Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 8, S. 258-264, 2, 2024
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 8, pp. 258-264, 2, 2024
Copyright © 2024 IJANSER
Research Article

A Novel RGB color plane chaotic scrambling-based image encryption algorithm

Kenan İNCE^{*1}, Cemile İNCE ^{2}, Davut HANBAY ^{3}

[1]İnönü University, Software Engineering Department, Turkey, kenanince@gmail.com
[2]İnönü University, Computer Engineering Department, Turkey, cemile.ince@inonu.edu.tr
[3]İnönü University, Computer Engineering Department, Turkey, davut.hanbay@inonu.edu.tr

(Received: 06 March 2024, Accepted: 08 March 2024)

(4th International Conference on Innovative Academic Studies ICIAS 2024, March 12-13, 2024)

ATIF/REFERENCE: İnce, K., İnce, C. & Hanbay D. (2024). A Novel RGB color plane chaotic scrambling-based image encryption algorithm. *International Journal of Advanced Natural Sciences and Engineering Researches, 8(2), 258-264.*

Abstract: The 20th century ushered in the digital age, driven by the development and widespread adoption of information systems. While this digital landscape offers numerous advantages in communication, information access, and sharing, it has also brought significant concerns regarding the security of digital data. Encryption stands as the sole defense against unauthorized access to this data, using various mathematical operations to render it unreadable to unauthorized individuals. However, unlike text data, image data presents a unique challenge due to the high correlation between pixels. This necessitates the use of specialized algorithms distinct from standard encryption methods. The two fundamental stages of image encryption, mixing and diffusion, have been subject to diverse approaches, each with its inherent strengths and weaknesses. This study proposes a novel approach that merges the mixing and spreading steps of image encryption algorithms. The proposed method leverages a non-linear chaotic random number generator to mix the RGB color channels within the image. By combining the spreading phase with the mixing phase, we achieve a reduction in time complexity. The successful application of the proposed approach is demonstrated through the presented results.

Keywords- Image Encryption, Chaos Theory, Random Number, Color Plane Scrambling, Chebyshev Chaotic Map

I. INTRODUCTION

The field of cryptography, particularly its subfield of cryptanalysis, gained significant importance after World War II due to the increasing need for secure communication as information systems proliferated. The 20th century saw the rapid introduction of computers into daily life, further emphasizing the role of cryptography. The rise of the Internet and the vast number of interconnected devices in the era of Industry 4.0 have made robust cryptographic solutions even more critical. Encryption algorithms are now standard components of many software systems and communication protocols.

Within the context of this study, the encryption process aims to ensure data reaches its intended recipient from the sender in a secure and, ideally, reversible manner, while protecting it from unauthorized access. (Irreversible algorithms, such as hash functions, also fall under the umbrella of cryptography which represented as integrity in Figure 1.) Historically, the need for encryption began with textual data. However, the growing use of medical images, security footage, and personal visual data has highlighted the importance of image encryption. Due to the high spatial correlation and redundancy within image data, standard encryption methods often prove inadequate, necessitating image encryption as a distinct field of study.

