Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 3, No. 1, 2025, Pages 1-11
DOI: 10.47831/mjpas.v3i1.75

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE - Computer Sciences

An Image Encryption Method Using Six-Dimensional Hyper Chaotic System and RC6

Mohammed Dhiaa Elden Taha[1*], Khalid Ali Hussein [2]

[*1,2] Department of Computer Sciences, Collage of Education, University of Mustansiriyah, Baghdad, Iraq
[*] Corresponding author E-mail: muhammed84 @uomustansiriyah.edu.iq , dr.khalid.ali68@gmail.com

Article Info.

Article history:

Received
28 December 2023

Accepted
02 May 2024

Publishing
30 January 2025

Abstract

In this study, a hybrid encryption scheme is proposed for secure encryption of various types of data such as images, text, documents, and videos. The scheme employs 6-D chaos to generate unpredictable and highly secure keys for the RC6 encryption algorithm. The proposed method also constructs eight new S-boxes and eight new P-layers to enhance the security of the encryption process. The S-boxes and P-layers are generated using chaotic initial state parameters and stored in arrays for use in the encryption process. The encryption process uses the RC6 algorithm, S-boxes, and P-layers, with eight rounds of encryption. The resulting cipher text is highly secure and suitable for protecting sensitive data. The proposed scheme is evaluated for security and efficiency using various metrics, and the results show that the proposed scheme outperforms existing methods in terms of security and efficiency. The proposed scheme is a promising approach for secure encryption of various types of data in real-world applications. The test results indicate to the highest value of peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI), number of pixel change rate (NPCR) are 7.748 dB, 33.4842 and 99.6082, respectively. While the encryption and decryption speed up 0.1735 and 0.1864 second respectively.

The official journal published by the College of Education at Mustansiriya University

Keywords: Chaotic System, RC6, S-box, P-layer, image Encryption, Hybrid algorithm

1. Introduction

In modern communication and computer networks, multimedia data such as images and videos are increasingly prevalent. Despite the widespread threats and attacks in communication systems, securing this data has become necessary. However, the security of multimedia data presents challenges due to their large volumes and real-time usage requirements. Encryption is a potential solution, but it requires additional computational resources for information processing [1]. Thus, a balance between security and synchronization is essential. To achieve this balance, lightweight and high-speed encryption algorithms are preferable[2]. Block encryption algorithms, such as DES, can be used by treating the data as binary strings. However, these algorithms are computationally complex, and their software implementation is not fast enough for processing large volumes of multimedia data [3][4] .

Encryption is a process that transforms plain text into cipher text, making it unintelligible to unauthorized parties. This technique ensures that the data remains confidential even if it is intercepted by a third party. However, encryption can be computationally intensive, which can cause a delay in processing large volumes of data in real-time applications [5] [6].

To address these challenges, lightweight encryption algorithms have been developed to ensure efficient processing of large volumes of data with minimal computational overhead[7]. One such algorithm is the RC6 encryption algorithm, which is a block cipher that supports variable block sizes, key sizes, and number of rounds. RC6 is known for its speed and resistance to attacks, making it a suitable algorithm for resource-constrained systems. Despite the development of these lightweight encryption algorithms, ensuring security and privacy in the IoT remains a significant challenge[5][6]. This study aims to contribute to the ongoing research in this area by proposing a novel lightweight encryption algorithm that is specifically designed for resource-constrained IoT devices. The proposed algorithm combines the strengths of RC6 ,and used S-box , P-layer for present algorithm and introduces a new technique for key generation that ensures efficient processing of large

volumes of data. The results of this study will contribute to the development of secure and efficient IoT systems that protect sensitive data transmitted over the network.

