PILEA, an Advanced Hybrid Lightweight Algorithm utilizing Logical Mathematical Functions and Chaotic Systems

Zahraa A. Mohammed
Department of Computer Science, College of Science for Women, University of Babylon, Iraq
zahraa.abed@uobabylon.edu.iq (corresponding author)

Khalid Ali Hussein
Computer Science Department, College of Education, Al Mustansiriyah University, Iraq
dr.khalid.ali68@gmail.com

Received: 11 May 2024 | Revised: 9 June 2024 | Accepted: 25 June 2024

ABSTRACT

In information security, data encryption plays a crucial role in preventing unauthorized access. Traditional methods often fall short when faced with sophisticated cyber threats. This research presents a hybrid encryption technique that integrates a recently devised 5D chaotic system, effectively bolstering data security by encoding information in an intricate, puzzle-like structure. This approach thwarts easy access to sensitive data, thus safeguarding them from potential interception and exploitation. The proposed encryption method combines the Linear Encryption Algorithm (LEA) and the Advanced Encryption Standard (AES) to create the Parallel Improved LEA (PILEA), blending key components of both algorithms to enhance data security. By integrating AES's S-box, Shift Rounds, Mix Columns, and Add Round Key operations, the PILEA significantly raises the complexity of the encrypted data, making them more resistant to unauthorized decryption attempts. A key innovation of this system is the use of a chaotic system for key generation, resulting in a strong, nonlinear, and dynamic key stream. Furthermore, by operating the entire system in a parallel mode, the proposed approach aims to decrease the number of rounds in the encryption process and the overall execution time for encryption and decryption. These enhancements further strengthen the encryption system's resilience against infiltration by malicious entities. Experimental results show that the PILEA method can withstand various types of cryptographic attacks, provides reduced computation times, and produces a highly random keystream, as confirmed by the NIST statistical test suite for randomness.

Keywords-hyperchaos; three positive Lyapunov exponents; PILEA; diffusion; confusion; SP-network

I. INTRODUCTION

With the rapid development of recent information technologies, data exchanging has become a daily routine for most people. Cryptography is the art of safeguarding data by changing them to an unreadable form while being transferred between two sides. It is obvious that there are many types of ciphering and a key point is choosing the suitable one depending on the occasional limitations. The attractive advancements of lightweight algorithms encouraged their adoption in comparison with heavy-weight algorithm types [1]. A wide range of lightweight algorithms, such as RC6, ChaCha, Present, LEA, etc. are characterized by the high security they offer despite their simple process in both encryption/decryption [2], which makes them suitable for environments, like IoT, IoE, and cloud computing [3]. Block ciphering and stream ciphering use the same key in two cipher routines and constitute a symmetric category, while asymmetric ciphering delivers two different keys for encryption and decryption routines [4, 5]. A chaos system in mathematics is a complex dynamic system that is very sensitive to the initial conditions, which leads to random behavior. The chaotic system can be represented by a set of nonlinear differential equations with n variables, where the value of n is determined according to the dimensions adapted to the chaotic system. The chaotic equations govern the system's evolution over time [6]. Conceptually, to keep up with the recent technology and to provide fast protection to vital files, the cipher algorithm should be able to handle its data in parallel. This produces faster results, which strengthen the protection system [7]. In general, it exploits the hardware equipment in parallel to perform the work in the shortest time possible.

A. Problem Statement

As cloud computing continues to evolve and manage increasingly sensitive data, the need for secure cloud network communications is intensified, whereas there is a growing demand for lightweight cryptographic solutions. These solutions should be designed to protect data transmission while minimizing CPU overhead, memory usage, and power consumption, making them ideal for modern cloud architectures. This approach ensures robust security without compromising the essential to cloud computing operations, which are efficiency and scalability.

