مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 126) 2024, pp. 10-29

A Lightweight Image Encryption based on Improving LED using Rossler Attractor

Suhad Fakhri Hussein[1]
suhad7242@gmail.com
[1]Ministry of Education, ALRusafa 1 , Baghdad, Iraq

Abstract:

Lightweight image encryption refers to the use of encryption algorithms designed to secure images while considering the limitations of resources, such as processing power and memory, typically found in devices like IoT devices, mobile phones, and embedded systems. This paper proposes a lightweight image encryption based on an LED encryption algorithm and a method for a pseudo number generator called Rossler attractor. Image is split into their three-color bands (RGB) and then partitioned into a block for encryption, a three-equations model (Rossler Attractor) is used for a pseudo number generator, a specific operation applied for producing key scheduled for rounds in LED to seem as random as possible. The experiment explains the objective test to ensure the performance. The contribution of this work is to present an efficient method for lightweight encryption that is applied to color images with a pseudo number generator-based Rossler attractor dependent on a three-dimensional equation. The technique makes it sensitive to initial conditions and could seem like dynamic encryption that resisted many types of attacks. Visually test represented by the histogram of the image before and after encryption is noted that the result is uniform and differs from the input one. The correlation of the output image is a low value which means no correlation is there between pixels horizontal, vertical and diagonal. The similarity test also applied such as MSE, PSNR and SSIM which also explain no similarity between plain and encrypted images. The randomness of generated numbers was tested using the standard test NIST for evaluation of the input key

Keywords: Lightweight encryption Algorithm, LED, Rossler Attractor, MSE, PSNR, SSIM.

Introduction:

The encryption process is an essential tool for protecting sensitive data and information in the digital age. It provides robust protection, ensuring the confidentiality and integrity of data during transmission and storage, building trust between organizations and their customers, and protecting sensitive business and research [1] and [2]. Lightweight encryption algorithms are specifically designed to work on resource-constrained systems. The primary importance of these algorithms lies in their efficiency and ability to encrypt data securely while providing low consumption of limited resources. These limited resources may include the computational capacity of the device, random memory, storage capacity, and communication speed [3]. By improving efficiency and achieving an optimal balance between security and resource consumption, lightweight encryption algorithms can meet the needs of resource-constrained devices, providing robust protection for critical data in these environments. These algorithms achieve many advantages, such as small code size, ease of implementation, high speed, low power consumption, and good levels of security [4] and [5].

One lightweight encryption algorithm is LED, a block cipher designed to provide efficient and secure encryption for resource-constrained devices [6]. To decrypt the image, the reverse operations are applied. This involves using the decryption process of the improved LED algorithm, reversing the shuffling operations, and reconstructing the original image from the decrypted blocks [7]. It's important to note that the security of the lightweight image encryption scheme depends not only on the choice of the underlying encryption algorithm but also on the quality of the key generation, key management, and implementation of the improvement techniques [8]. Additionally, experts should evaluate and test the encryption scheme to ensure its security and suitability.

Previous Studies:

There are several works related to image encryption some of these works are illustrated as follows:

•Mohammed S. Mahdi et al. [9]: suggested encrypting an image with a Hyperchaotic Map and a Cha-Cha symmetric stream cipher. Higher security is achieved by employing the initial seed number, the variance of parameters, and the unpredictable direction of chaotic maps because of the sensitivity features of initial circumstances, pseudo-randomness chaotic maps, and control parameters in chaotic, chaotic maps. By offering a large key space,

the proposed lightweight picture encryption has demonstrated resilience against brute force attacks. Additionally, the proposed lightweight picture encryption can protect against statistical cracking and image insecurity according to the entropy and histogram correlation criteria.

•Wassim Alexan et al. [10]: suggested a two-stage, lightweight picture encryption system. While a Lorenz system is used in the second step, Rule thirty cellular automata are used in the first stage. A few measures are used to assess the suggested encryption scheme's performance. The calculated values of the metrics show that at a relatively low processing time cost, the performance is similar to counterpart techniques from the literature. This feature suggests that real-time image security applications could benefit from the suggested picture encryption approach.

•Mohamed El-Beltagy et al. [11]: suggested a three-stage, lightweight picture encryption system. A PRNG S-Box is used in the second stage, the Rossler attractor for the Rossler system is used in the first stage, and Recamán's sequence is used in the third stage. A few measures are used to assess the suggested encryption scheme's performance. The calculated values of the metrics show that at a relatively low processing time cost, the performance is similar to counterpart techniques from the literature. This feature suggests that real-time image security applications could benefit from the suggested picture encryption approach.

•Hassan Noura et al. [12]: suggested evaluating the NCIES cipher's performance, it demonstrated that this cipher needs more than one cycle to guarantee the required cryptographic features. Here, it explained how an attack using a selected plaintext/ciphertext can breach such a cipher. The problems found in the NCIES cipher and other recent lightweight image encryption techniques are then addressed and resolved by our novel lightweight dynamic key-dependent cipher scheme. Compared to prior chaotic image cipher systems, the suggested encryption is meant to achieve a good balance between the required resources, the security level, and the latency.

