Using a Chaotic Digital System to Generate Random Numbers for Secure Communication on 5G Networks

Haider Th. Salim Alrikabi
Department of Electrical Engineering, College of Engineering, University of Wasit, Iraq
hdhiyab@uowasit.edu.iq (corresponding author)

Ibtisam A. Aljazaery
Department of Electrical Engineering, College of Engineering, University of Babylon, Iraq
sci.ibtisam.abdulwahid@uobabylon.edu.iq

Abdul Hadi Mohammed Alaidi
Department of Programming, Computer Science and Information Technology College, University of Wasit, Iraq
alaidi@uowasit.edu.iq

Received: 21 January 2024 | Revised: 23 February 2024 | Accepted: 24 February 2024

ABSTRACT

There are several encryption system applications in 5G networks where rapid response is needed, particularly in the military, health sector, traffic, and vehicular movement. This article presents a proposed data security system for 5G networks that fortifies the security of the network through the use of synchronized chaotic systems to produce pseudo-random numbers. The technique by which random numbers are generated during the encryption procedures is closely associated with 5G network security. Many synchronized chaotic systems are used to produce chaotic random models which are used as encryption bases for a wide variety of data. In this study, the encryption was carried out using a variety of data, including two and three-dimensional color images and audio signals of varying lengths, in addition to the use of Fast Fourier Transform (FFT) for encryption of the ingredient energy wave. The results revealed that the algorithm deployed in the process of encryption performed well. Simulations were performed in MATLAB.

Keywords-synchronized chaotic systems; 5G networks; Pseudo-Random Number Generator (PRNG); data security; FFT

I. INTRODUCTION

The ability of the 5G networks to deliver data is almost 40 times faster than other networks, and when they are used fewer delays occur in the transfer and reception of files. Through the 5G networks, the advancement of other new technologies such as the Internet of Things (IoT), virtual reality, etc. can be driven [7]. Cryptography is a requirement for the secure transmission of data and information, [1-4]. Using a robust technique for encryption and decryption of data becomes imperative in the transfer of data, and a 5G network enables the security of the data being transferred. There are two kinds of random number generators, the True Random Number Generator (TRNG) and the Pseudo Random Number Generator (PRNG) [5, 6]. In the PRNG, a random number is intentionally generated, but it is not completely random and it is generated by software. The TRNG, on the other hand, utilizes hardware to generate the random numbers. Nevertheless, PRNG is a deterministic system, and due to this, the safety and security of the number that has been generated is guaranteed when the initial value has high entropy. In this work, high entropy was obtained as a result of the use of the statistical algorithm for random chaotic systems, which in turn enabled the realization of high security for the data that were employed for encryption.

Chaotic signals are stable and constant. More so, they are characterized by random time evolution and a broadband spectrum that is generated through a deterministic nonlinear dynamical system whose behavior is irregular. Chaos communications is referred to as the application of chaos theory to the security of information that is transmitted using telecommunication technologies. Secured communication refers to communication that is carried out in a way potential eavesdroppers cannot access the content of the transmitted message. The security of communication in chaotic communications is determined by the complex and dynamic behaviors these systems demonstrate. In this type of communication, data are encoded using some features of the chaotic dynamics like spread spectrum, pseudorandom noise which is also referred to as noise-like dynamics, and complex behavior [8]. The decoding of chaos can be done using its deterministic characteristic given that it is a deterministic phenomenon. Practically, when the devices of chaos communications are being implemented, either chaos synchronization or chaos control is considered [9, 10]. The use of such properties of chaos for the implementation of chaos communications requires using two chaotic oscillators as a transmitter (or master) and receiver (or slave). At the transmitter, the message is hidden in the chaotic signal. Since the chaotic signal plays the role of conveying the information, it is also referred to as the chaotic carrier. The synchronization of the oscillators can be compared to the synchronization of random neutral nets in neural cryptography. When chaos synchronization is used, a basic scheme of a communications device [11] is made by two identical chaotic oscillators, i.e., transmitter and receiver. A connection between the two oscillators is established in a configuration where the transmitter drives the receiver toward the realization of identical synchronization of chaos between them. Information is transmitted from the transmitter by adding a message in the form of a small perturbation to the chaotic signal, which acts as a driver of the chaotic signal. Through this, the chaotic signal embeds the transmitted message. Upon the synchronization completion between the receiver and the transmitter, the decoding of the message occurs through a subtraction between the signal that has been transmitted by the transmitter, with a copy produced at the receiver through a mechanism known as chaos synchronization. This is possible because the chaotic carrier and the message are contained in the transmitter’s output, while the output of the receiver is produced by just one copy of the chaotic carrier without the message.