B. Research Contribution

- A new lightweight hybrid encryption algorithm named PILEA is proposed. It stands on the simple process principle with the ARX operations of LEA and the strong Substitution–Permutation Network (SPN) network of AES.
- The algorithm incorporates unique components into the encryption process, yet it is based on the well-known ciphers LEA and traditional AES. It uses a two-level scheme with one SPN for diffusion and modified LEA operations at the first level.
- Parallel processing methodology is deployed, which significantly reduces the computational cost associated with encrypted big data streams by distributing the encryption tasks over multiple CPU cores.
- According to the experimental security research, PILEA provided data transmission security at a level comparable to that of established standards like AES, but with far fewer processing resource requirements.

II. LITERATURE REVIEW

Cloud security: Authors in [8] proposed a simple and highly secure encryption/decryption method depending on the IDEA cipher. Besides shuffling bytes, it used XOR logical operation, and addition/subtraction mathematical operations to enter diffusion/confusion to the entire system. They adapted variable key size and round values, while strong security with faster encryption times was provided for the cloud cryptosystem. Authors in [9] adapted a small part of the original data as a key by using data partitioning and scrambling techniques. Small random keys were generated instead of user-provided data. Authors in [10] presented an advanced version of the LEA algorithm using three different key sizes: (256, 128, and 64) rather than the ordinary key values of traditional LEA. The paper implemented the encrypted image files, enhancing operating frequency levels up to 34%, 33%, and 131% compared to the original LEA algorithm with key sizes 128, 192, and 256 bits. In contrast to the latter, the former increased the hardware recourses. In [11], new updates were made to modify the LEA algorithm by adapting three architectures, two for area consideration and the third one for speed. These architectures for each key value related to the LEA algorithm were implemented in both FPGA and ASIC platforms. In [12], In order to generate the key required for cloud user registration, first the ECC technique was employed. Flamingo search optimization (FSO) was then utilized to select the optimal key. Both private and public keys are selected by this optimization approach. Next, the hybrid Elgamal lightweight method was used to encrypt data. The encryption key and data encryption were provided by HLEEE on the owner's side. The hash value was generated using the blockchain and the SHA-256 technique. To enhance security, every encrypted piece of data and timestamp was stored in a distinct block, and the blockchain was ultimately implemented utilizing the PoA approach.

Chaotic System: In [14], a lightweight technique for data encryption is used by adopting diffusion structure and permutation. Pseudorandom sequences (PRNS) were generated by permutation utilizing a 3D Lorenz chaotic map and diffusion was obtained employing a newly designed keystream generation (KSG). This KSG would combine XOR operations with only bit-shift. Despite being straightforward, the entire method is characterized as secure due to its sufficient level of protection and ability to withstand numerous known security threats, it is thus more appropriate for CPS devices.

Parallel mode: Authors in [7] adapted parallelization in order to implement ERC5-ERSA in parallel mode. The modification was the adaptation of four separate keys and four cores to employ the work. This speeds up the algorithm by 105.16% compared to the sequential one. Authors in [13], proposed a new message authentication algorithm in parallel mode. Two PNGRs and substitution boxes were employed for encrypting messages and authentication. Work average speed was enhanced by 2.99%.

III. THE PROPOSED ALGORITHM

This paper proposes a novel hybrid lightweight cipher algorithm designed to enhance cloud computing security while ensuring low processing overhead and high performance. PILEA integrates the effective confusion and diffusion properties of AES with the simple structure and robust performance of LEA. This leads to the creation of a secure and an efficient system ideally suited for cloud environments. At the core of this system is the fundamental ARX structure of LEA, which is employed across multiple rounds. This structure is interleaved with the Substitution-Permutation (SP) network borrowed from the AES algorithm, providing the reinforced security necessary for protecting data over untrusted channels. Figure 1 illustrates the PILEA structure.