2. Related Work

The study is centered around the utilization of chaotic systems and RC6 ,and used S-box and P-layer for PRESENT algorithms to construct lightweight algorithms for data encryption and decryption. Various algorithms are applied to achieve different encoding and decoding operations. Mohammed et al[8] This paper proposes an improved S-box and p-layer to address the problem that the primary PRESENT S-box and P-layer have an anti-fixed point. It also gives a brief description of the workings of the PRESENT algorithm. Ten new S-boxes and ten new P-layers are generated at random for the PRESENT algorithms by utilizing 6D chaotic systems. The security research has finally been finished, and the findings show that the chaos S-box and P-layer are excellent for securing sensitive data because they can withstand differential attacks and linear assaults better.Bhel B, and et.al[9] A novel modification of the RC6 algorithm for image encryption is proposed. A permutation-diffusion architecture employing a modified version of cyclic shift is introduced to augment the degree of permutation and diffusion mechanisms of RC6 for image encryption. The proposed method is tested for its security level, as well as its efficiency using image evaluation metrics such as correlation coefficient, number of pixel change rate (NPCR), unified average change intensity (UACI), and runtime analysis. The results indicate that the proposed approach exhibits a low correlation coefficient of -0.043004069 among pixels, and UACI value of 31.9% and NPCR value of 99.6%. Moreover, the encryption time for a lean image with a dimension of 128x128 and in JPEG format was recorded as 5.1 seconds. Mai Helmy, and et al. [10] In this paper, a novel encryption algorithm based on the 3-D Rubik's cube is proposed for 3D encryption of a group of images. The algorithm utilizes RC6 as the first step for separately encrypting multiple images, followed by further encryption with the 3-D Rubik's cube. The faces of the Rubik's cube are formed by the RC6 encrypted images, combining the permutation and diffusion mechanisms of the two algorithms for enhanced security. The proposed algorithm is evaluated for robustness and security using simulation results, followed by transmission over a wireless OFDM system and decryption at the receiver end. The quality of the decrypted images is evaluated using PSNR and correlation tests, with satisfactory results of 45.3784 dB and 0.0043, respectively, and a time encryption of 1,012.1734.

3. Research Methods

3.1 Chaotic System

Chaos is a phenomenon that arises from the complex, aperiodic behavior of deterministic systems, exhibiting high sensitivity to minor changes in initial conditions, known as the "butterfly effect [11][12][13].This property of chaos has been exploited in cryptography, particularly in the context of Shannon's confusion and diffusion concepts. By leveraging the mixing property and high sensitivity to small variations of chaotic systems, chaotic phenomena have shown promise as a potential source of pseudo randomness in information security [2][14][8]. Chaotic maps, which are nonlinear dynamical systems that exhibit chaotic behavior, have been particularly useful in cryptography due to their deterministic nature. Researchers have utilized these properties of chaotic systems to improve the security of various cryptographic applications, including image encryption algorithms, block and stream ciphers[15][14][16]. The six-dimensional hyper chaotic system demonstrates hyper chaotic behavior. Mathematically, it can be expressed as Eq.(1). [17]

$$\begin{aligned}\dot{x} &= -ax + by + cw - dv \\ \dot{y} &= ex - fxz - ge^{v} \\ \dot{z} &= -hz + xy + iv \\ \dot{w} &= -w - yz - gv \\ \dot{v} &= x + jy - iz\end{aligned} \tag{1}$$

$$\dot{u} = kx - Lu - jzw$$

The system described in Eq. (1) consists of six states, namely x, y, z, w, v, u ∈ R, and is characterized by hyper chaotic behavior. The parameters a, b, c, d, e, f, g, h, i, j, k and l are all positive constants[18].

3.2 RC6 Algorithm

The RC6 algorithm is a symmetric key block cipher encryption algorithm designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin in 1998. RC6 stands for "Rivest Cipher 6". The algorithm was developed to replace the aging and insecure Data Encryption Standard (DES) and triple DES algorithms [19]. RC6 is a variable block cipher, which means it can handle block sizes of 128, 192, or 256 bits. It uses a secret key that can be between 0 and 2040 bits in length. The algorithm uses a number of rounds, which is determined by the key size and block size. The rounds use a combination of substitution and permutation operations, which makes the algorithm resistant to various types of attacks such as differential and linear cryptanalysis[9][20].

The RC6 algorithm has four main steps: key expansion, initialization, encryption, and decryption. In the key expansion step, the secret key is expanded into an array of round keys using a pseudo-random function. The initialization step uses the round keys to set up the initial state of the cipher. The encryption and decryption steps use a series of rounds to transform the state of the cipher. The RC6 algorithm has several advantages over other block ciphers. It is computationally efficient, which means it can be implemented on a variety of devices. It is also flexible, allowing for different block sizes and key lengths. Additionally, it has a good security margin and has withstood many years of cryptanalysis [21][22], [23].