II. RELATED WORK

Authors in [4] introduced versatile steering, which is based on 5G Quality of Service (QoS) and Mobile Ad Hoc Networks (MANETs). To achieve versatile 5G steering, the geography of a virtualized climate was planned and CHAOS was also customized for network traffic flooding. Authors in [2] constructed a novel two-parameter chaotic system that is characterized by three dimensions. The evaluation of the system was first conducted by computing its diagrams of bifurcation and diagrams of Lyapunov exponents. Afterward, application of the system was done to two problems associated with encryption. In [12], a new voice encryption wireless system was presented. The proposed system was designed based on the characteristics of a massive Multiple Input Multiple Output (MIMO) wireless channel. The permutation of the channel fading values is carried out using the Minimum Mean Square Error (MMSE) precoding method, and afterward, the use of different chaotic generators was employed in substituting the permutated channel fading values. A combination of the voice samples with the chaotic sequence and channel values was carried out before transmission. The authors deployed their new system on a 5G network that is inclusive of Massive MIMO, Parallel Spatial Modulation (PSM), and Generalized Frequency Division Multiplexing (GFDM).

Authors in [13] proposed the Boltzmann machine (BMKG)-based encryption algorithm that could provide security for IoT-based 5G network device connectivity and coverage and expand the Encryption and Authentication Scheme (EAS) framework. For the exchange of keys, the authors did a comparison of different asymmetric algorithms. An efficient and highly secure encryption-decryption method was proposed in [14]. Moreover, other algorithms, e.g. those in [15, 16], can be used to optimize the chaotic shuffling process and the dynamic generation of substitution boxes. Authors in [17, 18] proposed a system that enable secured end-to-end communication through user authentication and key agreement. They aimed to address the security challenges that occur when multiple devices network for data collection and analysis. To achieve this aim, the authors presented a Subtree-Based Online/Offline Signature Procedure (SBOOSP) alongside its aggregation (AggSBOOSP) for massive devices in 5G WSNs using conformable chaotic maps. The authors reported that the proposed system is efficient, lightweight, and secure.

A TRNG algorithm was proposed in [19-21]. The source of noise used in this work was the visible spectrum. The authors assumed that if the data used by the cryptography system belong to the visible spectrum, high entropy will be obtained for the random numbers generated by the proposed TRNG. With the use of the random number generator, keys and seeds are generated randomly in numerous cryptographic systems. To this end, the use of keys for the encryption and decryption of the information being transferred is suggested.

III. METHODOLOGY

This section presents the mathematical model that was deployed in the generation of random numbers. The model involved devising a set of statistical equations, denoting the synchronized chaotic system for the formation of random statistical matrices with different dimensions as given below:

$$F1 = (1/5)\,x1 + (1/4)\,x2 - (1/3)\,x3 \qquad (1)$$

$$F2 = (2/5)\,x1 + (2/4)\,x2 - (1/3)\,x3 \qquad (2)$$

$$F3 = (1/5)\,x1 - (2/4)\,x2 + (2/3)\,x3 \qquad (3)$$

where, $x1$, $x2$, and $x3$ denote the chaotic system’s initial values. Chaotic systems are known to be overly sensitive to the initial values, and as such, it was ensured that the equations of the synchronized chaotic system were handled in a manner that guaranteed high accuracy. The aim of this was to realize the most appropriate values required for the construction of the random number generator.

