International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 87-94
Journal homepage: http://iieta.org/journals/ijsse

Color Image Encryption by Using Modified E0 Keystream Generator with Peter De Jong Chaotic Map

Rusul Basheer Bahedh*, Ali Shakir Mahmood

Computer Science Department, College of Education, Mustansiriyah University, Baghdad 10052, Iraq

Corresponding Author Email: rusulbasheer18@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.150110

Received: 6 December 2024
Revised: 29 December 2024
Accepted: 14 January 2025
Available online: 31 January 2025

Keywords:
dice, E0 keystream generator, image encryption, modified E0, Peter De Jong

ABSTRACT

In light of the current developments and the widespread use of the Internet and the sensitive data contained in images, it was necessary to develop new methods to protect data during its transmission. This paper will modify the E0 algorithm key generator by adding two additional records to the original generator to become 6, integrating them with dice to determine the choice of the bit resulting from the key, which increases the complexity and randomness of the generated key, additionally, included Peter De Jong's chaotic map features with image encryption procedure. The proposed method yielded promising results, as demonstrated by the NIST randomness test, confirming the generated key's randomness. Furthermore, the entropy values were close to the ideal value of 8, and correlation coefficients gives a good result close to 1, since all PSNR values are low, about 9.95dB the quality of the image encoding is good. In contrast to MSE around10128.22, all numbers are very high, indicating that the encoded image is very different from the original image. while the NPCR and UACI tests achieved about 99.60% and 33.50%, respectively. Other standard evaluations also confirmed that the proposed approach is robust against brute force attacks.

1. INTRODUCTION

With the rapid advancement of technology and the widespread use of the Internet, digital data protection has become a major concern, especially in applications involving personally identifiable information such as personal photos or medical images [1]. Cryptography has become very important in modern applications, as the secure transmission and storage of images poses fundamental challenges in the field of multimedia communications, and the importance of secure transmission of images in modern applications such as telemedicine, online banking, and surveillance systems due to the sensitive nature of these materials and their susceptibility to unauthorized access [2].

Encryption is crucial to providing highly secure transmission over insecure networks. Cryptography techniques they have been separated into block ciphers and stream ciphers. Blocks of bits are encrypted using block ciphers, whereas stream ciphers encrypt data encrypt with a secret key generator bit by bit [3]. Bluetooth's method of data encryption is E0 stream cipher. Four shift registers for linear feedback (LFSRs) of varying lengths and nonlinear mixer logic (finite state machine) form the basis of this stream encryption. The ciphertext is generated by xor-streaming the key with the plaintext, and the same stream that was used for encryption is used to decrypt in exactly the same way [4, 5]. Many image encryption systems have used the chaotic system due to its dynamic instability, unpredictability, and dynamism, properties that can be exploited in cryptographic applications [6]. One term for a deterministic system is a chaotic dynamical system, which cannot be precisely described and exhibits behavior that appears random due to its delicate reliance on the starting conditions [7]. Chaos-based encryption is a logical choice for secure communication and encryption because of the close connection between the two fields [8]. Chaos theory has been applied to cryptography because of its strong similarities to cryptography, which are defined by its extreme sensitivity to initial states, volatility, unpredictability, and randomness [9]. In this research paper, the keystream generator of the E0 algorithm will be modified by adding two additional records of different lengths and combining them with roll dice to increase the randomness of the generated key, also taking advantage of chaos features of Peter De Jong's map in image encryption, although the E0 algorithm is considered old and has not been used in image encryption applications, most previous research focuses on analyzing attacks, which necessitated the development of this algorithm and the integration of chaotic properties with it to increase the encryption strength and also contribute to enhancing security and computational complexity to resist attacks.

2. RELATED WORK

The studies were chosen because they share a lot of similarities with the subject matter of this study. Although some studies rely on old references, they remain of scientific value due to the lack of use of these methods in modern

research (Table 1). It is still an important point for developing new solutions, which requires the use of these references.

El-Fishawy et al. [10] modified a version of the Bluetooth standard encryption technique, known as E0 stream encryption, was employed. The upgraded model is controlled by incorporating a 5th Linear Feedback Shift Register (LFSR) into the E0 encoder's master key flow generator. By encrypting various images, it has also been shown that the application of certain measuring criteria, such as the highest deviation, non-uniform deviation, and correlation coefficient, improves the coding quality. The higher level of encryption has been proved by the parameter measured on the image encryption attained through increased encryption. This method was limited to grayscale images and did not extend the solution to color images or enhance the complexity of key generation.

