International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2022 | Issue 53 | Volume 14 | Number 4 | Pages 253-259

NEW ULTRA-LIGHTWEIGHT IoT ENCRYPTION ALGORITHM USING NOVEL CHAOTIC SYSTEM

N.M. Naser [1, 2] J.R. Naif [1]

1. Informatic Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq
ms202020624@iips.icci.edu.iq, newjolan@gmail.com
2. University of Information Technology and Communications, Baghdad, Iraq, noor.sarsam@uoitc.edu.iq

Abstract- Over the last several years, the applications and services of IoT have extended in almost all life arias and this led to the growth happening in protecting the data transferring between IoT applications due to the IoT well known limitations, new lightweight algorithms are always considered a good choice because of the many good characteristics these lightweight algorithms have, but nowadays it is much of a trend to merge these lightweight algorithms to reach the best protection level not to mention enhancing the speed of encryption/decryption and securing it from known cryptanalysis attacks, all this will lead the users to be more confident of the system. The proposed encryption algorithm is a new hybrid algorithm based on a novel 4-D NSJR chaotic system key generation while embedding the P-Layer from the PRESENT Block cipher with an old but strong block cipher Diamond2, the PRESENT block cipher is considered very efficient and used in many IoT applications since it uses three layers without the use of any algebraic computations with almost 1000 GE, this process will give the Diamond2 more security and speed up the encryption time.

Keywords: IoT Security, Hybrid Cryptography, PRESENT Block Cipher, Diamond2 Block Cipher, Chaotic System, Lorenz System

1. INTRODUCTION

Security is very important while storing information and transmitting them across the network or even across the internet, as a result, secure communication is a prerequisite for any network transaction [1]. Cryptographic primitives provide the achievement of all the necessary domains in security, including availability, access control, integrity, secrecy, authentication, and non-repudiation [2], [3]. Cryptography protects delicate information by converting it to incomprehensible data, the certified recipient will be the only one capable to access this information by switching into the original text, This procedure is known as encryption, while the opposite is known as decryption [4].

During technology revolution in the last decade, the need of developing cryptography has increased since the world entered the IoT era, this is why the development from conventional cryptography to lightweight cryptography is considered a big achievement to cover the needs and achieve all security areas in spite of the limitations of the IoT [5]. The designer of any encryption algorithm must take into consideration these characteristics: secure, effective, low-priced, need a small amount of memory, simple to develop and use across numerous systems [6], to be able to do that with the limitations of IoT and with cryptanalysts' persistent attempts to get into every accessible cryptographic system. Many designers are trying now a days chaotic cryptography (the concept of chaotic cryptography has risen in the prospect of cryptography) [7], which is the combination of mathematical chaos theory and cryptography with the help of chaos theory, the security will increase and the system will be random which will lead to a more secure encryption algorithms which protect the cryptographic components from cryptanalysis [8]. The Primary target of this article is to give a proposed encryption based on the Hybrid lightweight Diamond2-PRESENT security mechanism with Novel 4D-NSJR chaotic key generation (HLD2P-4DNSJR): for generating key stream used to encrypt text data. The proposed block cipher is implemented and tested on the NIST Tests. In lightweight cryptography, researchers adopt different methodologies in either developing or modifying an existing cipher to optimizing its performance or developing a new hybrid cipher from combining 2 ciphers with the help of chaotic systems which is considered a trend now adays, presenting some of the literature reviews: Abdulraheem, A.N. and Nema, B.M. presented a new method based on 2D-chaos system in the keys generation process combined with the block cipher PRESENT, to increase its security and offer a sharp encryption level transmitting data IoT systems and compared between them regarding the measurements of performance [9].

Hoomod, H.K. and Naif, J.R. proposed a security mechanism that was designed by using the Hummingbird encryption algorithm and 8-D chaos keys, this mechanism was designed to increase the speed and the security strength, the proposed novel Chaotic system was utilized because of its sensitivity for the initial conditions simple change in input that makes a big change in the output [10].

Albhrany, E.A. et al., introduced a new text encryption method in light of combination of a chaotic map and a block cipher, intended to encrypt and decode blocks of 8X8 bytes utilizing a random-key-generator depending on the Tent-map to produce the sequences of the key; all testing findings confirmed the scheme's security [11].

Hoomod, H.K., et al., presented a lightweight intelligent IoT data sensor - based cipher system that uses a new strong chaotic system and a combination of two encryption algorithms (PRESENT-SPECK) with several changes, the features of this system make the users more confident with each other [12].