The use of the synchronous chaotic system was employed in obtaining random numerical matrices characterized by different shapes and dimensions as in Figure 1.

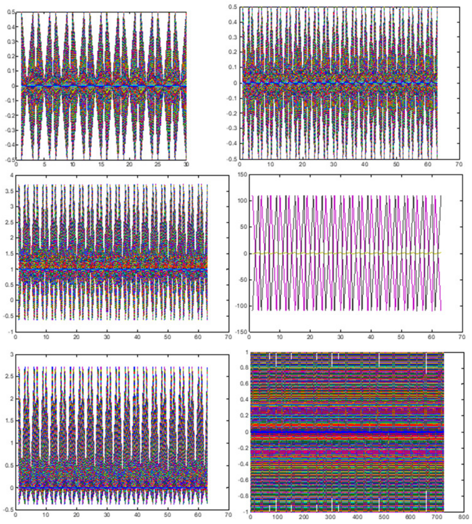

Fig. 1. Examples of the Chaotic Random Number Generator (CRNG).

IV. PROPOSED SYSTEM AND ALGORITHMS

In this section, the algorithms and schemes used for the processes of data decryption and encryption are presented. Figure 2 shows the algorithm which is proposed for the encryption operation.

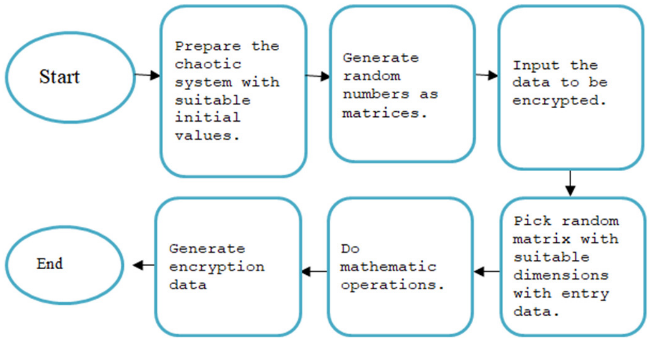
Start
Prepare the chaotic system with suitable initial values.
Generate random numbers as matrices.
Input the data to be encrypted.
Pick random matrix with suitable dimensions with entry data.
Do mathematic operations.
Generate encryption data
End

Fig. 2. The encryption algorithm.

The proposed algorithm for encryption operation follows:

```
Begin:
Step 1. Input initial values of
synchronized chaotic equations.
Step 2. Input synchronized chaotic
equations as a group of system equations.
Step 3. F1= (1/5) x1+(1/4) x2-(1/3) x3,
F2= (2/5) x1+(2/4) x2-(1/3) x3, F3= (1/5)
x1-(2/4) x2+(2/3) x3.
Step 4. for i=1:t
        f1r (: ,i+1)=f1r(:,1).*f1r(:,i);
        f2r (: ,i+1)=f2r(:,1).*f2r(:,i);
        f3r (: ,i+1)=f3r(:,1).*f3r(:,i);
    end
Step 5. Generate a new random matrix,
x=[f1r f2r f3r].
Step 6. Input data to encrypt.
Step 7. Choose suitable x-array dimensions
Step 8. Make math. Operations (data, x-
matrix).
Step 9. Plot encrypted data (stego data).
End.
```

The proposed algorithm for decryption operation follows:

```
Begin:
Step 1. Input encrypted data.
Step 2. Perform inverse math operations.
Step 3. Distinguish the result from the
previous step.
Step 4. Obtain the original data.
End.
```

The block diagram in Figure 3 shows the steps required for the decryption.

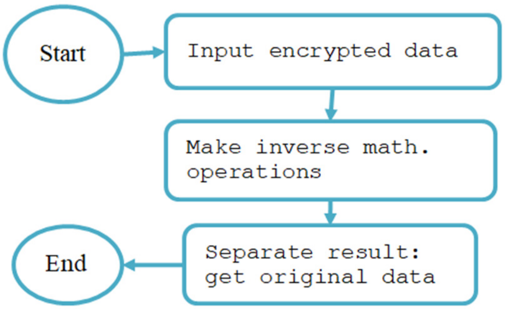
Start
Input encrypted data
Make inverse math. operations
Separate result: get original data
End

Fig. 3. The decryption algorithm.