Saikia et al. [11] presented a partial bit-plane encryption method that breaks down an image into its component bit-planes. The purpose of the chaotic map Peter De Jong is to encrypt these bit-planes. Bit-plane component coordinates serve as the chaotic map's initial input. Coordinates are changed after a number of iterations, but the bits in the bit-plane are not changed immediately. By permuting the bit-planes, bits can be modified, changing the pixel values in an image. When encryption is done over partial bit-planes, correlation analysis not only decreases computing time but also demonstrates that no information is wasted. This method it focused only on partial bit encryption, which could compromise overall security. The method was limited to grayscale images. Hanchinamani and Kulkarni [12] presented an effective image encryption technique according to a chaotic map of Peter De Jong, RC4 is the proposed stream cipher in this work. Using a Peter De Jong map, the RC4 stream generator's initial keys are produced, it also employed throughout stage of permutation. The values that are pseudo-random for the diffusion and rotation of pixel values are produced using RC4 stream generator. Three steps make up each encryption round diffusion, pixel value rotation, and permutation. In addition to rotating the rows and columns in different directions, confusion between the rows and columns is the basis for the permutation. This method focused on grayscale images. Giesl et al. [13] provided an image encryption method depending on Peter-de Jong attractor map of chaos. Upon moving image into wavelet domain, the wavelet coefficients are modified as necessary. The wavelet transformation is primarily used to decrease the amount of calculation time required for the method of encryption and to achieve a greater or comparable level of the encrypted image's security. This method limited scope as it exclusively targeted grayscale images and required wavelet transformation. Altaay et al. [14] used a lightweight encryption technique in conjunction with the chaotic Peter De Jong map, they suggest an images encryption method with exceptional security. they used Peter De Jong map for the Lilliput algorithm, a lightweight encryption technique, is used to create keys. The proposed method was able to match the historical requirements for transmission images in terms of complexity. The lightweight approach may limit robustness in highly sensitive applications compared to more complex encryption methods and it limited on grayscale image.

Table 1. Comparison between the proposed algorithm and related works

Author's Name	Encryption Method	Result
El-Fishawy et al. [10]	A modified version of the Bluetooth E0 standard encryption technology, adding a fifth linear shift register (5th LFSR) to the main E0 key generator.	Measurements (maximum deviation, irregular deviation, correlation coefficient) showed improvement in encryption quality. The method was limited to grayscale images and did not include color images or improve key generation complexity.
Saikia et al. [11]	Partial bit level coding using Peter De Jong chaos map for level coding. Bit levels are switched to change pixel values in the image.	Reduced computation time and improved correlation coefficient, but the method focused on partial encryption which could reduce overall security, and was limited to encrypting grayscale images.
Hanchinamani and Kulkarni [12]	Peter De Jong's chaos map for generating primary keys for an RC4 generator. Encryption is done in three stages: propagation, rotation of pixel values, permutation.	Improved grayscale image encryption using chaos map, but the method was limited to grayscale images and did not include color images.
Giesl et al. [13]	Using Peter De Jong's chaotic map and applying the wavelet transform.	Reduce computation time using wavelet transform while achieving reasonable security, but the method is limited to grayscale images and requires wavelet transform.
Altaay et al. [14]	Using Peter De Jong's chaos map with the Lilliput algorithm (a lightweight encryption technique) to generate keys.	Improved security for transmitted images with low complexity, but the method was limited to grayscale image applications, and the strength may be limited in sensitive applications compared to more complex algorithms.
Proposed method	6LFSRs E0 keystream generator with dice roll and Peter De Jong chaotic map.	tested on color image, High entropy, ideal metrics, and near-zero encryption correlation confirm security, while near-one decryption correlation ensures integrity. MSE, PSNR indicate noise; encryption is fast, key generation slower due to complexity.

3. E0 KEYSTREAM GENERATOR

A keystream generator based on LFSR, E0 is a component of Bluetooth security systems. Keystream generators based on LFSR consist of a linear bitstream generator and a nonlinear compression function. The bitstream Z is produced by the linear bitstream generator L, upon initialization. The function of compression C uses the output of four Linear Feedback Shift Registers (LFSR). Y=Ck is the key stream would be compression function's output [15]. The feedback polynomials of the four LFSRs have the following lengths: L0 was equal to 25, L1 to 31, L2 to 33, and L3 to 39.

$$P0(x) = x^{25} + x^{20} + x^{12} + x^{8} + 1 \quad (1)$$

$$P1(x) = x^{31} + x^{24} + x^{16} + x^{12} + 1 \quad (2)$$

$$P2(x) = x^{33} + x^{28} + x^{24} + x^4 + 1 \quad (3)$$

$$P3(x) = x^{39} + x^{36} + x^{28} + x^4 + 1 \quad (4)$$

For each of the four LFSRs, an initial value must be entered into the keystream generator and four bits that show the contents of the summation combiner's registers. Four inputs are needed to generate the 132-bit starting value using the keystream generator directly. The parameters that are entered consist of a Bluetooth address with 48 bits and the encryption key C K, 128-bit random integer, master clock 26 bits, as well, Kc key is changed to K'c within the payload key generator [16]. Figure 1 describes the E0 keystream generator engine concept.