•Muntaha Abdulzahra Hatem et al 2023 [13]: suggested a low-power cryptosystem that uses a five-dimensional chaotic map with the current block cipher to securely encode medical photos. The suggested approach was assessed using more than 25 photos from the Open Science Framework (OSF) public database of patients with coronavirus illness 2019 (COVID-19). "Digital Imaging and Communications in Medicine" is what DICOM stands

for. The National Institute of Standards and Technology (NIST), mean square error, information entropy, unified average changing intensity, peak-to-signal noise ratio, entropy, and structure similarity index image are used to demonstrate the effectiveness of the suggested system.

The Lightweight Encryption LED

The Lightweight Encryption Device (LED) is a symmetric key block cipher explicitly designed for lightweight and resource-constrained devices [14]. The characteristics and features of the LED encryption algorithm are represented as follows LED operates on 64-bit blocks, which means it encrypts data in chunks of 64 bits at a time; LED supports key sizes of 64, 128, or 256 bits [15]. The key size choice impacts the security level and the number of rounds used in the encryption process. LED is optimized for lightweight devices, such as embedded systems, Internet of Things (IoT) devices, and other resource-constrained environments [16]. The round operations in each round, LED performs three primary operations: Add Round Key, Step function, and key schedule operation. The key schedule applies various transformations to derive the round keys used in each round of encryption. The security analysis of LED has undergone extensive analysis, including cryptanalysis and evaluation of its resistance against various attacks. It is designed to provide a high level of security for lightweight applications [17]. LED offers a lightweight and efficient encryption solution suitable for constrained devices with limited memory and processing power resources. However, it's important to note that LED security depends on factors such as the key size, the number of rounds used, and the implementation details.

Rossler Attractor

The Rossler attractor is a chaotic system that exhibits complex and unpredictable behaviour. While it can be used as a source of pseudo-randomness, it is not commonly used for key generation in cryptographic algorithms [18]. Several steps should be taken to operate this type of chaotic system, such as specifying the values for the parameters of the Rossler attractor. The Rossler system is defined by three parameters: a, b, and c; select initial values for the variables x, y, and z of the Rossler attractor and iterate the Rossler attractor equations for a specified number of iterations, discarding the initial transient behaviour [19]

The equations for the Rossler attractor are:

$x(t+1) = -y(t) - z(t) \ldots (1)$

$y(t+1) = x(t) + a \times y(t)$ … (2)
$z(t+1) = b + z(t) \times (x(t) - c)$ ... (3)
Here, t represents the iteration step.
The Key Extraction of the generated numbers is represented by extracting bits or values from the Rossler attractor's variables x, y, and z to form the key. Transformations or operations may be applied to convert the attractor's continuous values into a binary or numerical key format suitable for encryption [18]. It's important to consider that the security of the key generated from the Rossler attractor relies on the properties of chaos theory and the ability to conceal the attractor's dynamics sufficiently. However, utilizing a single chaotic system for key generation may not offer the same level of security as established cryptographic algorithms.

Proposed Method

The proposed method is represented by mixing the LED encryption algorithm as a lightweight encryption algorithm with a new key generation method based on the Roessler attractor. The outcome of this proposed method is an image encryption scheme that aims to be lightweight, secure, and capable of providing confidentiality to the image data. By leveraging the chaotic nature of the Roessler attractor for key generation and combining it with the efficient LED encryption algorithm, the researchers aim to achieve a balanced solution suitable for practical applications. Several steps applied for encryption images are shown in Figure 1.

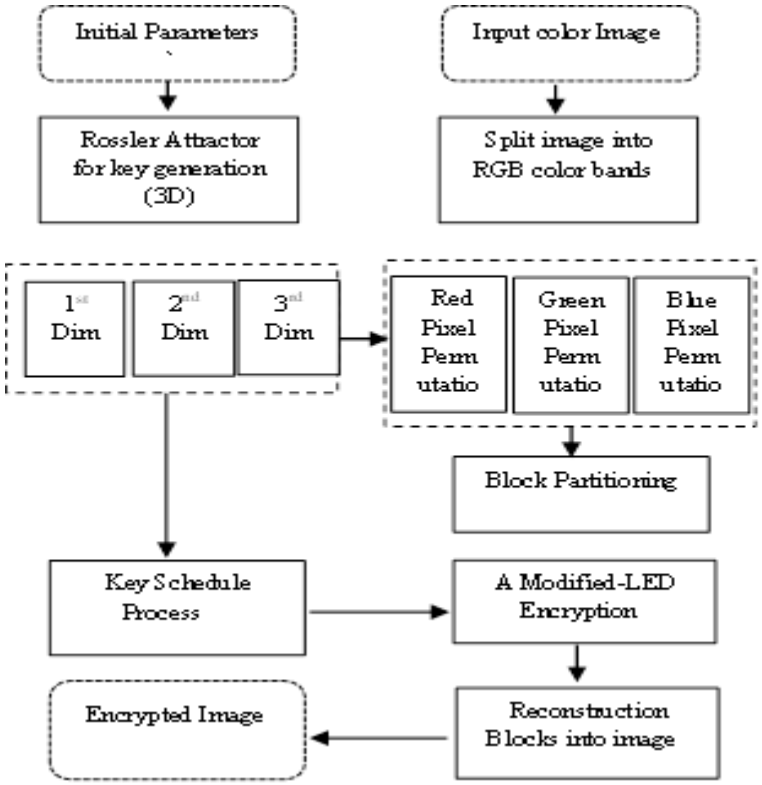

Figure 1: Proposed Encryption Method

The first step in the proposed method is to split the input image into three three-color bands: red, green, and blue. This is a common practice as most digital images are represented using the RGB (Red, Green, Blue) color model. Each color band represents the intensity values of the respective color channel in the image