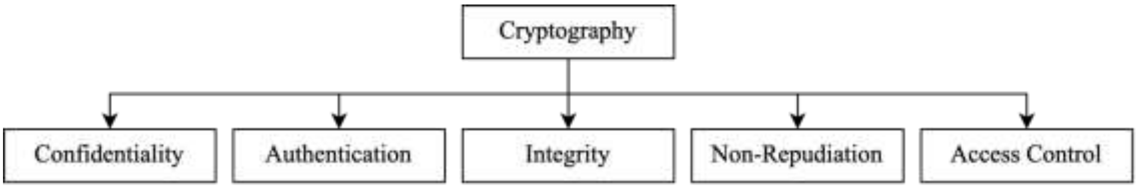


Figure 1. Basic fields of study and purposes of cryptography

Image encryption typically involves two fundamental stages: confusion and diffusion. The confusion stage generally focuses on altering the positions of image pixels without changing their values, essentially scrambling the image. The diffusion stage, on the other hand, modifies the pixel values themselves in a reversible manner to further enhance security. Common approaches for confusion in image encryption algorithms include permutation and substitution techniques. Well-known examples include ZigZag (Li, Zhao, & Yang, 2021; X. Wang & Chen, 2021; T. Zhang & Wang, 2023; X. Zhang & Liu, 2024), spiral (Q. Wang, Zhang, & Zhao, 2023; W. Zhang, Xu, & Zhao, 2023; X. Zhang, Liu, & Yang, 2023), corner traversal (İnce, İnce, & Hanbay, 2024), and 2D mapping (Alghamdi, Munir, & Ahmad, 2022). These techniques often have various modifications and optimizations. The primary goal of confusion algorithms is to obscure the original pixel relationships for unauthorized viewers. However, permutation-based approaches alone, while disrupting spatial correlation, leave pixel values unchanged, making them susceptible to statistical attacks like histogram analysis. Therefore, the confusion stage should be followed by a diffusion stage, or the chosen technique should incorporate both confusion and diffusion properties.

The proposed algorithm relies on a mathematical model to convert a two-dimensional image into a one-dimensional array, followed by reconstruction from this array. Figure 2 presents common serialization algorithms found in the literature. These algorithms have variations, including changes to starting points, increased sizes, and application to individual channels. However, Figure 2 depicts the most basic forms for clarity.

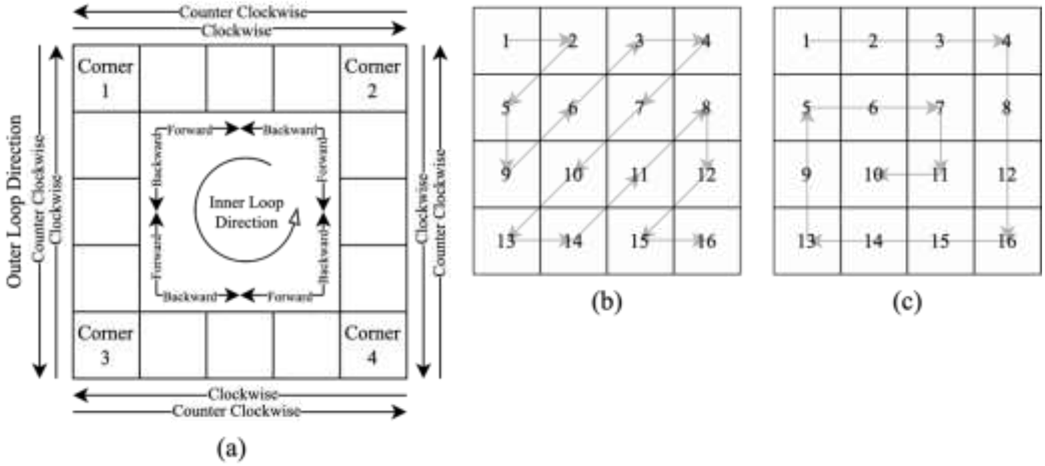


Figure 2. Basic serialization algorithm in the literature a) Cornering b) ZigZag c) Spiral

Different serialization algorithms offer distinct advantages and disadvantages. For instance, the Cornering algorithm boasts a high image mixing rate and positively affects the key area, but it suffers from implementation complexity. Conversely, ZigZag and spiral scan algorithms are relatively simpler to implement, yet they achieve lower mixing rates.

The proposed algorithm offers several key advantages:

1. Simple implementation: It is straightforward to implement.
2. Enhanced Scrambling: Unlike alternatives, it achieves a high shuffling ratio due to its method of mixing image color channels.

The remainder of the study will follow this structure:

Method Explanation: A detailed description of the proposed method will be presented.

Application Results: The practical results obtained by applying the proposed method will be presented and discussed.

Discussion: This section will include a critical analysis of the results, highlighting both strengths and weaknesses, and conclude the study.