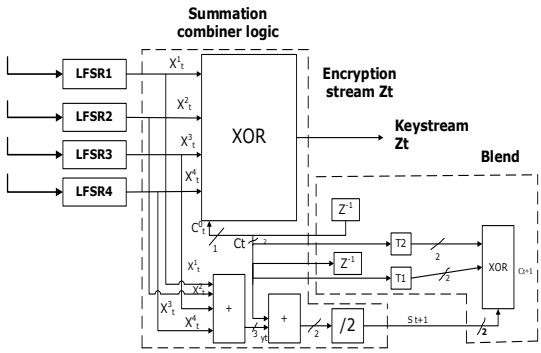


Figure 1. Concept of an E0 keystream generator engine [17]

Logic and Blend, a four-bit finite state machine that does summation, is the foundation of the E0 keystream generator and 4 LFSRs totaling 128 bits in length, as illustrated in Figure 1. All LFSRs are timed once at each clock tick, and the keystream bit is created by XORing their output bits with a single finite state machine output bit. The output bits from the four LFSRs are then added together. The finite state machine's state is updated with this three-bit sum's two most important bits [17, 18].

4. PETER DE JONG CHAOTIC MAP

The difference equations that Peter-De-Jong proposed and named for him are known as the Peter-De-Jong map. Despite its seemingly straightforward appearance, this chaotic system exhibits a number of intricate attractors that correlate to various parameter choices. The map is described as [19]:

$$X_{n+1} = sin(a_{yn}) - cos(b_{xn}) \quad (5)$$

$$Y_{n+1} = sin(a_{yn}) - cos(d_{yn}) \quad (6)$$

Using the parameters control parameters for a system that are chaotic are a, b, c, and d the values of xn and yn give the following two values: xn+1 and yn+1. The first step is to identify a rectangular portion of the plane that spans the image. It is necessary to choose a collection of distinct pixels. After that, calculate a number of map iterations and determine how long it takes to reach each pixel. Next, the mean and self-correlations of the chaotic output sequence should be computed. A selection of shapes from the map by Giesl et al. [13]. In Figure 2, Peter De Jong found this attractor, and the dynamic system where 1.4 for a, -2.3 for b, 2.4 for c, and -2.1 ford has been used for encryption.

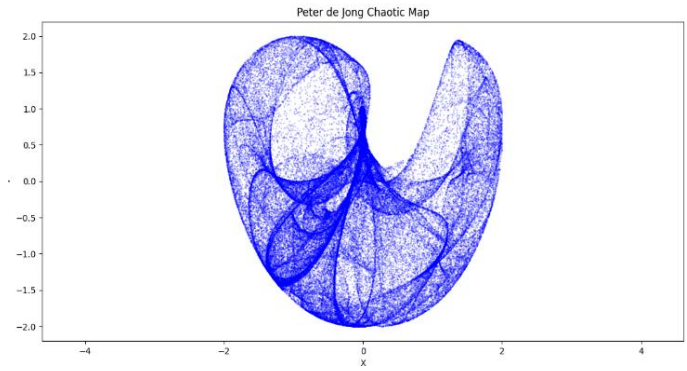


Figure 2. Peter De Jong discovered this attractor, and the dynamical system where a=1.4, b=-2.3, c=2.4, and d=-2.1 is used for encryption

5. PROPOSED METHOD

The proposed encryption method employs a structured approach, for securing color images. The process will be detailed in the following sections.

5.1 Modified keystream generator

The key generator E0 is improved by adding two LFSRs with different initial lengths, where LFSR5 has length 41 and LFSR6 has length 43 as show in Figure 3. The polynomial of these LFSRs is based on previous study [20] as shown in the following equations:

$$P0(x) = x^{25} + x^{20} + x^{12} + x^8 + 1 \quad (7)$$

$$P1(x) = x^{31} + x^{24} + x^{16} + x^{12} + 1 \quad (8)$$

$$P2(x) = x^{33} + x^{28} + x^{24} + x^4 + 1 \quad (9)$$

$$P3(x) = x^{39} + x^{36} + x^{28} + x^4 + 1 \quad (10)$$

$$P4(x) = x^{41} + x^{40} + x^{39} + x^{38} + 1 \quad (11)$$

$$P(x) = x^{43} + x^{42} + x^{38} + x^{37} + 1 \quad (12)$$

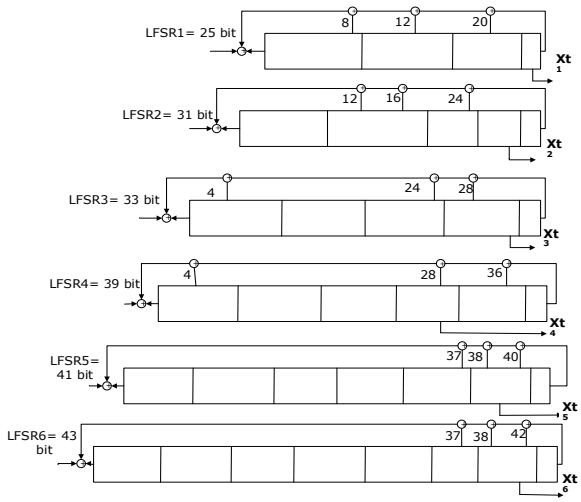


Figure 3. The modified E0 keystream generator with six registers

These six registers are then combined with a die roll where random numbers from 1 to 6 are generated. On each roll, the bit for the key is chosen based on the die roll and the register to take the bit from is chosen according to the polynomial parameters. The generated bits of the key are added together to produce the final key, and so on. Each time, the filling of the six registers is updated after each roll to prevent the repetition of key patterns and to add additional randomness to the resulting key.

5.2 Encryption process

Based on the properties of Peter De Jong's chaotic map, it is used in the image processing process before the encryption process by scrambling the image pixels (Figure 4). The pixels are arranged based on the sequence of the chaotic map, which gives a new arrangement of the pixels. Then the image is reshaped with the same dimensions as the input image to be encrypted using the generated key, as shown in the following steps:

Step 1: Image preparation and input: After loading a color image in RGB format, the image is converted to a collection of pixel values.

Step 2: Peter De Jong map based pixel scrambling: This sequence is used to create a new pixel position arrangement, which confuses the image.

Step 3: Key generation using modified E0 keystream generator: The key is generated by the 6 registers with the dice for each throw. The register is chosen based on the number of the dice, then the registers are updated with each throw to create a random key that is difficult to predict.

Step 4: Encrypt image: Each pixel's binary values are XORed with the altered keystream, and the encrypted pixel values are then stored.

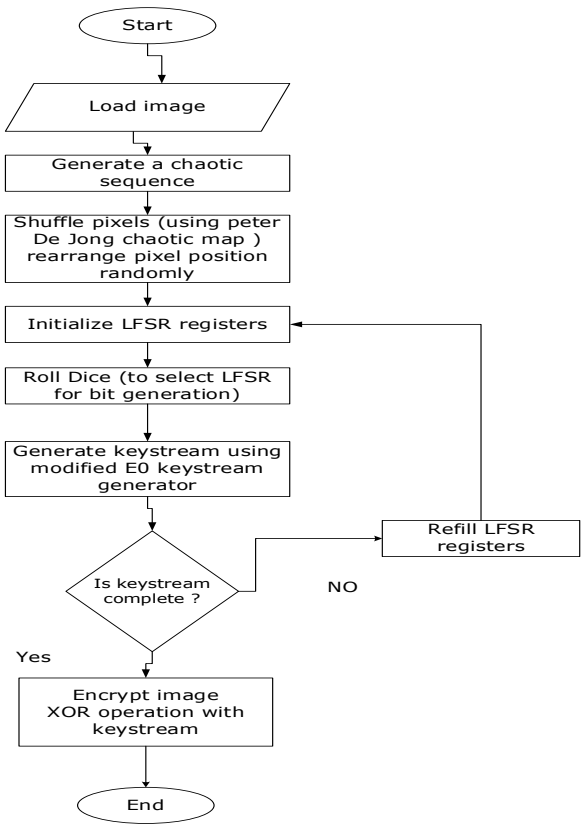


Figure 4. The encryption stages general framework

5.3 Decryption process

The decryption process is done in the opposite way to the previous processes, with the importance of using the same chaotic map parameters and the same key used to encrypt the image, as shown in the following steps (Figure 5):

Step 1: Load the encrypted image and convert it to array of pixels.

Step 2: Decrypt image using the E0 keystream that perform the decryption of image by applying an XOR operation between the encryption image pixels and generated keystream.

Step 3: Generate the chaotic sequence using Peter De Jong map using the same initial conditions (a,b,c,d,x0,y0).

Step 4: Reverse the scrambling (unscrambling) that used to compute the reverse indices to reorder the scrambled pixels back to their original positions.

