Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 4, No. 1, 2026, Pages 40-49
DOI: 10.47831/mjpas.v4i1.337

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

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

RESEARCH ARTICLE - COMPUTER SCIENCE

Color Image Encryption Using E0 Keystream Generator with Chaotic Map

Rusul Basheer Bahedh[1], Ali Shakir Mahmood[2]

[1, 2] Computer Science Department, College of Education, Mustansiriyah University

[*] Corresponding author E-mail: rusulbasheer18@uomustansiriyah.edu.iq

Article Info.

Article history:

Received
23 October 2024

Accepted
26 December 2024

Publishing
30 March 2026

Abstract

The development and advancement of technology and the transfer and sending of images over the Internet, protecting images from brute-force attacks has become necessary images from brute-force attacks. Therefore, one crucial step in securing images from intrusion or unwanted access is image encryption. In this paper, the E0 algorithm is used in Bluetooth encryption, but here we will use the keystream generator of this algorithm in image encryption once and use the logistic map and the E0 key stream generator again, and then we will compare the results of these methods. The new methods take advantage of the disordered movement of logistic maps to further improve the confusion and diffusion aspects of image encryption processes. The E0 algorithm can produce a stream that appears to be random, which is then used for image encryption, which leads to higher entropy and lower correlation with the image. Several different tests ware done to evaluate the performance of the encoder scheme generated using E0 algorithm and logistic map, including randomness tests, correlation coefficient analysis parameters, uniform average intensity of change (UACI) , number of pixels change rate (NPCR), and other tests that prove its efficiency. The paper concludes that the E0 algorithm enhanced by the logistic map not only provides more secure and efficient image encryption but also focuses on preserving the confidential information in the image more effectively.

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

Keywords: image encryption, E0, keystream generator, chaotic map, logistic map

1. Introduction

The information leakage occurs as computer networks grow during transmission and storage operations in an endless flow. Because of this, the majority of users of the network are alert of the opportunity for secrecy leakage [1]. Images can be encrypted to stop sensitive data from being viewed or altered [2]. Protected transmission and storage of images is one of the fundamental challenges in multimedia communications. In order to provide highly secure transmission over insecure networks, encryption is of paramount importance. Stream ciphers and block ciphers are two categories of encryption techniques. Blocks of bits are encoded with a block cipher, while stream ciphers encrypt the data is bit by bit using a generator for secret keys [3]. The short-range, high-speed communication technology known as Bluetooth has rapidly expanded across the world. Many wired and wireless devices, including digital cameras, PDAs, desktop and laptop computers, printers, and cell phones, use Bluetooth to communicate. Bluetooth uses stream encryption as a method of encrypting data. Four linear feedback shift registers (LFSRs) of various lengths and a nonlinear (finite state machine) mixing logic form the basis of this stream encoder, E0. To generate the ciphertext, the key stream performs an XOR operation with plaintext. Then the same stream that was used for encryption is used for decryption.[4]According to its characteristics and close similarity to cryptography, which is characterized by its great sensitivity to initial states, volatility, unpredictability, and randomness, chaos theory has been used in the cryptography approach . [5]. In this paper, we use properties of E0 algorithm to encode images and then use it again with the features of a logistic chaotic map to encode color images. Since the E0 algorithm is old and used in Bluetooth encryption, we have introduced it in image encryption and added the logistic map to increase the strength of image encryption in addition to the key generated by the algorithm.

2. Related Works

The studies were selected because they have a lot in common with the topic of this paper. One of the main topics of this study is the use of the E0 key generator with the chaotic logistic map, and some studies on the use of logistic map and E0 in image encryption are described. El-Docanny and others [6] used a modified model of the Bluetooth specification encryption scheme, the E0 stream encryption, provided. A 5th Linear Feedback Shift Register (LFSR) has been added to the E0 encoder's master key flow generator in order to manage the updated model. The use of a number of measurement criteria, including correlation coefficient, maximum deviation, and non-uniform deviation, has also been demonstrated to increase the coding quality by encoding different images. The improved level of encryption achieved by enhanced encryption has been proven by the parameter measured on the image encryption.

