Lightweight Secured-Image Transferring based on A Hybrid SPECK-RC5 Method

Suhad Fakhri hussein
Suhad7242@gmail.com

Abstract

Image transmission can be secured effectively, ensuring confidentiality, integrity, and authenticity of the transmitted image data by applying encryption process. IoT systems required lightweight method to satisfy the limitation in the resources. In this paper a hybrid lightweight encryption method that combining SPECK and RC5 algorithms is proposed with a method for self key establishing. The essential to implement secure key management practices and use robust transmission protocols to mitigate security risks and vulnerabilities. Security and speed have been achieved to encryption/decryption color images of different sizes and different kernels based on the number of kernels selected. It is carried out in four rounds, where the output of one of the two algorithms is RC5 Input for the present algorithm is executed four rounds, the outputs of the present algorithm are swapped with the outputs of the second algorithm, RC5, and merge them to obtain the final encryption output. The keys of these algorithms are generated using the Six-dimensional chaos system equation.

Keyword

SPECK Algorithm, RC5 algorithm, Lightweight Encryption, hyperchaotic map

1. Introduction

In the recent digital world, the image is an important type of information that properly transferred from their source to their destination. Secure image transfer with a secured transferring methodology aims to diverse image transferring techniques by developing a secured data transfer environment [1]. The maintaining digital visual data integrity requires an effeicient image encryption and decryption [2]. Cryptographic techniques must be more advanced and efficient to secure data in multi-core computing environments [3]. The eesource-constrained devices or networks with limited bandwidth may struggle with large-scale encrypted image processing [4]. The type of file formats or platforms that don't support image encryption algorithms can cause compatibility issues [5]. One solution for increase robustness of suggested encryption method is the quality of applied key that required in encryption process. The Chaos theory may be considered as a solution for dynamic key generation with some charactestics such as its sensitive dependence on initial conditions and deterministic dynamics [6]. Chaotic dynamics can improve pixel shuffling and diffusion security in encrypted images [7]. The goal of this work is to build an efficient algorithm that encrypts files such as color images by merging more than one method and to obtain an algorithm that balances high security with reducing the time required for encryption while trying to implement this algorithm in a parallel manner so that the results are as fast as possible.

2. Six-D Memristive Hyperchaotic System

Random numbers (RNs) are used to generate parameters for public keys of symmetric cryptosystems, digital signatures, and identity authentication [8]. With the advancement of the technologies of recent communication and data security, using pseudorandom number generators (PRNGs) is required to add a good level of randomness and complexity [9]. Many scientific fields use such numbers to model the non-deterministic and therefore unpredictable events that surround us in everyday life [10]. The basic characteristic of pseudorandom numbers, as opposed to truly random ones, is that they are predictable. For some purposes, predictability may be a good feature, but for other critical applications, it is fundamentally inappropriate or even dangerous [11]. One of chaotic system is 6-D memristive hyperchaotic autonomous system with complex and implicit extreme multistability has the following dynamic phenomena on a line or an equilibrium plane: hidden extreme multistability, transient chaos, bursting, and offset boosting phenomenon [12]. This 6D memristive hyperchaotic system is the first high-order system to present all these rich dynamic behaviors:

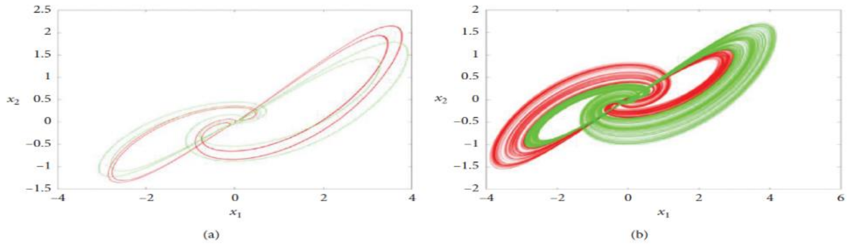

Figure 1: The typical attractors in the $x_1 - x_2$ plane with different values of x_6.

