Color Image Encryption Using a New Confusion and Diffusion Method Based on Hybrid Key Generation

Fadhil Hanoon Abbood
computer science dept.-collage of education
Mustansiriyah university- Baghdad, Iraq

Leila Ben Ayed
national school of computer science
university of la manouba- Manouba,Tunis

Abstract

Currently, images are transmitted via open channels that are open to possible assaults, necessitating enhanced security for image data interchange across several sectors, including medical, military, and finance. Security aspects are crucial in thwarting brute force and differential assaults on the system. This paper proposes a new method for color image encryption. This method consists of two stages; the first stage is confusion, which includes a new block scrambling technique as well as modified zigzag transformation for encryption phases such as permutation. The second stage is diffusion, where a new hybrid key generation is used to generate a sequence of stream random keys via a one-dimensional logistic map and a set of LFSR (Linear Feedback Shift Registers). The outcomes of encryption process are assessed using histogram analysis, correlation analysis, Number of Pixel Change Rate (NPCR), Unified Average Change Intensity (UACI), Peak-Signal-to-Noise Ratio (PSNR), and entropy measurement. The obtained results illustrate the security, dependability, efficiency, and versatility of the suggested strategy.

Keywords: LFSR, Logistic Map, ZT, Image scrambling

1.Introduction

The rapid development in the Internet of Things and social networking has rendered secure image data transfer continually significant. [1,2]. Especially, effective encryption of sensitive data shared through internet or wireless network in multimedia format is a crucial step in creating secure data communication channels of diversified types, including image and other types of data used in this study, and ensuring that not only those types of channels, but all elements have measures in place to prohibit any unapproved access, possession, processing, or distribution of transmitted Personal Data. For varied applications, information is exchanged in different forms such as text, images, audio, video, and even 3D, which include military, medical, banking systems, and so forth. Yet the question arises about the security of those images. The major aspect of image transmission is security issues, including how to protect an image from an unauthorized party or even tampering with it. This means applying cryptographic methods to encrypt the picture so that it is robustly secured. The cryptographic methods substitute the pixels for an un-understandable series of data, viewed by the intruder. In this paper, we aim for stronger levels of security against unwanted access in image encryption. Traditional methods of cryptography fall under the Advanced Encryption Standard in text communication implementations. The two basic categories of encryption system have to use a number of secondary techniques to achieve diffusion and confusion. A random sequence was obtained from logistic mapping and linear feedback shift register sequences. These structures are quite erratic and hard to analyze and predict [4,5]. A multitude of cryptographic techniques have been devised in this domain to enhance picture security. Recent methods operate by utilizing a cryptographic key and algorithm in the following manner: In 2019, Hussein et al. presented the logistic sine map for picture encryption [6]. In 2019, Said will employ a streamlined Double Humped (DH) logistic map for the creation of pseudo-random number keys (PRNG). The new generalized parameter allows for enhanced control over the map's chaotic range [7]. A novel hybrid chaotic system is introduced by combining four simultaneous waterfall logistic maps with dynamic parameter modification, aimed at attaining a high Lyapunov exponent and exhibiting completely chaotic bifurcation diagram behavior. In the year 2021. The methodology is based on a multi-modular chaotic fuzzy parallel logical map (PFMM-CLM), created by Mahmoud Gad and his associates. The innovative picture encryption method is anticipated to be launched by the conclusion of 2021. [8]. In 2022, Chen et al. utilized an enhanced Henon Map for a Hybrid Domain Image Encryption Algorithm [9]. Deb and Bhuyan suggested a unique approach for medical image encryption, employing a Linear Feedback Shift Register with a nonlinear filter function, which incorporates random shuffling and XOR operations. [10]. In 2021, Thinnukool et al. proposed a dual encryption approach employing a trigonometric chaotic map and the XOR operation on an image encryption [11]. In 2021, Momeni et al. suggested color image encryption employing LFSR through three-dimensional permutation and substitution techniques. [12]. In 2021, Masood et al. proposed the use of Linear Feedback Shift Registers and a logistic map to generate a random series of keys for encryption [13]. In Section 2, we shall delineate the employed stream cipher. Section 3 encompasses material and method. Section 4 presents the results and evaluation. Our observations and findings are encapsulated in Section 5.