Figure 2 Splitting color image

Key Generation

The key generation process in the proposed method is represented by using a chaotic map called Rossler Attractor which is a three-dimensional equation system used as a pseudo number generator. These numbers are used in two steps in the proposal, first in pixel permutation and second with the proposed lightweight encryption algorithm LED. Table 1 explains the sample of the proposed number generator. The key generation step is represented using the Rossler Attractor equation for a generated sequence of real numbers using equation1,2, and 3 as explained in Table 1. These numbers are processed by removing the floating point and getting several specific digits after the floating point. These numbers are converted to hexadecimal and merged into one sequence to be used as a key in the encryption algorithm.

Table 1 Key generation samples

Generated numbers		
1st Dim.	2nd Dim.	3rd Dim.
0.138948	0.599747	0.074599
0.674346	0.272691	0.683651
0.410959	0.613536	0.239279
0.374257	0.274141	0.721497
0.447356	0.43539	0.188619
0.624009	0.544448	0.415332
0.129116	0.502597	0.893465
0.390868	0.241195	0.281145
0.52234	0.444655	0.268756
0.175899	0.423182	0.933564
Removing floating point		
1st Dim.	2nd Dim.	3rd Dim.
138947	599747	74598
674346	272691	683650
410959	613535	239279
374256	274140	721496
447355	435390	188618
624008	544447	415332
129115	502596	893464
390868	241194	281145
522340	444654	268755
175898	423182	933564
1st Dim.	2nd Dim.	3rd Dim.
138947	599747	74598
Hexadecimal Number		
1st Dim.	2nd Dim.	3rd Dim.
'21EC3'	'926C3'	'12366'
'A4A2A'	'42933'	'A6E82'
'6454F'	'95C9F'	'3A6AF'
'5B5F0'	'42EDC'	'B0258'
'6D37B'	'6A4BE'	'2E0CA'
'98588'	'84EBF'	'65664'
'1F85B'	'7AB44'	'DA218'
'5F6D4'	'3AE2A'	'44A39'
'7F864'	'6C8EE'	'419D3'

'2AF1A'	'6750E'	'E3EBC'

Pixel Permutation

The pixel permutation is applied to each colour band (red, green, and Blue) by generating a pseudo number equal to the number of pixels in the image and then sorting these numbers to get the indices as the reordering positions. As mentioned in the previous section the generated pseudo-random numbers are operated by the Rossler Attractor method for each pixel in the image (regardless of the color band - red, green, or blue). This pseudo-random number could be any number between 0 and the total number of pixels in the image. The second step is sorting the numbers that have been generated Reordering Pixels: The sorted pseudo-random numbers now represent the new positions or indices of the pixels. By applying this sorting order to each color band (red, green, and blue) separately, the pixels' positions are reordered accordingly. This technique essentially shuffles the pixels in the image while maintaining the correspondence between the color bands. The final result of this process will be a permuted version of the original image, with the pixel order altered based on the generated pseudo-random numbers. The visual appearance of the image will be different from the original, but the pixel values themselves will remain unchanged. This process is explained in Figure 3.

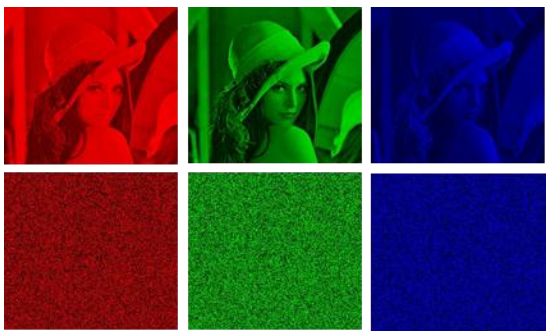

Figure 3: Color-band Permutation Process

Partitioning into Blocks

After splitting the image into its color bands, they are combined or merged into one array. This means that the individual arrays representing the red, green, and blue color channels are concatenated to create a single data array that contains all the color information. The merged array is then partitioned into specific-size blocks for encryption. This step involves dividing the data array into smaller fixed-size blocks. The exact size of these blocks may vary based on the encryption method's requirements or the research's proposal. During the partitioning process, the last block may have a

size smaller than the others, especially if the total number of pixels in the image is not an exact multiple of the block size. To ensure that all blocks have the same size for consistent processing during encryption, padding zeros are applied to the last block. The block partition is explained in Figure 4

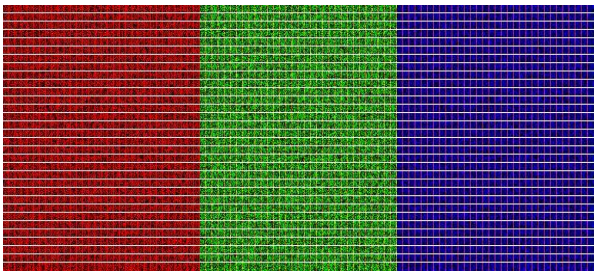

Figure 4: Blocks Partition Process.