4. Proposed Method

The proposed encryption scheme is a hybrid approach aimed at securely encrypting various types of data such as images, text, documents, and videos. Which used block sizes of 128 bits, key lengths of 256 bits, and eight rounds, a reduced number of rounds like eight may be used. This reduction in the number of rounds sacrifices some security in favor of improved performance. The system leverages 6D chaos to generate chaotic values, which are subsequently used to create keys for the RC6 encryption algorithm. 6D chaos is selected due to its high sensitivity to initial conditions, making it a suitable choice for generating pseudo-random numbers used in the cryptographic process. The keys generated for the RC6 algorithm are highly secure as they are derived from an unpredictable source. The proposed scheme constructs eight new S-boxes and eight new P-layers to enhance the security of the encryption process. The S-boxes are generated using the input initial state parameters x, y, z, w, v, u, ∈ R, a, b, c, d, e, f, g, h, i, j, k, and l, described in Eq. (1). The values of xi, yi, zi, wi, vi, and ui are calculated and converted into hexadecimal code. The first five digits, ranging from 7 to 11, are more random and extracted for each value, this ensures that each entry in the S-box array is unique, preventing redundancy and ensuring the effectiveness of the S-boxes in providing non-linearity and confusion. The resulting values are stored in a 16x8 array; this array represents the S-box array used for encoding in RC6. The 16x8 size indicates that there are 16 S-boxes, and 8 indicates the number of round of Rc6. which is used as the S-box array for encoding. Fig.1. shows the process of creating an S-box. Similarly, eight new P-layers are generated using chaotic described in Eq. (1). The values of xi, yi, zi, wi, vi, and ui are calculated and converted into hexadecimal code. The first five digits, ranging from 11 to 15, are more random and extracted for each value. The resulting unique values, obtained after extraction and duplicate removal, are stored in a 64x8 array. This array represents the P-layer used in RC6. The 64x8 size indicates that there are 64 P-layer elements, and 8 indicates the number of round of Rc6. which is used as the P-layer array for encoding. Fig..2. shows the process of creating a P-layer. Overall, this process ensures the generation of a unique and effective S-box and P-layer for RC6, contributing to the confusion and diffusion properties of the cipher, which are crucial for its

security. The use of a hyper chaotic system and the extraction of specific digits contribute to the randomness and complexity of the S-box and P-layer generation process. The encryption process uses the RC6 algorithm, S-box, and P-layer, with eight rounds of encryption. In each round, the data is divided into 16-byte blocks, which are further divided into four blocks of 4-byte size stored in A, B, C, and D. A and D are merged into eight bytes and entered into the first S-box. The resulting values are divided into A and D of four bytes each. Similarly, B and C are merged into eight bytes and entered into the first S-box. The resulting values are divided into B and C of four bytes each. A and B are merged and entered into the first P-layer. The resulting values are divided into A and B of four bytes each. Similarly, D and C are merged and entered into the first P-layer. The resulting values are divided into D and C of four bytes each. The resulting values are entered into the first round of the RC6 algorithm to obtain an encrypted and secure block. This process is repeated over eight rounds to obtain the encrypted (A, B, C, and D) block. Finally, the above process is repeated for all plaintext blocks to obtain the cipher text, which is stored in a text file. The resulting cipher text is highly secure and suitable for protecting sensitive data. Fig.3 depicts the block diagram of the encoding process utilizing the proposed method.