II. MATERIAL AND METHOD

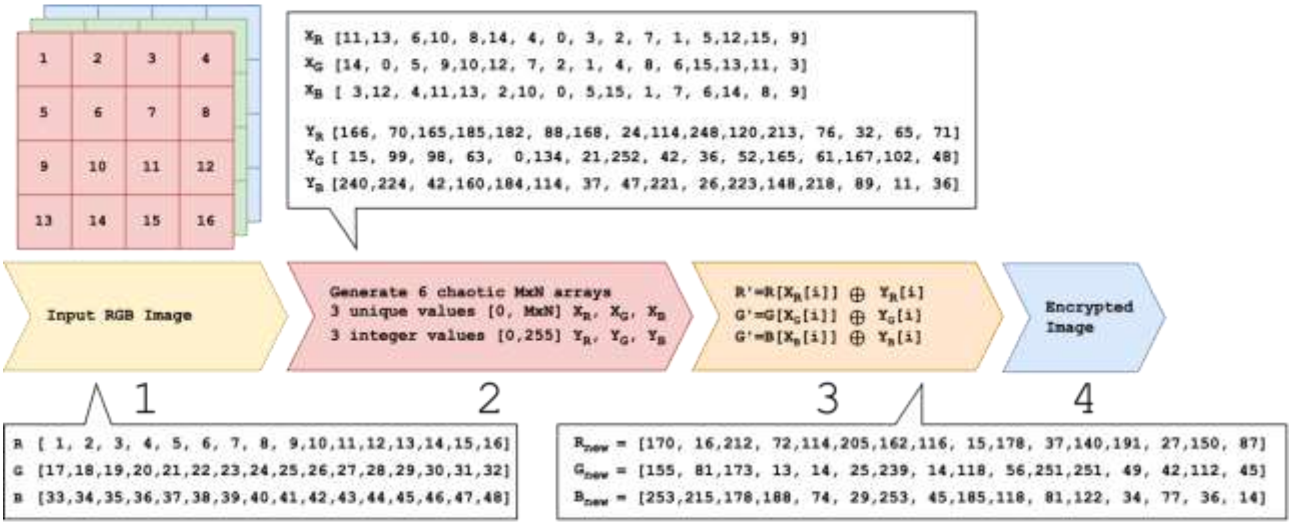
In this study, a new approach that mixes RGB color channels of color images is proposed. The proposed method uses a pseudorandom number generator, which is very important for cryptography (Ince, 2023). Although any pseudorandom number generator can be used (İNce, 2021), this study uses the Chebyshev chaotic map . Chebyshev map is a map with high chaotic properties and wide chaotic range. However, since it is 1B, it may cause a security vulnerability if not used carefully. The mathematical model of the Chebyshev map is presented in Equation 1.

$$X_{n+1} = \cos\left(\gamma \cos^{-1}(X_n)\right) \tag{1}$$

In Equation 1, γ is the control parameter of the map and X_n is the initial value. Chebyshev map shows chaotic behavior when $\gamma > 1$. However, when $1 < \gamma < 2$ the map shows unusual behavior. Therefore $\gamma > 2$ should be used for better randomness. And the starting point of X lies between [-1,1], however it is more chaotic at values close to the extreme points.

The proposed algorithm utilizes three distinct, non-repeating integer arrays, one corresponding to each color channel (red, green, and blue). These sequences are generated using the Chebyshev map. The map's initial values, $X_0 = 0.1578$ and $\gamma = 4.1871$, are chosen randomly, and then the sequences are produced. The dimensions of each array are MxN, matching the size of the input image.

A visual and simple numeric valued image encryption representation of the proposed scrambling algorithm is given in Figure 3.



```
XR [11,13, 6,10, 8,14, 4, 0, 3, 2, 7, 1, 5,12,15, 9]
XG [14, 0, 5, 9,10,12, 7, 2, 1, 4, 8, 6,15,13,11, 3]
XB [ 3,12, 4,11,13, 2,10, 0, 5,15, 1, 7, 6,14, 8, 9]

YR [166, 70,165,185,182, 88,168, 24,114,248,120,213, 76, 32, 65, 71]
YG [ 15, 99, 98, 63,  0,134, 21,252, 42, 36, 52,165, 61,167,102, 48]
YB [240,224, 42,160,184,114, 37, 47,221, 26,223,148,218, 89, 11, 36]
```

```
R [ 1, 2, 3, 4, 5, 6, 7, 8, 9,10,11,12,13,14,15,16]
G [17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32]
B [33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48]
```

```
Rnew = [170, 16,212, 72,114,205,162,116, 15,178, 37,140,191, 27,150, 87]
Gnew = [155, 81,173, 13, 14, 25,239, 14,118, 56,251,251, 49, 42,112, 45]
Bnew = [253,215,178,188, 74, 29,253, 45,185,118, 81,122, 34, 77, 36, 14]
```

Figure 3. Sample numerical presentation of proposed encryption algorithm

The heart of the proposed algorithm is the third step. In this publication, the third step was run as an iteration using a single chaotic map and the results were obtained. However, a total of 6 sequences can be produced with different chaotic maps, and the security of the encryption can be increased by running more rounds of the third step of the algorithm. As a result, the proposed framework implementation is a simple, high-security encryption scheme.