V. EXPERIMENTAL RESULTS AND DISCUSSION

Based on the experiments performed in this study, the proposed algorithm demonstrated a high level of performance in terms of data protection and security. The experiments involved the use of a wide range of data with PRNG alongside synchronized chaotic parameters. Tables I-III show the experimental results. It was observed that total concealing of the original data's features was achieved by the high entropy values of the CRNG models, and these in turn resulted in results that were encrypted with high entropy values. This result shows that a random generator is efficient in concealing the features of the original data. The PSNR values also reveal that higher values were obtained for the original data, as compared with the encoded values, as a result of the loss of clarity features. Consequently, this results in distortion which is regarded as a kind of high noise to the outputs obtained from the proposed technique. The results obtained in this study show the output of the correlation equation. A significantly low correlation coefficient was found, showing that there was a great difference in the data after the security procedure was applied. It was also observed that more time was required in the process of encryption than in decryption.

Figure 4 shows that the high entropy of the CRNG models completely hid the features of the original 3D image.

The various kinds of data used in testing the proposed algorithms, along with their encryption stages are shown below.

- 3D image is shown in Figure 4.
- 2D image is shown in Figure 5.
- Audio signal 1 is shown in Figure 6.
- Audio signal 2 is shown in Figure 7.
- The FFT power file is shown in Figure 8.

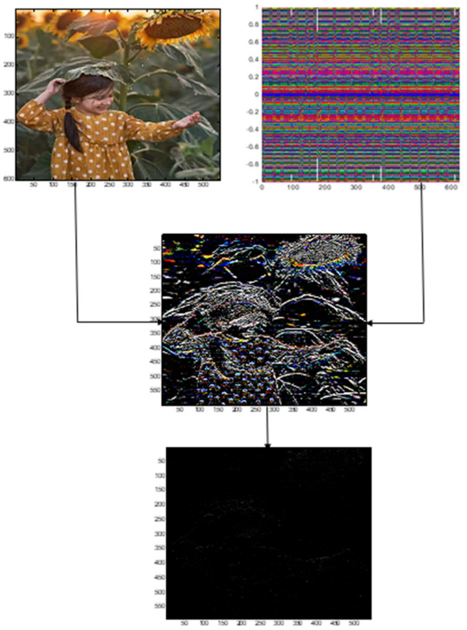

Fig. 4. Encryption stages of a 3D image.

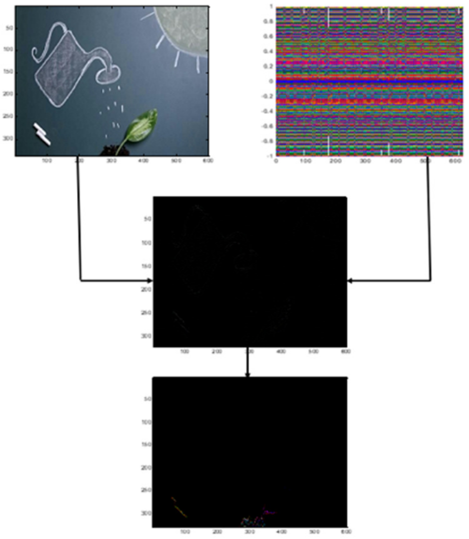

Fig. 5. Encryption stages of a 2D image.

Figure 5 shows a completely encrypted 2D image with small entropy. Figure 7 shows the hiding features of the original audio signal, while Figure 8 shows that a great difference was obtained in the FFT signal after the security processes.

