A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System

https://doi.org/10.3991/ijim.v15i02.19961

Hayder Najm (✉)
University of Technology, Baghdad, Iraq
cs.19.87@grad.uotechnology.edu.iq

Haider K. Hoomod
Mustansiriyah University, Baghdad, Iraq

Rehab Hassan
University of Technology, Baghdad, Iraq

Abstract—The concept Web of Things (WoT) goes well beyond the emphasis on the Internet as a means of sharing data, instead of introducing all resources and connections involving computers, data, and people to the Web. It, therefore, focuses on a range of problems and opportunities, thus paving the way for several exciting industries applications. In cryptography a range of main characteristics of chaotic systems such as non-linearity, initial condition sensitivity, and mixing properties are available. These characteristics provide an essential connection between cryptography and chaos. GOST is the Russian norm of encryption. GOST block cipher is based on secret key secrecy. However, when the encryption process with the same key is used for plaintext, the same cipher text is created. Message replication can be easily detected by an adversary who is a bad link in every communication. In this paper, we propose to use a 5d chaotic system combined with GOST block cipher to create a new secure Web of Things (WoT) cryptography system. GOST is a symmetric block cipher. It is the basis of most secure information systems in Russia. The 5D chaotic system was used to generate chaotic random keys that used in the GOST algorithm to provide security as a higher strength to increases randomly. The National Institute of Standards and Technology (NIST) designed a set of fifteen statistical tests and modifies key schedule as security operations.

Keywords—Web of Things (WoT), information security, cryptography, block cipher, GOST algorithm, and chaotic system

1 Introduction

A variety of experiments have been carried out to discourage third entities from accessing data through contact. In most technical approaches, flawless systems in safety electronics are still not accomplished. There is always a possibility that third entities will decode the data, even if the data is very well shielded. Different encryp-

tion methodologies are introduced to mitigate this possibility. In recent years, quick electronic technologies advances have led to more efficient data communication using microcontroller and computer-based systems [1] [2]. Currently, it is remembered that even effective encryption techniques may be exploited at a specified period. Modern encryption studies illustrate that chaotic systems' fundamental properties suggest a high correlation among chaos and cryptology [3]. High-speed, distortional, reactive, and aperiodic represented the characteristics of chaotic systems. There is a more personal point of view-based encryption for communications due to noise behavior and strong dependency on initial conditions and parameters [4]. Encrypted data shows a complex that is necessary for data to stay top-secret. In recent decades, researchers have found a fascinating relationship between cryptography and chaos. According to this, there are many properties of chaotic systems such as: ergodicity, sensitivity to initial conditions, mixing properties, deterministic, ease of use dynamics and structural complexity that are similar to confusion/diffusion with a simple shift in dynamics plain text key / secret key [5]. The term "chaos" was first used in the cryptographic field in 1989 when Matthews introduced chaos as a stream cipher on the basis of the chaotic 1D method [6]. Chaotic systems have important features that ensure the mechanism is extremely safe and resilient to cryptographic attacks. Due to their capability to attain diffusion-based confusion results, various chaos-based encryption algorithms were investigated and implemented in any cryptosystem [7]. The aim of this research in this paper, suggests a new WoT cryptography algorithm according to GOST and novel 5d chaotic system. It can provide high security at a very fast encryption rate and can be easily implemented by software and hardware. This paper performs a series of experiments to demonstrate the feasibility of the suggested solution. Detailed statistical analysis and experiments show that WoT's security and timing are much superior to our scheme. The following paper is organized: Section 2 includes a brief overview of information security. Traditional GOST algorithm and chaotic system are presented in section 3 and section 4. The related work Information will be presented on the proposed approach in Section 5. Sections 6, 7 presents the novel 5D chaotic system construction adopted in this paper and the proposed methodology. Section 8 describes the results and analysis. Section 9 ultimately offers a conclusion.

2 Information Security

InfoSec, a set of procedures to secure data from unauthorized alteration, is often referred to, both stored and transmitted from one device or physical location to another. Since intelligence has become one of the most valuable assets in the 21st century, efforts have become increasingly essential to preserve information security [8-10]. Information Security systems are designed around three goals, generally known as the CIA – Confidentiality, Credibility, and Availability. Information security is at the center of Information Assurance, which means that the CIA protects information and guarantees that information is not compromised in any way when sensitive issues occur [11-16]. Cryptography is a vital instrument for securing information that is transmitted by computers. Cryptography is an imaginative transformation of data into

an unreadable format such that it can only be interpreted and used by the intended receiver. The art and science of cryptography is the defense against improper access to sensitive or confidential information [17-20]. In general, therefore, cryptography is all about shielding and safeguarding information from cybercriminals or someone other than the intended recipient. Cryptography allows people to connect on the Internet and safely share critical and confidential information. Cryptography also helps individuals to use public and private media like the Internet, to shop and not be the victims of criminals and sniffing by a password. This is done through the use of modern technological advances in computer science [21-26].