Kubba, Z.M. and Hoomod, H.K. presents novel 5-D chaotic system for the lightweight modified-PRESENT. Comparatively speaking, the presented chaotic system is superior to the vast majority of existing systems with positive Lyapunov values this will make the system behavior unpredictable while presenting randomness and more complexity [13].

This paper's parts are organized as follows: section 2 contains general definitions for IoT, IoT security, chaos theory and chaos-base cryptography, Section 3 describes the block ciphers that were utilized Diamond2 and PRESENT, Section 4 introduces the methodology of the presented algorithm, section 5 produces the results and last but not least section 6 is the conclusion.

2. PRELIMINARIES

2.1. Internet of Things

IoT can be thought of as a network of physical things, by objects one can include devices, vehicles, buildings or any other items which has built-in electrical, sensor, and communication systems, the built-in items assist the objects to collect and share data. It allows for the sensing and controlling of items through preexisting network infrastructure. As a result, the physical world will be more directly integrated with computer-based systems, resulting in enhanced efficiency and accuracy [14].

Through different technologies and applications, IoT proves to be the trend of the next Internet generation, it has been progressively introducing huge development in technology that affects positively in our daily life's routine, hence serves to make our lives simpler, developed and more pleasant [15]. In other words, every available object (thing) is getting smart, IoT will help various technologies to emerge in the future taking us to a whole new level of a smart world. The Internet of Things has a bright future with countless interests in its applications in all domains including governance, medical, education, manufacturing, industrial, transportation, mining, habitation and so on, everything will be connected this will provide a better life style to humans [16].

2.2. IoT Security

It is important to realize that the physical objects connected through IoT communicate simultaneously without any assist of human interactions, and the IoT's architecture is considered a network [17], since security is essential in any network to inhibit the illegal data access, data manipulation, data monitoring, and data modification, therefore it is extremely important to preserve the security of an IoT system, as an illustration, the data shared between IoT applications must be protected due to the IoT applications limited resources as mentioned previously, These appliances are susceptible to malware and other threats [2], the rapid development in this field led to the transform from conventional cryptography to lightweight cryptography [12].

Lightweight encryption is considered an important part of classical cryptographic algorithms that is related to limited resource devices in IoT [18], lightweight encryption objective is providing the necessary protection for IoT objects, how could that be done? It's all about using the minimal memory, using less computing resources, and using minimal energy or power, as a matter of fact lightweight cryptographic algorithms (block ciphers, stream ciphers) are the most powerful solution or one can say ideal approaches for safeguarding these IoT applications, as cryptography conceals information by removing the risk of gathering any important information patterns. This guaranties that all data transmissions are safe, correct, verified, allowed, and can't be changed [2], [19].

2.3. Chaos-Baes Cryptography

Chaotic-Cryptography is a combination of the chaos theory and cryptography, the chaotic system is based on non-linear behavior this particular property makes it a powerful candidate for many encryption systems [20].

Chaos theory plays a dynamic role in improving cryptosystems security, both chaos theory and cryptographic methods have similar attributes such as sensitivity to changes in the parameters, unpredictability over long periods, and random behavior [21]. Table 1 shows similarities and the differences between them [22].

Table 1. Comparison of chaotic systems and cryptographic algorithms [22]

Properties of Chaotic System	Properties of Cryptographic Scheme
Parameters (Real)	Key (Boolean)
Sensitive to change initial parameters	Diffusion
Ergodicity	Confusion
Iteration	Rounds
Deterministic dynamical	Deterministic Pseudorandom
Using set of real numbers	Finite set of integers
Structure complexity	Algorithm complexity

2.4. Chaotic Maps

Chaotic maps are mainly continuous, although they may be discretized as needed for use in encryption methods. There are a number of well-known chaotic maps some of them are 1-D like Tent map and Logistic map while others are multi-dimensional for example: Henon map and Arnold's cat map both are 2-D while the Lorenz System are 3-D, etc. [23].

3. THE BLOCK CIPHERS

3.1. Diamond2

A block cipher presented by M.P. Johnson in 1995 it is a strong, royalty-free block cipher, its technique is based on a collection of nonlinear functions and is a symmetric-key encryption algorithm. It uses 128-bit of block size with a varying length of the key with 10 rounds. The design of the cipher provide security for the next generation. It consists of three main parts as shown in Figure 1 [24]:

• Key scheduling: this operation fills up the internal substitution arrays with respect to the key, for each encryption block there is one substitution array for each round, for 10 rounds it will be 160 substitution arrays, for Decryption it uses the inverse substitution array for the same number of rounds BUT it works in reverse order [24].
• Substitution steps: In every substitution round, every bite of the input block is substituted with the contents of the substitution array for the same round, byte location, and byte value. The identical technique is applied for decryption using the inverted substitution array [24].
• Permutation steps: fixed permutation performed between each substitution round; This step is important to rise the actual block size simply by making-up each output byte a function of eight input bytes and that is done by selecting only one bit from each one of the eight input bytes. As one may notice that each input block bit is used just once in the output block [24].