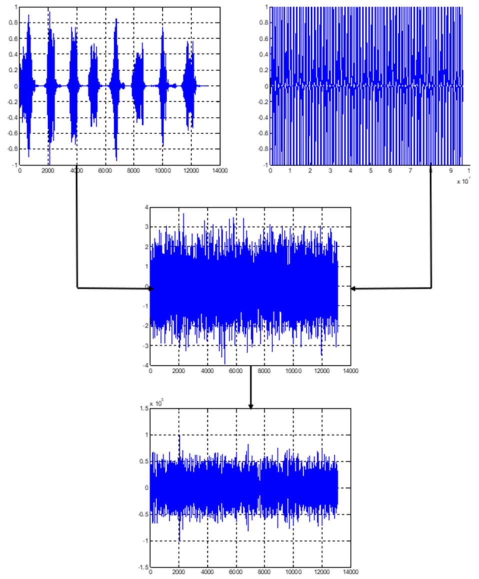

Fig. 6. Encryption stages of audio signal1.

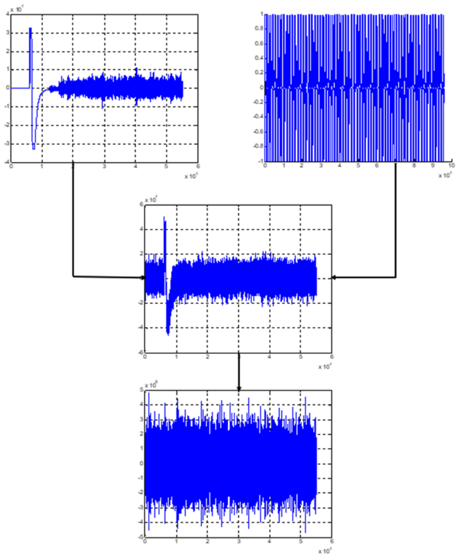

Fig. 7. Encryption stages of audio signal 2.

VI. QUALIFYING MEASUREMENTS

A. *Mean Square Error (MSE)*

This evaluation parameter measures the total squared error in all kinds of data. MSE is obtained by:

$$\mathrm{E} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[c(i,j)-c(i,j)']^{2} \qquad (4)$$

where m denotes the dimensions of the origin matrices and $c(i,j)$ the dimensions of the stego data.

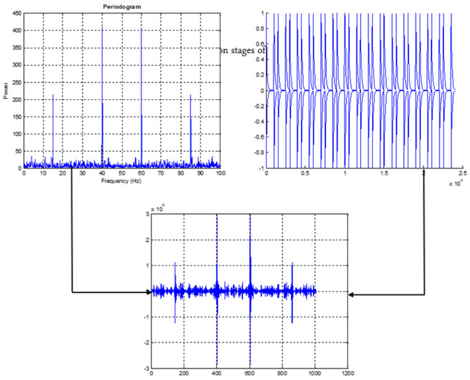

Fig. 8. Encryption stages of an FFT power signal.

B. *Peak Signal to Noise Ratio (PSNR)*

The PSNR parameter is a measure through which the peak error is determined. Thus, it is determined by the quality of the image, thus higher PSNR can be achieved when the quality of the image is high. The following equation can be used to calculate the PSNR:

$$PSNR = 10\, log_{10} \frac{R^2}{MSE} \tag{5}$$

where R represents the higher potential value of the pixel's density.

Performance can also be evaluated using the time frame used to encode and decode the data:

$$Corr = \frac{\sum_{i=1}^{N}\sum_{J=1}^{M}(I_1(i,j)-\bar{I}_1)(I_2(i,j)-\bar{I}_2)}{\sqrt{\left[\sum_{i=1}^{N}\sum_{J=1}^{M}(I_1(i,j)-\bar{I}_1)^2\right]\left[\sum_{i=1}^{N}\sum_{J=1}^{M}(I_2(i,j)-\bar{I}_2)^2\right]}} \tag{6}$$

where $I_1(i,j)$ is the value of the (i,j) pixel of the original data, $\bar{I}_1$ is the mean of the original data, calculated by (7), $I_2(i,j)$ presents the value of the (i,j) pixel of the reconstructed data, $\bar{I}_2$ is the mean of the reconstructed data calculated by (8), M is the height of the image, N is its width, and i and j represent the row and column numbers. Entropy is defined by (9) where S is the entropy and P_i is the probability.