2. The RC5 algorithm

One of method of encryption data is RC5 algorithm, The word sizes, cycles, and key length of (RC5-w/r/b) are all changeable, where word's bit size and value (16, 32, and 64) bits. The number of cycles is vary from 0 to 255. The private key's length in bytes, which can be anywhere between 0 and 255 [13]. The three stages of RC5 are key expansion in the first stage, encryption in the second stage, and the decryption method in the third stage. The algorithm's drawbacks are its slow execution and vulnerability to differential attacks. The RC5 method makes use of three elementary operations along with their inverses [14] Listed below are: Subtraction, the XOR operation and rotation.

3. Speck encryption (Lightweight Cryptographic LWC)

Algorithms are specifically engineered to operate in environments and devices with limited resources, including restrictions on computational power, memory, and energy efficiency. The objective of these algorithms is to ensure sufficient security while reducing the amount of time and resources required for operation. They find widespread implementation in a variety of applications, including sensors, IOT (Internet of Things) devices, smart cards, and embedded systems [15]. The diagram shows lightweight cryptography with symmetric and asymmetric ciphers [16].

4. Methodology

The proposal includes merging the RC5 algorithm with SPECK Lightweight algorithm, generating the key for these two algorithms using the six-dimensional chaos system equation, implementing in form faster and more resistant to differential attacks and the uing of the six-dimensional chaos system equation, gives dynamism to the proposed method so that the key generation results can be changed with each execution, making it difficult for an unauthorized person to guess these keys. The RC5-SPECK sequential hybrid encryption algorithm uses the strengths of both algorithms.SPECK is a lightweight, resource-constrained block cipher, while RC5 is flexible. Combining these two can create a secure and efficient algorithm for many applications. The peprocessing input image, after a 128-bit block cipher is divided into two 64-bit sections. Each section is encrypted using the RC5 algorithm for four rounds with a 64-bit key size generated using the algorithms. The key generation using six dimension equation system. The output of the first RC5 cipher is The 64-bit is the entry for a Speck algorithm with a key of 80 bits or 128 bits generated using the algorithms (3.2) and (3.4) for only four rounds. The other side is that the 64-bit block is encrypted using the second RC5 as well, and then the switching network uses the outputs between the present algorithm and the second RC5 and merges them.