A. Key Generation Phase

The key is the cryptography system's power, so choosing the generation key function is a crucial step in the encryption process. The proposed system discovers a dynamic, nonlinear method for producing the key, which is used in both the cipher and decipher sides. Differential equations offer a mathematical approach to the initial conditions by producing increasingly variable outcomes with little initial modifications.

B. Mathematical Model of the Proposed System

The main goal is to develop a mathematical model that designates a new five-dimensional chaotic system. The chaos system can be described by the following equations:

$$\begin{aligned}
\frac{dx}{dt} &= -\mathrm{a}x + \mathrm{b}\, z^2 - \mathrm{y} \\
\frac{dy}{dt} &= \mathrm{d}\, \sin z - y - xz + v \\
\frac{\mathrm{dz}}{\mathrm{dt}} &= \mathrm{e\, y - f\, z + g\, x\, y} \qquad (1) \\
\frac{\mathrm{du}}{\mathrm{dt}} &= \mathrm{h\, u + i\, \sin z}
\end{aligned}$$

$$\frac{dv}{dt} = -j\, z$$

where x, y, z, u, and w ∈ℝ+ are the states of the system and a, b, c, d, e, f, g, h, i, and j are positive parameters of the total system. A chaotic five-dimensional system can be styled by the mathematical model (1) as hyperchaotic with three positive Lyapunov exponents where the positive parameters are: a = 11, b = 1.27, c = 15, d = 13, e = 2.5, f = 5, g= 5, h = 12.3, i = 2 and j=8, while the initial conditions are: x (0) = 10, y(0) = 2, z(0) = 0.5, u(0), = 8 and v(0)=3.

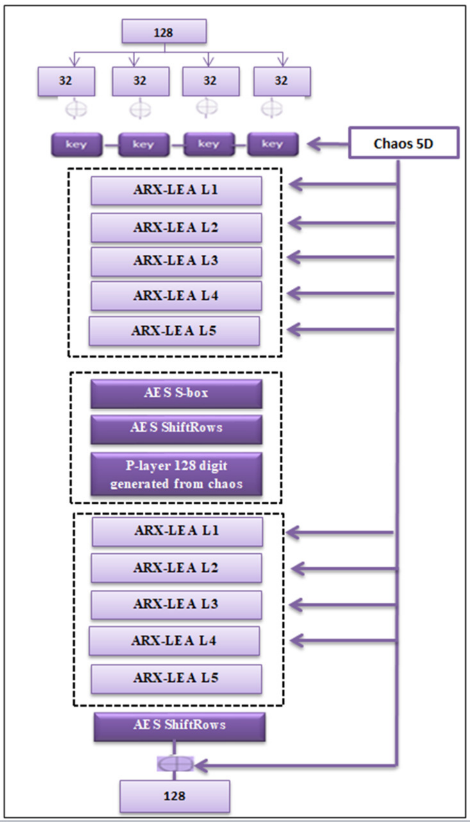

Fig. 1. Structure of PILEA.

C. Dynamic Properties of the Proposed System

Using the Mathematica software, the result of the Lyapunov exponent of the 5-D chaotic system (1) with (x(0),y(0),z(0),u(0),v(0))= (3, 6, 1, 2.5, 5, 8), (a, b, c, d, e, f, g, h, I, j) = (11, 1.5, 1.38, 15, 10, 2.5, 5, 14.3, 4, 3) is obtained by:

$$\begin{cases} L1 = 12.2985 \\ L2 = 0.2558 \\ L3 = 0.2542 \\ L4 = -7.1034 \\ L5 = -7.9055 \end{cases} \quad \dots. \qquad (2)$$