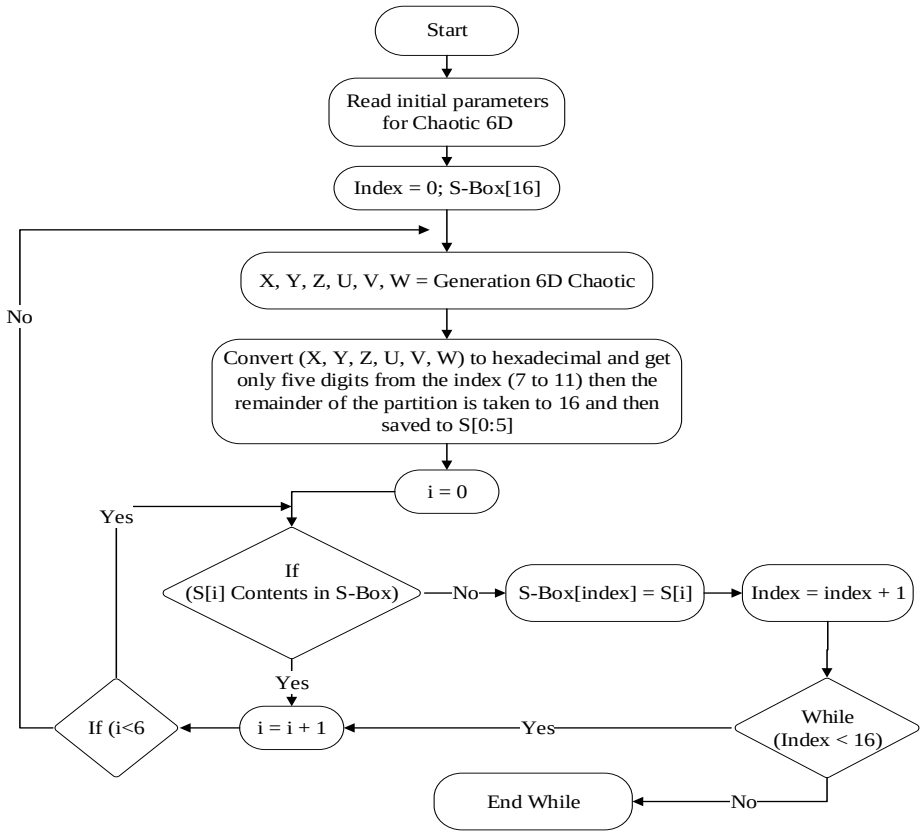


Fig. 1. Shows the process of creating an S-Box.

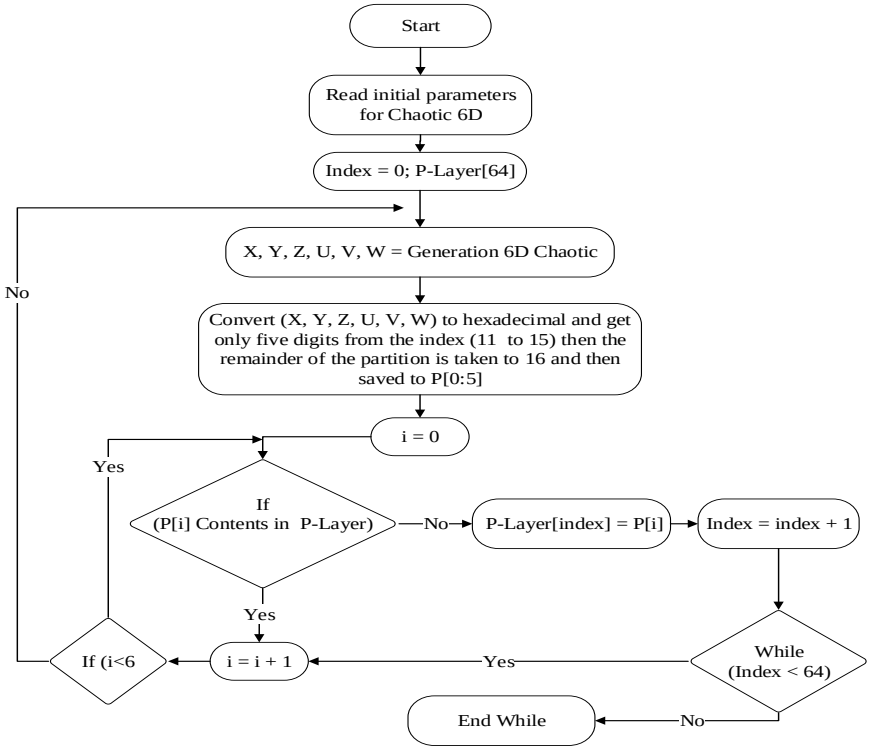


Fig. 2.Shows the process of creating a P-Layer.