Pak and others [7] present a technique for creating an efficient and simple chaotic system through the application of differentiation between the output sequences of two identical one-dimensional (1D) chaotic maps. Performance evaluations and simulations display that the anticipated system can generate a (1D) disordered system with larger chaos domains and better performance from previous chaotic maps. A novel linear and nonlinear encryption scheme based on full mixing is proposed to examine its uses in the encryption of images. Encryption algorithm validity is proven experimentally. Security studies and experiments validate the superior algorithm performance in image encryption and a range of threats. Jin, et all [8] use a DNA encoding and (1D) logistic chaotic map in three channels of YCbCr space as part of the selective encryption technique. According to experimental data, color image encryption is effective; It can withstand differential and brute force attacks and is comparable to RGB and L*a*b* spaces in YCbCr space. The primary difference is the significantly faster encoding and decoding speeds.

3. E0 Keystream Generator

In the Bluetooth Wireless LAN specification, the E0 encryption protocol was established to provide anonymity. When two Bluetooth devices need to communicate securely, they first go through a protocol called key exchange, which ends when both units agree on a shared secret that is used to generate the encryption key (KC). An intermediate key (K_C) is created by combining this private key (KC) with a publicly known salt value (EN RAND) to encrypt the packet. The initial state of the two-level key current generator is then formed by linearly leveraging K_C, Bluetooth address, publicly available values, and a unique clock for each packet [9].It employs four linear feedback shift registers (LFSR), with function C's output serving as their input. The main flow, Y = C(L(k)), will be the output of the pressure function. The four LFSRs have the following lengths: |L0| = 25, |L1| = 31, |L2| = 33, and |L3| = 39. Their feedback limits are as follows:

$$P0(x) = x25 + x20 + x12 + x8 + 1 \quad (1)$$
$$P1(x) = x31 + x24 + x16 + x12 + 1 \quad (2)$$
$$P2(x) = x33 + x28 + x24 + x4 + 1 \quad (3)$$
$$P3(x) = x39 + x36 + x28 + x4 + 1 \quad (4)$$

An initial value must be placed for each of the four LFSRs (128 bits total) in the linear generator [10]. Four bits indicating the values of the registers in the summate must be placed in the keystream generator, with a start value for each of the four LFSR registers. The same key stream generator is used to generate a 132-bit start value from four inputs. The 26-bit master clock bits, 48-bit Bluetooth address, 128-bit random integer, and K_C encryption key are the input parameters. K_C is changed to another key of the same name inside the payload key generator. The factory-configured maximum effective size of this switch can be changed to any multiple of eight, from one to sixteen, using a modulo polynomial operation. Figure (1) shows E0 Stream Cipher Architecture [11].