3 GOST Algorithm

GOST is a symmetric block cipher, it is the Russian norm of encryption. It was in 1989. It is the basis of most secure information systems in Russia. It has a simple structure suitable for compact hardware implementations. It has been classified as one of the cryptography block ciphers. Therefore, it is a target for the constrained environments. It is a network of 32 round functions, add a 32-bit sub-key module 232, bring the results through the S-box layer, and rotate the result left by 11 bits [27]. No advancement in standard cryptoanalysis was already made in existing studies except for a quick summary of the GOST design and the related key attack. The GOST encryption method is a block cipher with a 256-bit key and a 64-bit block size. GOST is designed as a 32 round Feistel network with a 32-bit round sub-key, as shown in fig.1 [28].

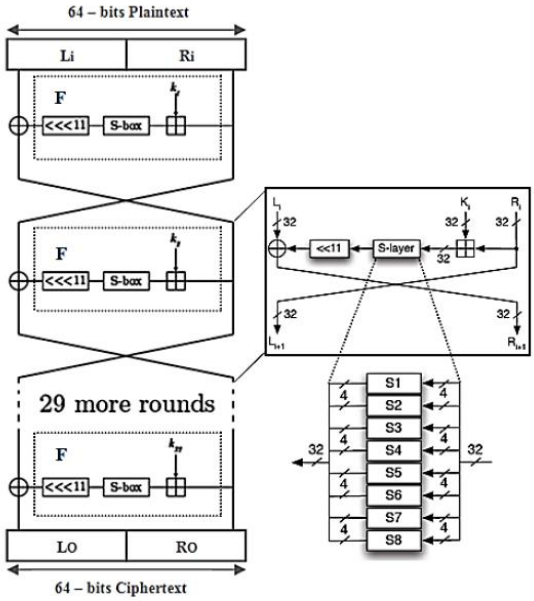


Fig. 1. Traditional GOST algorithm [29].

Table 1. Generation of Sub-Key in GOST [29]

Round	**R_1**	**R_2**	**R_3**	**R_4**	**R_5**	**R_6**	**R_7**	**R_8**
Sub-key	K1	K2	K3	K4	K5	K6	K7	K8
Round	R_9	R_{10}	R_{11}	R_{12}	R_{13}	R_{14}	R_{15}	R_{16}
Sub-key	K1	K2	K3	K4	K5	K6	K7	K8
Round	R_{17}	R_1	R19	R_{20}	R_{21}	R_{22}	R_{23}	R_{24}
Sub-key	K1	K2	K3	K4	K5	K6	K7	K8
Round	R_{25}	R_{26}	R_{27}	R_{28}	R_{29}	R_{30}	R_{31}	R_{32}
Sub-key	K8	K7	K6	K5	K4	K3	K2	K1

Key generation is simplistic; the 256-bit key is split into eight 32-bit sub-keys. The algorithm has 32 rounds, so each subkey includes the following scheme at four rounds [30].

The arrangement of the S-boxes shapes GOST stability. The structure of the S-boxes has not been released for a long time. The input and output of S-box are 4-bit numbers so that each S-box can be provided with a series of numbers from 0 to 15. Then the sequence number will be input and output to the S-box [31].

The Key Sequence split 256-bit main into eight 32-bit words K0… K7, and then using these key terms in the sequence K0, … K7, K0, … K7, K0, … K7, K7, K6, … K0.

The F-function is used in each round on the right side of the plaintext message, as shown in fig.2. Converts plaintext with three operations:

- Data addition and module 232 subkey.
- Data replacement with secure S-boxes.
- Left cyclical shift by 11 positions.

The output of F-function is applied to the left part of plaintext modulo 2, then the left and the right sides are adjusted to the next round. The general phase of the round function can be described in the formal syntax as follows [32]:

$$\text{Lefti+1} = \text{Righti} \tag{1}$$

$$\text{Righti+1} = \text{Lefti} \oplus (\text{S (Ki + Righti mod 232)} << 11) \tag{2}$$

Where $\oplus$ denotes a bitwise exclusive OR and << a rotation to the left by a bit.

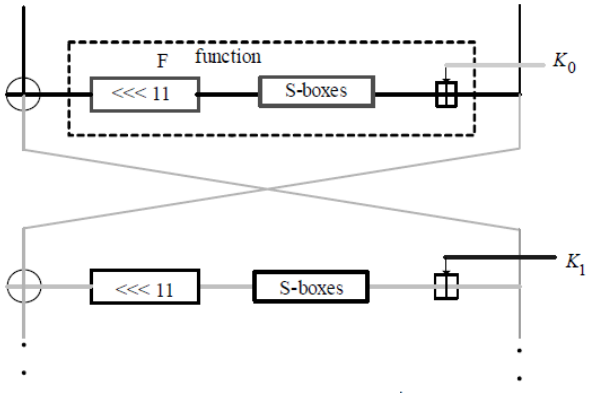


Fig. 2. F-function round [32].