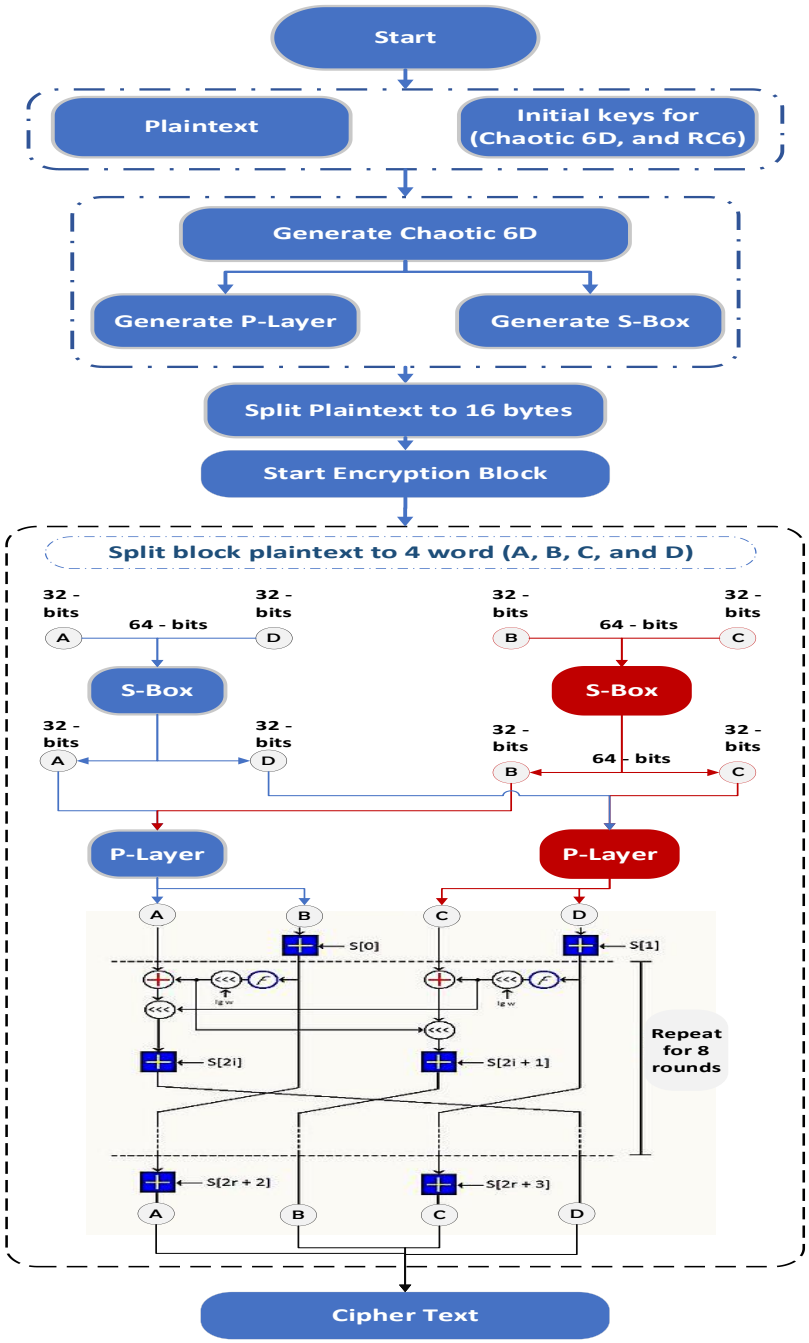
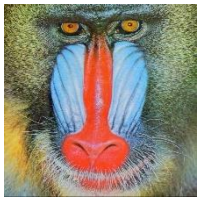


Fig3. Main diagram of proposed method steps.

The decrypting process is an essential step in the data recovery process and involves transforming the encrypted data back to its original form. In the proposed method, the decrypting process is performed by applying the inverse operations of the encrypting process.

5. Results and Discussion

The experimental evaluation of the proposed approach was conducted on a computational system with a 3.30 GHz CPU, 16 GB of RAM, and utilizing Python programming language on the 64-bit Windows 11 Home operating system. The test images used in the experiments were selected from a dataset, including Baboon, Bird, and Lena gray images with color depths of up to 24 bits per pixel for Baboon and Bird, and 8 bits per pixel for Lena. While the proposed system was tested on three images from the dataset, the results presented in this work are limited to three images as depicted in Fig.4.


Baboon
(512 * 512)


Bird
(620 * 413)


Lena grey-scale
(512 * 512)

Fig 4. A set of experimental images

The present cryptosystem's performance is evaluated based on the following criteria:

5.1 *Avalanche criteria (AC)*

Avalanche Criterion (AC) is a critical factor in determining the quality of a block cipher. The AC measures the lack of correlation between the input bits and output sequence by evaluating the effect of a minor change in plaintext on the cipher text. Eq. (1). calculates the AC value, which ranges from 0 to 1, and the ideal value is 0.5 [11]. Table 1. reports the AC test results for the presented cryptosystem.

$$AC = \frac{Number\ of\ Flipped\ Bits\ in\ Cipher\ Text}{Number\ of\ All\ Bits\ in\ Cipher\ Text} \qquad (2)$$

Table 1. Avalanche test

Image	AC
Baboon	0.4995
Bird	0.50024
Lena grey-scale	0.501140

5.2 *NIST Randomness Test*

The study conducted the NIST test, which is a standard for evaluating the randomness of random bits sequence, on the cipher text generated by the proposed encryption algorithm to test its robustness. Table 2, presents the results of the NIST test, which includes 16 different tests, and the P-value is computed for each test. A P-value greater than 0.01 means that the test is passed, indicating that the sequence is random [2]. The table shows that all 16 NIST tests were passed, indicating that the proposed algorithm successfully generated a random cipher text for the Baboon image encryption.