2. STREAM CIPHER AND CHAOTIC

Text may be encrypted via a stream cipher to generate ciphertext. one bit sequentially to each binary digit in a data stream. Bit-by-bit encryption refers to this process. A one-time pad refers to the key often employed with a stream cipher. A one-time pad is always at least equal in size to the message it encrypts. This form of encryption is theoretically unbreakable. The execution speed of stream ciphers is markedly superior than that of block ciphers, and the complexity of the necessary hardware is considerably reduced. This is a benefit of utilizing stream ciphers. Stream ciphers do not provide identical ciphertext for repeated plaintext blocks because to the constant alteration of keys for each bit of plaintext [14].

2.1 Linear Feedback Shift Registers

Computer simulations of stochastic processes, error-correcting codes, and many technological applications utilize a type of shift register known as a Linear Feedback Shift Register, frequently abbreviated as LFSR. It produces an extensive series of ones and zeros that seems arbitrary. A linear function of the prior state can serve as an input to a shift register. This function often manifests as an exclusive OR in Boolean representation (XOR). The bits capable of altering the state of other bits are termed taps, which is the designation used to describe these bits. LSFRs are applicable in several domains such as digital counting, encryption, and circuit testing [15][20].

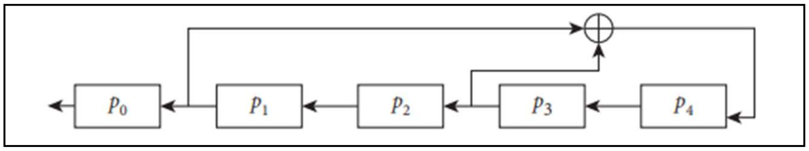


Fig. 1 Linear feedback shift register with five stages.

2.2 Chaos Theory

Chaos theory is a mathematical science that has been utilized across several fields, including physics, economics, biology, and philosophy. Researchers on chaos theory are more concerned with studying the behavior of dynamical systems that show extreme sensitivity at first conditions toward diving into a phenomenon called the butterfly effect. Little changes in the initial conditions create absolutely different outcomes in a chaotic system; therefore, any kind of accurate prediction in the long term is impossible. These maps include one-dimensional chaotic maps that iterate over time discretely with variables explicit, such as the logistic map, tent map, and sine map. This equation asserts that chaotic maps are simple in construction structure, low in complexity, and implement as they are a straightforward logic [15]:

$$x_{n+1} = rx_n\,(1 - x_n) \tag{1}$$

Where

xn+1 is within the interval [0, 1], r represents a regulatory parameter (sometimes referred to as the amplitude parameter), and n denotes the number of iterations. A logistic map is a one-dimensional discrete chaotic function commonly utilized in various applications, particularly in social science and economics. Figure (2) illustrates the bifurcation diagram of the logistic map.

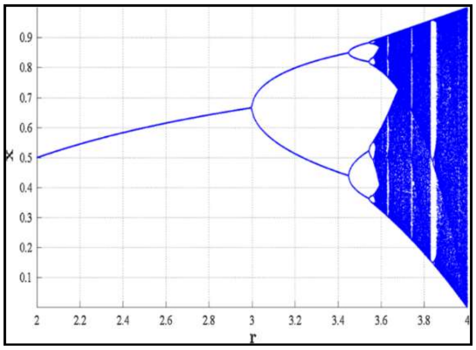


Fig. 2: Bifurcation Diagram of the Logistic Map

3. Material and Method

This section introduces a novel Encryption method and Key Generator for the encryption and decryption of image data.

3.1 Block Scrambling

RGB image of dimensions 256 × 256 × 3 is divided into four parts. Each of the quadrants is supplementary subdivided into four sub-quadrants, and each of these sub-quadrants is then rotated counter-clockwise by 90° to obtain 64 sub-blocks. This method will change the image a bit but will ensure that the locality between the neighbor pixels is not completely lost.

3.2 Modified Zigzag

Zigzag Transformation (ZT) is a simple algorithm for permuting an image. This considers red, green, and blue channels as discrete matrices, each of dimension 256 x 256. In ZT, the upper left pixel is moved, giving the observer some help in figuring out the algorithm. In the Modified ZT, the upper left pixel together with its immediate neighboring pixel on its right is swapped with the low right pixel. The transformation is achieved on the pixels for each matrix from the top left to the bottom right to carry out encryption. The elements at the top left and top right in the matrix are interchanged with those at the bottom right and bottom left, while other elements have also been interchanged in a zigzag fashion. It does the vice-versa process for driving the first two elements in the matrix to be replaced by those at the last and last but one positions while all other elements are interchanged in a zigzag manner. This method will be a transformation made for the pixels belonging to each of the frames. The relationship between adjacent pixels in an image is completely changed by this approach, resulting in the transformed ZT of the image.

