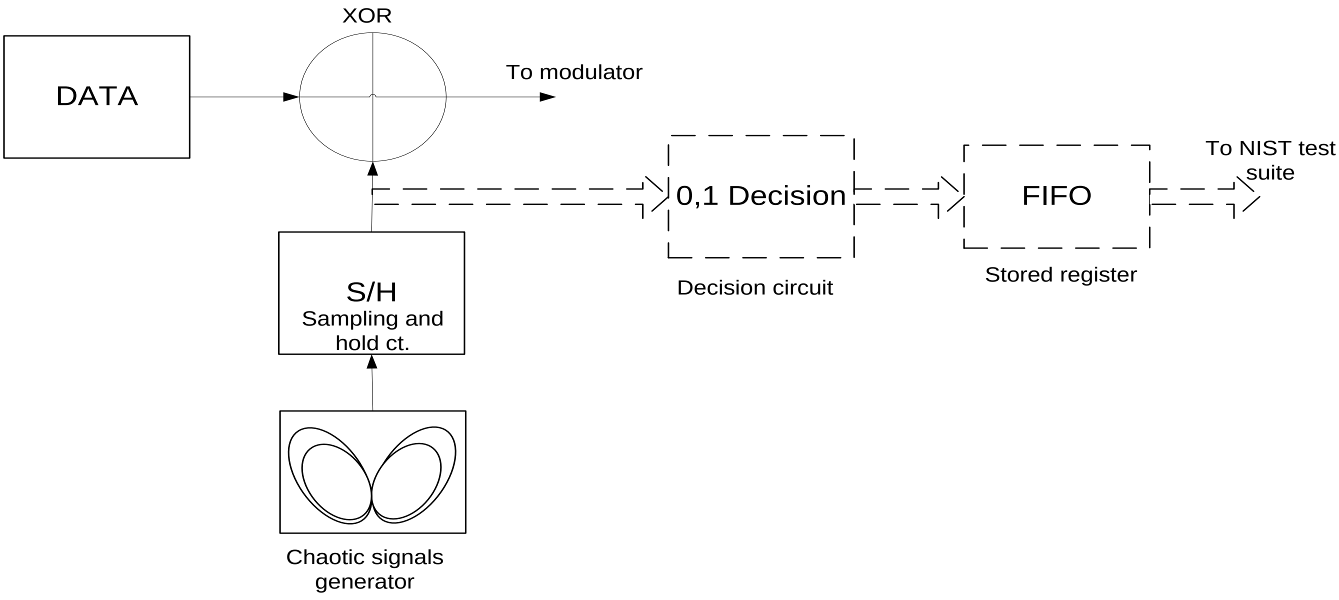


**Figure 4. Schematic Diagram for Chaotic Random Number Generator (CRNG)**

In statistical tests, the randomness of a bit sequence is characterized and described in terms of probability. The NIST Suite and the Diehard Suite are considered the most stringent statistical tests among all international randomness tests. They both include dozens of independent and computationally intensive statistical tests. Most of these tests return a test statistic and its corresponding probability value (p-value) [15]. The p-value is the probability of obtaining a test statistic as "impressive" as the one observed if the sequence is random so that the statistic was the result of chance alone. In other words, the p-value summarizes the strength of the evidence against the perfect randomness hypothesis. Small values (p-values < 0.01) are interpreted as evidence that a sequence is unlikely to be random. Here 0.01 is the significance level, usually denoted as α.

The NIST Suite [15] provides a battery of 16 statistical tests. They assess the presence of a pattern which, if detected, would indicate that the sequence is non-random. In each test, a p-value is calculated. The significance level α for all tests in the NIST Suite is set to 1%. A p-value of zero indicates that the sequence appears to be completely non-random. A p-value less than α would mean that the sequence is non-random with a confidence of 99%. If a p-value is greater than α, the sequence is random with a confidence of 99%.