$$\bar{I}_1 = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M} I_1\,(i,j) \tag{7}$$

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{i=1}^{N}\sum_{j=1}^{M} I_2\,(i,j) \tag{8}$$

$$S = -\sum_i P_i \, log\, P_i \tag{9}$$

TABLE I. QUALITY MEASUREMENTS FOR ONE-DIMENSIONAL DATA

	Signals	PSNR (db.)	Entropy	Corr.
Audio signal 1	Origin signal (1)	48	2.891	0.0003168
	CRNG model		5.857	
	Encrypted signal (1)	31	0.6527	
Audio signal 2	Origin signal (2)	45	3.034	0.000581
	CRNG model		5.857	
	Encrypted signal (2)	32	0.7531	
FFT power signal	Origin signal	41	1.352	0.000201
	CRNG model		2.855	
	Encrypted signal	30	0.301	

TABLE II. QUALITY MEASUREMENTS FOR TWO-DIMENSIONAL DATA

	Images	PSNR (db.)	Entropy	Corr.
3-D Image	Origin Image	43.78	4.583	0.0000384
	CRNG model		7.304	
	Encrypted Image	33.21	0.8980	
2-D Image	Origin Image	47	4.169	0.000022
	CRNG model		7.304	
	Encrypted Image	35.83	0.7998	

TABLE III. TIME OF ENCRYPTION AND DECRYPTION PROCESSES

Data type	Time of encryption (sec)	Time of decryption (sec)
Audio signal 1	1.005	0.2035
Audio signal 2	1.845	0.375
FFT power signal	1.013	0.210
3-D Image	3.590	1.001
2-D Image	2.720	0.990

VII. CONCLUSIONS

In this study, highly encrypted data were produced as a result of the construction of a random number generator from a synchronized chaotic system. The high rate of encrypted data is attributed to the high entropy values achieved by the models proposed in this study. This is why the features of the original data were totally hidden. With regard to the urgency with which the data are needed and considering the speedy nature of the 5G network, the focus of this work is to shorten the process of data recovery. The decryption algorithm has high efficiency in terms of returning data to its original values despite its straightforwardness and short steps. It was observed that the proposed algorithm consumed more time during data encryption and lesser time for decryption. The central idea of the current research is to create a mathematical model that is highly chaotic during the process of encoding.

REFERENCES

[1] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118–131, Mar. 2020, https://doi.org/10.1109/TNSM.2020.2969863.

[2] M. K. Abdul-Hussein and H. T. S. ALRikabi, "Secured Transfer and Storage Image Data for Cloud Communications," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 19, no. 06, pp. 4–17, May 2023, https://doi.org/10.3991/ijoe.v19i06.37587.

[3] A. H. M. Alaidi, R. M. Al_airaji, H. T. S. Alrikabi, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 10, pp. 122–139, May 2022, https://doi.org/10.3991/ijim.v16i10.30209.

[4] H. T. S. Alrikabi and H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 12, pp. 89–105, Sep. 2022, https://doi.org/10.3991/ijoe.v18i12.33817.

[5] M. Gafsi, N. Abbassi, R. Amdouni, M. A. Hajjaji, and A. Mtibaa, "Hardware implementation of a strong pseudo-random numbers generator with an application to image encryption," in *2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, Hammamet, Tunisia, Feb. 2022, pp. 510–515, https://doi.org/10.1109/SETIT54465.2022.9875453.

[6] M. Tuna, "A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation," *Analog Integrated Circuits and Signal Processing*, vol. 105, no. 2, pp. 167–181, Nov. 2020, https://doi.org/10.1007/s10470-020-01703-z.

[7] M. Eisenbarth *et al.*, "Toward Smart Vehicle-to-Everything-Connected Powertrains: Driving Real Component Test Benches in a Fully Interactive Virtual Smart City," *IEEE Vehicular Technology Magazine*, vol. 16, no. 1, pp. 75–82, Mar. 2021, https://doi.org/10.1109/MVT.2020.3008018.