The figure presents a symbolic image for illustrative purposes. This image is a 4x4 color image consisting of three channels: red, green, and blue. Each channel is assigned a consecutive sequence of numbers: 1-16 for red, 17-32 for green, and 33-48 for blue. Random arrays are then generated with dimensions matching the image size (4x4) to facilitate the confusion and diffusion processes. Three sets of these arrays are used to confuse the color planes, while three additional sets are employed for the diffusion stage. Finally, the image is reconstructed using the new, scrambled values. The resulting image exhibits a transitional confusion of values between the color channels.

Figure 4 illustrates the results obtained using the proposed approach. Notably, only the mixing results for three color channels are presented individually. When comparing the image in the second row of Figure 4 with the scrambling results in Figure 5, the superior scrambling effectiveness of the proposed algorithm is evident.

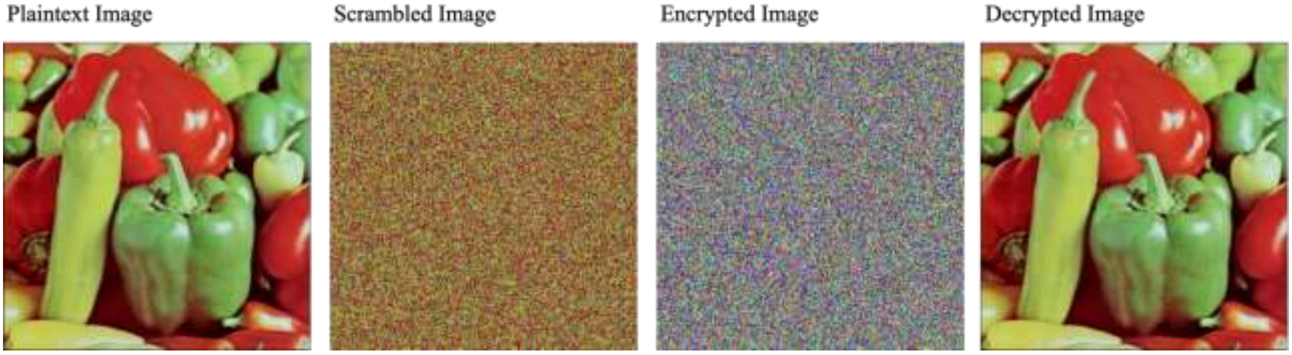


Figure 4. Scrambled and encrypted image results of proposed scheme

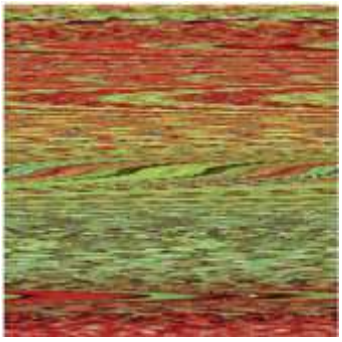


Figure 5. Standart ZigZag scrambling result of Peppers image

III. RESULTS

Statistical analysis is a cornerstone of cryptanalysis methods. It involves analyzing the frequency of characters in ciphertext, regardless of any shifts applied to the plaintext. Disrupting this statistical distribution is a key strategy to thwart such attacks. In the case of images, the color channels exhibit inherent statistical order in their frequency values. This vulnerability allows for statistical attacks on encrypted images. However, encryption methods that disrupt this order and achieve a uniform histogram distribution in the image are resistant to such attacks. Figure 6 demonstrates the effectiveness of the proposed approach, as it achieves a uniform histogram distribution across the independent color channels of the image.

Another crucial evaluation criterion is correlation analysis. Image data inherently possesses high correlation between neighboring pixel values. Ideally, an effective encryption algorithm disrupts this correlation. Therefore, a lower correlation coefficient between adjacent pixels in the encrypted image signifies a more robust encryption algorithm. Figure 7 illustrates the correlation analysis results obtained using the proposed approach.