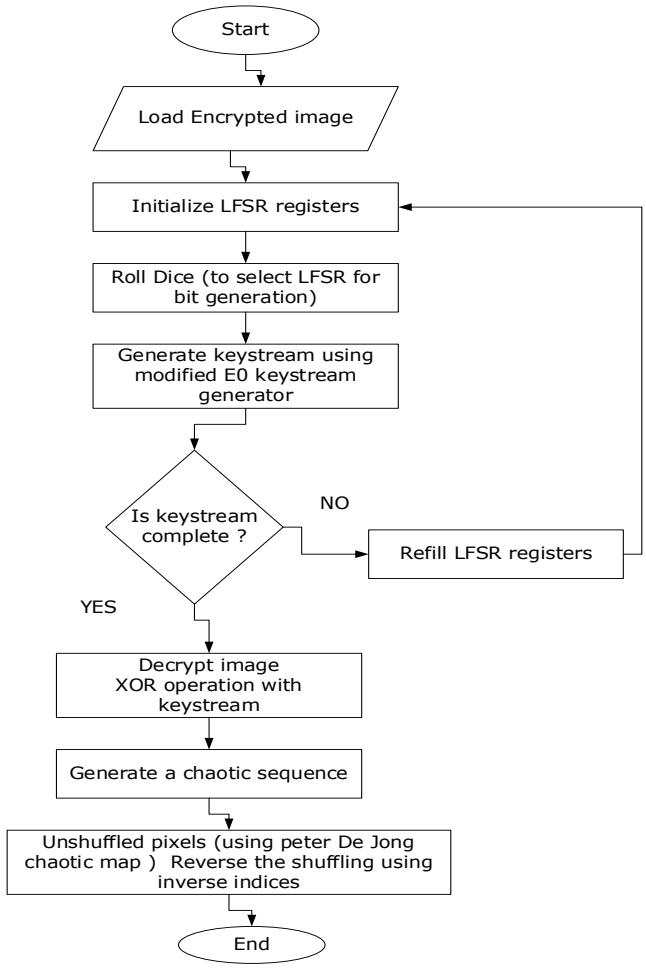


Figure 5. The decryption stages general framework

6. SECURITY ANALYSIS AND RESULTS

The proposed method is calculated and compared with the results of previous research, despite the previous research that used Peter De Jong in the encryption process for grayscale images with map encryption research using Peter De Jong due to the complexity of the color image encryption process in that it contains 3 color channels, and will compare the efficiency of the method. Where used Python 3.9 for Dell laptop Intel(R) Core (TM) 64-bit Windows 11 Pro i7-9850H 16.0 GB of RAM with a 2.60GHz CPU.

6.1 Data set

From images in the database of the USC-SIPI (sipi.usc.edu/db/), the test images were selected. from the Miscellaneous volume. chosen color images that has 24 bits per pixel in different sizes (256*256, 512*512). similar to the one used in previous study [12]. This dataset's images are available in ".tiff" format. The dataset's samples are displayed in Table 2.

Table 2. Data set samples

Image	Dimension	Title
	256*256	Female
	256*256	House
	512*512	Pepper

6.2 NIST standard test

The results of the NIST randomness test all showed positive results, which indicates the randomness of the key utilized throughout the encryption procedure, which indicates ability to use the key in different applications. It appears random and unpredictable, as 0.01 is the minimum randomness in the test. Table 3 shows the results of the randomness that was tested on the key.

Table 3. NIST results

Test	Proposed Method Result
Approximate Entropy Test	Success
Block Frequency Test	Success
Cumulative Sums	Success
FFT Test	Success
Frequency Test	Success
Longest Runs of One's Test	Success
Nonperiodic Templates Test	Success
Overlapping Template of All Ones Test	Success
Random Excursion Test	Success
Random Excursion Variant Test	Success
Linear Complexity	Success
Rank Test	Success
Runs Test	Success
Serial Test	Success
Universal Statistical Test	Success

6.3 Key space analysis

One important metric is the key space for assessing the extent to which the method recommended endures brute force attacks [21]. The key generated by the E0 algorithm is 128 bits. After adding the new registers in the proposed method, the key size is 2^{212}, which is a large size that is resistant to brute-force attacks.

6.4 Information entropy analysis

The most significant indicator of a cryptosystem's strength is its information entropy. Eq. (13) defines a plain image's information entropy. Information entropy should be 8 for an 8-bit truly random image, which would prevent attackers from learning anything of value from the image. According to Eq. (13), the technique achieves better entropy through uniform distribution [22]. The proposed method showed good results close to 8 as shown in Table 4, where it was compared with the results of the study [12]. The proposed method consistently shows slightly higher entropy values, indicating better uniformity and stronger encryption.

$$Entropy\ E(X) = \sum_{i=1}^{x} p(X_i) \log \frac{1}{p(X_i)} \tag{13}$$

Table 4. Information entropy analysis

Image	Proposed Method	Ref. [12]
Female	7.999034	7.996859
House	7.999044	7.997036
Pepper	7.999764	7.997114

6.5 Differential attack analysis

An effective encryption technique should prevent differential attack by making sure that even little changes to the ciphered image differ noticeably from source image. evaluating and analyzing differential attacks with UACI and NPCR. The NPCR measurement establishes the impact of a single pixel alteration on the entire image [23]. The NPCR and UACI value calculation formulas are provided in (14) and (15). The source image (plain image) and the ciphered image of size m×n is compared to calculate the results.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{14}$$

$$\mathrm{UACI} = \frac{1}{WXH}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{15}$$

$$\text{where, } f = \begin{cases} 0, \text{if} C_1(i,j) = C_2 \\ 1, \text{if} C_1(i,j) \neq C_2 \end{cases}$$