Algorithm 1. Diamond2 encryption algorithm

```
Input: plaintext (initial (16byte), (feedback    16byte)
Output: Encryption Data
Begin
Step 1: Initialize makesbox
          makesbox(feedback) and return Sbox, Feedback
step 2: update Feedback
         feedback = feedback ⊕ initial
Step 3: for each block in plaintext do size block 16byte
Step 3-1:  encrypt (feedback, outbuffer)
Step 3-2:  for each byte in block do
             Enc_Data[i]= Enc_Data [i] ⊕ block[i]
             Feedback[i] = Enc_Data [i]
Step 3-3:  endfor
Step 3-4:  endfor
Step 4: return Enc_Data
End
```

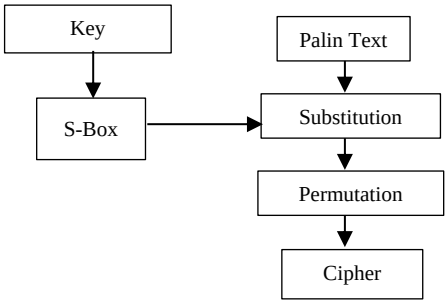

Figure 1. Block diagram of the Original Diamond2 [24]

3.2. Present

Introduced in 2007 by A. Bogdanov et al, to be amongst the first ciphers created for use on devices with tiny resource requirements [2], has an SPN structure. In 2017 PRESENT Cipher was counted a standard in the ISO/IEC 29192 [25]. It uses a 31-round process with a 64-bit block size and either an 80-bit or 128-bit key, the routing is simple and uncomplicated, with each round passing via a single S-box and a single P-Layer. It is one of the smallest and least resource-intensive algorithms, since it uses nearly 1000 GE [2].

Each of the 31 rounds entails a number of significant basic operation that are performed to ensure that data is encrypted at high level, these operations include [9]: Key Registration, Add-Round-key, S-Box Layer and the P-Layer: this level is utilized to permute the data, what come out of this process is the input to the next round while the final permuted output data go along an additional encryption process [26]. Table 2 clarifies the bit-position replacement process [26].

Table 2. P-layer of PRESENT Block Cipher [26]

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

4. PROPOSED ALGORITHM

4.1. Key Generation

The "key" is a crucial component of the process of cryptography, as it deals with encryption for data encoding or decoding, also it indicates sharing the sender and the recipient a confidential section to convey secretive information that is not accessible to anybody who does not have the key for reading and accessing the content [27]. As a matter of fact the key generation process is nothing but keys creation process, where the keys are integers that are used by the cryptographic algorithm, one can generate the keys either by (TRNG) or by (PRNG) [9] it's essential to use an appropriately extended key length; Longer keys are much more difficult to crack, it takes more time and this will make a brute force attack obscure and useless [20], all this could be easily guaranteed when randomness is around, with randomness there won't be prior knowledge about the key since it is randomly generated [28].

4.2. Proposed Novel Chaotic System (4-D NSJR)

Due to the plenty good characteristics of the output numbers of any chaotic system (specially randomness), it is a trend now a days that researchers propose embedding the chaotic system into the encryption operations through key generation. This section presents a novel 4-D chaotic system which was designed based on mathematical analysis. It contains four-dimensional chaos equations. The following is the four chaotic maps that represent the new chaotic system of this work. The proposed 4-D chaotic system used the Equation (1).

$$
\begin{aligned}
xt[i+1] &= xt[i] + yt[i] - b \times (s \times xt[i] \times (1 - s \times yt[i] \times (1 - r \times zt[i] \times (xt[i] - u \times kt[i])))) dt \\
yt[i+1] &= yt[i] - u \times xt[i] + (u \times s \times yt[i] \times (1 + u \times xt[i] \times (1 - r \times kt[i] \times (1 - s \times zt[i])))) dt \\
zt[i+1] &= zt[i] + (u \times zt[i] \times (1 - u \times kt[i] \times (1 - r \times yt[i] \times (1 + s \times xt[i])))) dt \\
kt[i+1] &= kt[i] + u \times kt[i] \times (u \times zt[i] \times (1 - u \times xt[i] \times (1 - u \times yt[i])) \times (1 + s \times xt[i])) dt
\end{aligned} \tag{1}
$$