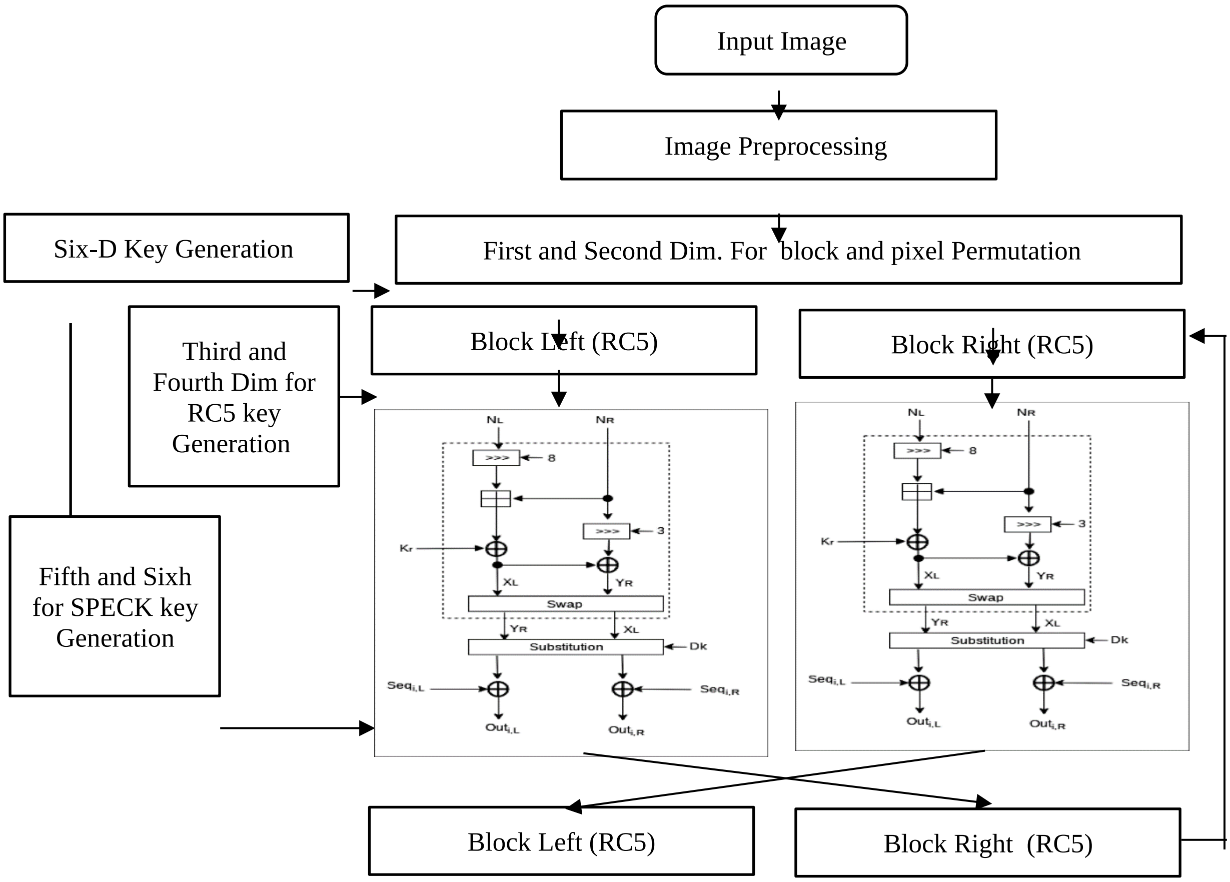

Figure 2: present algorithm For RC5 input

- **PerProcessing**

The preprocessing represented by split image into three color bands (red, green, and blue) the each band reashpe to vector and the three vectors merg into one vector represent hole image. The last vector split into blocks that will entered the proposed ecryption method and could processed in parallel mechanisem.

- **Six-Dimension Key Generation**

the set of equations represent the chaotic system are used for key generation (that explain in the key generation paragraph). The first dimension used for reorder the blocks in the in put blocks this means the blocks encrypted in a non uniform blocks (not sequential). The second dimension used for reorder bits in each block by applying permutation process on each block with shiftinig process to avoid the periodicity. The third and fourth dimension dimension used in RC5 for left and right block respectively. The fifth and sixth dimension used for SPECK methd that will encrypt the output from the privous step.

- **Encryption Process**

The encryption process represented by several steps keep the security with reducing rounds in the two proposed algorithms (RC5 and SPECK). Each block split into two blocks left and right each one applied RC5 in four rounds, the output of it be input to the SPECK algorithm with four rounds also. The out left will be new right and the right be left. These steps are apllide several time to produce the encrypted block. The encypted blocks merged into new vector and split into three vecrors coreesponding to he input colr band image. Each vector are reshaped into two dimension array having same number of rows and columns of the inputs. The last step are meged the three arrays into one array with three dimension (three layers RGB) represented the encrypted image.

- **Dencryption Process**

The decryption process represented by several steps similar to encryption process in reverse order. The key generation process generated the same numbers of sequences used from end to start one. The process apllied RC5 decryption on block after partiion into left and right the applied SPECK then flip the left to right and right to left block these process applied several times equal to the encryption procee. The permutation process here is in the last by inverse bit permutation and inverse block permutation to retrived the extracted image without any lose in the information.

5. Experemintal Test Result

The efficiency metrics include the cryptosystem's security, encryption/decryption time, and overall system capability. Several tests are applied to evaluate their robustness and resistance to the most common attacks. The proposed method used standard image for testing as explain in figure 3 and the saple of encryption also explaining.