## IV. NUMERICAL ANALYSIS

In the following section, NIST test results for a CRNG like that shown in Fig. 4 are demonstrated. where the chaotic source is represented by the Lorenz oscillator. The sampling should be done at a frequency much less than the fundamental frequency of the chaotic oscillator ($f_{sampling} << f_{fundamental}$). The fundamental frequency is the inverse of the time of one rotation around a chaotic attractor. That means the variation of the chaotic signal between two passive samples is varying enough to increase the randomness processing and satisfy the frequency aliasing technique. Fig. 5 (a),(b),(c) represent the Lorenz u-signal with time scaling 200 *ms*, 20 *ms*, and 1 ms respectively, and Fig. 5.(d) represents the sampling signal that will apply for all cases and its value is supposed to be constant and equals 50 Hz for all three cases. As shown in Fig. 5(c), *u*-signal for high-time scaling of 1 *ms* seems to be a noise signal with respect to the sampling signal; therefore, the randomness of this case is expected to be higher than the other two cases.

Fig. 6 shows the Simulink® model used in numerical analysis. The time scaling for three Lorenz differential equations is 250 μs and the initial conditions for u, v, and w are taken as 15, 20, and 30 respectively. Tables 1 to 7 represent the numerical results of P-values for the 16 statistical tests of NIST for different Lorenz time scaling and sampling frequencies.

## V. RESULTS AND CONCLUSIONS

It has been demonstrated by simulation that mainly two factors control the randomness of the CRNG: the sampling frequency and the time scaling of the Lorenz generator. As verified by the previous results of the NIST test, these factors are subjected to a trade-off process. The compromising will incorporate two cases:

The first case involves maintaining a constant sampling frequency while reducing the scaling time, which will result in an enhancement of the randomness characteristics of the generated bits.

The second case involves maintaining a constant scaling time while decreasing the sampling frequency, which will result in an improvement in the randomness properties of the generated bits as well. On the other hand, in either scenario, the computer simulation time will increase. In the first case, the computer needs to increase the simulation steps to follow the rapid variation of Lorenz signal. In the second case, the simulation time of our model should be increased to produce the same number of bits before decreasing the sampling frequency.

During our study, some basic points that will be worthwhile are concluded, these are:

The stream cipher will be selected as the encryption type, to use its valuable advantages in terms of low encryption/decryption process time. This agrees with designing a high-speed transmission system with real-time application; moreover, it is implemented by a simple circuit such as XOR.

The principle of sampling theory is applied to chaotic signals to design a true CRNG. At the same time, the frequency aliasing principle makes it too hard to reconstruct the original continuous-time chaotic signal from the running-key sequence.