Table 5. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI)

Image	Proposed Method	
	NPCR	UACI
Female	99.5854%	33.5197%
House	99.6154%	33.4940%
Pepper	99.6114%	33.4855%
Average values	99.60%	33.50%

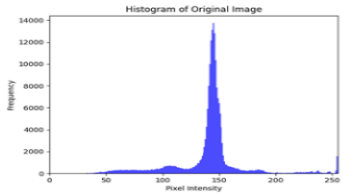
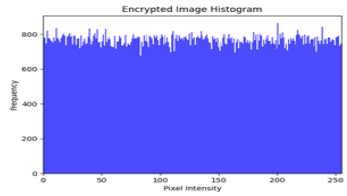
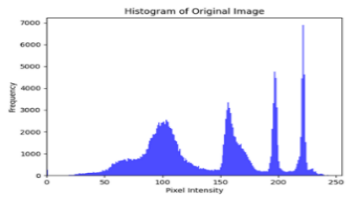
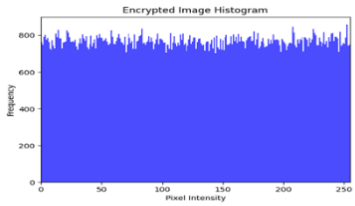
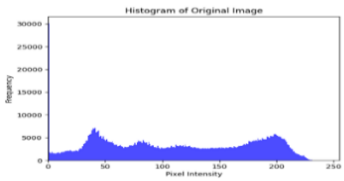
The results are compared with the study [12], where in the study [12] the average values to NPCR and UACI 99.616815% and 33.465988% respectively, where our proposed method the UACI is 33.50% and the NPCR is 99.60%. These results indicate that the proposed method performs similarly to the

research [12], with a slight improvement in NPCR and a very close UACI value (Table 5). This means that it is resistant to attacks.

6.6 Histogram analysis

Analyzing the relative occurrence frequency of various pixel values is done via histogram analysis. Table 6 displays the histograms for the encrypted and plain images. A plain image has a particular histogram pattern. The encrypted image's histogram indicates that the pixel values are distributed as uniformly as possible. This suggests that the proposed method is difficult to attack statistical attack. The results are compared to the study [12], where they used grayscale images with the color images that encrypted using the proposed method. In both methods, the histograms of the encrypted images show a similar distribution pattern, indicating that the proposed method performs well to that in the research [12] for color images.

Table 6. Histogram analysis

Image	Original Image Histogram	Proposed Method	Ref. [12]
Female			
House			
Pepper			

6.7 Time analysis

Time in seconds is used to assess the speed execution for the proposed method that required for the encryption, decryption and key generation procedures, and the proposal shows different performance levels over time, as shown in Table 7.

Table 7. Time analysis

Image	Proposed Method		
	Key Generation Time	Encrypt Time	Decrypt Time
Female	45.4237201 seconds	0.0879967 seconds	0.0950000 seconds
House	45.8482692 seconds	0.0799706 seconds	0.0869901 seconds
Pepper	180.4374454 seconds	0.3250344 seconds	0.3689804 seconds

According to previous study [12], the time required to encrypt the image is 0.000006 While encrypting color images takes longer than grayscale images, as noted in previous study [12], the execution times of encryption and decryption remain efficient, demonstrating the feasibility of the proposed method for practical applications despite the increasing complexity of dealing with color images. Future work could focus on improving the key generation and encryption processes to further reduce the computation time, perhaps through parallel processing techniques or lightweight encryption algorithms, while maintaining the high levels of security achieved.

6.8 MSE and PSNR

This study uses the MSE and PSNR, which are calculated using Eqs. (16) and (17) to determine the difference between the plain and encrypted images.

$$MSE = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} (|I(i,j) - K(i,j)|)^2 \tag{16}$$

$$PSNR = 20X \log_{10} \left(\frac{255}{\sqrt{MSE}} \right) db \tag{17}$$

where, the pixel value of the source (original image) is I (i, j), and the pixel value of the cipher image (encrypted image) at position (i, j) is K (i, j) [24].

MSE values of the encrypted images indicate a significant difference between the encrypted and original images. The proposed method achieves high MSE values, which is expected in a strong encryption technique, as higher MSE values indicate that the encrypted image differs significantly from the original image, making it resistant to cryptographic attacks (Table 8).

Table 8. MSE result for proposed method between encrypted image and original

Image	Proposed Method
Female	6576.1064148
House	8386.1675059
Pepper	10128.2253850

Table 9. PSNR result for proposed method between encrypted image and original image compare with Ref. [12]

Image	Proposed Method	Ref. [12]
Female	9.9511153dB	10.029229dB
House	8.8951683dB	9.211928dB
Pepper	8.0754700dB	9.950633dB

Table 9 shows that the proposed method achieves lower PSNR values compared to the study [12], indicating stronger encryption. Future work could explore methods to optimize PSNR while preserving security.