Several criteria are employed to evaluate image encryption algorithms, including PSNR (Peak Signal-to-Noise Ratio), NPCR (Number of Point Changes), UACI (Unified Average Changing Intensity), and entropy. Notably, NPCR and UACI values assess an algorithm's resistance to differential attacks, where minor changes in the original image should result in significant alterations in the encrypted image. Table 1 presents the results for these four-evaluation metrics applied to the proposed algorithm. Ideally, NPCR and UACI values should approach 99.6094070% and 33.4635070%, respectively (Wu, Noonan, & Agaian, 2011), and Table 1 demonstrates the proposed algorithm's performance in achieving these targets.

For RGB images where each pixel has 8 bits, the maximum entropy value is 8. In an ideal scenario, the encrypted image's entropy should be close to 8. As evident in Table 1, the proposed algorithm achieves a high entropy value, indicating strong randomness in the encrypted image.

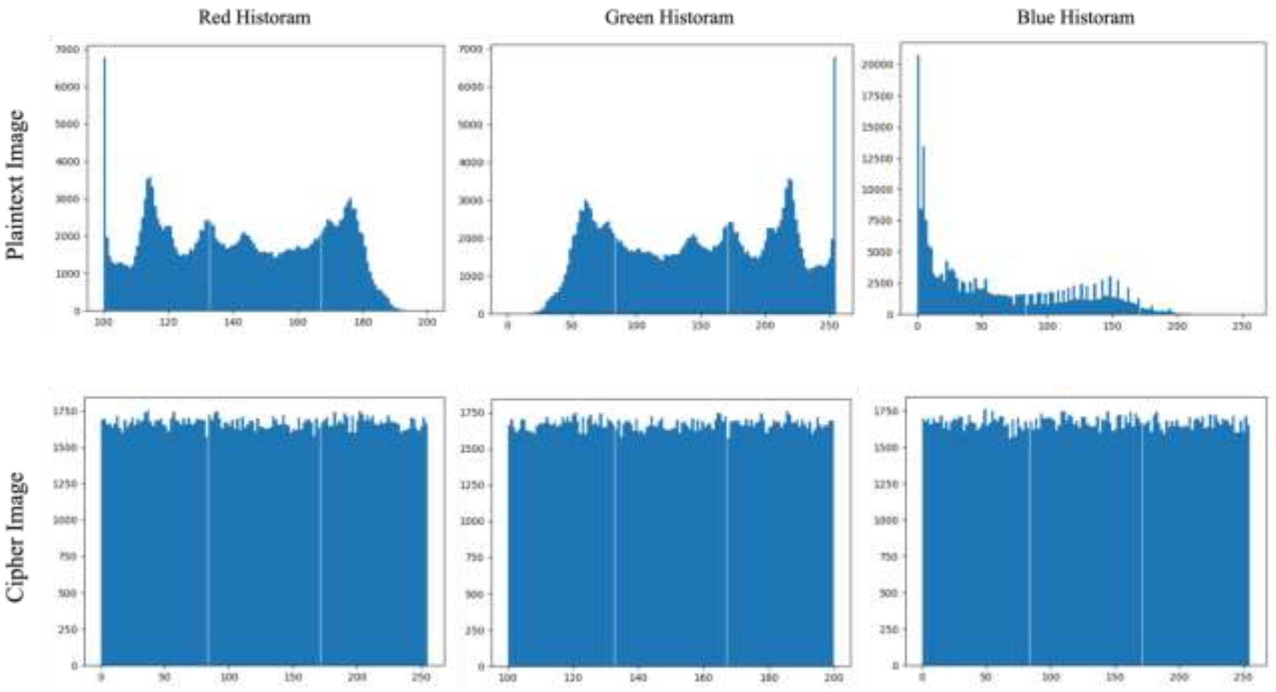


Figure 6. Histogram graphics of plaintext Peppers and cipher Peppers image

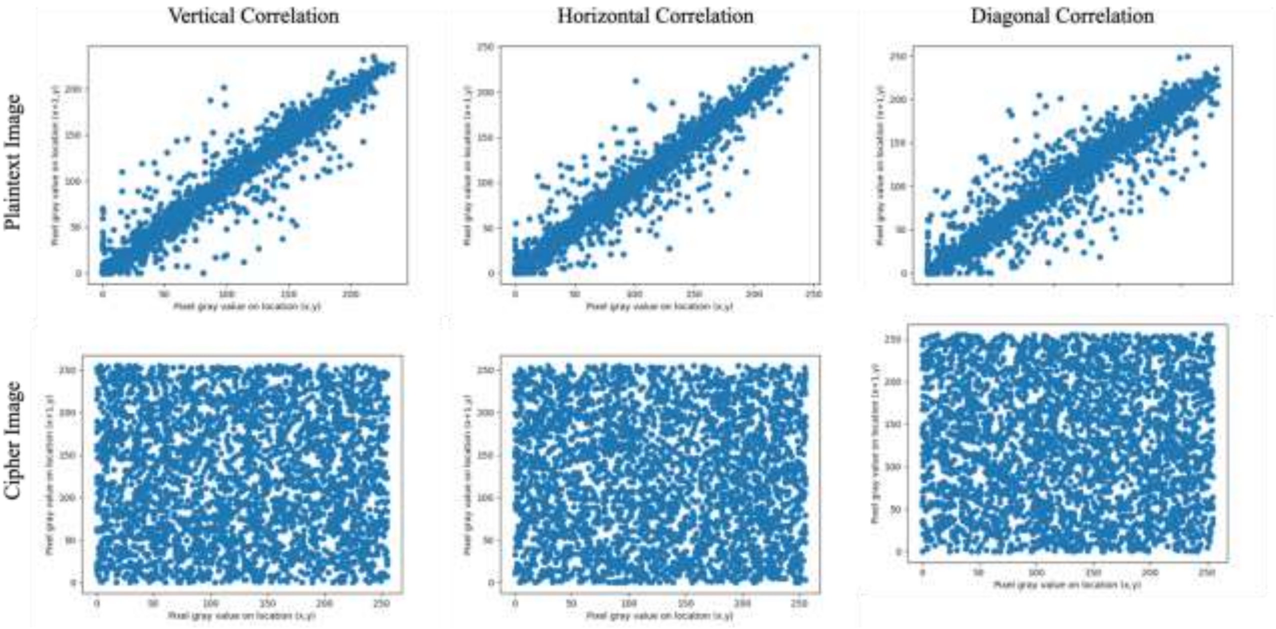


Figure 7. Vertical, horizontal and diagonal correlation comparison of plaintext and cipher Peppers image

Table 2. Image encryption evaluation metric results of proposed framework

Test Image	**PSNR**	**UACI**	**NPCR**	**Cipher Entropy**
Peppers	27.8916	33.4433	99.6455	7.9992
Baboon	27.9047	33.4637	99.6045	7.9997
Airplane	27.8929	33.4569	99.6051	7.9997

The resistance of an encryption algorithm to brute-force attacks is directly linked to the size of its key space. Smaller key spaces are more susceptible to being cracked with modern computing power. Currently, the minimum acceptable key size is generally considered to be 2^{128} or 2^{256} bits (Technology, 2023).