where, the initials (where x=0.4, y=0.1, z=0.1, k=0.1 and d(t)= 0.01 in addition to values of (b, r, s, u) where b= 2.567, r= 1.80, s= 0.850 and u= 0.05125) with num steps = 1000000 as parameters of the proposed system. The Equations (1) are used in the proposed system for generating dynamic keys K_1, K_2, K_3 and K_4, to be sensitive to initial values, any slight alteration in initial values drives to a big change in output values, Figure 2 presents the block diagram of the suggested chaotic key generator (4-D NSJR).

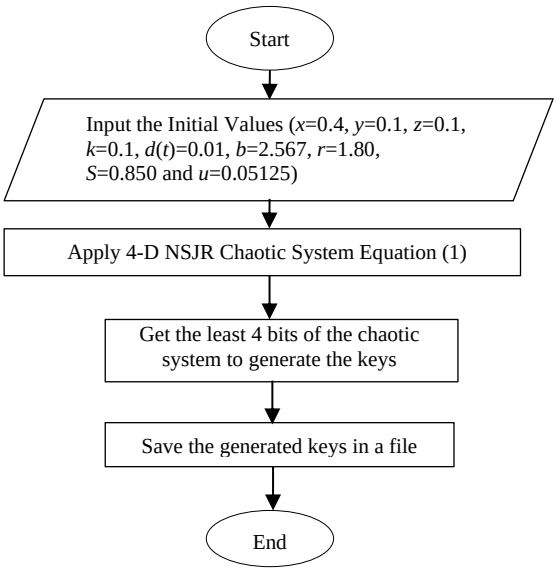

Figure 2. Block diagram of the Chaotic Key Generation Process of the Proposed System (HLD2P-4DNSJR)

Algorithm 2. Generation of the chaos keys

Input: Parameters and Initial variables.
Output: Chaotic Keys: (K_1, K_2, K_3, K_4).
Begin
Step1: Input the initial values of 4-D NSJR Lorenz system (x, y, z, k, d(t)) where x=0.4, y=0.1, z=0.1, k=0.1 and d(t)= 0.01 in addition to values of (b, r, s, u) where b= 2.567, r= 1.80, s= 0.850 and u = 0.05125
For I = 1 to 1000000.
Step 2: Apply equation (1) to Compute the values of (xt [i + 1]), yt [i + 1], zt[i + 1] and kt[i + 1] and generate the chaos keys (K_1, K_2, K_3, K_4)
Step 3: Apply V1 for output xt,
Step 4: Get the last significant digits from the chaos keys (K_1 to K_4).
Step 5: Add the split significant digits to the selected initials values of NSJR 4-D chaotic
End

4.3. The Encryption Process

The main idea here is modifying the Diamond2 Algorithm and include novel chaotic system in order to enhance the original algorithm to be appropriate for IoT environment and to avoid different types of attacks.

4.3.1. Hybrid Lightweight Diamond2 -PRESENT Algorithm with the Novel 4-D NSJR Chaotic System (HLD2P-4DNSJR)

This scenario contains three stages first to generate keys using the novel 4-D NSJR chaos system, then embed the PRESENT Algorithm with the Diamond2 Lightweight Algorithm by replacing the P-Layer from PRESENT Cipher with the permutation layer in Diamond2 after that applying the novel 4-D NJSR chaos system on the replaced P-layer to achieve the optimal level of security and make the encryption process more efficient and fast, this way will help defeat any attempt of differential cryptanalysis, and as mentioned earlier data encryption is done through algorithm inverse. Figure 3 represents the block diagram of the algorithm (HLD2P-4DNSJR).

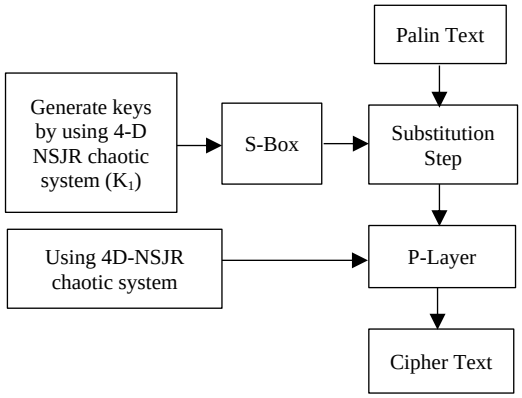

Figure 3. The Block Diagram of the Proposed System (HLD2P-4DNSJR)