3.3 Key Generation

The key generator integrates Stream cipher and Chaotic systems. This section introduces a novel design for the Stream Cypher Key Generator (SCKG), which produces byte-keys that may be analyzed alongside unprocessed picture data. The primary key, known as the Basic key (BK), varies with each picture and necessitates a fundamental private key including twenty characters, which are transformed into binary to initialize the LFSR (Linear Feedback Shift Register) of the SCKG. The key's transmission must take place via a secure route.

3.4 Algorithm 1: Key Generation

Input: monochromatic picture

Result: encoded image

Step 1: Initialize four LFSRs with distinct seed values to produce a unique sequence of pseudo-random bytes.

Step 2: Initialize a BLFSR using an alternative seed value.

Step 3: Generate B1, B2, B3, and B4 using LFSRs.

Step 4: Using a logistic map generate Bj1, Bj2, Bj3, and Bj4.

Step 5: KB = Bi XOR Bj

Step 6: Produce a byte from the LFSR5, called B5.

Step 7: Key = KB XOR B5.

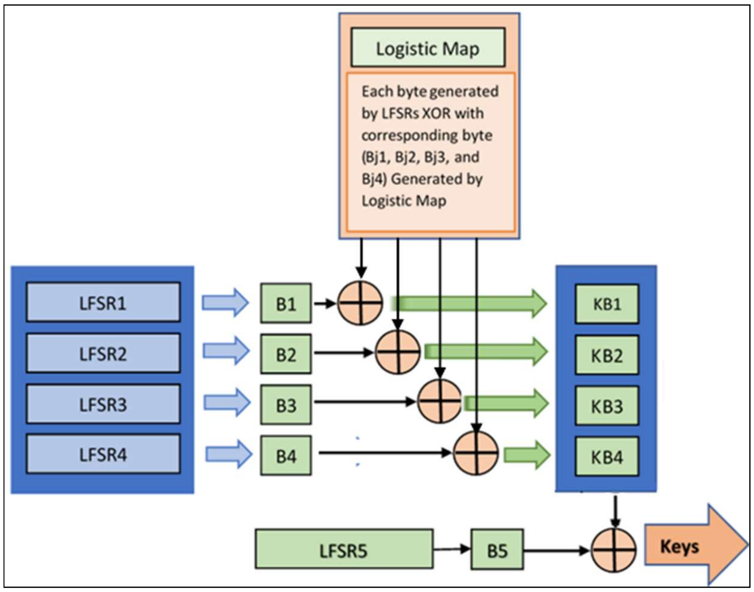

Logistic Map
Each byte generated by LFSRs XOR with corresponding byte (Bj1, Bj2, Bj3, and Bj4) Generated by Logistic Map
LFSR1
LFSR2
LFSR3
LFSR4
B1
B2
B3
B4
KB1
KB2
KB3
KB4
LFSR5
B5
Keys

Fig. 3. Key Generation Using SCKG

3.5 Encryption Method

The proposed scheme is suitable for any M × N color image. The encryption of the digital image has two basic components, that is confusion and diffusion. The blocks scrambling will apply in the generation of 64 squares during the diffusion process. The modified ZT performs well in eradication the correlation seen in between the neighboring pixels. Since the XOR operation is considered, key space generation through 3D ELM makes secret keys for each X, Y, and Z coordinates within the range of 0 to 255. In the final stage, the images are EX-ORed to get a cipher image. Algorithm 2 describes the encryption steps.

Algorithm 2: Encryption Process

Input: image P size 256 × 256
Output: encrypted image C
Step 1: Apply Scrambling on image P, which is separated into 64 blocks, each measuring 16 × 16, denoted as P1.
Step 2: Apply The zigzag transform (ZT) on P1 to scrambling the blocks in P1 to provide P2.
Step 3: P2 is separated into three channels RGB, each one size 256 × 256.
Step 4: Initialize LFSRs and logistic map with distinct seed and initial values to produce a unique sequence of pseudo-random bytes.
Step 5: The pseudo-random keys is XORed with the obtained RGB channels after the ZT updating to produce P1.

The encryption procedure illustrates in Figure 4. The decryption procedure is executed in the inverse manner of encryption to retrieve the image P.