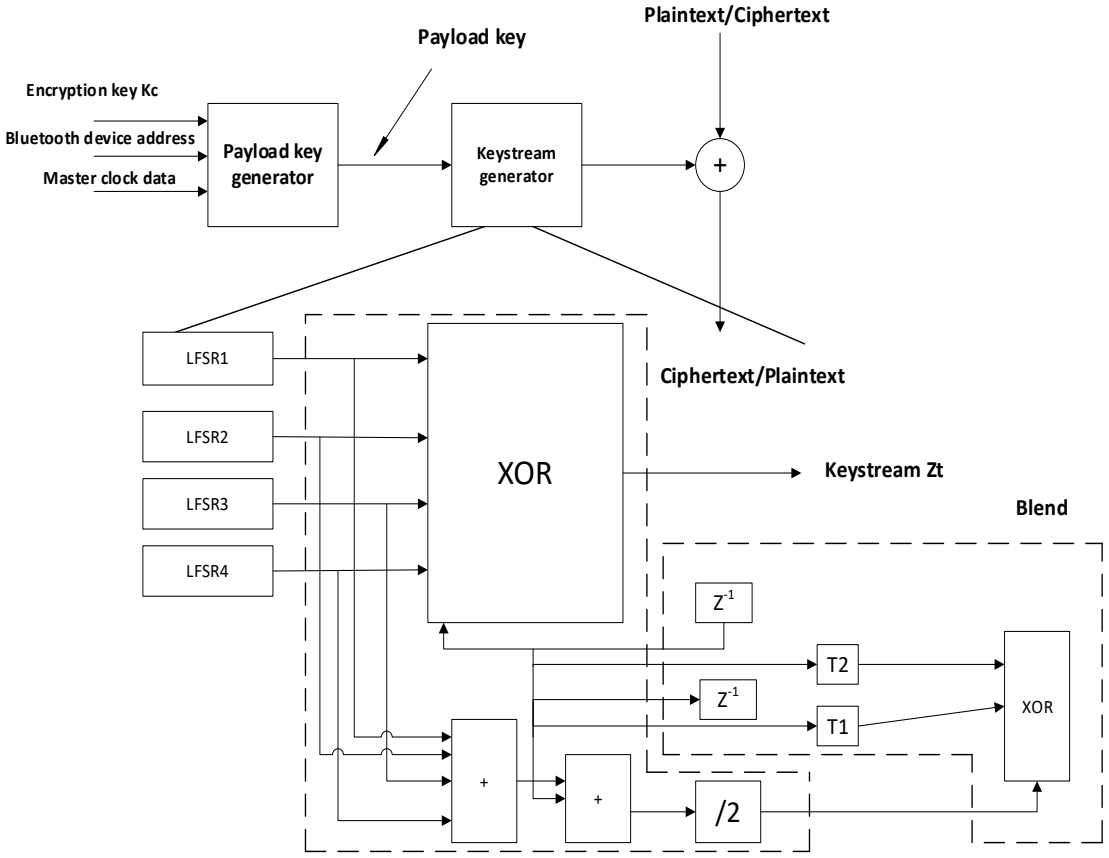


Figure (1) Architecture of the E0 Stream Cipher [11]

4. Logistic Chaotic Map

In 1976, biologist Robert May was the first to present the logistic map[12]. Many branches of studies and technology, chaotic maps have proven to be extremely important. One-dimensional chaotic maps have prominent chaotic properties and are evident. Compared to chaotic maps with higher dimensions, they can be evaluated more quickly. Logistic maps are second-order polynomial maps. The following equation represents the mathematical expression for the logistic maps:

$$x_n + 1 = r x_n (1 - x_n) \qquad (5)$$

where xn+1 is placed next to xn in the sequence and r ∈ (0, 4] is the map parameter. When r lies between 3.57 and 4.0,chaos appears on the logistics map[13]. Figure (2) The branch diagram of the one-dimensional logistic map is displayed [14].

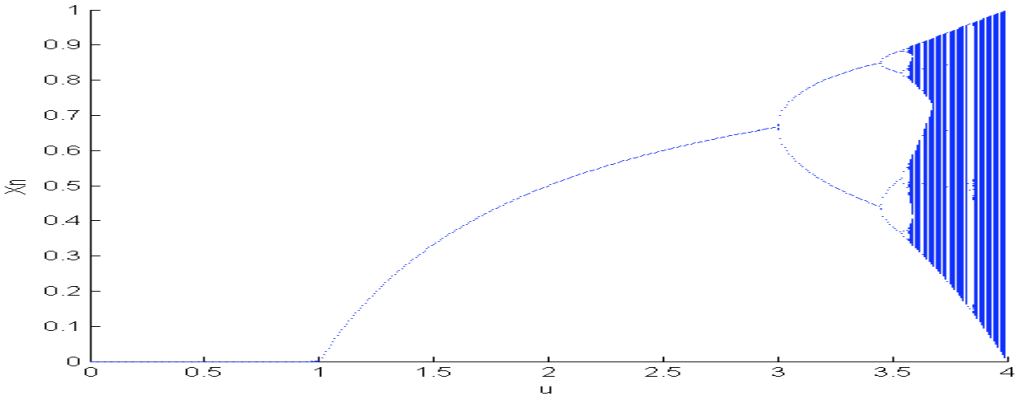


Figure (2) Diagram of Bifurcation on a 1D Logistic Map [12]