The proposed algorithm utilizes six distinct arrays, which significantly contributes to its key space size. Even though the employed chaotic map may be one-dimensional, different initial values are chosen for each array, requiring at least twelve decimal numbers as key parameters. Additionally, to enhance the chaotic complexity, a random number can be generated before producing the actual key parameters. This introduces further complexity, requiring a key size of at least 18 decimal digits (equivalent to the precision of single-precision IEEE floating-point numbers).

Based on these considerations, the estimated key space of the proposed approach is approximately 2^{576}. Furthermore, this key space can be readily increased by employing higher-order chaotic maps.

Table 3 compares the performance of the proposed method against existing studies based on key evaluation metrics, including entropy, NPCR, UACI, and key space. Among these crucial metrics, the proposed method demonstrates superior performance compared to alternative algorithms.

Table 3. Evaluation metric results literature comparison

Test Image	**Proposed**	**(Liu & Wang, 2023)**	**(Xie et al., 2023)**	**(Zhou, Qiu, Qi, & Zhang, 2023)**
Entropy	**7.9995**	7.9971	-	7.9987
NPCR	**99.6183**	99.61	99.63	99.60
UACI	**33.4546**	33.55	33.53	33.44
Key Space	**2^{576}**	2^{340}	2^{318}	2^{279}

IV. DISCUSSION

The evaluation results in the previous section demonstrate the effectiveness of the proposed algorithm. However, a potential concern regarding its time complexity might arise due to the generation of numerous random, non-repeating sequences using chaotic maps, equal to the number of image pixels. This is a valid criticism.

Fortunately, this challenge can be readily addressed through methods like 2D chaotic maps. By implementing such techniques, the required number of random numbers would significantly decrease, dropping from MxN size (image resolution) to M or N size.