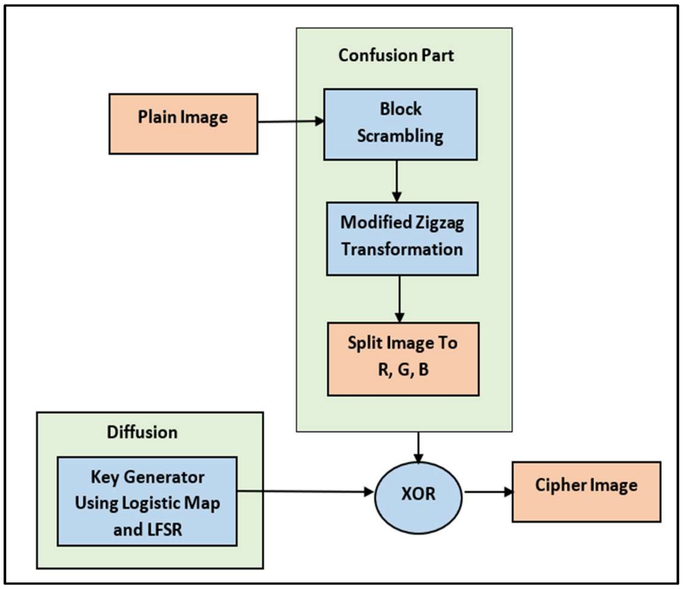


Fig. 4 Proposed Method Block Diagram

3.6 Evaluation

The security attributes of the proposed system are evaluated through histogram analysis, information entropy analysis, correlation coefficient, NPCR, and UACI along with MSE and PSNR.

3.6.1 Analysis of Key Space

The suggested technique is significantly depending on the key; it must guarantee the key's security and ensure that the key space is sufficiently extensive to render brute force attacks infeasible. The suggested approach employs a 256-bit key, resulting in 2^{256} possible secret key set for R, G, and B individually, rendering it exceedingly challenging to compromise by brute force methods.

3.6.2 Key Sensitivity Analysis

The encryption system should be very sensitive to key alterations. A slight alteration in the encryption key would cause a big variance in the output image from the image that was originally obtained from encryption.

3.6.3 Histogram Analysis

It shows how pixel intensities are distributed within an image. A perfect encrypted image should have a regular basis histogram distribution to hinder the attacker from deriving information from it. The strength of the proposed encryption will be reflected in a well-distributed pixel values in the cipher image.

3.6.4 Analysis of Correlation Coefficient

In a normal image, both nearby and neighboring pixels show a connection. However, the adjacent pixels of the encrypted image do not exhibit any correlation. Hence, there is no link between them. It is done through an analysis, that is, Correlation Coefficient, to assess the level of likeness among a couple of pixels. It involves computing and checking the Pearson correlation coefficient in both vertical, horizontal, and diagonal manners for both the plain and cipher images. One of the efficient techniques for encryption would be an interruption of relations between neighboring pixels. This means that a lower correlation is an indication of better effectiveness of the strategy [18].

3.6.5 NPCR and UACI

NPCR (Number of Pixels Change Rate): It is a measure that determines the percentage of pixels changing when the smallest editing is done on the original image. That tests the sensitivity of the cipher image to changes applied to the plain image. Good diffusion will in near 100%NPCR, where minimal input change results in drastic changes in the cipher image.

UACI (Unified Average Changing Intensity): It determines the unified average change of intensity between the cover image and the stego image. This is actually used to determine the strength of the encryption because it measures how much intensity in the pixels of the image changed due to encryption. More UACI values denote better encryption where even minute changes bring about substantial variations in intensity [16].

3.6.6 Entropy Analysis

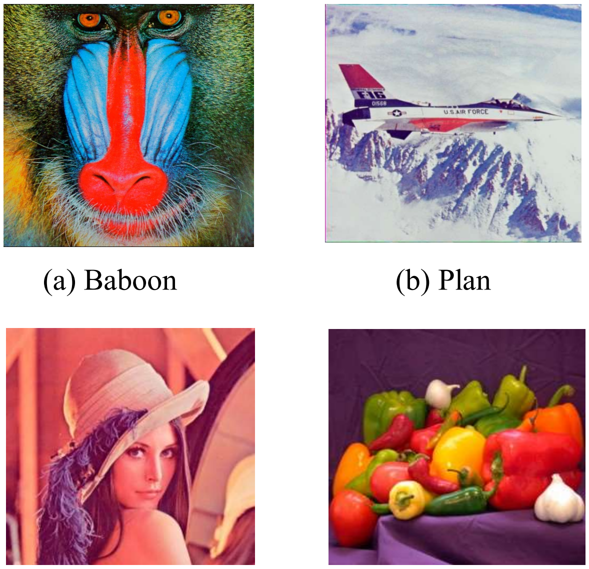
In image encryption, entropy is used to measure how much randomness is present in the pixel values of the encrypted image. If entropy value is high and nearing of 8 is deemed secure against brute force attacks. then patterns such as that of the pixel in question are very complex and not easily predictable; hence, attackers will find it very hard to break the image being encrypted. This kind of randomness guarantees better security by reducing the chances for successful attacks and keeping the image confidential [16].