4 Chaotic System

The chaos that can occur with certain system values/parameters is among the potential actions associated with the growth of a nonlinear physical system. Chaotic systems are defined as flows from the point of view of differential equations and differential equations are known as maps. Trajectory and orbit describe the creation of these non-static structures. The direction is defined as the trajectory, followed by the flow as time passes and the set of points travel over the map [33-34]. Chaos Theory deals with processes that develop into a specific form of complex action in time. In general, these processes usually adopt a variety of evolutionary principles and are thus deterministic. Chaos is only present in such non-linear deterministic systems. It must be stated. Explicitly, there is chaos when long-term and sustainable development fulfils those mathematical requirements [35]. Non-linear maps of chaotic behavior are chaotic maps. During the encryption method, chaotic maps generate pseudo-random variations. Initial conditions and parameters are aligned in mixing and adaptation to certain fundamental concepts of chaos theory. The most critical advantage of chaos is that unlicensed consumers like noise receive a noisy signal. In addition, generating chaotic values with simple iterations is also cheap and suitable for ciphers of blocks [36].

4.1 Chaos-cryptographically partnership

Deterministic nonlinear dynamic systems that produce the deterministic pseudo-randomness required in cryptography are implemented with chaotic systems. Furthermore, non-linear dynamic systems are able to generate complex progressive patterns. This gives chaotic systems the requisite algorithmic complexity [37]. The intrinsic characteristics of chaos specifically contribute to uncertainty and diffusion's cryptographic characteristics. It is evident, in answer to the properties, that the properties are directly linked to uncertainty, auto similarity, and topological mixing. Aperi-

odic orbits, generating identical statistical patterns, give dynamics of the chaotic attractor. Such designs may use substitution techniques to obscure simple signals [38]. On the other hand, diffusion is closely linked to chaotic systems sensitivity to starting conditions and parameters of regulation. Diversion induces an avalanche effect in order to generate a completely different output with a minimal variance of the cryptosystems input. This behavior is generated by a chaotic system when the original conditions or control parameters are modified slightly. The same avalanche effect is created by using those variables as inputs to the algorithm cryptosystem. The relationship between chaos and encryption is summarized in table 2 [39].

Table 2. Chaotic and cryptography relationships [39]

Chaotic characteristic	Cryptographic property	Description
Ergodicity, Mixing property Auto-similarity	Confusion	The output of the system seems similar for any input.
Sensitivity to initial conditions and control parameters	Diffusion	A small difference in the input produces a very different output
Deterministic	Deterministic pseudo randomness	A deterministic procedure that produces pseudo randomness
Complexity	Algorithmic complexity	A simple algorithm that produces highly complex outputs

5 Related Works

Many papers are talking about cryptographic and chaotic theory. In [40], to improve communication protection, a chaos-based encryption approach with non-linear equations is proposed. Methods of encryption are studied using the properties of three separate chaos generators. Applications are rendered by logistical map, pinchers map, sinus map, chaos generators generally referred to in the literature. In [41], this study proposed to encrypt WSN's message digester MD, a new encoding scheme known as Chaotic Block Cipher (CBC). This approach uses a logistic map approach to construct a set of chaotic values to get the encryption/decryption keys to a plaintext that mixes them for cipher text. In [42], using the data, the 4D chaotic system, and three control parameters, the proposed algorithm permutation matrix P is generated. Half of the picture data is used for building P and three test parameters are defined. There are still a lot of real chaotic sequences. In [43], the hyper-chaos has more than one exponent of Lyapunov and complex dynamic features as well as one-dimensional chaos, it's investigated by the author, and it is safer than the safety algorithm chaos. Encryption is performed in two stages in the proposed algorithm. Next, the picture is absolutely mixed with a messy logistic map. Second, the gray values of the mixed image are encoded using a hyper-chaos system. In [44], using the logistic map. The first small permutation matrices are the chaotic logistic map sequence. The logistic map's initial value and small matrices are known as an algorithm. These small parameters are used to construct a comprehensive parameter matrix. Then construct an image with a plaintext with the entire matrix. To mask the image, use the permutation mask. The suggested methodology provides adequate protection against numerical cryptanalysis.

In [45], the author has suggested the encryption of a picture based on chaotic, non-linear logistic map sequences. Encrypting and decrypting algorithms are designed with a non-linear function, which produces a secret key using a single logistic map for these functions. The combined non-linear and chaotic logistic functions have been demonstrated to provide good statistical features on the reception of the cipher image and image data. The proposed system is not, however, sufficiently sonic. It is also demonstrated to be adaptive not only to initial condition x but also to the logistic equation bifurcation parameter.