5. Proposed Method

Based on the properties of the E0 algorithm and logistic map that are initial state sensitive, they were combined to improve security and efficiency by taking advantage of the properties of the E0 algorithm used in Bluetooth wireless communication with the properties of the chaotic logistic map that shows high sensitivity to initial conditions, which is a required feature in encryption applications. This is accomplished through following steps:

Step 1: Initialize and Input Image: Load color image from the user (RGB format) then Convert the image into an array of pixel values.

Step 2: Logistic Map-Based Pixel Shuffling (Confusion): This sequence is used to generate a new order of pixel positions, effectively scrambling the image.

Step 3: Key generation using E0 (diffusion) algorithm: The E0 keystream generator is employed to produce a pseudo-random keystream for the diffusion of pixels. The diffusion process is performed by using the XOR procedure between mixed pixel values and the resulting keystream. This ensures that any correlation between neighboring pixels is minimized, increasing the security of encryption.

Step 4: Encrypt Image: By XOR each pixel's binary values with the generated keystream and then Store the encrypted pixel values.

Step 5: Decryption: Reverse the previous steps to restore the original image.

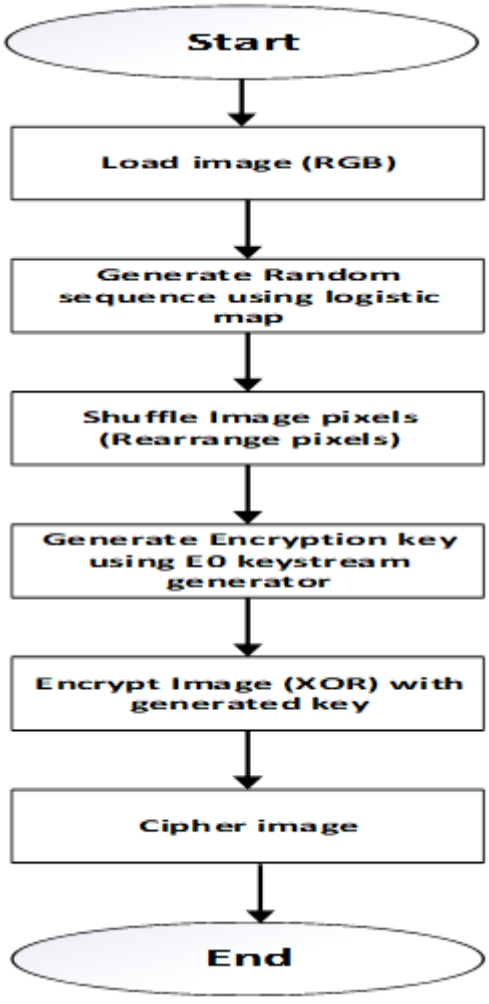


Figure (3) The Encryption Stages General Framework

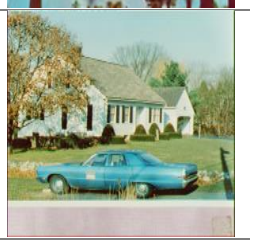
6. Security Analysis and Results

The two models are used to test color images in order to evaluate the encryption performance., the first of which the images were encoded using E0 keystream generator, and the other E0 keystream generator with a logistic chaotic map and we will compare the results. The tests were calculated and worked in Python 3.9 for Dell laptop Windows 11 Pro 64-bit, Intel(R) Core(TM) i7-9850H 2.60 GHz processor, 16.0 GB RAM .

6.1.Data Set

The USC-SIPI images database (sipi.usc.edu/database/) is the test images were selected. from the volume (Miscellaneous). We select images of varying sizes(256*256), (512*512) with 24 bits/pixel for color images. The images from this dataset are available in ".tiff" format. Table (1) shows the samples of the dataset.