By following these steps, the proposed image encryption method aims to ensure that the image data is divided into manageable blocks and encrypted securely, providing confidentiality and protection against unauthorized access. The utilization of the Roessler attractor for key generation and the LED encryption algorithm for encryption helps achieve a lightweight yet robust image encryption technique.

Modified LED Encryption

64-bit plaintext block p is conceptually arranged in a 4×4 matrix of 16 nibbles (4- net of GF (24) with an underlying polynomial for finite field multiplication as (X4 ⊕ X ⊕ 1). The proposed key schedule used in Modified LED is represented by getting the generated sequences of the Rossler Attractor. The main block diagram is explained in Figure 5

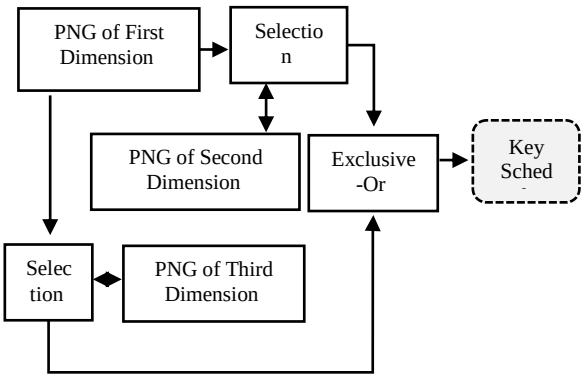

Figure 5 The main block diagram of the proposed method

The LED encryption algorithm typically consists of a fixed number of encryption rounds, where each round applies a series of cryptographic

operations to the input data (plaintext) using a specific set of encryption keys. The number of encryption rounds used in the algorithm contributes to the overall security and complexity of the encryption process. The LED encryption round is a single iteration of the LED encryption algorithm, where the plaintext is transformed through a series of cryptographic operations using specific encryption keys to generate the ciphertext. The process is repeated for multiple rounds to enhance the security of the encryption scheme. The block diagram of the LED block cipher encryption method. The main stages of the proposed method are as follows: add a round number (add Round Key) method mixes the subkey that is generated using Rossler attracter with the state using binary Exclusive-Or (xor) operation (⊕), the step stage updates the state by applying a variable number of rounds from 1 to 8 depending on the generated number, each round consists of four operations, add numbers, sub-cells, shift rows and mix columns as shown in Figure 6

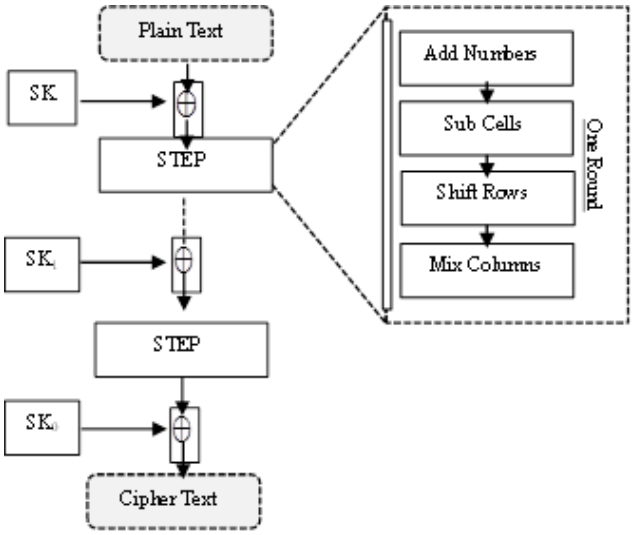

Figure 6 The block diagram of the LED

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 126) 2024, pp. 10-29

Block Construction

All states in each block are merged to produce an encryption block, then the total block will concatenate to construct the encryption image that is equal to the size of the input image. The partition of images into blocks makes a chance to process them in a parallel form which increases the efficiency of the proposed algorithm.

Experimental Results

The experimental result tests the proposed algorithm to find the efficiency when used in applications. A successful encryption algorithm should produce encrypted images with histograms that are vastly different from those of plain images. The reason is that a similar histogram may indicate that the encrypted image still possesses recognizable patterns or features, which could potentially lead to information leakage or cryptanalysis**.**

Histogram test

It is important to note that the histogram test is just one evaluation metric, and a robust image encryption algorithm should undergo a battery of security tests and analyses to ensure its strength against various attacks [19]. In the context of your proposed method, Figure 6 likely represents the histograms of the plain images and the corresponding encrypted images of the standard images used for testing, such as woman, Baboon, Pepper, Lenna, car, and house images. By comparing the histograms, researchers can gain insights into how well the proposed method preserves the statistical properties of the images during encryption, which is crucial for assessing its effectiveness as an image encryption technique. The experiment results of the implementation of the proposed method are represented by testing it on a set of standard images, woman, Baboon, Pepper, Lenna, car, and house images respectively. The first test is the histogram test which is applied to plain and encrypted images as shown in Figure 7.