[8] M. P. Kennedy and G. Kolumbán, "Digital communications using chaos," *Signal Processing*, vol. 80, no. 7, pp. 1307–1320, Jul. 2000, https://doi.org/10.1016/S0165-1684(00)00038-4.

[9] S. Banerjee, Ed., *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption*, 1st ed. Hershey, PA, USA: Information Science Reference, 2010.

[10] M. Roy *et al.*, "Data Security Techniques Based on DNA Encryption," in *Proceedings of International Ethical Hacking Conference 2019*, Singapore, 2020, pp. 239–249, https://doi.org/10.1007/978-981-15-0361-0_19.

[11] K. M. Cuomo and A. V. Oppenheim, "Chaotic signals and systems for communications," in *1993 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Minneapolis, MN, USA, Apr. 1993, vol. 3, pp. 137–140 vol.3, https://doi.org/10.1109/ICASSP.1993.319454.

[12] M. J. M. Ameen and S. S. Hreshee, "Securing Physical Layer of 5G Wireless Network System over GFDM Using Linear Precoding Algorithm for Massive MIMO and Hyperchaotic QRDecomposition," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 5, pp. 579–591, Oct. 2022, https://doi.org/10.22266/ijies2022.1031.50.

[13] B. Bordel, R. Alcarria, T. Robles, and M. S. Iglesias, "Data Authentication and Anonymization in IoT Scenarios and Future 5G Networks Using Chaotic Digital Watermarking," *IEEE Access*, vol. 9, pp. 22378–22398, 2021, https://doi.org/10.1109/ACCESS.2021.3055771.

[14] M. O. Al-Dwairi, A. Y. Hendi, and Z. A. AlQadi, "An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images," *Engineering, Technology & Applied Science Research*, vol. 9, no. 3, pp. 4165–4168, Jun. 2019, https://doi.org/10.48084/etasr.2525.

[15] A. H. Alaidi, C. Soong Der, and Y. Weng Leong, "Increased Efficiency of the Artificial Bee Colony Algorithm Using the Pheromone Technique," *Engineering, Technology & Applied Science Research*, vol. 12, no. 6, pp. 9732–9736, Dec. 2022, https://doi.org/10.48084/etasr.5305.

[16] A. H. Alaidi, S. D. Chen, and Y. Weng Leong, "Artificial Bee Colony with Crossover Operations for Discrete Problems," *Engineering, Technology & Applied Science Research*, vol. 12, no. 6, pp. 9510–9514, Dec. 2022, https://doi.org/10.48084/etasr.5250.

[17] W. Jinqiu, Q. Gang, and K. Pengbin, "Emerging 5G Multicarrier Chaotic Sequence Spread Spectrum Technology for Underwater Acoustic Communication," *Complexity*, vol. 2018, Oct. 2018, Art. no. e3790529, https://doi.org/10.1155/2018/3790529.

[18] B. Jovic, "Chaotic Signals and Their Use in Secure Communications," in *Synchronization Techniques for Chaotic Communication Systems*, B. Jovic, Ed. Berlin, Heidelberg, Germany: Springer, 2011, pp. 31–47.

[19] H. B. Meitei and M. Kumar, "FPGA Implementation of a Wireless Communication System for Secure IR Sensor Data Transmission using TRNG," *International Journal of Engineering Trends and Technology*, vol. 70, no. 7, pp. 220–237, 2022, https://doi.org/10.14445/22315381/IJETT-V70I7P223.

[20] K. Lee, S.-Y. Lee, C. Seo, and K. Yim, "TRNG (True Random Number Generator) Method Using Visible Spectrum for Secure Communication on 5G Network," *IEEE Access*, vol. 6, pp. 12838–12847, 2018, https://doi.org/10.1109/ACCESS.2018.2799682.

[21] J. S. Teh, A. Samsudin, M. Al-Mazrooie, and A. Akhavan, "GPUs and chaos: a new true random number generator," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1913–1922, Dec. 2015, https://doi.org/10.1007/s11071-015-2287-7.