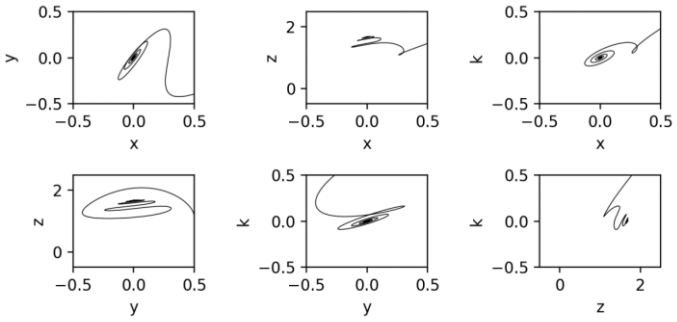
In [46], two distinct, non-invertible, two-dimensional, discrete-time cryptosystems were proposed. Chaotic attractors, which are thought to be pseudo-random generators, are some map paths, while the initial conditions are the main. They suggested using non-invertible two-dimensional maps that show chaotic encryption dynamics. In [47], the method of building the cipher algorithm that can use long keys and the variable key length is specified. An efficient way to encrypt and decrypt data is through discrete chaotic maps. A constructed algorithm was simple and provided fair security and efficiency. In [48], proposed a secure system using the new 4D chaotic system in combination with the Advanced Encryption Standard (AES) modified lightweight. The proposed 4-dimensional (4D) chaos system Lyapunov was tested and passed for several initial periods and a super chaos system (4 positive Lyapunov) was developed. In lightweight AES and Secure Hash version 3 (SHA3-256), chaos keys created (used from JORN) are used. In order to decrease CPU cycles and AES complexity, the Lightweight AES was developed. Results indicate a decrease in the computation time for the method proposed (up to 145 percent). The performance of the improved lightweight AES encryption framework includes strong statistical tests that can prevent several attacks similar to the original AES.

6 Novel 5D Chaotic System Construction

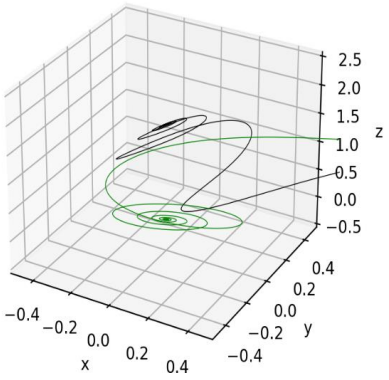
Chaotic is a unique non-linear, dynamic system; the chaotic 5D system has more complex dynamic properties than the chaotic system of lower dimensions. A numerical indicator to determine if the system is chaotic is Lyapunov exponent. A positive Lyapunov exponent implies more than one hyper-chaotic exponent of chaos and positive Lyapunov exponents. Our proposed new algorithm is based on the following equations:

$$
\begin{aligned}
&xi+1 = -r \cdot xi + b \cdot yi \cdot ki - 2.5 \cdot s \cdot pi \\
&y_{i+1} = -q \cdot y_i - s \cdot x_i \cdot z_i + r \cdot x_i - u \cdot p_i \\
&zi+1 = 2 \cdot zi \cdot xi \cdot yi - 1.1 \cdot r \cdot pi - q \cdot ki \\
&ki+1 = r \cdot xi + s \cdot yi - u \cdot ki \\
&pi+1 = b \cdot ((xi + ki) / zi) + r \cdot yi
\end{aligned}
\tag{3}
$$

Where x, y, z, k and p represent the system states, where b, r, s, u and q represent positive constant parameters. When the value of b=0.001, r=0.7, s=0.5, u=1.9 and q=0.2 and the initial state are x_0=2.1, y_0=0.5, z_0=1.1, k_0=1.1and p_0=0.1; the system displays a chaotic behavior and the Lyapunov exponents are as follows: LE_1= 0.04187490335084436, LE_2= 0.056182990598499266, LE_3= 4.541784300356545, LE_4= 0.04356762255380923 and LE_5= 0.057322573098809185. Fig.3 show our chaotic attractors.



a. The behavior of the system at two-dimensional view xy, xz, xk, yz, yk and zk.



b. The behavior of the system at three-dimensional view xyz

Fig. 3. (a, b) Chaotic system behavior.

7 Proposed Approach Methodology

The main idea of the proposed approach is to use the GOST algorithm and the novel 5d chaotic system by combing the strengths of each other. The GOST algorithm

key schedule will not be used; the 5d chaotic keys will be used as the GOST algorithm keys to control the weak point in the GOST algorithm. Initially, sensing data (Plaintext) collection from sensors connected to a web of things (WoT) system. In this work, the proposed system was checked by five sensors. These sensors are powered by Raspberry Pi 3 type B. The data of each sensor is obtained and aggregated during slice times. 64-bit data blocks are reached and transformed to 64-bit encrypted data blocks by a 256-bit key generated from 5d chaotic system. In every round as showing in fig.4, right-hand side of plaintext is handled by F-fun, that converting messages to three cryptographic processes: Data addition and sub-key module 232, data substitution using Sboxes, and the left-cyclical-shift to 11-positions. The output of F-fun is added to the plaintext in modulo 2 at the left side; then the next round is swapped to the right and left sides. There are 32 rounds in the algorithm. The right and left sections are not changed during the last encryption round. GOST uses eight S-boxes, converting 4bit input into a 4bit output. GOST does not have standardized Sboxes, and any values can be used, unlike most encryption algorithms. The secret key (generated by 5d chaotic) is 256bit and is given as an eight-word sequence: (K_1 to K_8). Every 32-bit word is added in any encryption round as a round subkey. The following principle is applied when the round subkey is determined: the order at 1-round 24 is simple (K_1-K_8). The order is reversed at 25-round32 (K_8-K_1). Due to the high randomness of the chaotic key, there is good encryption of robustness. Deciphering is the same method of encrypted, but the 5d chaotic system's reverse key.