The Kaplan-Yorke dimension of the 5-D system (1) is calculated by arranging the Lyapunov exponent in descending order as $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ [7, 26]. Let j be the largest index for which [37]:

$$\sum_{i=1}^{j} \lambda_i \geq 0 \qquad \dots \qquad (3)$$

Then the conjecture is that the dimension of the attractor is designed as follows:

$$D_{KY} = 4 + \frac{LE1+LE2+LE3+LE4}{LE5} = 4.7216 \quad \dots \qquad (4)$$

From (4), it is deduced that the 5-D system (1) is a dissipative hyperchaotic system with three positive Lyapunov exponents. Since the value of the Maximum Lyapunov Exponent (MLE) in (4) is large, it is concluded that the 5-D system is highly hyperchaotic and this property is very useful for applications in cryptosystems and secure communications [15, 16]. The presence of a large positive Lyapunov exponent indicates rapid exponential expansion in the phase space, contributing to stronger hyperchaotic behavior [6, 17, 18]. Based on these criteria, a robust 5-D hyperchaotic system exhibits the following characteristics:

- Three positive Lyapunov exponents: Ensuring that the system's dynamics expand in three distinct directions within the phase space.
- A high positive Lyapunov exponent: To facilitate a swift exponential expansion in the phase space.
- A high Kaplan-Yorke dimension: Reflecting significant complexity in the attractor.

This study's analysis, conducted using the Mathematica software, confirms these characteristics for the system (1). Its nonlinear dynamics are sensitive to initial conditions, as demonstrated in Figure 2, where slight variations in the parameter u result in markedly different outcomes.

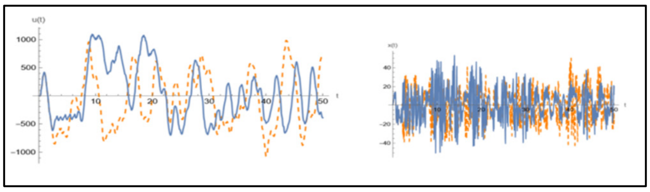

Fig. 2. The proposed 5D-chaotic system sensitivity to small value example: u[0] = 5.00000000000001 and u[0] = 5.

D. Encryption Phase

This section addresses the proposed method for enhancing the security of data outsourcing in a cloud environment. The required protection is achieved by combining the advantages of two LWC algorithms, LEA and AES and particularly by taking advantage of each algorithm's strengths. Specifically, LEA's simplicity and excellent security are leveraged, while AES's four s-boxes and permutation row are entered as the next stages:

1) First Stage: XOR

The XOR function has a fundamental impact on the encryption algorithm. Its assistance lies in adding randomness and strengthening the encryption procedure's defenses against diverse cryptographic attacks, such as differential and linear cryptanalysis [9]. This phase is robust since it is applied twice, once at the start and once at the end of the proposed PILEA. The XOR function is applied between plain text and the chaos key, at the beginning of the work, while the intermediate encrypted data and the chaos key are XORed at the end of the work. The PILEA has 128-bit block size.

2) *Second Stage: LEA Algorithm*

The enhanced LEA, in each round function, works with 128-bit size. It uses the ARX (modular Addition, bitwise Rotation, and bitwise XOR) operation. The proposed work starts by dividing the data stream into four 32-bit blocks, and then applies the core function of LEA:

- Bitwise XOR: each block of plain text is XORed with a corresponding key bit (chaotic key).
- Modular Addition is applied between every two adjacent blocks.
- Bitwise Rotation is conducted to the addition result.

These three operations are applied many times according to the proposed round chosen.

3) *Third Stage: AES's Dunctions*

After combining the second stage's data blocks and forming an array with 16 elements, the next phase involves entering the AES sub-steps [20]:

a) *SubBytes*

At this step, substitution is implemented. Each byte is replaced with a new one by using a 16 pre-build (S-box) lookup table to swap out a byte from the stage 1 result for another byte based on the chosen row/column values. A fixed 8-bit lookup table, S, is utilized to replace each byte in the state with its corresponding entry:

$$b_{ij} = S(a_{ij}) \qquad (5)$$

The way the entire procedure is built ensures that a byte is never substituted with itself [20].

b) *ShiftRows*

This step moves each row of the matrix a specific number of times.

c) *MixColumns*

In essence, this step is a matrix multiplication. Every column is multiplied by a particular matrix, which modifies each byte's location within the column [20, 21].