3.6.7. PSNR Evaluation

PSNR is a standard measure in image processing to determine the quality of the image obtained after the process of encryption with respect to the original. The difference between the two images is calculated through it; higher PSNR values mean less distortion in resemblance of the original image features after the process of encryption. High PSNR means that the algorithm of encryption does not incorporate a big amount of noise or degradation that would make the image visually unrecognizable. In quality minimization with security for the images that are exchanged through encryption, one needs this trade-off and learns it through PSNR [16].

4. Results and Evaluation

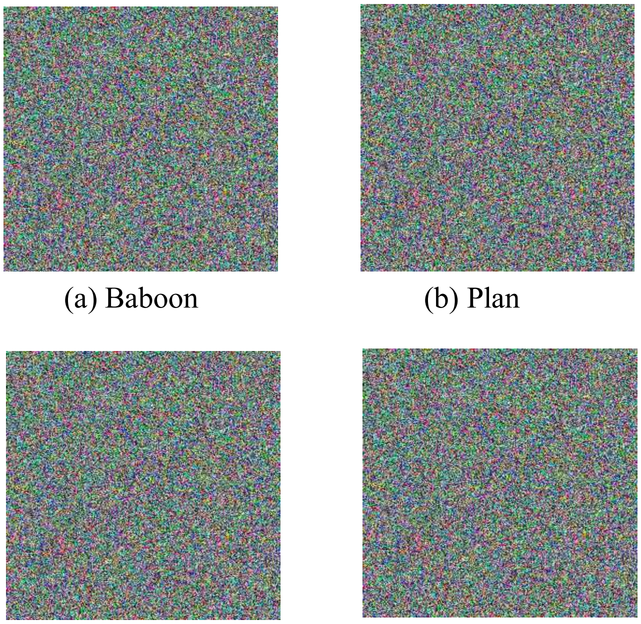
The assessment of color image encryption emphasizes evaluating the efficacy of the encryption technique for security, visual quality, and performance. Essential measures such as NPCR, UACI, entropy, PSNR, and visual assessment are employed to evaluate the efficacy of the encryption in converting the initial image into a random, indecipherable format. We employed the publicly available photographs from the USC-SIPI image dataset, as the original protected images. Figure 5 depicts the encrypted image.



(a) Baboon (b) Plan

(a) Lena (b) Peppers

Fig. 5 Original Images



(a) Baboon (b) Plan

(a) Lena (b) Peppers

Fig. 6 Encrypted Images

Standard methodologies and evaluations should be used in evaluating outcomes. A good encryption technique would result in an encrypted image with pixel values uniformly distributed, based on the results of histogram analysis. See Figure 7a–c for histogram views of the Peppers image in red, green, and blue channels. In Figures 7d–f, the RGB channels of the encrypted Peppers image are shown. A uniform distribution in these channels implies that an attacker would find it hard to get the information.