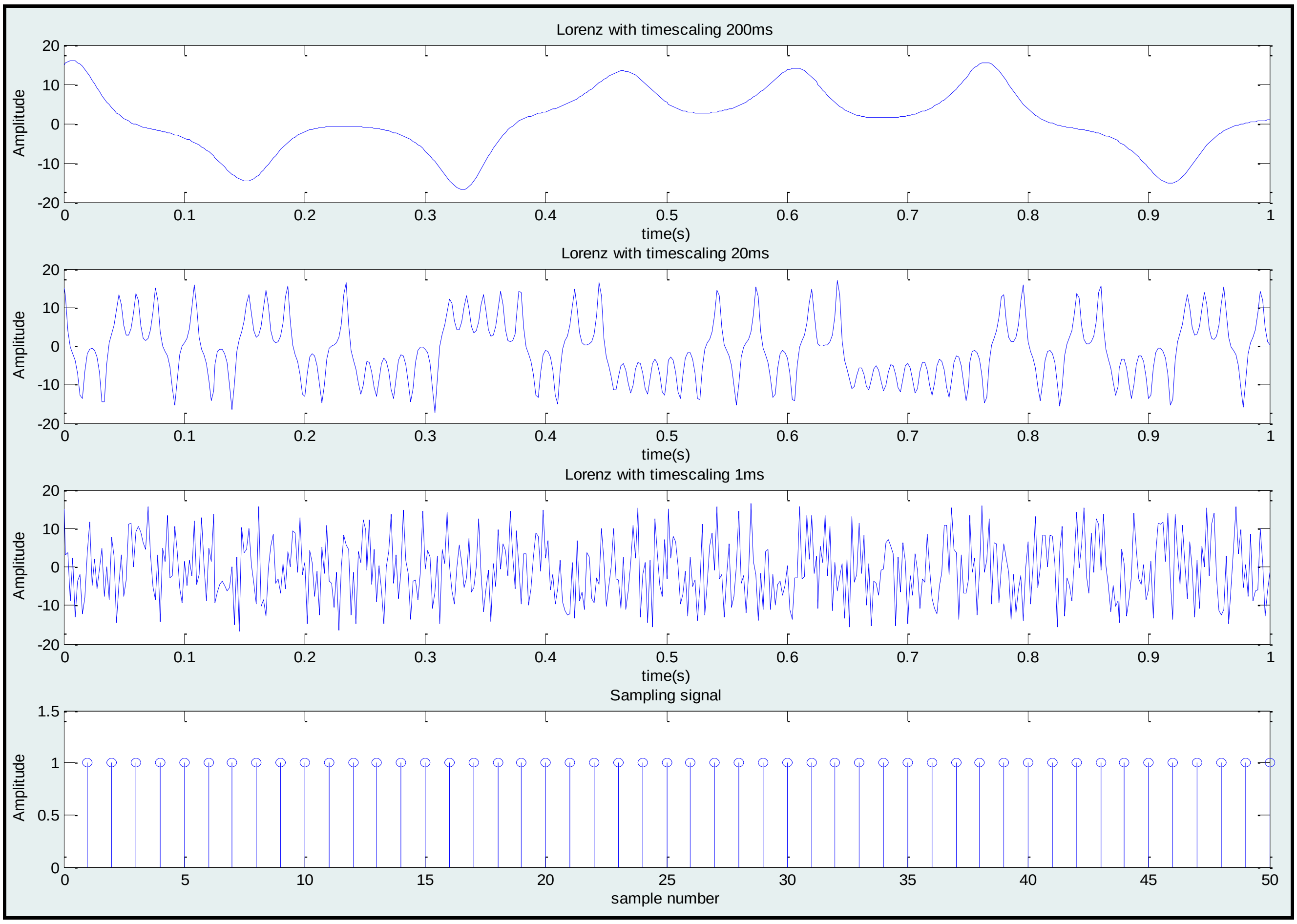


**Figure 5. *u*-Lorenz chaotic signal with different time scaling versus sampling frequency (a) *u*-Lorenz signal with time scaling equals 200 ms (b) *u*-Lorenz signal with time scaling equals 20 ms (c) *u*-Lorenz signal with time scaling equals 1 ms (d) sampling signal.**