Table (1) Data Set Samples

Dimension	Title	Image
256*256	House	
256*256	Tree	
512*512	Lack	
512*512	Car	

6.1. NIST Standard Test

Positive results from all tests, including those conducted via the National Institute of Standards and Technology, reveal that data exhibits legitimate unexpected behavior free of strange patterns or obvious distortions. This is a good result because it shows that the sequence has statistical properties that are consistent with randomization. We can determine whether the data is appropriate for use in applications that require consistent and reliable unpredictability because ,in these experiments, 0.01 is usually the optimal limit of unpredictability. To ensure that the generated key is dependable for use in cryptographic applications. where unpredictability is essential that the requirements are carefully examined and that the key is unpredictable. Table (2) Displays the results of randomization tests performed using the NIST standard.

Table (2) NIST Standard Test

Test	E0 Result	E0 With Logistic Result
Approximate Entropy Test	Success	Success
Block Frequency Test	Success	Success
Cumulative Sums	Success	Success
FFT Test	Success	Success
Frequency Test	Success	Success
Longest Runs of One's Test	Success	Success
Nonperiodic Templates Test	Success	Success
Overlapping Template of All Ones Test	Success	Success
Random Excursions Test	Success	Success
Random Excursions Variant Test	Success	Success
Linear Complexity	Success	Success
Rank Test	Success	Success
Runs Test	Success	Success
Serial Test	Success	Success
Universal Statistical Test	Success	Success

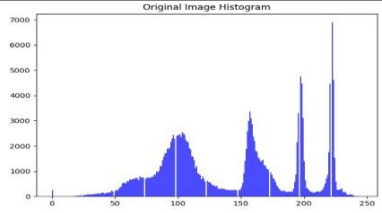
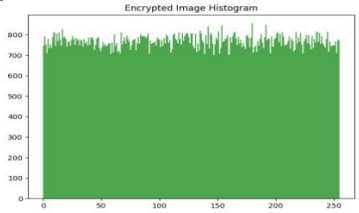
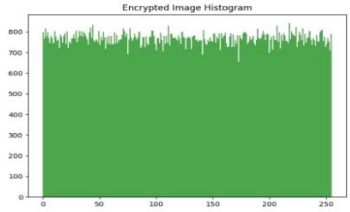
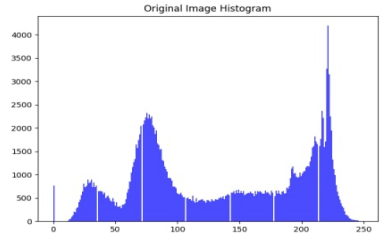
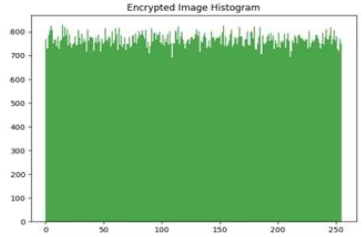
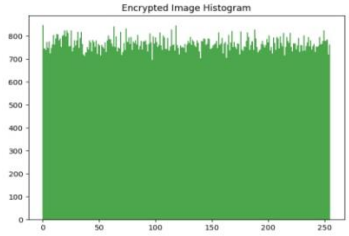
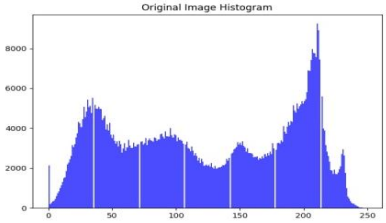
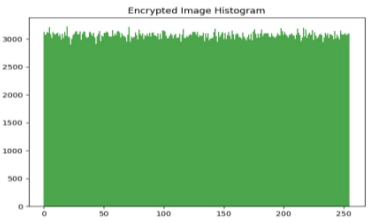
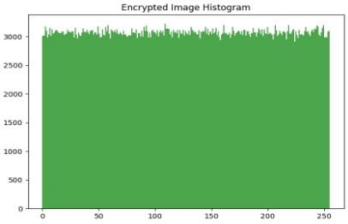
6.3.Key space analysis