4) *Fourth Stage: LEA Algorithm*

Repetition of all the procedure of the first stage is done while lowering the round number.

E. *Decryption*

Every procedure that was previously outlined to encrypt data was completed. To recover the plain data under consideration, these steps are repeated in reverse order using the same round number and encryption key produced by the 5D chaotic system (1).

F. *Parallelism*

Parallelization can be deployed to the advantage of encryption and decryption operations carried out simultaneously. This suggests that portions of the encryption procedure can operate simultaneously on two cores or processors, potentially speeding up both encryption and decryption operations. PILEA is executed twice in a single pass, handling a portion of the necessary data on a single core each time. A single core can carry out the intended encryption method using 128 bits of data, 128 key bits, 10 round numbers, and the previously stated total encryption stages. Decryption can also be carried out in the same scenario.

IV. RESULTS AND DISCUSSION

A. *Comparative Analysis of Parameters*

In this section, an analysis of various lightweight symmetric cryptographic algorithms is made by executing them in a steady parallel environment. Table I presents a comparative analysis that explains key features of popular LWC cryptographic techniques, in addition to the proposed PILEA. The comparison result emphasizes PILEA's advanced features, particularly those that provide strong security with a comparatively minimal computing burden, which makes it highly suitable for a wide range of cryptography applications. The comparative analysis demonstrates how the PILEA stands out in terms of security. Significantly, PILEA's architecture is meant to be as minimal as possible in terms of computational complexity and processing resource requirements. It consists of only 10 rounds. Simple mathematical operations that are completed in each round are a reliable indicator of how well the algorithm under study is working. This is an essential component for lessening the encryption's workload, which is further reinforced by the chaotic system's dynamic key generation. The current work in the area of lightweight algorithms stands out because it carefully avoids mathematically difficult procedures and instead uses fundamental arithmetic operations with no extra overhead. PILEA algorithm structure has employed the ARX process, which is characterized by simple mathematics, instead of complex multiplications like RC6. In addition, in contrast to Simon, RC5, and RC6, it adopts S-box to spread diffusion inside the work. The security of S-box-based symmetric-key ciphers against differential cryptanalysis depends on how many S-boxes are in use at any given time. On the other hand, it avoids the usage of large-scale S-boxes [12].

It just deploys a 4×4 S-box while Present uses 8×8 and AES utilizes 16×16. The small S-box size saves both time and memory. The round number significantly impacts the cipher system's process, The suggested method avoids using as many rounds as Present does, requiring only five rounds to complete the encryption process and the same number of rounds to decrypt data. The proposed algorithm has a specific feature that it exceeds the limitation of the fixed block size of data dealt in [2]. Plus, the key creating function stands against brute force attacks. It has the option to deal with two parts simultaneously, 128-bit each, and then in total it encrypts a large amount of data at once since it does that consequently. This attractive point of PILEA makes it more efficient with a large amount of data in just a few seconds. Parallel processing along with the round number reduction make PILEA suitable for a wide range of applications.

TABLE I. A COMPARISON AMONG SOME SYMMETRIC ALGORITHMS.