Algorithm 3. shows The HLD2P-4DNSJR Algorithm

Input: Data (Plaintext 64-bits), initial vector of 4-D NSJR.
Output: Encrypted Data (Ciphertext)
Begin
Step 1: Apply equations (1) to Generate keys
Step 2: Enter the plain text
Step 3: If the plain text (message) less than (<) 64 bit then goto step 2 Else go to step 5
Step 4: Padding State
Step 5: Generate S-Box
Step 6: For i = 1 to 10 do
Step 7: Substitution Layer
Step 8: Apply equations (1) on the embedded P-Layer
Step 9: permutation step (using P-Layer from PRESENT)
Step 10: End For
Step 11: Generate the ciphertext
End

5. RESULTS

The generated chaotic keys K_1, K_2, K_3 and K_4 are employed in any encryption algorithm and will be stored in a file in the system to be easier to use in the other operations. Figures 4 and 5 show the maps of the novel proposed 4-D chaotic system.

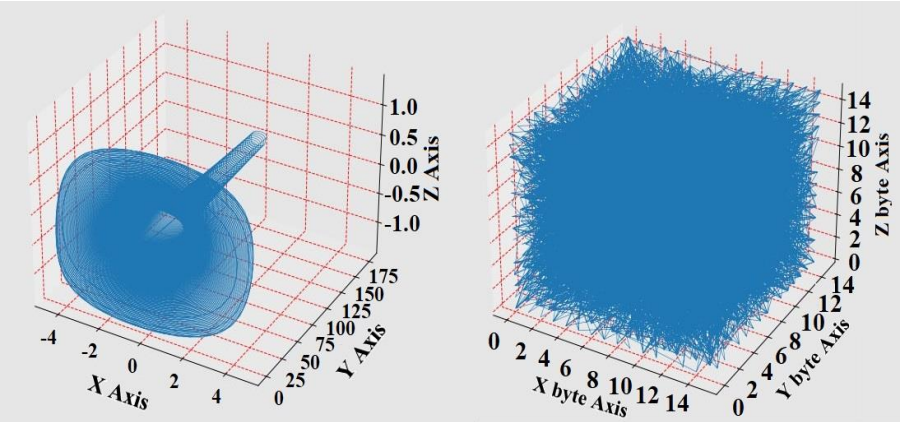

Figure 4. The novel 4-D NSJR chaotic map of the proposed system (HLD2P-4DNSJR)