6.9 Correlation coefficient analysis

An original image's high the correlation relationship between neighboring pixels in the diagonal, vertical, and horizontal directions is one of most crucial features. Two pixels' degree of resemblance is assessed by the correlation test [25]. Estimating the similarities between the encrypted image and the original is made easier with using the correlation coefficient analysis. When both the original and encrypted images match exactly, it should be 1 for the correlation coefficient. The color bytes' correlation coefficients are computed using Eq. (18). The correlation coefficient values in Tables 10 and 11 are becoming closer to "0" and negative, indicating that the plain and cipher images are unrelated [26].

$$Y_{x,y} = \frac{\sum(x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}\,\sqrt{\sum(y_i - \bar{y})^2}} \tag{18}$$

Table 10. Correlation coefficient analysis for encrypted image and original image compare with Ref. [12]

Image	Proposed Method			Ref. [12]		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Female	0.0017297	0.0013836	0.0015573	0.000394	-0.000085	-0.00223
House	-0.0013188	-0.0011178	-0.0006124	0.001395	-0.002920	0.007965
Pepper	0.0002423	0.0002027	0.0003521	0.009052	-0.000347	0.000524

Table 11. Correlation coefficient analysis for decrypted image and original image compared with Ref. [12]

Image	Proposed Method			Ref. [12]		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Female	0.9196361	0.9756294	0.9030987	0.974345	0.921996	0.900548
House	0.9597132	0.9798019	0.9450291	0.978137	0.941437	0.931483
Pepper	0.9819743	0.9812528	0.9720559	0.960712	0.966791	0.940809

The results in Table 10 show that the correlation values of the encrypted images in the proposed method are slightly higher than those in Reference [12] in some directions. While this indicates a slightly lower spread compared to Reference [12], the values remain close to zero, ensuring sufficient encryption security. On the other hand, Table 11 highlights that the proposed method achieves higher correlation values for the encrypted images, confirming better accuracy in restoring the original image.

7. CONCLUSION

The proposed encryption method demonstrated strong performance by augmenting the E0 key stream generator with additional registers and a dice mechanism to improve randomness and diversity. While this increased the key generation time due to the complexity of the operations and register refilling, the results justified the trade-off, with the entropy approaching the ideal value of 8, and the NIST tests confirmed the key randomness. The method demonstrated competitive performance in UACI, NPCR, MSE, and PSNR when compared to previous work. Unlike previous studies that used grayscale images, this method was applied to color images, which are more complex due to their three-channel architecture. The effectiveness of the method in securing color images highlights its robustness against brute force attacks and its potential for practical applications in modern cryptographic systems. Future work could focus on reducing the key generation time by improving computational efficiency, extending the method to high-resolution images and video encryption, and evaluating its resilience against advanced cryptographic attacks to further enhance its applicability.

ACKNOWLEDGMENT

The author would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

REFERENCES

[1] Shnaen, H.J., Mehdi, S.A. (2023). Enhancing key exchange security: Leveraging RSA protocol in encryption algorithm based on hyperchaotic system. International Journal of Safety and Security Engineering, 13(6): 1127-1134. https://doi.org/10.18280/ijsse.130616

[2] Mehdi, S.A. (2021). Image encryption algorithm based on a novel 4D chaotic system. International Journal of Information Security and Privacy (IJISP), 15(4): 118-131. https://doi.org/10.4018/IJISP.2021100107

[3] Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A.M., Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. Multimedia Tools and Applications, 80: 2753-2772, https://doi.org/10.1007/s11042-020-09648-1

[4] Gajbhiye, S., Karmakar, S., Sharma, M., Sharma, S. (2019). Bluetooth secure simple pairing with enhanced security level. Journal of Information Security and Applications, 44: 170-183. https://doi.org/10.1016/j.jisa.2018.11.009

[5] La Scala, R., Polese, S., Tiwari, S.K., Visconti, A. (2022). An algebraic attack to the Bluetooth stream cipher E0. Finite Fields and Their Applications, 84: 102102, https://doi.org/10.1016/j.ffa.2022.102102

[6] Ahmed, M.H., Shibeeb, A.K., Abbood, F.H. (2020). An efficient confusion-Diffusion structure for image encryption using plain image related Henon map. International Journal of Computing, 19(3): 464-473, https://doi.org/10.47839/ijc.19.3.1895

[7] Mehdi, S.A., Kadhim, A.A. (2019). Image encryption algorithm based on a new five-dimensional hyperchaotic system and Sudoku matrix. In 2019 International Engineering Conference (IEC), Erbil, Iraq, IEEE, pp. 188-193. https://doi.org/10.1109/IEC47844.2019.8950560