In its current form, the algorithm takes an average of 15 seconds to encrypt a 512x512 image on a 2.3 GHz processor. While this encryption time surpasses conventional image encryption methods, it's important to consider the significant enhancement in encryption complexity and nonlinearity achieved by the proposed approach. This trade-off between speed and security justifies the use of a high number of chaotic sequences in the current implementation.

V. CONCLUSION

This study proposes a novel image encryption algorithm that deviates from conventional approaches. A key advantage is the ability to perform the mixing and diffusion steps concurrently during processing. The application of the proposed algorithm is straightforward and easy to grasp. Furthermore, the study demonstrates promising results based on established evaluation metrics. In conclusion, this work presents a highly efficient and extensible encryption scheme. The comparison results carried out in the study also reveal the success of the proposed method.

REFERENCES

Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution. *Entropy*, *24*(10), 1344. https://doi.org/10.3390/e24101344

İnce, C., İnce, K., & Hanbay, D. (2024). Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-18620-2

İNce, K. (2021). Java SecureRandom Kütüphanesi Güvenlik Analizi. *European Journal of Science and Technology*. https://doi.org/10.31590/ejosat.900956

Ince, K. (2023). Exploring the potential of deep learning and machine learning techniques for randomness analysis to enhance security on IoT. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00783-y

Li, S., Zhao, L., & Yang, N. (2021). Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion. *Security and Communication Networks*, *2021*, e6624809. https://doi.org/10.1155/2021/6624809

Liu, L., & Wang, J. (2023). A cluster of 1D quadratic chaotic map and its applications in image encryption. *Mathematics and Computers in Simulation*, *204*, 89–114. https://doi.org/10.1016/j.matcom.2022.07.030

Technology, N. I. of S. and. (2023). *Advanced Encryption Standard (AES)* (No. Federal Information Processing Standard (FIPS) 197). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.197-upd1

Wang, Q., Zhang, X., & Zhao, X. (2023). Color image encryption algorithm based on bidirectional spiral transformation and DNA coding. *Physica Scripta*, *98*(2), 025211. https://doi.org/10.1088/1402-4896/acb322

Wang, X., & Chen, X. (2021). An image encryption algorithm based on dynamic row scrambling and Zigzag transformation. *Chaos, Solitons & Fractals*, *147*, 110962. https://doi.org/10.1016/j.chaos.2021.110962

Wu, Y., Noonan, J., & Agaian, S. (2011). *NPCR and UACI Randomness Tests for Image Encryption*. Retrieved from https://www.semanticscholar.org/paper/NPCR-and-UACI-Randomness-Tests-for-Image-Encryption-Wu-Noonan/2b479abce221135af6065f9f8352e09cbfb5733a

Xie, Z., Sun, J., Tang, Y., Tang, X., Simpson, O., & Sun, Y. (2023). A K-SVD Based Compressive Sensing Method for Visual Chaotic Image Encryption. *Mathematics*, *11*(7), 1658. https://doi.org/10.3390/math11071658

Zhang, T., & Wang, S. (2023). Image encryption scheme based on a controlled zigzag transform and bit-level encryption under the quantum walk. *Frontiers in Physics*, *10*. Retrieved from https://www.frontiersin.org/articles/10.3389/fphy.2022.1097754

Zhang, W., Xu, J., & Zhao, B. (2023). DNA image encryption algorithm based on serrated spiral scrambling and cross bit plane. *Journal of King Saud University - Computer and Information Sciences*, *35*(10), 101858. https://doi.org/10.1016/j.jksuci.2023.101858

Zhang, X., & Liu, M. (2024). Multiple-image encryption algorithm based on the stereo Zigzag transformation. *Multimedia Tools and Applications*, *83*(8), 22701–22726. https://doi.org/10.1007/s11042-023-16404-8

Zhang, X., Liu, M., & Yang, X. (2023). Color Image Encryption Algorithm Based on Cross-Spiral Transformation and Zone Diffusion. *Mathematics*, *11*(14), 3228. https://doi.org/10.3390/math11143228

Zhou, S., Qiu, Y., Qi, G., & Zhang, Y. (2023). A new conservative chaotic system and its application in image encryption. *Chaos, Solitons & Fractals*, *175*, 113909. https://doi.org/10.1016/j.chaos.2023.113909