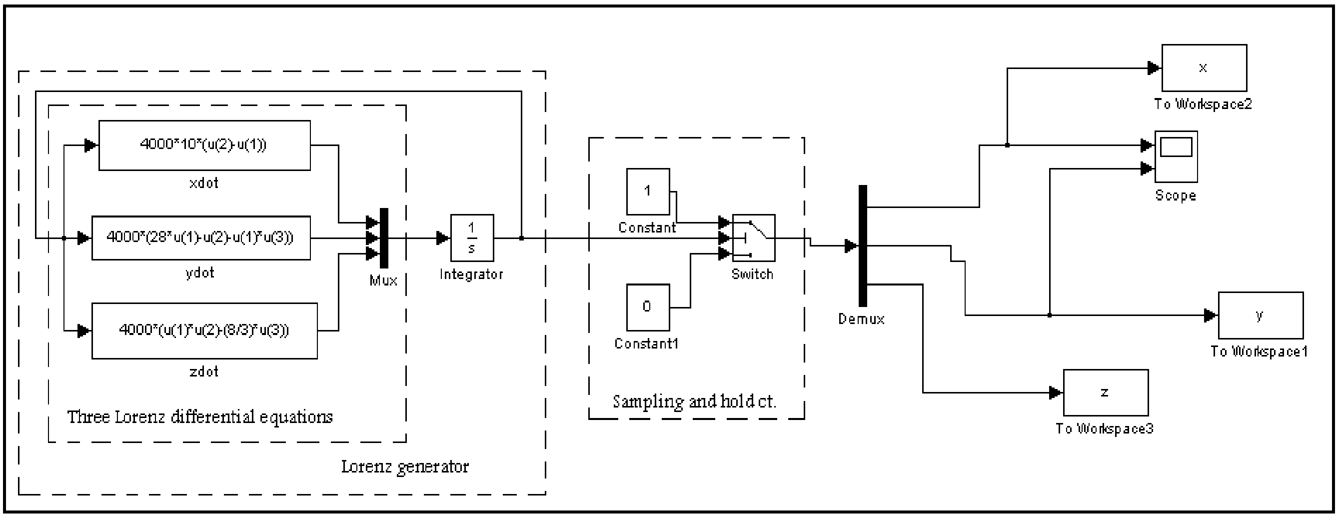


**Figure 6. Simulink® simulation for Lorenz CRNG used in the analysis**

Retrieval Number: 100.1/ijrte.A75240512123
DOI: [10.35940/ijrte.A7524.0512123](10.35940/ijrte.A7524.0512123)
Journal Website: [www.ijrte.org](www.ijrte.org)



Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

**Table 1. NIST results for Lorenz with time scaling 1 ms and sampling $f_{sampling}$=50 kHz**

| Test ID | | u | v |
|---|---|---|---|
| Frequency (monobit) test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Frequency Test within a Block | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Runs Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Test for the Longest Run of Ones in a Block | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Binary Matrix Rank Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Discrete Fourier Transform (Spectral) Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Non-overlapping Template Matching Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Overlapping Template Matching Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Maurer's "Universal Statistical" Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Linear Complexity Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Serial Test | P_value1 | 0.0 | 0.0 |
| | P_value2 | 0.0 | 0.0 |
| | status | Failure | Failure |
| Approximate Entropy Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Cumulative Sums forward Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Cumulative Sums Reverse Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Random Excursions Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Random Excursions Variant Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |

Note: The NIST test suite was performed on 1-bit streams, each stream containing 1 million random bits.

**Table 2. NIST results for Lorenz with time scaling 400 μs and sampling $f_{sampling}$=50 kHz**

| Test ID | | u | v |
|---|---|---|---|
| Frequency (monobit) test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Frequency Test within a Block | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Runs Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Test for the Longest Run of Ones in a Block | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Binary Matrix Rank Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Discrete Fourier Transform (Spectral) Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Non-overlapping Template Matching Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Overlapping Template Matching Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Maurer's "Universal Statistical" Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Linear Complexity Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Serial Test | P_value1 | 0.0 | 0.0 |
| | P_value2 | 0.0 | 0.0 |
| | status | Failure | Failure |
| Approximate Entropy Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Cumulative Sums forward Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Cumulative Sums Reverse Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Random Excursions Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| Random Excursions Variant Test | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |

Note: The NIST test suite was performed on 1-bit streams, each stream containing 1 million random bits.