Algorithm	Structure	Block size	Key size	Round No.	Performance	Math functions	S-box No	Attack patterns	Security Rate
Present [24]	SPN	128 bits	64, 128	24	Offers a good balance between security and efficiency.	Feistel	8	Algebraic attacks aiming to solve cipher operations.	Secure
AES [12]	SPN	128 bits	128, 192, 256 bits	10, 12, 14	Allows different levels of security based on performance needs.	XOR, mixing, substitution, shifting, multiplication, addition (16 bits)	1	Weak key schedules can expose vulnerabilities.	Secure
Simon SIMECK [21]	FN	128 bits	128 bits	20,27, 35	Efficient in hardware & software.	ARX function, rotational-XOR	N/A	Differential attacks.	Secure
RC5 [22]	FN	32 bits	128 bits	12	Fast, simplicity of operations.	XOR, subtraction, multiplication, shift	N/A	Cryptanalysis attacks.	Secure
RC6 [23]	FN	32 bits	64 bits	n	Efficient in time and space, suitable for environments with limited resources.	Addition, subtraction, XOR, left and right rotation	4	Attacks that analyze the differences in input pairs and how they affect the resultant of output	Secure
SEA [25]	SPN	16 bit	256 bits	4	Requires minimal computational resources.	OR, rotations, 2n mod addition, substitution	N/A	Brute force attacks.	Secure
Proposed (PILEA)	SPN	256 bit	128, 192, 256 bits	10	Exploits parallelism and functions that enhance confidentiality and generate keys in a robust manner	XOR, ARX function, substitution (16 bits)	4	A non-periodic key, when used, is vulnerable to key-related attacks and security hardening functions utilize it to combat text-based attacks.	Highly Secure

B. Experimental Evaluation

The PILEA uses a 5-D chaotic system as a dynamic system to generate random keys, wherein dimension X is chosen to produce a key value for the randomness of the key stream. NIST tests the randomness of the binary key stream produced by the 5D chaotic system. NIST is a statistical test to determine whether the key is random or not, based on the p-value (0.01). It can be therefore declared that the key stream is random if the p-value is large and vice versa. Table II explains the concept.

TABLE II. NIST EXPERIMENTS RESULTS OF THE PILEA

Chaotic key name	p-value	Result
Frequency Test (Monobit)	0.9619	Random
Frequency	0.49817	Random
Runs	0.5878	Random
Longest Run	0.61479	Random
Binary Matrix Rank Test	0.0391	Random
Discrete Fourier Transform (Spectral) Test	0.6617	Random
Non-Overlapping Template Matching Test	0.2255	Random
Overlapping Template Matching Test	0.02073	Random

1) Image Entropy

Table III displays the entropy change for some images. It is a good point to utilize the average Entropy change of 9.92% by PILEA.

2) Correlation Analysis

Table IV shows the correlation between the Lena plain image and the Lena cipher image. The similarities and their effects on two adjacent pixels are displayed. The correlation between the two neighboring pixels in the Lena cipher image has significantly decreased.

3) Execution Time

It is one of the most vital assessing parameters of encryption algorithms besides security. It is defined as the entire amount of time the algorithm takes to encrypt and decrypt specific data. Table V mentions the total execution time with PILEA of the four considered images.

TABLE III. IMAGE ENTROPY TEST FOR PILEA

Image	Dimension	Entropy (ENC)	Entropy (ORG)
BABOON	128×128	7.9891	2608
	220×220	7.9958	7.1662
	256×256	7.9973	7.2091
LENA	128×128	7.9885	7.4810
	220×220	7.9962	7.4618
	256×256	7.9970	7.4436
BANDA	256×256	7.9969	7.5966
	512×512	7.9982	7.5217
PEPPERS	256×256	7.9969	7.5966
	512×512	7.9982	7.5217

TABLE IV. CORRELATION RESULTS

Image	Size	Correlation	
		Original	Encrypted
BABON	256×256	0.9000	0.0026
BANDA	256×256	0.9764	0.0012
LENA	256×256	0.9576	0.0055
PEPPER	256×256	0.9309	-0.0031

TABLE V. EXECUTION TIME RESULTS

Image	Size	Total enc./dec. time (ms)
BABOON	128	1.1810
	220	3.7104
	256	4.6078
LENA	128	1.2910
	220	3.4531
	256	5.0388
PEPPER	256	6.0214
	512	25.220
BANDA	256	4.7363
	512	19.880