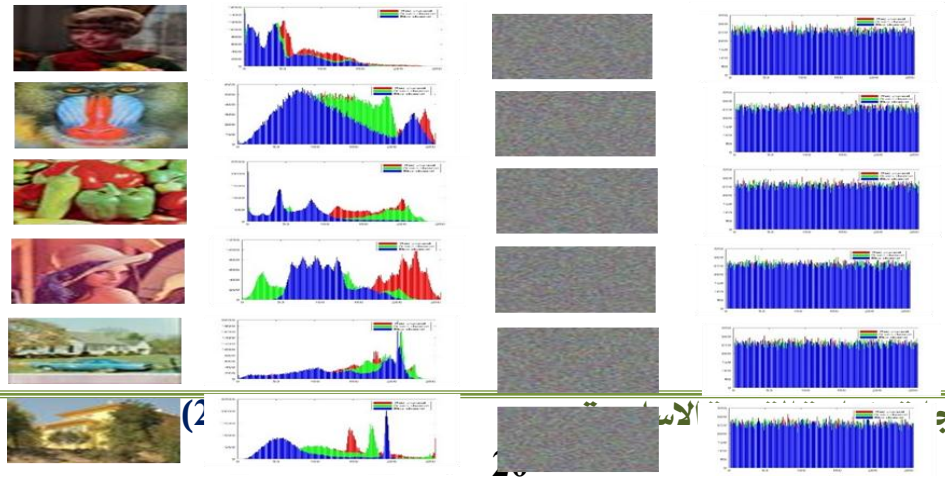

Figure 7 Images visual test

A uniform histogram implies that the pixel intensity values are distributed evenly across the entire range of possible values (0 to 255 for an 8-bit grayscale image or each color channel in a color image). In the context of image encryption, a uniform histogram is desirable and indicates that the encryption process has randomized the pixel values effectively.

Correlation test

The second test is the correlation test which is applied to the three-color band of an input image and output image (encrypted image) [20]. The correlation test is another evaluation method used to analyze the relationship between the pixel values of the original (plain) image and the corresponding encrypted image. The goal of this test is to assess how well the encryption process has randomized the pixel values and reduced any visible correlations between neighboring pixels. The correlation test is performed in three directions: horizontal, vertical, and diagonal. In a horizontal correlation test, each pixel in a row is compared to its neighboring pixel on the right side. The goal is to determine if there is any visible correlation or pattern between adjacent pixels along a row, in a vertical correlation test, each pixel in a column is compared to its neighboring pixel below it, and in diagonal correlation test involves comparing each pixel to its neighboring pixel in a diagonal direction. All three directions test Visualization in Figure 8

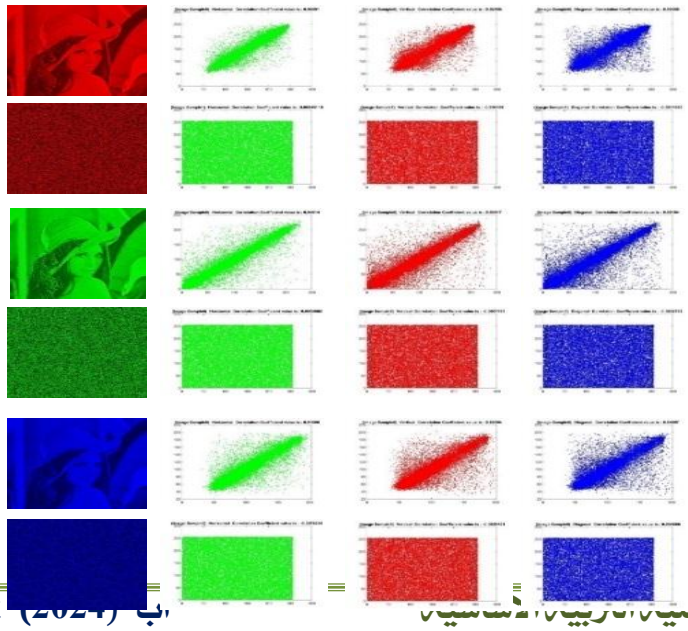

Figure 8 Correlation test for Lenna image

The encrypted image should exhibit low correlation values in all three directions (horizontal, vertical, and diagonal), which suggests that the encryption process has effectively randomized the pixel values. This is an essential property of a strong encryption algorithm as it prevents attackers from identifying any discernible patterns or structures in the encrypted image. The correlation test provides insights into the diffusion aspect of the encryption algorithm. Diffusion ensures that a change in one pixel of the plain image affects a large number of pixels in the encrypted image. A good encryption algorithm should scatter the pixel relationships in such a way that any changes in the input image result in a completely different pattern in the encrypted image. Figure 8 explains all results of correlation in three directions horizontal, vertical, and diagonal for input images as well as measured after encryption and as shown A, B, and C respectively which have been applied on all images used for all existing three color-pandas RGB.