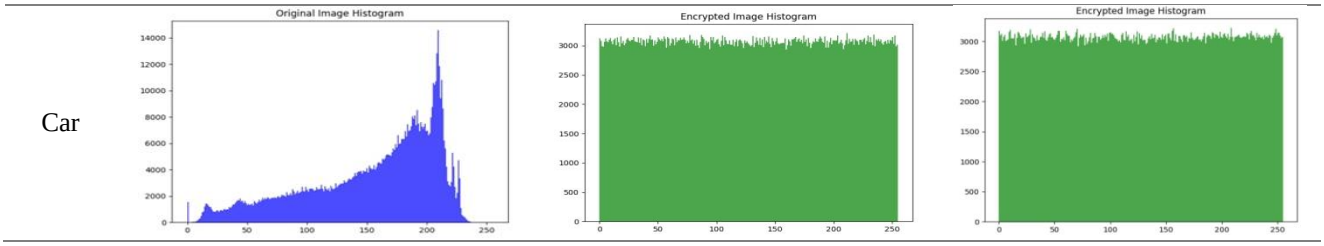
in evaluating the ability of the proposed algorithm to resist brute force attacks, one important indicator is the key space[15]. The E0 keystream generator utilizes a 128-bit key, the key space size is 2128 Given enormous number of possible keys and time and computational resources required to test them all, this large key space makes the cryptosystem very secure.

6.4. Histogram Analysis

The pixel distribution frequencies in images that graphically displayed through histogram. Regarding the properties of the original image, a strong image encoding system should generate a unified image histogram.[16] The table displays the original and cipher image histograms (3).

Table (3) Histogram Analysis

Image	Original Image Histogram	E0 Cipher Histogram	E0 with logistic Histogram
House			
Tree			
Lack			



6.4. Information Entropy Analysis

Entropy is the term used to describe the randomness of the appearance of the encryption image. Shannon's method is used to calculate the entropy of information [17]. The encryption image entropy is nearly eight bits, according to the results, cipher entropy in Table (5), this indicates that the system can withstand entropy attacks. Since X is the total number of symbols, Formula (6) can be used to determine the entropy of a sequence of random information X the chance of occurrence of symbol x is represented by P(x) [18].

$$Entropy\ E(X) = \sum_{i=1}^{x} p(X_i) \log \frac{1}{p(X_i)} \qquad (6)$$

Table (4) Information Entropy Analysis

Image	E0	E0 with logistic
House	7.99890930	7.9990693
Tree	7.99914715	7.9990437
Lack	7.999771807	7.9997736
Car	7.999777951	7.9997798

6.6. Differential Attack Analysis

The effect of single pixel changing in the normal image on encryption unified averaged changed intensity average change intensity (UACI) and number pixel change ratio (NPCR) is used for image analysis[18] [19] . Formulas for calculating the (UACI) and (NPCR) values are presented in (7) and (8). Suppose the encoded images are C and C' before and after changing one pixel in a normal image. Here is a list of equations:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (7)$$

$$UACI = \frac{1}{WXH}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (8)$$

The width of the image is denoted by W, and its height is denoted by H. C1 and C2 refer to the images encoded before and after a single pixel change in the source image.[20], as shown in Table (5).