V. CONCLUSION

This study presents a new version of an LWC algorithm for cloud data security. Many improvements are made to the proposed algorithm, making it able to protect outsourcing data in semi-trust channels. PILEA applies LEA with five rounds at first, then utilizes AES sub-step (subBytes, shiftRows, MixColumn), and then applies five rounds of LEA again. PILEA is compared to alternative encrypting methods and exhibits better qualities of confusion and diffusion. Notably, PILEA's architecture, which consists of just 10 rounds, is intended to be as simple as possible in terms of processing resource requirements and computational complexity. This is a crucial part of reducing the workload associated with encryption, which is further supported by the dynamic key generation of the chaotic system. A 5D chaotic system is used as a key stream to enhance key detection and avoid key attacks. PILEA utilizes 4×4 instead of big-scale S-boxes saving memory and time. PILEA also utilizes parallelism. It can handle two separate files of data at once, each containing 128 bits, and as a result, it can encrypt a sizable quantity of data faster. PILEA is more effective with big amounts of data in a short length of time, with increased ability to withstand differential and brute force attacks and low memory as well as computation time requirements.

REFERENCES

[1] Z. A.Mohammed and K. A. Hussein, "Lightweight Cryptography Concepts and Algorithms: A Survey," in *Second International Conference on Advanced Computer Applications*, Misan, Iraq, Feb. 2023, pp. 1–7, https://doi.org/10.1109/ACA57612.2023.10346914.

[2] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *Journal of Cyber Security Technology*, vol. 1, no. 3–4, pp. 187–201, Oct. 2017, https://doi.org/10.1080/23742917.2017.1384917.

[3] Z. A. Mohammed, H. Q. Gheni, Z. J. Hussein, and A. K. M. Al-Qurabat, "Advancing Cloud Image Security via AES Algorithm Enhancement Techniques," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12694–12701, Feb. 2024, https://doi.org/10.48084/etasr.6601.

[4] A. Berisha and H. Kastrati, "Parallel Implementation of RC6 Algorithm," *Journal of Computer Science and Technology Studies*, vol. 3, no. 2, pp. 1–9, Jun. 2021, https://doi.org/10.32996/jcsts.2021.3.2.1.

[5] Z. A. Mohammed and K. A. Hussein, "PRC6: Hybrid lightweight cipher for enhanced cloud data security in parallel environment," *Security and Privacy*, 2024, Art. no. e413, https://doi.org/10.1002/spy2.413.

[6] H. K. Zghair, S. A. Mehdi, and S. B. Sadkhan, "Bifurcation of Novel Seven-Dimension Hyper Chaotic System," *Journal of Physics: Conference Series*, vol. 1804, no. 1, Oct. 2021, Art. no. 012051, https://doi.org/10.1088/1742-6596/1804/1/012051.

[7] K. A. Hussein and T. B. Kareem, "Proposed Parallel Algorithms to Encryption Image Based on Hybrid Enhancement RC5 and RSA," in *International Engineering Conference*, Erbil, Iraq, Jun. 2019, pp. 101–106, https://doi.org/10.1109/IEC47844.2019.8950593.

[8] L. M. Al-Ramini, "Implementation of proposed lightweight cryptosystem for use in Cloud Computing Security," M.S. thesis, Middle East University, Beirut, Lebanon, 2018.

[9] S.-D. Bao, Y. Lu, Y.-K. Yang, C.-Y. Wang, M. Chen, and G.-Z. Yang, "A data partitioning and scrambling method to secure cloud storage with healthcare applications," in *International Conference on Communications*, London, UK, Jun. 2015, pp. 478–482, https://doi.org/10.1109/ICC.2015.7248367.

[10] Z. Mishra, P. K. Nath, and B. Acharya, "High throughput unified architecture of LEA algorithm for image encryption," *Microprocessors and Microsystems*, vol. 78, Oct. 2020, Art. no. 103214, https://doi.org/10.1016/j.micpro.2020.103214.