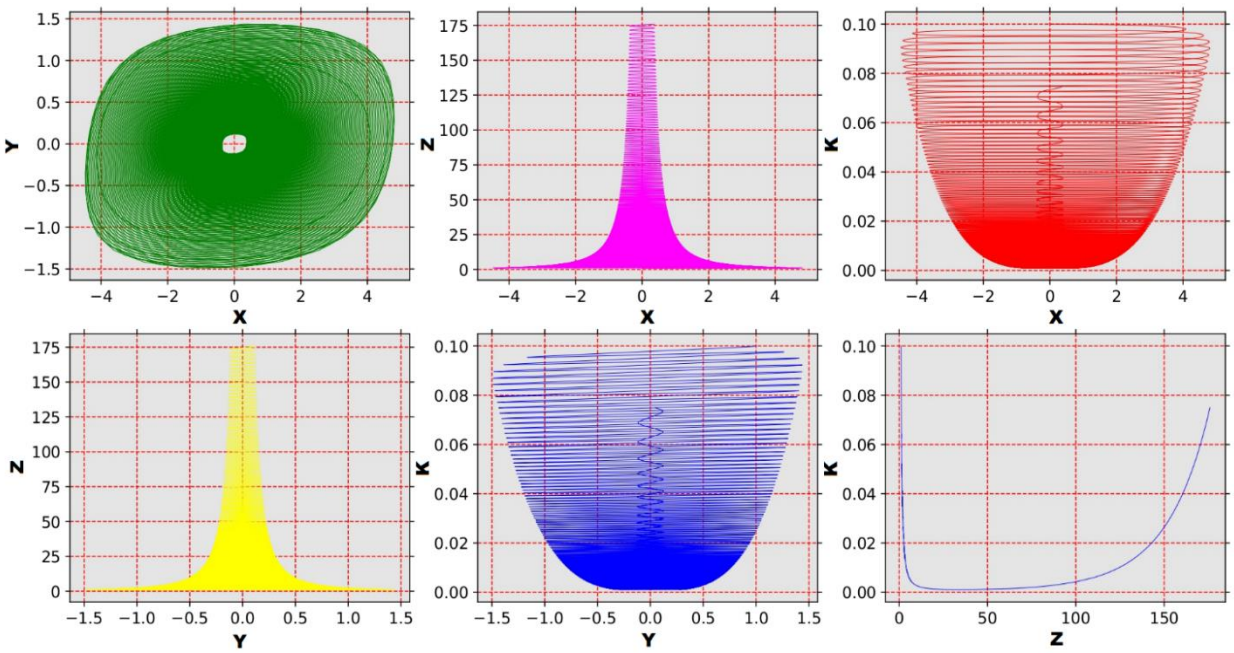

Figure 5. The novel 4-D NSJR chaotic maps of the proposed system (HLD2P-4DNSJR)

5.1. Tests and Measurements

A. Standard tests and measurements were used for testing encryption such as time tests, Entropy, throughput, Hamming distance, UACI and randomness NIST tests. Tables 3 to 7 demonstrates the proposed measurements of files of various sizes:

Table 3. Benchmarking Performance of the Proposed System (HLD2P-4DNSJR) -64 bit (5 rounds), Average Time in msec by Using Random Data Entered

File Size	Original Diamond2		HLD2P-4DNSJR	
	Encryption Time	Decryption Time	Encryption Time	Decryption Time
1 KB	2.26688	2.06350	1.475499	1.1676
5KB	1.924958	1.6765	1.586199	1.23857
10KB	2.965495	2.49834	2.275797	2.0945
25KB	3.165417	2.87652	2.956168	2.67834
75KB	4.922784	4.2098	4.259396	3.9354
100KB	5.026843	4.38734	5.980753	5.69243
1000KB	25.255623	23.6583	35.493849	34.5387

Table 4. Throughput Results of Encrypted Text of the Proposed System (HLD2P-4DNSJR)

Text Size (KB)	Original Diamond2	HLD2P-4DNSJR
1	3.429136	5.268343
5	21.023188	25.513043
10	26.940068	35.104462
25	65.209113	69.824871
75	122.11555	141.134654
100	158.590771	133.296079
1000	324.970021	231.232185

Table 5. Unified Average Changing Intensity (UACI) Results of Encrypted Text of the Proposed System (HLD2P-4DNSJR)

Text Size (KB)	Original Diamond2	HLD2P-4DNSJR
1	0.272914	0.026956
5	0.28372	0.026988
10	0.314115	0.027003
25	0.282191	0.026385
75	0.289093	0.026889
100	0.297442	0.027064
1000	0.292607	0.027157

Table 6. CCA of Encrypted Text of the Proposed System (HLD2P-4DNSJR)

Text Size (KB)	Original Diamond2	HLD2P-4DNSJR
1	-0.976499	0.90449
5	-0.963495	0.909288
10	-0.986236	0.929886
25	-0.998807	0.919616
75	-0.999065	0.907424
100	-0.999768	0.905696
1000	-0.999743	0.903806

Table 7. Entropy Results of Encrypted Text of the Proposed System (HLD2P-4DNSJR)

Text Size (KB)	Original Diamond2	HLD2P-4DNSJR
1	4.862877	5.756791
5	5.135652	6.063171
10	5.460649	6.395977
25	4.99865	5.961461
75	5.087997	6.026318
100	5.169179	6.084998
1000	5.126252	6.051786

B. Randomness Tests (The NIST Tests): NIST refer to the National Institute of Standards and Technology which is a science lab established in 1901 in United States, its major job is establishing standards and metrics that will help in the development of science and technology [29]. the NIST Test Suite is used for the purpose of estimating the randomness of the output binary sequences, which is a package of 15 statistical tests, in other words, it is considered as genuine analyses which was and still applied for the randomness measurement of any cryptosystems that are either hardware or software based [30]. Table 8 is showing the NIST Test Results for the proposed algorithm.