**Table 3. NIST results for Lorenz with time scaling 250 μs and sampling $f_{sampling}$=50 kHz**

| Test ID | | u | v |
|---|---|---|---|
| Frequency (monobit) test | P_value | 0.257214 | 0.459300 |
| | status | PASS | PASS |
| Frequency Test within a Block | P_value | 0.044656 | 0.098090 |
| | status | PASS | PASS |
| Runs Test | P_value | 0.455496 | 0.749383 |
| | status | PASS | PASS |
| Test for the Longest Run of Ones in a Block | P_value | 0.271688 | 0.371372 |
| | status | PASS | PASS |
| Binary Matrix Rank Test | P_value | 0.480366 | 0.233657 |
| | status | PASS | PASS |
| Discrete Fourier Transform (Spectral) Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Non-overlapping Template Matching Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Overlapping Template Matching Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Maurer's "Universal Statistical" Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Linear Complexity Test | P_value | 0.958956 | 0.224222 |
| | status | PASS | PASS |
| Serial Test | P_value1 | 0.000000 | 0.000000 |
| | P_value2 | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Approximate Entropy Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Cumulative Sums forward Test | P_value | 0.041007 | 0.010509 |
| | status | PASS | PASS |
| Cumulative Sums Reverse Test | P_value | 0.000403 | 0.000587 |
| | status | Failure | Failure |
| Random Excursions Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| Random Excursions Variant Test | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |

Note: The NIST test suite was performed on 1-bit streams, each stream containing 1 million random bits.

**Table 4. NIST results for Lorenz with time scaling 250 μs and sampling $f_{sampling}$=500 Hz**

| Test ID | | u | v |
|---|---|---|---|
| Frequency (monobit) test | P_value | 0.257214 | 0.459300 |
| | status | PASS | PASS |
| Frequency Test within a Block | P_value | 0.044656 | 0.098090 |
| | status | PASS | PASS |
| Runs Test | P_value | 0.455496 | 0.749383 |
| | status | PASS | PASS |
| Test for the Longest Run of Ones in a Block | P_value | 0.271688 | 0.371372 |
| | status | PASS | PASS |
| Binary Matrix Rank Test | P_value | 0.480366 | 0.233657 |
| | status | PASS | PASS |

Note: The NIST test suite was performed on 1-bit streams, each stream containing 1 million random bits.

*Retrieval Number: 100.1/ijrte.A75240512123*
*DOI: 10.35940/ijrte.A7524.0512123*
*Journal Website: www.ijrte.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

**Table 4. cont.**

| Test ID | | u | v |
|---|---|---|---|
| Discrete Fourier Transform (Spectral) Test | P_value | 0.578611 | 0.890517 |
| | status | PASS | PASS |
| Non-overlapping Template Matching Test | P_value (mean) | 0.5134 | 0.5293 |
| | status | PASS | PASS |
| Overlapping Template Matching Test | P_value | 0.301860 | 0.049567 |
| | status | PASS | PASS |
| Maurer's "Universal Statistical" Test | P_value | 0.306558 | 0.202464 |
| | status | PASS | PASS |
| Linear Complexity Test | P_value | 0.049207 | 0.354250 |
| | status | PASS | PASS |
| Serial Test | P_value1 | 0.737745 | 0.504885 |
| | P_value2 | 0.724442 | 0.351622 |
| | status | PASS | PASS |
| Approximate Entropy Test | P_value | 0.718234 | 0.851571 |
| | status | PASS | PASS |
| Cumulative Sums forward Test | P_value | 0.331430 | 0.468936 |
| | status | PASS | PASS |
| Cumulative Sums Reverse Test | P_value | 0.414308 | 0.774705 |
| | status | PASS | PASS |
| Random Excursions Test | P_value (mean) | 0.3277 | 0.5884 |
| | status | PASS | PASS |
| Random Excursions Variant Test | P_value (mean) | 0.2607 | 0.5167 |
| | status | PASS | PASS |