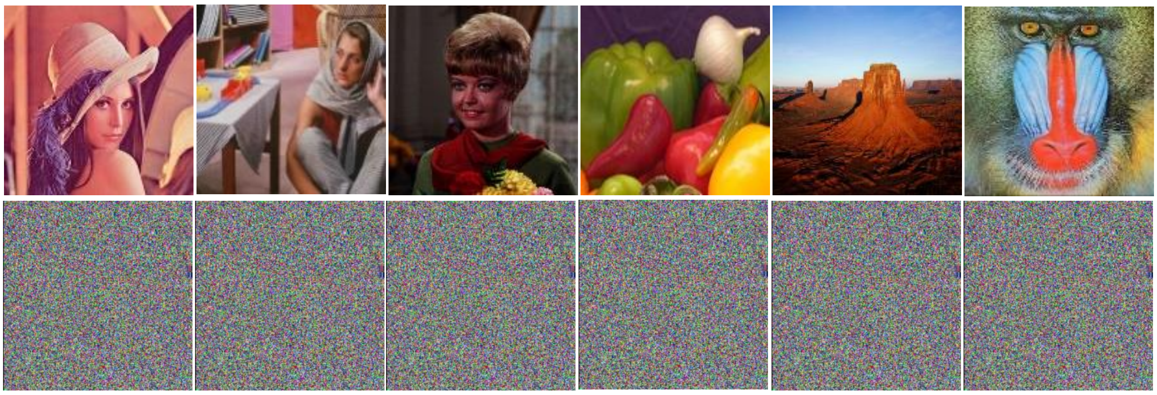

Figure 3: plain images and encryted images

The PSNR test represented the similarity of encypted image with respect to refernces (plain image) small value means no similarity high value means high simlairty. Table 1. presented the PSNR value between input images and output image.

Table 1: PSNR test proposed method

Image	١	٢	٣	٤	٥	٦
PSNR	0.92511	0.89752	0.61318	-0.30622	0.00989	0.64743

The previous table explain the low vlue of PSNR means that no similarity between them.

Differential analysis measures the change in pixels between the encrypted images and the original image. The main idea behind the NPCR test is that if you change a small part of the original image, like a single pixel, the encrypted image should be very different.

Table 2: NPCR test of proposed method

Image	١	٢	٣	٤	٥	٦
NPCRT	99.149%	99.241%	99.351%	99.166%	99.261%	99.346%

Unified Average Changing Intensity (UACI) is the amount by which pixel values change on average during the encryption procedure is measured.

Table 3: UACI of proposed method

Image	١	٢	٣	٤	٥	٦
UACI	31.012%	32.935%	29.715%	30.909%	32.792%	31.912%

The previous table explain the UACI test with accurate values that ressist to deferential attack.

Statistical analysis is using statistical methods involves calculating the histogram analysi, correlation coefficient, and entropy of information between adjacent pixels in color images. The first test is histogram analysis that evaluate the encrypted image must have a uniform distribution and this indicates a high level of security. The results are explain in figue 4. to illustrate the differences between the two sets of images of proposed method.

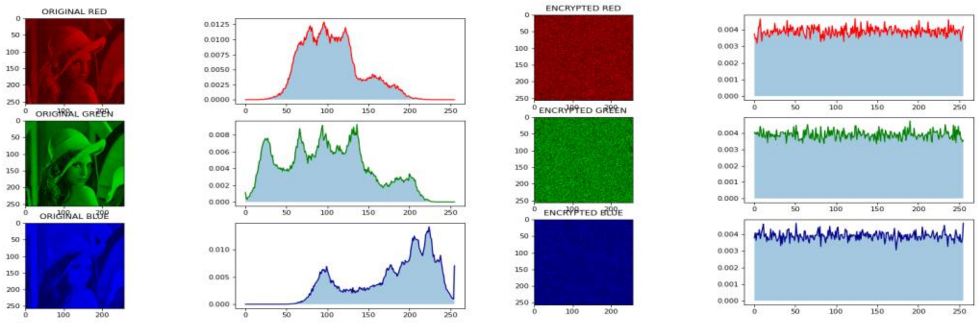

Figure 4: Histogram analysis of proposed method

The result was that there was a uniform distribution of the encrypted image, which was completely different from the non-uniform distribution of the original image. One example has a picture of number one.

The Correlation Coefficient Test represented the distributions of the correlation coefficients for both the plain images and their encrypted images are displayed in figure 5.

The values range between [1,-1] for the correlation coefficients between the two images and neighboring pixels in the three directions (vertical, horizontal, diagonal) to evaluate the strength (strong, medium, weak) and direction (positive, negative) of the linear relationship between the two images. .