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

Image	E0		E0 with logistic	
	NPCR	UACI	NPCR	UACI
House	99.58953857%	50.0332123%	99.6103923%	50.0527795%
Tree	99.610392252%	50.04885604%	99.5819092%	49.9702384%
Lack	99.61268107%	49.99994564%	99.6148427%	50.0736376%
Car	99.60861206%	50.0299206%	99.6047974%	50.0398763%

6.7.Correlation Coefficient Analysis

With the aid of correlation coefficient analysis, the similarities between the encrypted images and the plain image are evaluated. When there is a perfect match between the encrypted images and the plain image, the correlation coefficient value should be 1 [18]. Correlation coefficients are calculated by using equation (9).

$$Y_{x,y} = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2}\sqrt{\sum(y_i - \bar{y})^2}} \qquad (9)$$

Table (6) Correlation Coefficient Analysis

Image	E0			E0 with logistic map		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
House	0.957802	0.9697432	0.935456	0.9597132	0.9798019	0.9450291
Tree	0.941134	0.9632729	0.9270436	0.9425248	0.9644732	0.9271981
Lack	0.968942	0.9692218	0.9419612	0.9663005	0.9694929	0.9519500
Car	0.949854	0.9534360	0.9233218	0.9598647	0.9594594	0.9262411

6.8. Time Analysis

The speed performance of the proposed system is evaluated by measuring the time duration in seconds required for encryption, decryption, and key generation procedures, and the proposal displays different performance levels over time, as shown in the table(7).

Table (7) Time Analysis

Image	E0			E0 with logistic map		
	Key Generation Time	Encrypt Time	Decrypt Time	Key Generation Time	Encrypt Time	Decrypt Time
House	7.986649 seconds	0.0973701 seconds	0.1019378 seconds	6.5386045 seconds	0.0817819 seconds	0.0903373 seconds
Tree	7.794038 seconds	0.0931711 seconds	0.1017270 seconds	6.5331361 seconds	0.0827260 seconds	0.0927315 seconds
Lack	31.798139 seconds	0.3794141 seconds	0.3906033 seconds	26.5888548 seconds	0.3250988 seconds	0.3419688 seconds
Car	31.572297 seconds	0.3878624 seconds	0.4536865 seconds	26.8568690 seconds	0.3353171 seconds	0.3331404 seconds

6.9. MSE and PSNR result

The common PSNR, or peak signal-to-noise ratio, is the primary metric used to assess the suggested system for image decoding needs. The primary statistic used to evaluate image coding quality is (PSNR), which compares the standard test image signal-to-noise ratio with the corresponding decoding images .The zero MSE values and infinite PSNR and for each image examined show that the result is in the table. (8) is very good in terms of image decoding criterion. This indicates that the technology is suitable for uses that require high-quality image decoding.

Table (8) MSE and PSNR result

Image	E0		E0 with logistic	
	MSE	PSNR	MSE	PSNR
House	0	∞	0	∞
Tree	0	∞	0	∞
Lack	0	∞	0	∞
Car	0	∞	0	∞

7. Conclusion

The E0 keystream generator used in Bluetooth encryption was used to encrypt color images and the results showed its efficiency in encrypting images. Security testing and simulation experiments show that the proposed algorithm performs well as it has a large key space of (2128) keys. The proposed method when combining the chaotic logistic map with the main current generator E0 showed better effective results than using it alone, as it showed a slight improvement in the results, as the NPCR and UACI values are close to the ideal values (99%) (50%), and entropy is close to the ideal value (8), the histogram is uniform, and respectively. The results indicate that the methods used in encryption were effective and had a powerful resistance to a range of attacks.

8. Reference

[1]. S. Dhall, S. K. Pal, and K. Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic system," *Signal Processing*, vol. 146, pp. 22–32, May 2018, doi: https://doi.org/10.1016/j.sigpro.2017.12.021.

[2]. A. Fakhfakh, "Image Encryption Performance Analysis Using Reversible Logic Gates," Mustansiriyah journal of pure and applied sciences., vol. 2, no. 1, Jan. 2024, doi: https://doi.org/10.47831/mjpas.v2i1.102.

[3]. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," Multimedia Tools and Applications, vol. 80, no. 2, pp. 2753–2772, Sep. 2020, doi: https://doi.org/10.1007/s11042-020-09648-1.

[4]. Y. Shaked and A. Wool, "Cryptanalysis of the Bluetooth E 0 Cipher Using OBDD's," Lecture Notes in Computer Science, pp. 187–202, 2006, doi: https://doi.org/10.1007/11836810_14.