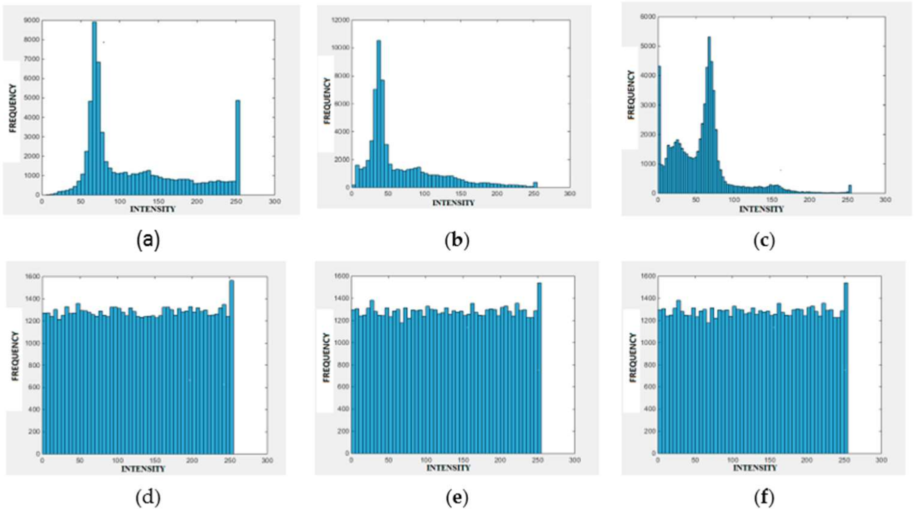


Fig. 7 Histograms of the Peppers picture for the red (a), green (b), and blue (c) channels, together with the histograms of an encrypted Peppers image for the red (d), green (e), and blue (f) channels

The dispersed graph can illustrate the relationships among adjacent picture pixels. One thousand arbitrary adjacent pixels from an image are utilized to illustrate the correlation. Figure 8a–c demonstrates a robust connection among adjacent pixels, including horizontal, vertical, and diagonal neighbors, in the Peppers simple picture. The correlation among adjacent pixels is poor in an encrypted Pepper image.

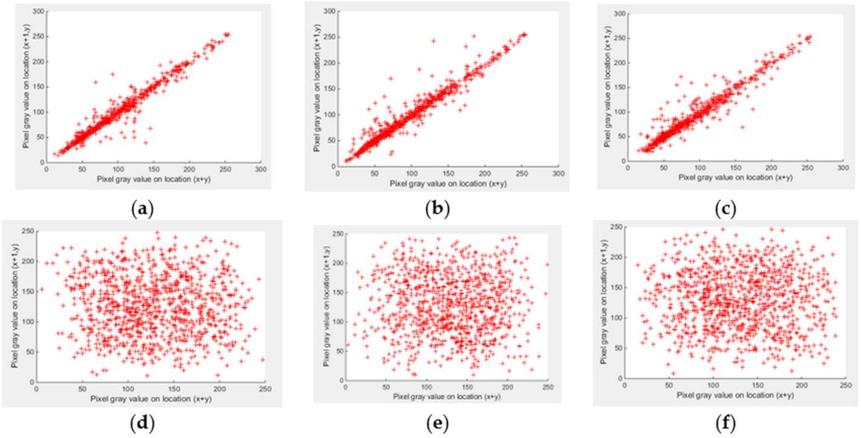


Fig 8. Correlation among adjacent pixels in horizontal (a), vertical (b), and diagonal (c) orientations of the plain Pepper image, as well as the correlation among adjacent pixels in horizontal (d), vertical (e), and diagonal (f) orientations of the encrypted Pepper image.

Table 1 displays the correlation values between plain and encrypted images.

Images	Horizontal		Vertical		Diagonal	
	Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	0.9504	-0.0247	0.9735	-0.0245	0.9554	-0.0274
Peppers	0.9686	-0.0736	0.9760	-0.0346	0.9721	-0.0243
Plan	0.9554	-0.0297	0.9565	-0.0617	0.9224	-0.0297
Baboon	0.9717	-0.0252	0.9776	-0.0554	0.9565	-0.0355

Table 2. NPCR, UACI, PSNR, and Entropy for the Encrypted Image. From this view, the scores of both NPCR and UACI show that the algorithm has presented a strong differential attack. Almost optimal values of entropy, such as 8, indicate that the proposed encryption technique has actually randomly permutated pixels in the encrypted image. These attained PSNR values are low, signifying its efficacy.

Table 2. Results of (NPCR), Entropy, (UACI), and (PSNR).

Image	NPCR	UACI	PSNR	Entropy	
				Plain	Cipher
Baboon	99.6116	33.5059	9.8337	7.6744	7.9991
Plan	99.6174	33.5683	8.7934	7.6522	7.9993
Lena	99.6422	33.5847	6.6496	7.6339	7.9995
Peppers	99.5984	33.8050	9.8464	7.5786	7.9992

The proposed method is tested on the 256 x 256 Lena picture using a variety of methodologies, including entropy, NPCR, UACI, and correlation analysis, as shown in Table 3. Recent articles in the same area are compared to our method.

Table 3. Evaluation of performance and comparison with alternative approaches (best values are highlighted in bold).