**Table 5. NIST results for Lorenz with time scaling 250 μs and sampling $f_{sampling}$=20 kHz**

| Test ID | | u | v | Remarks |
|---|---|---|---|---|
| Frequency (monobit) test | P_value | 0.3856 | 0.3399 | |
| | status | PASS | PASS | |
| Frequency Test within a Block | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Runs Test | P_value | 0 | | |
| | status | Failure | Failure | |
| Test for the Longest Run of Ones in a Block | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Binary Matrix Rank Test | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Discrete Fourier Transform (Spectral) Test | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Non-overlapping Template Matching Test | P_value | 0* | 0 | * The mean of all 3 streams are zero |
| | status | Failure | Failure | |
| Overlapping Template Matching Test | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Maurer's "Universal Statistical" Test | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Linear Complexity Test | P_value | 0.6486 | 0.4196 | |
| | status | PASS | PASS | |
| Serial Test | P_value1 | 0 | 0 | |
| | P_value2 | 0 | 0 | |
| | status | Failure | Failure | |

Note: The NIST test suite was performed on 3-bit streams, each stream containing 1 million random bits.

**Table 5. cont.**

| Test ID | | u | v | Remarks |
|---|---|---|---|---|
| Approximate Entropy Test | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| Cumulative Sums forward Test | P_value | 0.0013 | 8.4000e-004 | |
| | status | Failure | Failure | |
| Cumulative Sums Reverse Test | P_value | 0.0042 | 0.0041 | |
| | status | Failure | Failure | |
| Random Excursions Test | P_value | test not applicable | test not applicable | There are an insufficient number of cycles to complete the test |
| | status | Failure | Failure | |
| Random Excursions Variant Test | P_value | Test not applicable | Test not applicable | There are an insufficient number of cycles to complete the test |
| | status | Failure | Failure | |

**Table 6. NIST results for Lorenz with time scaling 25 μs and sampling $f_{sampling}$=20 kHz**

| Test ID | | u | v |
|---|---|---|---|
| Frequency (monobit) test | P_value | 0.162714 | 0.649829 |
| | status | PASS | PASS |
| Frequency Test within a Block | P_value | 0.000078 | 0 |
| | status | Failure | Failure |
| Runs Test | P_value | 0 | 0 |
| | status | Failure | Failure |
| Test for the Longest Run of Ones in a Block | P_value | 0.532683 | 0.001174 |
| | status | PASS | Failure |
| Binary Matrix Rank Test | P_value | 0.233986 | 0.348678 |
| | status | PASS | PASS |
| Discrete Fourier Transform (Spectral) Test | P_value | 0.457296 | 0.440804 |
| | status | PASS | PASS |
| Non-overlapping Template Matching Test | P_value (mean) | 0.1294 | 0.0397 |
| | status | PASS | PASS |
| Overlapping Template Matching Test | P_value | 0 | 0 |
| | status | Failure | Failure |
| Maurer's "Universal Statistical" Test | P_value | 0.009265 | 0.000271 |
| | status | Failure | Failure |
| Linear Complexity Test | P_value | 0.762675 | 0.407226 |
| | status | PASS | PASS |
| Serial Test | P_value1 | 0.002504 | 0 |
| | P_value2 | 0.931594 | 0.046910 |
| | status | Partial PASS | Partial PASS |
| Approximate Entropy Test | P_value | 0 | 0 |
| | status | Failure | Failure |
| Cumulative Sums forward Test | P_value | 0.266181 | 0.915089 |
| | status | PASS | PASS |
| Cumulative Sums Reverse Test | P_value | 0.110476 | 0.516382 |
| | status | PASS | PASS |
| Random Excursions Test | P_value | 0.4488 | 0.4549 |
| | status | PASS | PASS |
| Random Excursions Variant Test | P_value | 0.7325 | 0.5215 |
| | status | PASS | PASS |

Note: The NIST test suite was performed on 1-bit streams, each stream containing 1 million random bits.