Table 8. Results of NIST Tests for the Proposed System (HLD2P-4DNSJR)

No.	Name of test	Original Diamond2	HLD2P-4DNSJR
1	Frequency Test	0.24826	0.51723
2	Frequency within Block Test	0.74194	0.63808
3	Run Test	0.54569	0.36058
4	Longest-Run-of-Ones in a Block Test	0.07103	0.34626
5	Binary Matrix Rank Test	0.0217149	0.41943
6	Discrete Fourier Transform Test	0.739102	0.41056
7	Non-Overlapping Template Matching	0.4918449	0.45576
8	Overlapping Template Matching Test	0.2101428	0.21014
9	Maurer's Universal Statistical	0.6272206	0.90901
10	Linear Complexity	0.883207	0.40063
11	Serial Test	0.0970409	0.29807
12	Approximate Entropy	0.343026	0.13678
13	Cumulative Sums Test	0.32758449	0.58266
14	Random Excursions Test	0.530534	0.57488
15	Random Excursions Variant	0.4948519	0.50708

6. CONCLUSION

A chaotic keys generation was suggested in this paper based on the novel 4-D NSJR chaotic systems. the proposed system is capable of generating a big number of key sequences. The system consists of four phases: input, key generation, encryption and output. In the key generation phase novel 4-D NSJR chaotic system was applied, the system also proposes embedding the P-Layer from the PRESENT Block Cipher with the Diamond2 lightweight Block Cipher to make the algorithm reaches the best protection level not to mention enhancing the speed of encryption/decryption and securing it from known cryptanalysis attacks, the system passes the NIST test suit and many measurements were done.

REFERENCES

[1] S. Sicari, A. Rizzardi, A. Coen Porisini, "5G in the Internet of Things Era: An Overview on Security and Privacy Challenges", Comput. Networks, Vol. 179, p. 107345, 2020.

[2] N.M. Naser, J.R. Naif, "A Systematic Review of Ultra-Lightweight Encryption Algorithms", Int. J. Nonlinear Anal. Appl., Vol. 13, No. 1, pp. 3825-3851, 2022.

[3] H. Damghani, H. Hosseinian, L. Damghani, "Cryptography Review in IoT", The 4th Conference on Technology in Electrical and Computer Engineering (ETECH2019), pp. 1-6, 2019.

[4] M.F. Mushtaq, S. Jamel, A.H. Disina, Z.A. Pindar, N. S.A. Shakir, M.M. Deris, "A Survey on the Cryptographic Encryption Algorithms", Int. J. Adv. Comput. Sci. Appl., Vol. 8, No. 11, pp. 333-344, 2017.

[5] M.U. Bokhari, S. Hassan, "A Comparative Study on Lightweight Cryptography", Cyber Security, Springer, pp. 69-79, 2018.

[6] S.S. Dhanda, B. Singh, P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT", Wirel. Pers. Commun., Vol. 112, No. 3, pp. 1947-1980, 2020.

[7] M.I. Mihailescu, S.L. Nita, "Software Engineering and Applied Cryptography in Cloud Computing and Big Data", International Journal on Technical and Physical Problems of Engineering, Issue 24, Vol. 7, No. 3, pp. 47-52, September 2015.

[8] A. Sharif, N. Intan Raihana, A. Samsudin, "Chaos-Based Cryptography: A Brief Look into An Alternate Approach to Data Security", Journal of Physics: Conference Series, Vol. 1566, No. 1, p. 12110, 2020.

[9] A.N. Abdulraheem, B.M. Nema, "Secure IoT Model Based on PRESENT Lightweight Modified and Chaotic Key Generator", The 1st Information Technology to Enhance e-learning and Other Application (IT-ELA), IEEE, pp. 12-18, 2020.

[10] J.R. Naif, Haider K. Hoomod, "A Novel Chaotic System for IoT Security Mechanism", Int. J. Adv. Eng. Manag., Vol. 3, No. 8, pp. 1770-1776, 2021.

[11] E.A. Albhrany, L.F. Jalil, and H.H. Saleh, "New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps", Int. J. Sci. Res. Sci. Eng. Technol. (IJSRSET), Vol. 2, pp. 67-73, 2016.

[12] H.K. Hoomod, J.R. Naif, I.S. Ahmed, "A new Intelligent Hybrid Encryption Algorithm for IoT Data