Measure	[50]	[56]	[27]	[58]	Our
Horizontal Correlation	0.0327	0.9407	**0.0018**	-0.0230	- 0.0236
Vertical Correlation	0.0219	-0.0273	0.0011	0.0019	- 0.0188
Diagonal Correlation	0.0180	-0.0140	**-0.0012**	-0.0034	- 0.0273
Entropy	7.9993	n/a	7.9994	7.9974	**7.9996**
UACI	n/a	15.38	33.4365	3.5100	**33.6867**
NPCR	n/a	99.10	99.6166	99.6200	**99.6232**

5. Conclusions

We presented a novel image encryption method that uses a Stream Cipher Key generation scheme. The system encompasses Block Scrambling and Modified Zigzag Transformation with key generation done by the logistic map and linear feedback shift register. Two levels of security in any encryption of an image performed are confusion and diffusion. It gives priority to the defense against brute-force assault on the proposed algorithm. In the experimental results, it was established that the proposed method produced an encrypted image with uniform pixel histograms. Also, this work shows that the method proposed can assure that the encrypted images have an information entropy nearing 8. Comparative trials were held with various contemporary algorithms. Statistical testing results entitle this new pseudo-random bit combiner to secure file encryption and decryption. It is now known to be both safe and efficient on computation, as the evaluation of the proposed approach is stated. The approach recommended is general, fast, and of much practical interest.

References

[1] Kadhim, I.J. , Premaratne P. , Vial, P.J. , Halloran B., "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research", *Neurocomputing* 2019, *335*, 299–326.

[2] Qasim A.F., Meziane F. and "Aspin R. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Comput. Sci. Rev.* 2018, *27*, 45–60.

[3] Arul Murugan C. and KarthigaiKumar P.," Survey on image encryption schemes, bio cryptography and e*ffi*cient encryption algorithms", *Mob. Netw. Appl.* 2018, 1–6.

[4] Kozioł F., Borowik, G., Woz´niak M. and Chaczko Z, "Toward dynamic signal coding for safe communication technology", In *Proceedings of the Asia-Pacific Conference on Computer-Aided System Engineering, APCASE, Washington, DC, USA,* 14 July 2015; pp. 246–251.

[5] Khalifa N., Filali R.L. and Benrejeb M "A Fast Selective Image Encryption Using Discrete Wavelet Transform and Chaotic Systems Synchronization" *Inf. Technol. Control.* 2016, *45*, 235–242.

[6] M. T. Elkandoz, W. Alexan and H. H. Hussein, "Logistic Sine Map Based Image Encryption," 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 2019, pp. 290-295, doi: 10.23919/SPA.2019.8936718.

[6] Manjit Kaur, Ahmad Ali Alzub, Dilbag Singh, Vijay Kumar, And Heung-No Lee "Lightweight Biomedical Image Encryption Approach", *IEEE Access,* 12 July (2023)

[7] Samar. M. Ismail, Lobna A. Said, at al, Generalized double –humped logistic map based medical image encryption, Journal of advanced research, Vol.(10), Pp(85-98), (2018).

[8] Mahmoud Gad, Esam Hagras, Hasan Soliman1, and Noha Hikal, A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption, The International Arab Journal of Information Technology, Vol. 18, No. 2, March (2021).

[9] Chen, Y.; Xie, S.; Zhang, J. A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map. Entropy 2022, 24, 287. https://doi.org/10.3390/e24020287

[10] Deb, Subhrajyoti & Bhuyan, BubuChaos-based medical image encryption scheme using special nonlinear filtering function based LFSR. Multimedia Tools and Applications. 80. 1-24. (2021). 10.1007/s11042-020-10308-7.

[11] Orawit Thinnukool, Thammarat Panityakul and Mahwish Bano, "Double Encryption Using Trigonometric Chaotic Map and XOR of an Image,Computers", *Materials and Continua*,Volume 69, Issue 3,2021,Pages 3033-3046,2021.

[12] Momeni Asl A, Broumandnia A, Mirabedini SJ , Color image encryption using linear feedback shift registers by three dimensional permutation and substitution operations. Int J Nonlinear Anal Appl 12:903– 921(2021).

[13] Masood F, Driss M, Boulila W et al, A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wirel Pers Common. https://doi.org/10.1007/s11277-02108584-z (2021).

[14] Whia alemami, m. afendee and s. atiewi, research on various, cryptography techniques, (2019).

[15] Momeni Asl A, Broumandnia A, Mirabedini SJ , "Color image encryption using linear feedback shift registers by three dimensional permutation and substitution operations@. *Int J Nonlinear Anal Appl* 12:903– 921(2021).