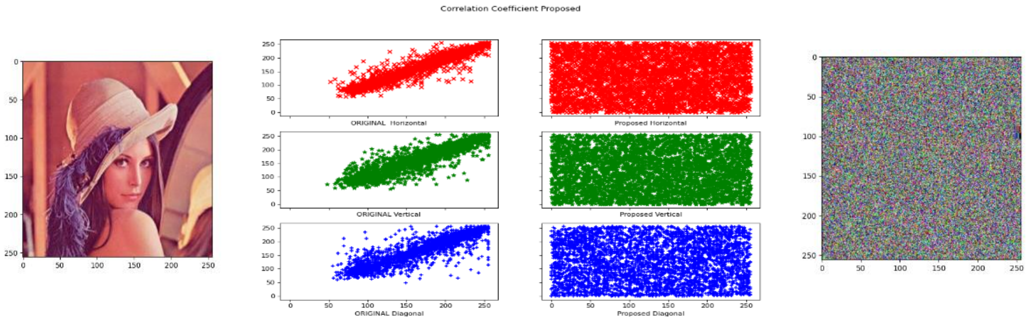

Figure 5: the correlation coefficient of proposed method

The result all of the images and directions in the results have extremely low correlation coefficients, which suggests that the encryption process successfully randomized the pixel values and eliminated any linear relationships between them. A secure image encryption system should have this feature since it makes it difficult for an attacker to decipher the cipher text and deduce the original image.

Table 5: the Correlation Coefficient of proposed method

Image	Horizontal correlation	Vertical correlation	Diagonal correlation
١	0.0116	-0.0213	0.0175
٢	-0.0044	-0.0246	-0.0417
٣	0.0312	-0.0097	0.0271
٤	0.0452	0.0268	-0.0184
٥	0.0179	-0.0084	-0.0160
٦	-0.0133	0.0143	-0.0231

Information Entropy is one of the most useful tests used to conduct an information entropy analysis on both the original color images and encrypted image. The normally used value "8" should be quite close to the grayscale encrypted image's value.

Table 4: Entropy of proposed method

Image	Entropy original	Entropy encryption
١	7.8731	7.992
٢	7.699	7.994
٣	7.6981	7.987
٤	7.1793	7.991
٥	7.6847	7.992
٦	7.6255	7.997

The proposed method achieved a high information entropy value for the encrypted images, which is very close to the typical value, thanks to permutation and substitution.

The structural similarity index (SSIM) is a useful metric for measuring structural similarity the value One indicates the similarity of the two structures of the ideal image; a negative value indicates no similarity; and zero indicates a complete difference in similarity between the original image and the encoded image.

Table 5: structural similarity index of proposed method

Image	١	٢	٣	٤	٥	٦
SSIM	0.02095	0.0173	0.0209	0.0916	0.0142	0.0164

The result indicates that the two algorithms proposed for the encrypted image do not have any structural similarity to the original image.

6. Conclusions

By using an encryption procedure, picture transmission can be properly secured, guaranteeing the authenticity, secrecy, and integrity of the sent image data. IoT systems needed a lightweight approach to overcome resource constraints. This work proposes a hybrid lightweight encryption scheme that combines the RC5 and SPECK algorithms along with a self-key establishment mechanism. To reduce security risks and weaknesses, it is crucial to adopt strong transmission protocols and safe key management procedures. Encrypting and decrypting color images with varying sizes and kernels has been made faster and more secure depending on the number of kernels chosen. There are four rounds to it, and RC5 is the result of one of the two algorithms. The current algorithm does four rounds of input, the

7. References

[1] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar ,"Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home," Electronics, Vol.11,no.7,pp. 1083,2022.

[2] W.Xu, J. Zhang, S. Huang, C. Luo, and W.Li,"Key generation for Internet of Things: a contemporary survey," ACM Computing Surveys (CSUR), vol.54,no.1,pp. 1-37,2021.

[3] O.S.Guma'a , Q.M. Hussein, and Z.T.Mustafa," Dynamic keys generation for Internet of things," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol.18,no.2, pp.4897-4909,2019

[4] R. B Naik and U. Singh,"A Review on Applications of Chaotic Maps in Pseudorandom Number Generators and Encryption," Annals of Data Science, pp.1-26,2022.

[5] M.T.Taha and J.M. Al-Tuwaijari ,"Improvement of Chacha20 Algorithm based on Tent and Chebyshev Chaotic Maps," Iraqi Journal of Science, pp.2029-2039,2021.

[6] U. Zia, M. McCartney, B. Scotney, J. Martinez, and A. Sajjad,"A novel pseudorandom number generator for IoT based on a coupled map lattice system using the generalized symmetric map," SN Applied Sciences, vol.4,no.2,1-17,2022.