Table 2. NIST Testing for Baboon image encryption

Type of Test	P-Value	Status	Type of Test	P-Value	Status
Frequency Test (Monobit)	0.62696	Ok	**Maurer's Universal Statistical**	0.56697	Ok
Frequency Test within a Block	(0.25652	Ok	**Linear Complexity**	0.02272	Ok
Run Test	0.69523	Ok	**Serial test**	0.0638	Ok
Longest Run of Ones in a Block	0.43326	Ok	**Approximate Entropy**	0.74404	Ok
Binary Matrix Rank	0.71919	Ok	**Cummulative Sums (Forward)**	0.74396	Ok
Discrete Fourier Transform (Spectral)	0.57563	Ok	**Cummulative Sums (Reverse)**	0.89059	Ok
Non-Overlapping Template Matching	0.11091	Ok	**Random Excursions (+1)**	0.42370	Ok
Overlapping Template Matching	0.53420	Ok	**Random Excursions Variant (+1)**	0.05623	Ok

5.3 *Entropy:*

Entropy is a measure of the randomness of data within an image. A high entropy value indicates that the data within the image is more disordered [15]. The entropy can be measured using Eq. (3), where the entropy value should be close to or equal to 8 [11]. Specifically, the equation is given by:

$$\text{Entropy} = \sum_{i} P(S_i) \log_2 \left(\frac{1}{P(S_i)}\right) \quad (3)$$

Here, P(Si) represents the probability of pixel Si (i=0 to 255) in an image. Table 3 displays the entropy value, which is close to 8. A value closer to 8 indicates a lower probability of accidental information leakage. The proposed scheme outperforms previous studies.

Table 3. The results of the information entropy

Method	**Image**	**Entropy**
Our Proposed	Baboon	7.9995
	Bird	7.9985
	Lena grey-scale	7.9959

5.4 *Correlation analysis*

This study examines the correlation analysis between original and encrypted images to evaluate the effectiveness of an encryption scheme. The proposed encryption method maintains low correlation values and outperforms previous methods. Correlation values are calculated using a mathematical formula and are observed to be close to zero, using Eq. (4) [24]–[26], indicating no significant correlation among neigh boring pixels in any of the encrypted images [11][2]. Results show that the proposed encryption scheme is effective in maintaining low correlation values.

$$\text{Correlation} = \sum \left(\frac{(i - \mu i)(j - \mu j)}{\sigma_i \sigma_{ji}}\right) \quad (4)$$

Table 4. The outcomes of the correlation coefficients

Method	**Image**	**Correlation**
Our Proposed	Baboon	0.0018
	Bird	0.000067
	Lena grey-scale	-0.00144
[27]	Tux	− 0.00075
[28]	Lena grey-scale	0.0052
[9]	Lena grey-scale	-0.0063
[10]	Lena grey-scale	0.0043

5.5 *PSNR and MSE analysis*

The evaluation of the quality of the encryption process is based on the Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) values of the original and encrypted images[15], as presented in Table 5 for the Baboon, Peppers, and Bird images. A higher MSE value is indicative of a better encryption result, while a lower PSNR value suggests better encryption quality. In addition, it is worth noting that the decrypted image should have an MSE value of 0 and a PSNR value of infinity.

Table 5. MSE and PSNR values were calculated for both encrypted and decrypted images.