[16] Ahmad, J.and Hwang, S.O. "A secure image encryption scheme based on chaotic maps and affine transformation".*Multimed. Tools Appl*. 75, 13951–13976, 2016.

[17] Li Y., Li X., Jin X., Zhao G.and Ge, S., "Tian, Y.; Wang, Z. An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map. In Applications and Techniques in Information Security,*Springer: Berlin/Heidelberg*, Germany, pp. 3–13, 2015.

[18] Xu L., Li Z., Li J.and Hua W.," A novel bit-level image encryption algorithm based on chaotic maps". *Opt. Lasers Eng* , 78, 17–25, 2016.

[19] Zhang Y., Xiao D. ,"An image encryption scheme based on rotationmatrix bit-level permutation and block diffusion", *Commun. Nonlinear Sci. Numer. Simul*. ,19, 74–82,2014

[20] Krishnapriya P V, Smitha Suresh, "Image Security Using Linear Feedback Shift Register", *International Journal of Innovative Science and Research Technology*, Vol. 2, Issue 6, June - 2017.

[21] M. Din, S. Pal, S. Muttoo and A. Jain, "Applying Cuckoo Search for analysis of LFSR based cryptosystem", Perspectives in Science, Vol. 8, pp. 435-439, 2016.

[22] S. Al-Ageelee and R. Kadhum, "Cryptanalysis of nonlinear stream cipher cryptosystem based on improved particle swarm optimization", *International Journal of applied information systems*, Vol. 19, No. 1, pp. 78-84, 2017.

[23] S. Sadkhan and B. Yaseen, "A DNA-Sticker Algorithm for Cryptanalysis LFSRs and NLFSRs Based Stream Cipher," In *Proc. of International Conf. On Advanced Science and Engineering (ICOASE)*, Duhok, Iraq, pp. 301-305, 2018.

[24] I. Polak, and M. Boryczka, "Tabu Cryptanalysis of VMPC Stream Cipher", *Tatra Mountains Mathematical Publications,* Vol.73, No.1, pp.145-162, 2019.

[25] R. Jawad and F. Ali, "Using Evolving Algorithms to Cryptanalysis Nonlinear Cryptosystems", *Baghdad Science Journal*, Vol. 17, No. 2, 2020.

[26] S. Lee, C. Cheng, C. Lin and Y. Huang, "PSO-Based Target Localization and Tracking in Wireless Sensor Networks", *Electronics*, Vol. 12, No. 4: 905, 2023.

[27] Ahmed KS, Mohammed HA, Ahmed HM." A New Chaotic Image Cryptosystem Based on Plaintext Associated Mechanism and Integrated Confusion Diffusion Operation", *Karbala International Jornal Mod Sci*.; 7(3): 176-188, 2021

[28] Khalid Kadhim Jabbar, Fahmi Ghozzi and Ahmed Fakhfakh." Robust Color Image Encryption Scheme Based on RSA via DCT by Using an Advanced Logic Design Approach", *Baghdad Science Journal*, 20(6 Suppl.): 2593-2607, 2023,

[29] Mahmoud Gad, Esam Hagras, Hasan Soliman1, and Noha Hikal, A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption, *The International Arab Journal of Information Technology*, Vol. 18, No. 2, March (2021).

[30] Yong Chen, Shucui Xie, and Jianzhong Zhang, A Hybrid Domain Image Encryption Algorithm Based on Improved Henon Map, *Entropy (Basel)*, 24(2): 287, (2022).

[31] Deb S, Bhuyan B, Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR. *Multimed Tools Appl* 80(13):19803–19826(2021).

[29] Ahmed HM, Ahmed K, Mohammed H. Image Cryptosystem for IOT Devices Using 2-D Zaslavsky Chaotic Map. *TEM J.* 2022 ;15(2): 543-553.

[30] Ekhlas Abbas Al-Bahrani, Riyam N.J Kadhum. A New Cipher Based on Feistel Structure and Chaotic Maps. *Baghdad Sci J.* 2019 ;16 (1): 270-280.

[31] Amal AM, Zahraa SD, Raniah AM. " Image Confusion and Diffusion Based On Multi-Chaotic System and Mix-Column" , *Bull Electr Eng Inform*. 2021; 10(4): 2100-2109.

[32] Ahmed, M.H., Shibeeb, A.K., Abbood, F.H.,An Efficient Confusion-Diffusion Structure For Image Encryption Using Plain Image Related Henon Map,*International Journal of Computing*, 2020, 19(3), pp. 464–473