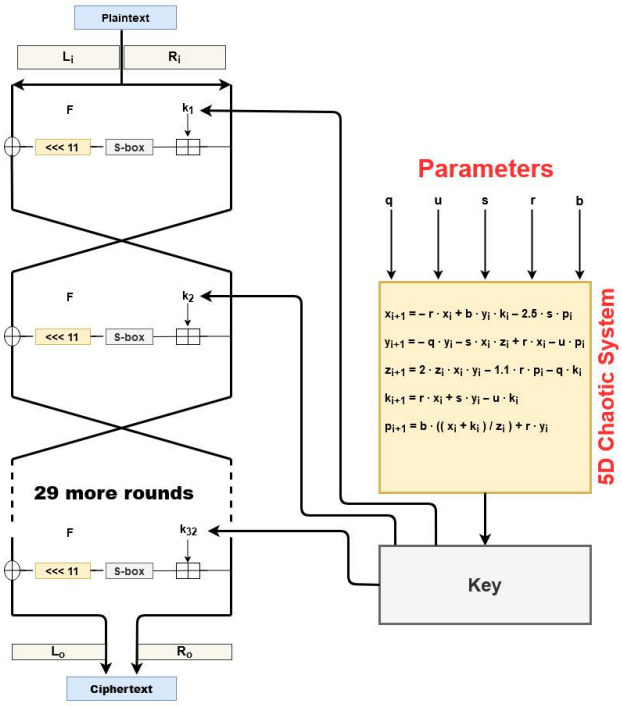


Fig. 4. Block diagram of the proposed approach.

8 Experimental Results and Statistical Analysis

Many tests are conducted using the proposed approach to encrypt/decrypt sensing data by using the characteristics of GOST block cipher and chaotic system, ensuring that the software and hardware encryption and decryption scheme is fast and easy to implement for resource-controlled devices such as smart devices and wireless nodes. This work examines the possibility of mixing a block cipher (GOST) and a chaotic system to produce a strong chaotic-cryptographic. It involves a specific plan to combine GOST 256-bit and chaotic random keys, that is significantly quicker than the standard GOST and possibly more reliable. The encryption process needs 64-bit or 16-hex data or eight characters input plaintext data through 32 iteration stages (rounds), while the deciphering process involves the reverse of the ciphering process. The energy consumption can be reduced, and the system's encryption speed is higher. Our proposal is for high-security low-cost devices since it is resistant to most of the cryptanalytical attacks common to block chips and chaotic systems. The National Institute of Standards and Technology (NIST) designed a set of fifteen tests to evaluate and quantify the randomness of binary sequences produced by either software or hardware-based random or pseudo-random number generators for cryptographic applications. The NIST has adopted two approaches: the examination of the proportion of sequences that pass a statistical test and the distribution of P-values to check for uniformity. The system proposed provides adequate safety and reliability, according to a table 3.

Table 3. NIST Fifteen Statistical Tests

Test	P - Value
Monobit	0.500110
Frequency	0.498078
Runs	0.487880
Longest Run	0.504698
Binary Matrix Rank	0.477522
DFT	0.451004
Non Overlapping Template Matching	0.679095
Overlapping Template Matching	0.990653
Maurer's Universal	0.311035
Linear Complexity	0.500672
Serial	0.495460
Approximate Entropy	0.520565
Cumulative Sums	0.418182
Random Excursion	0.549397
Random Excursion Variant	0.501425

Table 4 illustrates the encryption and decryption processes, as well as execution time of traditional GOST algorithm. While, table 5 illustrate the encryption and decryption processes, as well as execution time of proposed approach.

Table 4. Traditional GOST encryption and decryption processes

Plain Text	Temperature ECG Heart beat
Encrypted Text	152355312c167321321423110072213404211230df9293e6fe40
Encryption Time	0.0001 in second
Decrypted Text	Temperature ECG Heart beat
Decryption Time	0.0009 in second

Table 5. Proposed approach encryption and decryption processes

Plain Text	Temperature ECG Heart beat
Encrypted Text	54656d706572617475726520454347204865e3003221c33f1c01
Encryption Time	0.0269 in second
Decrypted Text	Temperature ECG Heart beat
Decryption Time	0.0279 in second

A different statistical measure can be used to evaluate the proposed approach. These are hamming distance and entropy measures. Hamming distance is the difference measurement between plain text and cipher text, is measured at a bit level so we transform the strings into a byte array, convert each byte to the bits, and then count the number of differences. The randomness produced by the proposed approach, as shown in table 6, is more accurate than the randomness produced by the traditional GOST and this prefers the proposal.

Table 6. Hamming distance

Hamming distance	Traditional GOST	Proposed Approach
	0.2692	0.2884

Entropy must be given by the cipher to be injected into the plain text of a message in order to neutralize the amount of structure that is present in the unsecured plain text message. How this is calculated depends on the cipher. According to table 7, entropy of the proposed approach is greater (secure) and better than traditional GOST.