Objective Tests

There are several tests used for evaluating the similarity and dissimilarity between two images (plain image and encrypted image), particularly focusing on encrypted images compared to their original counterparts. The tests mentioned include; Mean Square Error (MSE) which calculates the average squared difference between the pixel values of the original and encrypted images. A higher MSE value indicates higher dissimilarity between the images. The second test is the signal-to-noise ratio (SNR) which is calculated based on MSE and represents the ratio of the signal power (pixel values of the original image) to the noise power. A higher SNR value suggests a higher image quality [21]. The third test is the Peak Signal-to-Noise Ratio (PSNR) which is similar to SNR but uses a logarithmic scale. It is a commonly used metric to evaluate image quality, and a higher PSNR value corresponds to better image quality. The fourth test is SIM which is used to find the interior correlation between image objects. It likely measures the similarity of the structures and patterns within the images. The last test is the Entropy Test which measures the amount of information or randomness in the encrypted images. If the entropy value is near the maximum required bits (8 bits), it indicates that the encryption process preserves the information in the image. Table 4 provides detailed results of these tests for image set 1, allowing for a

comprehensive evaluation of the encrypted images' quality and similarity to the original images**.**

Table 4 Image quality test for data set 1 using a proposed encryption algorithm

#	MSE	PSNR	SNR	SIM	Entropy
1	8760.50837	0.00454	2.01572	117.324	7.98129
2	8046.58102	0.00512	1.78946	103.971	7.72136
3	9885.70665	0.00444	1.54534	151.293	7.96683
4	9308.74693	0.00466	1.87381	114.079	7.71967
5	8283.91159	0.00485	1.87665	128.197	7.74252
6	9617.87948	0.00485	1.60606	108.261	7.61548
av	8983.88901	0.00474	1.78451	120.521	7.79119

The previous table explains the value of each test and that each of these tests serves a specific purpose in assessing image quality and similarity, and they are used to gauge the effectiveness of encryption techniques in maintaining image integrity and confidentiality. Depending on the specific application, different tests may be more relevant or important**.**

Key Generation Analysis

The key generation method represented by using the Rossler attractor method for key generation can add a layer of randomness to the encryption process, which is important for security. Chaotic sequences can be difficult to predict or reproduce without knowledge of the initial conditions and the exact equations used to generate them, making them suitable for cryptographic applications. Based on the information provided, it appears that the key space analysis has been performed to assess the strength of the encryption scheme against brute force attacks. The key space represents the total number of possible combinations of key values that can be generated using the Rossler attractor method with the given initial parameters; the three initial variables x_0, y_0, z_0, and the three constants; a, b, c each with a precision of $10^{14.}$ The calculated key space is $(10^{12})^8 \approx 10^{96}$ which is greater than 2^{128}, and is an extremely large number [22]. A key space of this magnitude makes it infeasible for an attacker to perform a brute force attack, where they systematically try every possible key until they find the correct one. The size of the key space exceeds the recommended threshold of 2^{128}, which is considered a minimum requirement for cryptographic key space strength to resist brute force attacks effectively. The encryption scheme utilizing keys generated from the Rossler attractor method can be considered highly secure

against brute force attacks. With such a large key space, the likelihood of an attacker guessing the correct key by trial and error is practically impossible within a reasonable timeframe, making the encryption and decryption operations robust and reliable.

Time-Consuming of Image Encryption

In cryptographic applications, there is a need to balance between security and speed. While strong encryption is vital for data protection, excessively long processing times might be impractical in some real-time or time-sensitive scenarios. Therefore, performance optimizations are often considered to maintain an acceptable level of security while keeping encryption and decryption times within reasonable limits. The time consumed for applying the proposed algorithm is measured and explained in Table 2 for the encryption of three sizes of image 128×128, 256×256, and 512×512 in encryption and decryption time.

Table 2: Time-consuming for the first hybrid encryption/decryption algorithm

	Image size					
	128x128		256x256		512x512	
	Enc. Time (MS)	Dec. time (MS)	Enc. Time (MS)	Dec. time (MS)	Enc. Time (MS)	Dec. time (MS)
1	0.00180	0.0080	0.0049	0.00200	0.01650	0.00520
2	0.00140	0.0040	0.00550	0.00240	0.01260	0.00520
3	0.00120	0.0020	0.00510	0.00170	0.01110	0.00600
4	0.00130	0.0030	0.00600	0.00190	0.01820	0.00420
5	0.00120	0.0020	0.00460	0.00200	0.01280	0.00380
6	0.00130	0.0050	0.00510	0.00250	0.01550	0.00330
7	0.00136	0.0040	0.00520	0.00208	0.01445	0.00462
Av.	0.00180	0.00800	0.00490	0.00200	0.0165	0.0052

Statistical tests (NIST tests)

The NIST provides a set of standardized tests to assess the quality, randomness, and security of random number generators and cryptographic algorithms [23]. If the proposed algorithm has passed the NIST tests, it indicates that the key generation process exhibits high security and randomness, making it more resilient to various cryptographic attacks. The NIST tests evaluate the following properties the randomness of the generated key should appear statistically random and exhibit no discernible patterns,

uniformity of generation of distribution of key values should be uniform across the entire key space, the independence should be satisfied in which each key value should be independent of previous and future key values, and finally the sensitivity to seed or key changes such as small changes in the initial parameters (seeds) or keys should produce drastically different output sequences. Bypassing the NIST tests demonstrates that the proposed algorithm's key generation process satisfies these properties and can be considered a robust and secure method for generating cryptographic keys. It suggests that the keys are resistant to attacks that rely on predicting or exploiting patterns in the key sequences. When conducting the NIST tests, it's crucial to use experimentally known test keys, as these are carefully designed keys that help to verify the algorithm's performance against various attacks. The algorithm is evaluated with these known test keys to ensure its security under controlled conditions**.**