[5]. Y. Wan, S. Gu, and B. Du, "A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding," Entropy, vol. 22, no. 2, p. 171, Feb. 2020, doi: https://doi.org/10.3390/e22020171.

[6]. N. El-Fishawy, I. El-Docanny, and E. Soltan, "A MODIFICATION OF THE BLUETOOTH E0 STREAM CIPHER," JES. Journal of Engineering Sciences, vol. 34, no. 5, pp. 1575–1590, Sep. 2006, doi: https://doi.org/10.21608/jesaun.2006.111076.

[7]. C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing, vol. 138, pp. 129–137, Sep. 2017, doi: https://doi.org/10.1016/j.sigpro.2017.03.011.

[8]. X. Jin et al., "Color image encryption in YCbCr space," 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), vol. 2, pp. 1–5, Oct. 2016, doi: https://doi.org/10.1109/wcsp.2016.7752646.

[9]. S. Fluhrer and S. Lucks, "Analysis of the E 0 Encryption System," Lecture notes in computer science, pp. 38–48, Jan. 2001, doi: https://doi.org/10.1007/3-540-45537-x_3.

[10]. M. Ghasemzadeh, C. Meinel, M. Shirmohammadi, and M. H. Shahzamanian, "ZDD-Based Cryptanalysis of E0 Keystream Generator," Oct. 11, 2008.

[11]. L. Wei, D. Zibin, N. Longmei, and Z. Xueying, "Research and Implementation of a Reconfigurable Parallel Low Power E0 Algorithm," Lecture Notes in Electrical Engineering, pp. 71–78, 2010, doi: https://doi.org/10.1007/978-3-642-05173-9_10.

[12]. H. A. Qasim, "A new Audio Encryption Algorithm Based on Hyper-Chaotic System," Mustansiriyah journal of pure and applied sciences, vol. 1, no. 3, 2023, Accessed: Dec. 24, 2024. [Online]. Available: https://www.iasj.net/iasj/article/287205

[13]. C. Fu *et al.*, "An efficient and secure medical image protection scheme based on chaotic maps," vol. 43, no. 8, pp. 1000–1010, Sep. 2013, doi: https://doi.org/10.1016/j.compbiomed.2013.05.005.

[14]. L. Rui, "New Algorithm for Color Image Encryption Using Improved 1D Logistic Chaotic Map," The Open Cybernetics & Systemics Journal, vol. 9, no. 1, pp. 210–216, Apr. 2015, doi: https://doi.org/10.2174/1874110x01509010210.

[15]. Y. Xing, M. Li, and L. Wang, "Chaotic-Map Image Encryption Scheme Based on AES Key Producing Schedule," vol. 4, pp. 596–600, Jun. 2018, doi: https://doi.org/10.1109/dsc.2018.00095.

[16]. H. R. Huda, S. A. Sadiq, and A. A. Anwar, "A New Method for Color Image Encryption Using Chaotic System and DNA Encoding," Mustansiriyah journal of pure and applied sciences., vol. 1, no. 1, pp. 68–79, Nov. 2022, doi: https://doi.org/10.47831/mjpas.v1i1.9.

[17]. Iqbal, N., Hussain, I., Khan, M.A. et al. An efficient image cipher based on the 1D scrambled image and 2D logistic chaotic map. Multimed Tools Appl 82, 40345–40373 (2023). https://doi.org/10.1007/s11042-023-15037-1

[18]. M.Y. Mohamed Parvees, J. Abdul Samath, I. K. Raj, and B. P. Bose, "A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map," vol. 18, pp. 1067–1072, Mar. 2016, doi: https://doi.org/10.1109/iceeot.2016.7754851.

[19]. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, Jul. 2004, doi: https://doi.org/10.1016/j.chaos.2003.12.022.

[20]. K. Ma, L. Teng, X. Wang, and J. Meng, "Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory," Apr. 2021, doi: https://doi.org/10.1007/s11042-021-10847-7