[7] M. Kohli and S. Arora," Chaotic grey wolf optimization algorithm for constrained optimization problems," Journal of computational design and engineering, vol.5,no.4,pp. 458-472,2018.

[8] A.R.Kashani, M. Gandomi, C.V. Camp, and A.H. Gandomi," Optimum design of shallow foundation using evolutionary algorithms," Soft Computing, vol.24, pp.6809-6833,2020.

[9] D.Yang, G. Li, and G. Cheng,"On the efficiency of chaos optimization algorithms for global optimization Chaos, " Solitons & Fractals, vol.34,no.4,pp.1366-1375,2007.

[10] G.Kaur and S. Arora,"Chaotic whale optimization algorithm," Journal of Computational Design and Engineering,vol. 5,no.3, pp.275-284,2018.

[11] J.R.Naif, G.H. Abdul-majeed, and A.K.& Farhan,"Internet of things security using new chaotic system and lightweight AES, " Journal of Al-Qadisiyah for computer science and mathematics, vol.11,no.2,pp. 45-52,2019.

[12] R.Vohra and B. Patel,"An efficient chaos-based optimization algorithm approach for cryptography," Communication Network Security, vol.1,no.4, pp.75-79,2012.

[13] Z.Rahman, X. Yi, I. Khalil, and M. Sumi,"Chaos and logistic map-based key generation technique for AES-driven IoT security," In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (pp. 177-193). Springer, Cham,2021.

[14] A.Ali and R.A. L. ,"Random Number Generator based on Hybrid Algorithm between Particle Swarm Optimization (PSO) Algorithm and 3D-Chaotic System and its Application," Iraqi Journal of Information Technology. V, vl.8,no.3,2018.

[15] M.H. Ismael and A.T. Maolood,"Proposed Secure Key for Healthcare Platform," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol.22,no.1,2022.

[16] M.Khan and T. ShahA novel construction of substitution box with Zaslavskii chaotic map and symmetric group," Journal of Intelligent & Fuzzy Systems,vol. 28,no.4,pp. 1509-1517,2015.

[17] R.Hamza and F. Titouna,"A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," Information Security Journal: A Global Perspective, vol.25.no.4-6,pp. 162-179,2016.

[18] N.Balaska, Z. Ahmida, A. Belmeguenai, and S. Boumerdassi,"Image encryption using a combination of Grain-128a algorithm and Zaslavsky chaotic map," IET Image Processing, vol.14,no.6, pp.1120-1131,2020.

[19] S.Arunkumar and M. Krishnan ,"Enhanced Audio Encryption using 2-D Zaslavsky Chaotic Map," In 2022 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE,2022.

[20] H. Faris, I., Aljarah, M.A. Al-Betar,and S. Mirjalili,"Grey wolf optimizer: a review of recent variants and applications,"Neural computing and applications, vol.30,no.2, pp.413-435,2018.

[21] N.M.Hatta, A. M., Zain, R. Sallehuddin, Z. Shayfull, and Y. Yusoff, " Recent studies on optimization method of Grey Wolf Optimiser (GWO): a review (2014–2017) ," Artificial Intelligence Review, vol.52,no.4, pp.2651-2683,2019

[22] H.H.Alyas and A.A. Abdullah, " Enhancement the ChaCha20 Encryption Algorithm Based on Chaotic Maps," In Next Generation of Internet of Things (pp. 91-107). Springer, Singapore,2021.

[23] J.N.Hasoon, B.A. Khalaf, R.S. Hameed, S.A. Mostafa, ans A.H.Fadil, "A Light-Weight Stream Ciphering Model Based on Chebyshev Chaotic Maps and One Dimensional Logistic," In International Conference on Advances in Cyber

Security (pp. 35-46). Springer, Singapore,2021.

[24] M.S.Mahdi, N.F. Hassan, and G.H. Abdul-Majeed, " An improved chacha algorithm for securing data on IoT devices," SN Applied Sciences, vol.3,no.4, pp.1-9,2021.

[25] P.Yadav, I. Gupta, and S.K. Murthy, "Study and analysis of eSTREAM cipher Salsa and ChaCha," In 2016 IEEE International Conference on Engineering and Technology (ICETECH) (pp. 90-94),2016.