Table 3 Randomness Test of the Proposed Algorithm

#	Test name	P-Value	Status
1	The first test (Run Test)	0.101245	Pass
2	The second Test (Serial Test)	0.027221	Pass
3	The third test (Random excursion variant test)	0.690011	Pass
4	The fourth test (Random excursion test)	0.766554	Pass
5	The fifth test (Non-overlapping template matching test)	0.890005	Pass
6	The sixth test (Frequency Monobit Test)	0.003333	Pass
7	The seventh test (Maurer's universal statistical test)	0.000041	Pass
8	The eighth test (The longest run of ones in a block test)	0.001111	Pass
9	The ninth tests (Linear complexity Test)	0.023333	Pass
10	The tenth test (Frequency test within a Block test)	0.034423	Pass
11	The tenth test (Discrete Fourier Transform test)	0.788651	Pass
12	The eleventh test (Cumulative sums Test)	0.004567	Pass

Conclusion:

Lightweight image encryption is required in limited resources systems such as IoT systems. It helps maintain data privacy and security without compromising the overall functionality and efficiency of the devices. Objectives of LED are to investigate the function of extremely light, actually nonexistent key scheduling and resistant ciphers against related-key assaults, with LED ciphers in particular. The paper proposed a lightweight image encryption approach that combines the LED encryption algorithm and a pseudo-random number generator based on the Rossler attractor. An efficient security solution by demonstrating uniform histograms, low correlations, and low similarity between the original and encrypted images. The randomness of the generated numbers is also evaluated using standardized tests. This paper contributes to the field of lightweight encryption methods tailored for image security in resource-constrained environments. the method could be developed to be used with all types of multimedia such as video, speech audio, etc.

References

[1] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.

[2] Duggineni, Sasidhar. "Impact of controls on data integrity and information systems." Science and Technology 13.2 (2023): 29-35.

[3] Singh, Saurabh, et al. "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions." Journal of Ambient Intelligence and Humanized Computing (2017): 1-18.

[4] Khashan, Osama A., Rami Ahmad, and Nour M. Khafajah. "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks." Ad Hoc Networks 115 (2021): 102448.

[5] Khan, Muhammad Nauman, Asha Rao, and Seyit Camtepe. "Lightweight cryptographic protocols for IoT-constrained devices: A survey." IEEE Internet of Things Journal 8.6 (2020): 4132-4156.

[6] Kushwaha, Prabhat Kumar, M. P. Singh, and Prabhat Kumar. "A survey on lightweight block cyphers." International Journal of Computer Applications 96.17 (2014).

[7] Al-Azzeh, Jamil, et al. "A Novel Based on Image Blocking Method to Encrypt-Decrypt Color." JOIV: International Journal on Informatics Visualization 3.1 (2019): 86-93.
[8] Ali Hussein Fadel, Rasha Subhi Hameed, Jamal N Hasoon, Salama A Mostafa, Bashar Ahmed Khalaf, "A light-weight ESalsa20 Ciphering based on 1D logistic and Chebyshev chaotic maps", Journal Solid State Technology, Vol. 63, Issue 1, Pages 1078-1093, 2020.
[9] Mohammed Salih Mahdi, Raghad Abdulaali Azeez, Nidaa Falih Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps", Periodicals of Engineering and Natural Sciences ISSN 2303-4521, Vol. 8, No. 4, November 2020, pp.2138-2145.
[10] W. Alexan, M. ElBeltagy and A. Aboshousha, "Lightweight Image Encryption: Cellular Automata and the Lorenz System," 2021 International Conference on Microelectronics (ICM), New Cairo City, Egypt, 2021, pp. 34-39, Doi: 10.1109/ICM52667.2021.9664961.
[11] M. ElBeltagy, W. Alexan, A. Elkhamry, M. Moustafa and H. H. Hussein, "Image Encryption Through Rossler System, PRNG S-Box and Recamán's Sequence," 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2022, pp. 0716-0722, Doi: 10.1109/CCWC54503.2022.9720905.
[12] Noura, H., Chehab, A., Noura, M. et al. Lightweight, dynamic and efficient image encryption scheme. Multimed Tools Appl 78, 16527–16561 (2019). https://doi.org/10.1007/s11042-018-7000-7.
[13] Muntaha Abdulzahra Hatem, Balsam Abdulkadhim Hameedi, and Jamal Nasir Hasoon, "Lightweight digital imaging and communications in medicine image encryption for IoT system", TELKOMNIKA Telecommunication, Computing, Electronics and Control ISSN: 1693-6930, Vol 21, No 4, 2021.
[14] Chai, Xiuli, et al. "An image encryption scheme based on multi-objective optimization and block compressed sensing." Nonlinear Dynamics 108.3 (2022): 2671-2704.
[15] Biswas, A., Majumdar, A., Nath, S. et al. LRBC: a lightweight block cypher design for resource-constrained IoT devices. J Ambient Intell Human Comput 14, 5773–5787 (2023). https://doi.org/10.1007/s12652-020-01694-9.
[16] G. Bansod, N. Raval and N. Pisharoty, "Implementation of a New Lightweight Encryption Design for Embedded Security," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 142-151, Jan. 2015, doi: 10.1109/TIFS.2014.2365734.