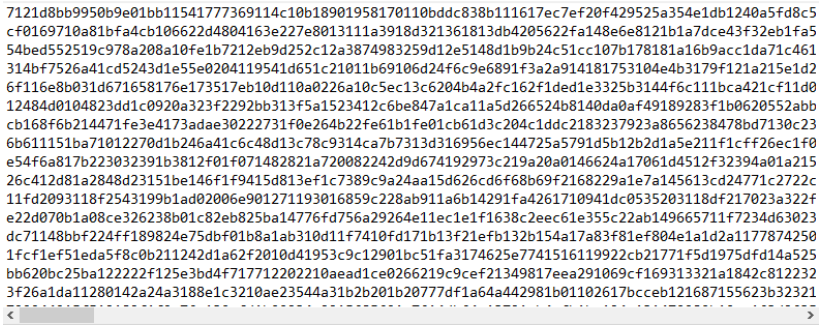
Table 7. Entropy

Entropy	Traditional GOST	Proposed Approach
	3.3669	3.4298

The power of cryptography lies in the choosing of keys, which are secret parameters used in encryption. An intruder should not be able to guess the key. Chaotic systems are highly adaptive and the best characteristics of the system's initial conditions and parameters. Being sensitive implies that the chaotic system's every point is approximated arbitrarily by other points with considerably different potential directions or paths. Thus, an arbitrarily small shift or disruption in the current path will lead to

dramatically different future behavior. The best randomness chaotic keys of proposed approach is generated at x0=2.1, y0=0.5, z0=1.1, k0=1.1and p0=0.1, as shown below:

Any changing in values of initial state that will be giving different keys don't get the required randomness, as example lets changing one of the initial condition like x_0 to 0.5 and y_0=0.500001, the keys that generated is shown below:



9 Conclusion

Speed and a reliable cryptography system for applications are usually very desirable. In this paper, the WoT encryption/decryption efficient algorithm is implemented according to GOST and novel 5D chaotic systems, and the results achieved following the implementation of the proposed algorithm shown in fig.4 illustrating the chaotic-cryptographic existence of the proposed method and showing chaotic behavior. The limitation of the GOST algorithm is simple key scheduling so that, in some cases, it is the weak point of the cryptanalysis process as related-key cryptanalysis. Even so, it is solved by the proposed approach by moving the GOST keys to the chaotic system has the perfect mixture and greater security of robustness. Its need for 2^{256} probable keys to breaking keys that are not to be used for brute force attack due to its awkward procedure in this case. NIST fifteen statistical tests and statistical analysis (hamming distance and entropy) have already successfully exceeded the randomness of the proposed approach. The proposed 5-dimension (5D) chaotic system was tested and pass and get a super chaotic system (5 positive Lyapunov).

10 References

[1] Aljazaery Ibtisam A, Alrikabi Haider Th Salim, and Aziz Mustafa Rabea, "Combination of Hiding and Encryption for Data Security," International Journal of Interactive Mobile Technologies, vol. 14, no. 9, pp. 34-47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[2] J. M. Amigó, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," Phys. Lett. Sect. A Gen. At. Solid State Phys., vol. 366, no. 3, pp. 211–216, 2007, https://doi.org/10.1016/j.physleta.2007.02.021.

[3] Mohammed Bahaa, Chisab Raad, and Alrikabi Haider, "Efficient RTS and CTS Mechanism Which Save Time and System Resources," International Journal of Interactive Mobile Technologies, vol. 14, no. 4, pp. 204-211, 2020. https://doi.org/10.3991/ijim.v14i04.13243

[4] M. S. Al-Ani, "Efficient Image Encryption Approach Based on Chaos Technique," IOSR J. Electr. Electron. Eng., vol. 12, no. 03, pp. 54–60, 2017, https://doi.org/10.9790/1676-1203025460.

[5] Alseelawi Nawar S, Adnan Enas K, Hazim Hussein T, Alrikabi Haider, and Nasser Khalid, "Design and Implementation of an E-learning Platform Using N-Tier Architecture," International Journal of Interactive Mobile Technologies, vol. 14, no. 6, pp. 171-185, 2020. https://doi.org/10.3991/ijim.v14i06.14005

[6] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," Cryptologia, vol. 13, no. 1, pp. 29–42, 1989. https://doi.org/10.1080/0161-118991863745

[7] P.-L. Carmen and L.-R. Ricardo, "Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem," Appl. Cryptogr. Netw. Secur., 2012, https://doi.org/10.5772/36419.

[8] M. W. Habiby and D. Lestari, "Cryptography System for Information Security Using Chaos Arnold ' s Cat Map Function," ICRIEMS Proc., pp. 61–66, 2017.

[9] I. Jabbar, "Using Fully Homomorphic Encryption to Secure Cloud Computing," Internet Things Cloud Comput., vol. 4, no. 2, p. 13, 2016, https://doi.org/10.11648/j.iotcc.20160402.12.

[10] I. Jabbar and S. N. Alsaad, "Design and implementation of secure remote e-voting system using homomorphic encryption," Int. J. Netw. Secur., vol. 19, no. 5, pp. 694–703, 2017, doi: 10.6633/IJNS.201709.19(5).06.

[11] H. Najm, H. K. Hoomod, and R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," Period. Eng. Nat. Sci., vol. 8, no. 3, pp. 1829–1835, 2020, [Online]. Available: http://pen.ius.edu.ba/index.php/pen/article/view/1619 .