*Retrieval Number: 100.1/ijrte.A75240512123*
*DOI: [10.35940/ijrte.A7524.0512123](https://doi.org/10.35940/ijrte.A7524.0512123)*
*Journal Website: [www.ijrte.org](http://www.ijrte.org)*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

**Table 7. NIST Results for Lorenz with Time Scaling 16.667 µs and Sampling $f_{samplig}$=20 kHz**

| Test ID | | *u* | *v* | Remarks |
|---|---|---|---|---|
| **Frequency (monobit) test** | P_value (mean) | 0.485177 | 0.353408 | |
| | status | PASS | PASS | |
| **Frequency Test within a Block** | P_value | 0.000354 | 0.000955 | |
| | status | Failure | Failure | |
| **Runs Test** | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.730426 | 0.256572 | |
| | status | PASS | PASS | |
| **Binary Matrix Rank Test** | P_value | 0.441499 | 0.197806 | |
| | status | PASS | PASS | |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.514698 | 0.526611 | |
| | status | PASS | PASS | |
| **Non-overlapping Template Matching Test** | P_value (mean) | 0.2649 | 0.3207 | |
| | status | PASS | PASS | |
| **Overlapping Template Matching Test** | P_value | 0.048116 | 0.019115 | |
| | status | PASS | PASS | |
| **Maurer's "Universal Statistical" Test** | P_value | 0.143473 | 0.810594 | |
| | status | PASS | PASS | |
| **Linear Complexity Test** | P_value | 0.712669 | 0.819432 | |
| | status | PASS | PASS | |
| **Serial Test** | P_value1 | 0.077330 | 0.004559 | |
| | P_value2 | 0.486258 | 0.270332 | |
| | status | PASS | Partial PASS | |
| **Approximate Entropy Test** | P_value | 0 | 0 | |
| | status | Failure | Failure | |
| **Cumulative Sums forward Test** | P_value | 0.763576 | 0.206624 | |
| | status | PASS | PASS | |
| **Cumulative Sums Reverse Test** | P_value | 0.712989 | 0.682964 | |
| | status | PASS | PASS | |
| **Random Excursions Test** | P_value | 0.4492 | TEST NOT APPLICABLE* | There are an insufficient number of cycles to complete the test |
| | status | PASS | Failure | |
| **Random Excursions Variant Test** | P_value | 0.5313 | TEST NOT APPLICABLE* | There are an insufficient number of cycles to complete the test |
| | status | PASS | Failure | |

Note: The NIST test suite was performed on 1bit streams, each stream containing 1 million random bits.

## DECLARATION

| | |
|---|---|
| Funding/ Grants/ Financial Support | No, I did not receive. |
| Conflicts of Interest/ Competing Interests | No conflicts of interest to the best of our knowledge. |
| Ethical Approval and Consent to Participate | No, the article does not require ethical approval and consent to participate with evidence. |
| Availability of Data and Material/ Data Access Statement | Not relevant. |
| Authors Contributions | I am only the sole author of the article. |

## REFERENCES


1. Amr Sayed, "CAM: Chaotic Adaptive Modulation Secure System", International Journal of Engineering Applied Sciences and Technology (IJEAST), 2018, Vol. 3, Issue 6, ISSN No. 2455-2143, Pages 32-40.
2. Joseph Chang Lun Chan; Tae H. Lee; Chee Pin Tan "Secure Communication Through a Chaotic System and a Sliding-Mode Observer", IEEE Transactions on Systems, Man, and Cybernetics: Systems (Volume: 52, Issue: 3, March 2022). [CrossRef]
3. Viktor Fischer, "A Closer Look at Security in Random Number Generators Design", Proceedings of the Third international conference on Constructive Side-Channel Analysis and Secure Design, May 2012 [CrossRef]
4. Fei Yu, Lixiang Li, Qiang Tang, Shuo Cai, Yun Song, and Quan Xu,"A Survey on True Random Number Generators Based on Chaos", Hindawi Discrete Dynamics in Nature and Society, Volume 2019, Article ID 2545123, December 2019. [CrossRef]
5. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology (NIST), Special Publication 800-22, Revision 1a, April 2010, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf
6. Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, and Ahmed Abdel-Hafez, "Synchronization Recovery of Chaotic Signal Through Imperfect Channel Using Optimization Approach", 6th International Conference on Internet Technology and Secured Transactions , Abu Dhabi, United Arab Emirates, pp. 73-78, December 2011
7. Amr Sayed Abdel Fattah, Salwa Elramly, Magdy Ibrahim, and Ahmed Abdel-Hafez, "Denoising Algorithm for Noisy Chaotic Signal by Using Wavelet Transform: Comprehensive Study", 6th International Conference on Internet Technology and Secured Transactions , pp. 79-85 , Abu Dhabi, United Arab Emirates, December 2011.
8. Amr Sayed Abdel Fattah, "An Adaptive Power Output Control System for CAM", 2021 International Symposium on Networks, Computers and Communications (ISNCC) | 2021 IEEE | DOI: 10.1109/ISNCC52172.2021.9615844. [CrossRef]