[17] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M. (2011). The LED Block Cipher. In: Preneel, B., Takagi, T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_22.
[18] Jovanovic, P., Kreuzer, M., Polian, I. (2012). A Fault Attack on the LED Block Cipher. In: Schindler, W., Huss, S.A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2012. Lecture Notes in Computer Science, vol 7275. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29912-4_10.
[19] S. Zhang, C. Li, J. Zheng, X. Wang, Z. Zeng and G. Chen, "Generating Any Number of Diversified Hidden Attractors via Memristor Coupling," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 12, pp. 4945-4956, Dec. 2021, Doi: 10.1109/TCSI.2021.3115662.
[20] Qingdu Li, "A topological horseshoe in the hyperchaotic Rössler attractor", Physics Letters A,
Volume 372, Issue 17, 2008, Pages 2989-2994.
[21] Sara, U., Akter, M. and Uddin, M. (2019) Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. Journal of Computer and Communications, 7, 8-18. Doi 10.4236/jcc.2019.73002.
[21] Zhai, Guangtao, and Xiongkuo Min. "Perceptual image quality assessment: a survey." Science China Information Sciences 63 (2020): 1-52.
[22] Fu, Xueyang, and Xiangyong Cao. "Underwater image enhancement with global–local networks and compressed-histogram equalization." Signal Processing: Image Communication 86 (2020): 115892.
[23] K. Ding, K. Ma, S. Wang and E. P. Simoncelli, "Image Quality Assessment: Unifying Structure and Texture Similarity," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 5, pp. 2567-2581, 1 May 2022, Doi: 10.1109/TPAMI.2020.3045810.
[24] D. M. Wang, L. S. Wang, Y. Y. Guo, Y. C. Wang, and A. B. Wang, "Keyspace enhancement of optical chaos secure communication: chirped FBG feedback semiconductor laser," Opt. Express 27, 3065-3073 (2019).
[25] A. Carlson, G. Gang, T. Gang, B. Ghosh and I. K. Dutta, "Evaluating True Cryptographic Key Space Size," 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2021, pp. 0243-0249, doi: 10.1109/UEMCON53757.2021.9666530.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
Journal of the College of Basic Education Vol.30 (NO. 126) 2024, pp. 10-29

خوارزمية تشفير خفيفة للصور بالاعتماد على تحسين خوارزمية LED باستخدام Rossler Attractor

سهاد فخري حسين
وزارة التربية ، الرصافة 1، بغداد، العراق
suhad7242@gmail.com

مستخلص البحث:
يهدف تشفير الصور الخفيف إلى توفير حلول أمنية فعالة لمختلف الأجهزة والتطبيقات التي تستخدمها من خلال مجموعة من الخوارزميات المصممة لتأمين هذه الصور مع الأخذ بنظر الاعتبار نوع الأجهزة التي تستخدم في التطبيقات الحديثة مثل قوة المعالجة والذاكرة، والتي توجد عادةً في أجهزة مثل أجهزة إنترنت الأشياء والهواتف المحمولة والأنظمة المدمجة والتي تكون محدودة الخصائص. في هذا البحث، تم اقتراح طريقة تشفير خفيفة للصور بالاعتماد على خوارزمية تشفير LED وطريقة لمولد أرقام زائفة يسمى روسلر اذ يتم تقسيم الصورة إلى نطاقاتها ثلاثية الألوان (RGB) ثم يتم تقسيمها إلى كتل للتشفير، ويتم استخدام نموذج المعادلات الثلاثة (Rossler Attractor) لمولد أرقام يتم تطبيقها لإنتاج مفتاح مجدول للدورات في LED لتبدو عشوائية قدر الإمكان. للتحقق من جودة الطريقة المقترحة يتم اختبارها من خلال مجموعة من الاختبارات للتأكد مثل الاختبار البصري ممثل بالرسم البياني للصورة قبل وبعد التشفير والذي يبين عدم وجود تميز لتدرج لوني عن الاخر ويختلف عن الرسم البياني للصور المدخلة وكذلك اختبار الترابط للصورة الناتجة والحصول على قيمة منخفضة مما يعني عدم وجود ارتباط بين وحدات البكسل الأفقية والرأسية والقطرية. تم تطبيق اختبار التشابه أيضًا مثل MSE وPSNR وSSIM والذي يفسر أيضًا عدم وجود تشابه بين الصور العادية والمشفرة. تم اختبار عشوائية الأرقام الناتجة باستخدام اختبار NIST القياسي لتقييم مفتاح الإدخال.

الكلمات المفتاحية : خوارزمية التشفير خفيفة الوزن خوارزمية(LED) ، طريقة توليد المفاتيح Rossler Attractor، مقياس معدل مربع الخطأMSE ، مقياس نسبة قمة الإشارة الى الضوضاء PSNR، مقياس التشابه الهيكليSSIM