Based on Modified PRESENT-Speck and Novel 5D Chaotic System", Period. Eng. Nat. Sci., Vol. 8, No. 4, pp. 2333-2345, 2020.
[13] Z.M. J. Kubba, H.K. Hoomod, "Modified PRESENT Encryption algorithm based on new 5D Chaotic System", IOP Conference Series: Materials Science and Engineering, Vol. 928, No. 3, p. 32023, 2020.
[14] P. Gokhale, O. Bhat, S. Bhat, "Introduction to IOT", Int. Adv. Res. J. Sci. Eng. Technol., Vol. 5, No. 1, pp. 41-44, 2018.
[15] M.H. Miraz, M. Ali, P.S. Excell, R. Picking, "Internet of Nano-Things, Things and Everything: Future Growth Trends", Futur. Internet, Vol. 10, No. 8, p. 68, 2018.
[16] N.A. Ragimova, V.H. Abdullayev, "Overview of Cyber-Physical Technologies and their Perspectives in Healthcare", Int. J. Tech. Phys. Probl. Eng., Vol. 13, No. 2, pp. 98-106, 2021.
[17] M. Oppitz, P. Tomsu, "Internet of Things, Inventing the Cloud Century", Springer, 1st ed., pp. 435-469, 2018.
[18] A.T. Lo'ai, H. Tawalbeh, "Lightweight Crypto and Security", Secur. Priv. Cyber□ Phys. Syst. Found. Princ. Appl., pp. 243-261, 2017.
[19] V.A. Thakor, M.A. Razzaque, M.R.A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities", IEEE Access, Vol. 9, pp. 28177-28193, 2021.
[20] J.R. Naif, "Design and Implementation of Secure IoT for Emergency Response System Using Wireless Sensor Network and Chaotic", Dissertation, Informatics Institute for Postgraduate Studies (IIPS), Iraq, 2019.
[21] F. Ozdemir, C.K. Koc, "Development of Cryptography since Shannon", Cryptol. ePrint Arch., pp. 1-48, 2022.
[22] S. Ramzan, "Review on an S-Box Design Algorithm Based on a New Compound Chaotic System", M.Sc. Thesis, Capital University of Science and Technology (CUST), Islamabad, Pakistan, 2021.
[23] S. Dhall, S.K. Pal, K. Sharma, "A Chaos-Based Probabilistic Block Cipher for Image Encryption", J. King Saud Univ. Inf. Sci., Vol. 34, No. 1, pp. 1533-1543, 2018.
[24] M.P. Johnson, "The Diamond2 Block Cipher", University of Colorado, Technical Report, pp. 1-16, Colorado, USA, 1995.
[25] A. Kuznetsov, Y. Gorbenko, A. Andrushkevych, I. Belozersev, "Analysis of Block Symmetric Algorithms from International Standard of Lightweight Cryptography ISO/IEC 29192-2", The 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 203-206, 2017.
[26] A. Bogdanov, et al., "PRESENT: An Ultra-Lightweight Block Cipher", International Workshop on Cryptographic Hardware and Embedded Systems, pp. 450-466, 2007.
[27] K.S. Mohamed, "New Frontiers in Cryptography", New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA (1st ed.), Springer, pp. 41-63, Fremont, CA, USA 2020
[28] H. Liang, M. Wang, "Cryptanalysis of the Lightweight Block Cipher BORON", Secur. Commun. Networks, Vol. 2019, pp. 1-12, 2019.
[29] A. Rukhin, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Special Publication (NIST SP), Report No. 800-22 Rev 1a, pp. 1-164, September 2010.
[30] P. Burciu, E. Simion, "A Systematic Approach of NIST Statistical Tests Dependencies", J. Electr. Eng. Electron. Control Comput. Sci., Vol. 5, No. 1, pp. 1-6, 2019.

BIOGRAPHIES

Noor Maher Naser was born in Baghdad, Iraq in March, 1978. She received the B.Sc. degree in Electrical Engineering from University of Technology, Baghdad, Iraq in 2000. She received a High Diploma degree in Computer Science from the same university in 2001. From 2002 to 2018 she worked in the Iraqi Commission for Commuters and Information as a programmer in designing database systems, following up with the users, giving training courses for the users or trainer students. From 2018 till now she is working in University of Information Technology and Communication, Baghdad, Iraq, vice president for Scientific Affairs Department. Currently, she is a full time Master student in Informatic Institute for Postgraduate Studies, Iraqi Commission for Commuters and Information (ICCI). Her current researches interests include the areas of Information Security and internet of things security (IoT).

Jolan Rokan Naif was born in Salahaldeen, Iraq in October 1975. She received a four-year degree in Electrical Engineering from College of Engineering, University of Al-Mustansiriyah, Baghdad, Iraq in 1997. She received a M.Sc. degree in Computer Science from Informatics Institute for Postgraduate Studies in 2002, after that she received the Ph.D. degree in Computer Science from the same institute, Iraqi Commission for Commuters and Information (ICCI) in 2019. Since 2005 till now she worked in the ICCI and progressed in the academic field until she reached the degree of Assist Professor in 2021. She has co-authored of two books in computer science, both of them in data structures and algorithms using java and C++ languages. Her current researches interests include the areas of information security and internet of things security (IoT). She has co-authored over 6 papers in journals and international conference proceedings. she also supervised many master and high diploma students through the past years.