Method	**image**	**Encrypt**		**Decrypt**	
		MSE	***PSNR***	***MSE***	***PSNR***
Our Proposed	Baboon	10913.15	7.7513	0	∞
	Bird	10920.65	7.748	0	∞
	Lena grey-scale	10914.40	7.750	0	∞

[27]	Tux grey-scale	-	8.026	0	∞

5.6 *Differential Attack*

The proposed image encryption approach was evaluated against differential attacks using two metrics: NPCR and UACI, calculated using Eq.(5) and (6) for M×H image size [11][15][2]. The results, presented in Table 6, show that the proposed scheme outperforms previous studies, being highly sensitive to a one-pixel change.

$$NPCR = \left[\frac{1}{W.H}\sum_{i,j} D(i,j)\right].100\% \quad (5)$$

$$UACI = \frac{1}{W*H}\left[\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] * 100\ \% \quad (6)$$

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & C_1(i,j) = C_2(i,j) \end{cases} \quad (7)$$

The variables C1 and C2 refer to the encryption of the original image and the encryption of the original image after the modification of a single pixel, respectively.

Table 6. NPCR and UAC values with comparison to related works

Method	**Image**	**NPCR**	**UACI**
Our proposed	Baboon	99.6085	33.4285
	Bird	99.6082	33.4842
	Lena grey-scale	99.5651	33.4626
[27]	Tux	99.5937	0
[28]	Lena grey-scale	61	52
[9]	Baboon	99.6	31.9

5.7 *Analysis based on Execution Time*

Table 7, compares the encryption and decryption times of the proposed method with previous studies on different images. The results show that the proposed method has faster execution times than previous studies.

Table 7. Encryption and Decryption Time Comparison(S)

Method	**Image**	**Encrypt**	**Decrypt**
Our Proposed	Baboon	1.7506	1.5059
	Bird	0.4998	0.4600
	Lena grey-scale	0.1735	0.1864
[9]	Baboon	5.1	6.5
[10]	Baboon	1,012.17	-

6. Conclusion

The proposed encryption method is designed to provide robust protection of sensitive data in resource-limited environments. By incorporating Chaotic 6D, S-Box, P-Layer, and RC6 algorithms, the method ensures data confidentiality and integrity while preventing attacks. Various tests were conducted, such as the avalanche test, NIST testing, information entropy analysis, correlation

coefficients, MSE and PSNR values, NPCR and UAC values, and encryption and decryption time comparison, which demonstrate the proposed algorithm's effectiveness and suitability for securing data in applications such as financial transactions, personal information, and confidential communications. Additionally, the algorithm's suitability for use in mobile devices and IoT systems underscores its potential for widespread adoption in emerging technologies. In summary, the proposed algorithm's performance demonstrates its significant contribution to data security and highlights the need for further research into encryption methods for safeguarding sensitive data.

Reference:

[1] R. W. Daoud and Y. M. B. I. Al-Khashab, "Design and Simulation of Smart Control System for Internet Traffic Distribution on Servers by Using Fuzzy Logic System," *Al-Kitab J. Pure Sci.*, vol. 2, no. 1, 2018.

[2] A. A. Rashid and K. A. Hussein, "Image encryption algorithm based on the density and 6D logistic map," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1903–1913, 2023, doi: 10.11591/ijece.v13i2.pp1903-1913.

[3] S. Bahrami and M. Naderi, "Image encryption using a lightweight stream encryption algorithm," *Adv. Multimed.*, vol. 2012, 2012.

[4] A. O. Abdalrahman, K. K. Jabbar, A. B. Karim, and O. Y. Abdulhammed, "Secure Communication of the Integrated IoT and Cloud Computing," *Passer J. Basic Appl. Sci.*, vol. 4, no. Special issue, pp. 40–50, 2022.

[5] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight Hardware Architectures for the Piccolo Block Cipher in FPGA," *2020 Int. Conf. Adv. Technol. Signal Image Process. ATSIP 2020*, pp. 1–12, 2020, doi: 10.1109/ATSIP49331.2020.9231586.

[6] J. C. S. Fernandes, "Choosing the Future of Lightweight Encryption Algorithms," 2018.

[7] J. Damodharan, E. R. Susai Michael, and N. Shaikh-Husin, "High Throughput PRESENT Cipher Hardware Architecture for the Medical IoT Applications," *Cryptography*, vol. 7, no. 1, p. 6, 2023, doi: 10.3390/cryptography7010006.

[8] M. D. Taha and K. A. Hussein, "Generation S-box and P-layer For PRESENT Algorithm Based On 6D Hyper Chaotic System," *Al-Kitab J. Pure Sci.*, vol. 7, no. 1, pp. 48–56, 2023.

[9] C. B. B. Aguila, A. M. Sison, and R. P. Medina, "Enhanced RC6 permutation-diffusion operation for image encryption," *ACM Int. Conf. Proceeding Ser.*, pp. 64–68, 2018, doi: 10.1145/3239283.3239308.