[12] M. Salih Mahdi and N. Flaih Hassan, "a Suggested Super Salsa Stream Cipher," Iraqi J. Comput. Informatics, vol. 44, no. 2, pp. 1–6, 2018, https://doi.org/10.25195/2017/4422.

[13] M. S. Mahdi and N. F. Hassan, "Design of keystream Generator utilizing Firefly Algorithm," J. Al-Qadisiyah Comput. Sci. Math., vol. 10, no. 3, pp. 91–99, 2018, https://doi.org/10.29304/jqcm.2018.10.3.441.

[14] M. S. Mahdi, "Proposed Secure Internet of Everything (IoE) in Health Care," 2018.

[15] A.-M. G. Mohammed Salih Mahdi, Yaser M. Abid, Alaa Hamza Omran, "A NOVEL AIDED DIAGNOSIS SCHEMA FOR COVID 19 USING CONVOLUTION NEURAL NETWORK," 5th Int. Conf. Adv. Technol. Appl. Sci. 6th Malaysia-japan Jt. Int. Conf., 2020.

[16] M. S. Mahdi, “Computer Aided Diagnosis System for Breast Cancer using ID3 and SVM Based on Slantlet Transform,” Qalaai Zanist J., vol. 2, pp. 142–148, 2017. https://doi.org/10.25212/lfu.qzj.2.2.16

[17] Q. Lawande, B. Ivan, and S. Dhodapkar, “Chaos based cryptography: a new approach to secure communications,” BARC Newsl., vol. 258, no. 258, pp. 1–12, 2005.

[18] Duha Khalid Abdul-Rahman Al-Malah Saad Ibrahim Hamed, Haider TH. Salim ALRikabi, "The Interactive Role Using the Mozabook Digital Education Application and its Effect on Enhancing the Performance of eLearning," International Journal of Emerging Technologies in Learning (iJET), vol. 15, no. 20, pp. 21-41, 2020. https://doi.org/10.3991/ijet.v15i20.17101

[19] H. K. Tayyeh, M. S. Mahdi, and A. S. A. AL-Jumaili, “Novel steganography scheme using Arabic text features in Holy Quran,” Int. J. Electr. Comput. Eng., vol. 9, no. 3, pp. 1910–1918, 2019, https://doi.org/10.11591/ijece.v9i3.pp1910-1918.

[20] M. S. Mahdi and N. F. Hassan, “A Proposed Lossy Image Compression based on Multiplication Table,” Kurdistan J. Appl. Res., vol. 2, no. 3, pp. 98–102, 2017, https://doi.org/10.24017/science.2017.3.34.

[21] M. Barakat, C. Eder, and T. Hanke, “An Introduction to Cryptography,” 2018.

[22] A. Kadhim and M. Salih, “Proposal of New Keys Generator for DES Algorithms Depending on Multi Techniques,” Eng. Technol. J., vol. 32, no. 1 Part (B) Scientific, pp. 94–106, 2014.

[23] D. R. A. Kadhim and T. M. Salih, “Proposal Dynamic Keys Generator for DES algorithms,” Islam. Coll. Univ. J., vol. 9, no. 29, pp. 25–48, 2014.

[24] H. Najm, H. Ansaf, and O. A. Hassen, “An Effective Implementation of Face Recognition Using Deep Convolutional Network,” J. Southwest Jiaotong Univ., vol. 54, no. 5, 2019. https://doi.org/10.35741/issn.0258-2724.54.5.29

[25] H. Najm, H. K. Hoomod, and R. Hassan, “Intelligent Internet of Everything (IOE) Data Collection for Health Care Monitor System,” vol. 29, no. 4, pp. 2341–2350, 2020.

[26] H. Ansaf, H. Najm, J. M. Atiyah, and O. A. Hassen, “Improved Approach For Identification Of Real And Fake Smile Using Chaos Theory And Principal Component Analysis,” J. Southwest Jiaotong Univ., vol. 54, no. 5, 2019. https://doi.org/10.35741/issn.0258-2724.54.5.20

[27] N. T. Courtois, “Feistel Schemes and Bi-linear Cryptanalysis,” Crypto 2004, no. Cc, pp. 23–40, 2004. https://doi.org/10.1007/978-3-540-28628-8_2

[28] G. S. Oreku, J. Li, T. Pazynyuk, and F. J. Mtenzi, “Modified S-box to Archive Accelerated GOST,” vol. 7, no. 6, pp. 88–98, 2007.

[29] B. W. Aboshosha, M. M. Dessouky, and R. A. Ramadan, “Enhanced Version of GOST Cryptosystem for Lightweight Applications,” no. July, 2019.

[30] A. Biryukov and and L. Perrin, “State of the Art in Lightweight Symmetric Cryptography.”

[31] A. Sciences, Springer Encyclopedia of Cryptography and Security, no. March. 2016.

[32] L. Khelladi, Y. Challal, A. Bouabdallah, and N. Badache, “On security issues in embedded systems: Challenges and solutions,” Int. J. Inf. Comput. Secur., vol. 2, no. 2, pp. 140–174, 2008, https://doi.org/10.1504/ijics.2008.018515.

[33] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," Neural Comput. Appl., vol. 31, no. 7, pp. 2395–2405, 2019, https://doi.org/10.1007/s00521-017-3195-1.