[8] Shakir, H.R., Mehdi, S.A., Hattab, A.A. (2023). A new method for color image encryption using chaotic system and DNA encoding. Mustansiriyah Journal of Pure and Applied Sciences, 1(1): 68-79. https://doi.org/10.47831/mjpas.v1i1.9

[9] Wan, Y., Gu, S., Du, B. (2020). A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy, 22(2): 171. https://doi.org/10.3390/e22020171

[10] El-Fishawy, N., El-Docanny, I., Soltan, E. (2006). A modification of the Bluetooth E0 stream cipher. JES. Journal of Engineering Sciences, 34(5): 1575-1590. https://doi.org/10.21608/jesaun.2006.111076

[11] Saikia, M., Hazarika, N., Kathing, M. (2014). Partial image encryption using Peter De Jong chaotic map based bit-Plane permutation and it's performance analysis. In Fifth International Conference on Recent Trends in Information, Telecommunication and Computing, Chandigarh, India. https://doi.org/02.ITC.2014.5.5

[12] Hanchinamani, G., Kulkarni, L. (2015). An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher. 3D Research, 6(3): 30. https://doi.org/10.1007/s13319-015-0062-7.

[13] Giesl, J., Behal, L., Vlcek, K. (2009). Improving chaos image encryption speed. International Journal of Future Generation Communication and Networking, 2(3): 23-36. https://article.nadiapub.com/IJFGCN/vol2_no3/3.pdf.

[14] Altaay, A.A.J., Hasoon, J.N., Albahadily, H.K. (2024). Lightweight image encryption based on a hybrid approach. JOIV: International Journal on Informatics Visualization, 8(2): 977-982. https://doi.org/10.62527/joiv.8.2.2757

[15] Alibadi, S.H., Sadkhan, S.B. (2018). A proposed security evaluation method for Bluetooth E0 based on fuzzy logic. In 2018 International Conference on Advanced Science and Engineering (ICOASE), Duhok, Iraq, IEEE, pp. 324-329. https://doi.org/10.1109/ICOASE.2018.8548918

[16] Shaked, Y., Wool, A. (2006). Cryptanalysis of the Bluetooth E0 cipher using OBDD's. In Information Security: 9th International Conference, ISC 2006, Samos Island, Greece. Proceedings. Springer Berlin Heidelberg, 9: 187-202. https://doi.org/10.1007/11836810_14

[17] Suresh, S., Nagarajan, R., Prabhu, R., Karthick, N. (2017). Energy efficient E0 algorithm for wireless transceivers. International Journal of Engineering and Computer Science (IJECS), 6(7): 21982-21985. https://doi.org/10.18535/ijecs/v6i7.15

[18] Jan, D. (2024). Algebraic cryptanalysis of small-scale variants of stream cipher E0 (Master's Thesis, České Vysoké Učení Technické V Praze. Vypočetní A Informačn Centrum.). http://hdl.handle.net/10467/113772.

[19] Wontchui, T.T., Effa, J.Y., Fouda, H.P.E., Fouda, J.S.A.E. (2017). Dynamical behavior of Peter-De-Jong map using the modified 0-1 and 3ST tests for chaos. Ann. Annual Review of Chaos Theory, Bifurcations and Dynamical Systems, 7: 1-21.

[20] Ward, R.W., Molteno, T.C.A. (2012). Table of linear feedback shift registers. Electronics Group, University of Otago.

[21] Xing, Y., Li, M., Wang, L. (2018). Chaotic-Map image encryption scheme based on AES key producing schedule. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, pp. 596-600. https://doi.org/10.1109/DSC.2018.00095

[22] Kanwal, S., Inam, S., Cheikhrouhou, O., Mahnoor, K., Zaguia, A., Hamam, H. (2021). Analytic study of a novel color image encryption method based on the chaos system and color codes. Complexity, 2021(1): 5499538. https://doi.org/10.1155/2021/5499538

[23] Jasim, S.H., Hoomod, H.K., Hussein, K.A. (2024). Image encryption based on hybrid parallel algorithm: DES-present using 2D-chaotic system. International Journal of Safety and Security Engineering, 14(2): 633-646. https://doi.org/10.18280/ijsse.140229

[24] Abd Qasim, O., Golshannavaz, S. (2024). Data protection enhancement in smart grid communication: An efficient multi-Layer encrypting approach based on chaotic techniques and steganography. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 10: 100834. https://doi.org/10.1016/j.prime.2024.100834

[25] Jasim, O.A., Amer, S.R., Hussein, S.F., Mehdi, S.A. (2024). Enhanced image encryption using a novel chaotic system and scramble dithering technique. International Journal of Safety and Security Engineering, 14(5): 1465-1476. https://doi.org/10.18280/ijsse.140514

[26] Parvees, M.M., Samath, J.A., Raj, I.K., Bose, B.P. (2016). A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, IEEE, pp. 1067-1072. https://doi.org/10.1109/ICEEOT.2016.7754851