[11] D. Lee, D.-C. Kim, D. Kwon, and H. Kim, "Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA," *Sensors*, vol. 14, no. 1, pp. 975–994, Jan. 2014, https://doi.org/10.3390/s140100975.

[12] A. Soltani and S. Sharifian, "An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA," *Microprocessors and Microsystems*, vol. 39, no. 7, pp. 480–493, Oct. 2015, https://doi.org/10.1016/j.micpro.2015.07.005.

[13] D. Tiwari, B. Mondal, S. K. Singh, and D. Koundal, "Lightweight encryption for privacy protection of data transmission in cyber physical systems," *Cluster Computing*, vol. 26, no. 4, pp. 2351–2365, Aug. 2023, https://doi.org/10.1007/s10586-022-03790-1.

[14] R. Hedayati and S. Mostafavi, "A Lightweight Image Encryption Algorithm for Secure Communications in Multimedia Internet of Things," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1121–1143, Mar. 2022, https://doi.org/10.1007/s11277-021-09173-w.

[15] K. Benkouider *et al.*, "A New 5-D Multistable Hyperchaotic System With Three Positive Lyapunov Exponents: Bifurcation Analysis, Circuit Design, FPGA Realization and Image Encryption," *IEEE Access*, vol. 10, pp. 90111–90132, Jan. 2022, https://doi.org/10.1109/ACCESS.2022.3197790.

[16] M. Hussam, G. Majeed, and H. Hoomod, "New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 2531–2540, Jan. 2021.

[17] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple Chaotic Maps," in *Annual Conference on New Trends in Information & Communications Technology Applications*, Baghdad, Iraq, Mar. 2017, pp. 132–137, https://doi.org/10.1109/NTICT.2017.7976141.

[18] S. B. Sadkhan and H. Ali, "A proposed speech scrambling based on hybrid chaotic key generators," in *Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications*, Baghdad, Iraq, Dec. 2016, pp. 1–6, https://doi.org/10.1109/AIC-MITCSA.2016.7759941.

[19] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing," *International Journal of Intelligent Networks*, vol. 3, pp. 16–30, Jan. 2022, https://doi.org/10.1016/j.ijin.2022.04.001.

[20] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," *International Journal of Artificial Intelligence Research*, vol. 4, no. 1, pp. 49–57, Apr. 2020, https://doi.org/10.29099/ijair.v4i1.154.

[21] J. Lu, Y. Liu, T. Ashur, B. Sun, and C. Li, "Rotational-XOR Cryptanalysis of Simon-Like Block Ciphers," in *Australasian Conference on Information Security and Privacy*, Wollongong, NSW, Australia, Nov. 2022, pp. 105–124, https://doi.org/10.1007/978-3-030-55304-3_6.

[22] R. Shahzadi, S. Anwar, F. Qamar, M. Ali, and J. Rodrigues, "Chaos Based Enhanced RC5 Algorithm for Security and Integrity of Clinical Images in Remote Health Monitoring," *IEEE Access*, vol. 7, pp. 52858–52870, Jan. 2019, https://doi.org/10.1109/ACCESS.2019.2909554.

[23] O. S. Faragallah *et al.*, "Improved RC6 Block Cipher Based on Data Dependent Rotations," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1921–1934, 2022, https://doi.org/10.32604/cmc.2022.019798.

[24] A. Zakaria, A. Halim, F. Ridzuan, N. Zakaria, and M. Daud, "Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT," *IEEE Access*, vol. 8, pp. 198646–198658, Jan. 2020, https://doi.org/10.1109/ACCESS.2020.3035375.

[25] Z. Yang, Y. Li, B. Wang, S. Ding, and P. Jiang, "A Lightweight Sea Surface Object Detection Network for Unmanned Surface Vehicles," *Journal of Marine Science and Engineering*, vol. 10, no. 7, Jul. 2022, Art. no. 965, https://doi.org/10.3390/jmse10070965.