[34] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," no. November, 2020.

[35] E. Mosekilde, Z. T. Zhusubaliyev, V. N. Rudakov, and E. A. Soukhterin, "Bifurcation analysis of the Henon map," Discret. Dyn. Nat. Soc., vol. 5, no. 3, pp. 203–221, 2000, https://doi.org/10.1155/s1026022600000534.

[36] R. R. Kumar, A. Sampath, and P. Indumathi, "Enhancement and Analysis of Chaotic Image Encryption Algorithms," Technology, pp. 143–153, doi: 10.5121/csit.2011.1215.

[37] J. De Dieu Nkapkop, J. Y. Effa, M. Borda, L. Bitjoka, and A. Mohamadou, "A secure and fast chaotic encryption algorithm using the true accuracy of the computer," Inform., vol. 40, no. 4, pp. 437–445, 2016, doi: 10.31449/inf.v40i4.1118.

[38] W. Yao et al., "A fast color image encryption algorithm using 4-pixel feistel structure," PLoS One, vol. 11, no. 11, pp. 1–30, 2016, https://doi.org/10.1371/journal.pone.0165937.

[39] Z. Elhadj and J. C. Sprott, "A two-dimensional discrete mapping with C∞ multifold chaotic attractors," Electron. J. Theor. Phys., vol. 5, no. 17, pp. 107–120, 2008.

[40] A. Akgül, S. Kaçar, B. Aricioglu, and I. Pehlivan, "Text encryption by using one-dimensional chaos generators and nonlinear equations," ELECO 2013 - 8th Int. Conf. Electr. Electron. Eng., no. November, pp. 320–323, 2013, https://doi.org/10.1109/eleco.2013.6713853.

[41] H. M. Al-Mashhadi, H. B. Abdul wahab, and R. Hassan, "Chaotic Encryption Scheme for Wireless Sensor Network's Message," World Symp. Comput. Networks Inf. Secur., no. June, 2014.

[42] X. Huang, "A New Digital Image Encryption Algorithm Based on 4d Chaotic System," Int. J. Pure Appl. Math., vol. 80, no. 4, 2012.

[43] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," Phys. Lett. Sect. A Gen. At. Solid State Phys., vol. 372, no. 4, pp. 394–400, 2008, https://doi.org/10.1016/j.physleta.2007.07.040.

[44] Y. Zhang, "Comments on 'an image encryption scheme with a pseudorandom permutation based on chaotic maps,'" Proc. 2011 Cross Strait Quad-Regional Radio Sci. Wirel. Technol. Conf. CSQRWC 2011, vol. 2, no. July 2011, pp. 1251–1255, 2011, https://doi.org/10.1109/csqrwc.2011.6037190.

[45] H. Ogras and M. Turk, "Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function," vol. 6, no. 7, pp. 885–888, 2012.

[46] L. Bénéteau, D. Fournier-Prunaret, V. Guglielmi, P. Pinel, S. Rouabhi, and A. K. Taha, "Two encryption schemes using the chaotic dynamics of two-dimensional noninvertible maps," NDES '02 Nonlinear Dyn. Electron. Syst. Izmir, Turquie, pp. 21–23, 2002.

[47] R. Hucka, "A Ciphering Algorithm Based on Discrete Chaotic Map," Dept. Radio Electron. Brno Univ. Technol., pp. 87–90, 2007.

[48] J. Rokan Naif, G. H. Abdul-majeed, and A. K. Farhan, "Internet of Things Security using New Chaotic System and Lightweight AES," J. Al-Qadisiyah Comput. Sci. Math., vol. 11, no. 2, pp. 45–52, 2019, https://doi.org/10.29304/jqcm.2019.11.2.571

11 Authors

Hayder Najm is received his B.E degree in computer science from University of Technology in 2011, received his M.S.C degree in computer science from University of Technology in 2014, and currently he is Ph.D student in computer science from University of Technology in 2020. He is currently working at Imam Al-kadhum College (IKC), Computer Technique Engineering Department, Wasit, Iraq. E.mail: cs.19.87@grad.uotechnology.edu.iq, haidernajem@alkadhum-col.edu.iq.

Assist. Prof. Dr. Haider K. Hoomod is received his BS.C degree in Electrical Engineering from university of Technology in 1996. Received M.Sc. degree in Computer Science from Iraqi Commission for Computers and Informatics \Informatic Institute for Postgraduate Studies in 2002. Received Ph.D. Degree in Computer Science from Iraqi Commission for Computers and Informatics \Informatic Institute for Postgraduate Studies in 2008. Email: drhjnew@gmail.com

Assist. Prof. Dr.Rehab Hassan Fleah Kadhim is received her B.E degree in computer science from University of Technology in 1989, received her M.S.C degree in computer science from University of Technology in 1995, and received her Ph.D.degree in computer science from University of Technology in 2005. She is currently working in University of Technology/ Iraq–Baghdad. Email: 110019@uotechnology.edu.iq.

Article submitted 2020-10-20. Resubmitted 2020-11-26. Final acceptance 2020-11-26. Final version published as submitted by the authors