*Retrieval Number: 100.1/ijrte.A75240512123*
*DOI: 10.35940/ijrte.A7524.0512123*
*Journal Website: www.ijrte.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

9. Jiu Chao Feng and Chi Kong Tse, "Reconstruction of Chaotic Signals with Applications to Chaos-Based Communications", World Scientific Publishing Company, September, 2008
10. Huaguang Zhang, Derong Liu, and Zhiliang Wang, "Controlling Chaos: Suppression, Synchronization and Chaotification", Springer, 1st edition, 2009.
11. Steven H. Strogatz, "Nonlinear Dynamics and Chaos: With Applications To Physics, Biology, Chemistry, And Engineering", Westview Press, 1st edition, 2001
12. Santo Banerjee, "Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption", IGI Global; 1st edition, 2010. [CrossRef]
13. Ljupco Kocarev and Shiguo Lian, "Chaos-based Cryptography: Theory, Algorithms and Applications", Springer; 1st Edition, 2011 [CrossRef]
14. G. Hu, Z. Feng and R. Meng, "Chosen Ciphertext Attack on Chaos Communication Based on Chaotic Synchronization", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 50, no. 2, pp. 275–279, Feb. 2003. [CrossRef]
15. Claude E. Shannon., "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28, no. 4, pp.656-715, October 1949. [CrossRef]
16. Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer, 2nd edition, November 2010.
17. Manfred Schroeder, "Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity", Springer, 5th edition, November 2010.
18. James E. Gentle, "Random Number Generation and Monte Carlo Methods (Statistics and Computing) ", Springer, November 2010.
19. James Stone, "Bayes' Rule: A Tutorial Introduction to Bayesian Analysis", Sebtel Press; 1st edition, December 3, 2021.
20. Ljupco Kocarev and Shiguo Lian, "Chaos-based Cryptography: Theory, Algorithms and Applications", Springer; 1st Edition, 2011. [CrossRef]
21. Frank C. Hoppensteadt, "Analysis and Simulation of Chaotic Systems", Applied Mathematical Sciences, Springer, 2nd edition, 2000.
22. Edward Lorenz, "The Essence of Chaos", Taylor & Francis, April 2007.
23. Floriane Anstett, Gilles Millerioux, and Gérard Bloch, "Chaotic CryptoSystems: Cryptanalysis and Identifiability", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 53, no. 12, pp.2673-2680, December 2006. [CrossRef]
24. Naoki Masuda and Kazuyuki Aihara, "CryptoSystems With Discretized Chaotic Maps", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 49, no. 1, pp. 28-40, January 2002. [CrossRef]

## AUTHOR PROFILE

**Amr S. Youssef** was born on December 6th, 1976 in Cairo, Egypt. He received his Bachelor of Electronics and Communication Engineering (B.Sc.) from Ain Shames University, Cairo, Egypt, in 1999. He completed his Master, and Ph.D. in Electronics and Communication Engineering, from the same university in 2006 and 2013 respectively. He has been working at the Higher Colleges of Technology HCT in UAE since 2009. His research interests lie in the areas of signal processing and chaotic signals. He has collaborated actively with researchers in several other areas including adaptive modulation and security systems.