[10] M. Helmy, E. S. M. El-Rabaie, I. M. Eldokany, and F. E. A. El-Samie, "3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm," *3D Res.*, vol. 8, no. 4, 2017, doi: 10.1007/s13319-017-0145-8.

[11] R. S. Salman, A. K. Farhan, and A. Shakir, "Creation of S-Box based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 5, pp. 378–389, 2022, doi: 10.22266/ijies2022.1031.33.

[12] Z. M. J. Kubba and H. K. Hoomod, "Modified PRESENT Encryption algorithm based on new 5D Chaotic system," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, no. 3, p. 32023.

[13] E. H. Haseeb, S. A. Kadhim, and A. S. Mahmood, "A Six-Dimensional Hyperchaotic Pseudorandom Sequence for Enhanced Voice Encryption.," *Ingénierie des Systèmes d'Information*, vol. 28, no. 4, 2023.

[14] M. Almazrooie, A. Samsudin, and M. M. Singh, "Improving the diffusion of the stream cipher salsa20 by employing a chaotic logistic map," *J. Inf. Process. Syst.*, vol. 11, no. 2, pp. 310–324, 2015.

[15] A. A. Rashed and K. A. Hussein, "A Lightweight Image Encryption Algorithm Based on Elliptic Curves and Chaotic In Parallel," *2022 3rd Inf. Technol. To Enhanc. e-learning Other Appl.*, 2022, doi: 10.1109/IT-ELA57378.2022.10107924.

[16] N. N. Jasem and S. A. Mehdi, "Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System," *system*, vol. 5, p. 6, 2023.

[17] S. A. Mehdi and Z. L. Ali, "A New Six-Dimensional Hyper-Chaotic System," in *2019 International Engineering Conference (IEC)*, 2019, pp. 211–215.

[18] S. A. Mehdi, "A New Six-Dimensional Hyper-Chaotic System," *2019 Int. Eng. Conf.*, no. January, pp. 211–215, 2021.

[19] A. T. Hashim, J. A. Mahdi, and S. Abdullah, "A Proposed 512 bits RC6 Encryption Algorithm," *Ijcce*, vol. 10, no. 1, pp. 11–25, 2010.

[20] H. K. Verma and R. K. Singh, "Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6," *Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013*, pp. 556–561, 2013, doi:

10.1109/IAdCC.2013.6514287.

[21] M. Mardiana, F. Fajrillah, Y. D. Lestari, and U. Khair, “MODIFICATION of RC6 BLOCK CIPHER ALGORITHM on DIGITAL IMAGE,” *J. Phys. Conf. Ser.*, vol. 930, no. 1, 2017, doi: 10.1088/1742-6596/930/1/012047.

[22] Y. Wanbo, Z. Qinwu, and Z. Qingjian, “Chaotic Image Encryption Method Based on Three-Dimensional Nonlinear System,” *Mustansiriyah J. Pure Appl. Sci.*, vol. 1, no. 3, pp. 1–27, 2023.

[23] A. A. Salih and A. S. Mahmood, “Enhance Key Stage Generation for Developing Kasumi Encryption Algorithm,” vol. 2, no. 4, pp. 104–112, 2024.

[24] M. A. Rajab and K. M. Hashim, “Dorsal hand veins features extraction and recognition by correlation coefficient,” *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 20, no. 4, pp. 867–874, Aug. 2022, doi: 10.12928/telkomnika.v20i4.22068.

[25] M. A. Rajab and L. E. George, “An efficient method for stamps recognition using Haar wavelet sub-bands,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 3, pp. 792–800, 2021, doi: 10.12928/TELKOMNIKA.v19i3.18763.

[26] M. A. Rajab and L. E. George, “An Efficient Method for Stamps Recognition Using Histogram Moment with Haar Wavelet Sub-bands,” *Iraqi J. Sci.*, vol. 62, no. 9, pp. 3182–3195, 2021, doi: 10.24996/ijs.2021.62.9.32.

[27] O. S. Faragallah, H. S. El-sayed, A. Afifi, and S. F. El-Zoghdy, *Small Details Gray Scale Image Encryption Using RC6 Block Cipher*, vol. 118, no. 2. Springer US, 2021.

[28] H. E. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, “Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images,” *2007 Int. Conf. Electr. Eng. ICEE*, 2007, doi: 10.1109/ICEE.2007.4287293.