European Journal of Interdisciplinary Research and Development
Volume-18 August 2023
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

# A NEW IMAGE ENCRYPTION AND DECRYPTION ALGORITHM BASED ON A FOUR-DIMENSIONAL DYNAMIC SYSTEM

Abdulghafor Waedallah Abdulghafor 1,
Muthana S. Mahdi 2,
Amer Jelwy Mohammed 3
1 Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq, vip.mostansirya@gmail.com
2 Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq, muthanasalih@uomustansiriyah.edu.iq
3 Dewan Al-Waqf Al-Sunni, Baghdad, Iraq, amerjelewy@gmail.com

**Abstract**
With the rapid developments in the fields of multimedia and widespread use of the Internet, multimedia protection has become extremely necessary. Encryption, which prohibits an unauthorized individual from accessing sensitive data, is one of the best alternatives for achieving multimedia data protection that is sent over IoT devices. The chaotic systems of image cryptography have become an effective way to encrypt images in recent years due to their excellent protection. This study introduces a brand-new method for image encryption and decryption schemes. The new algorithm uses the Latin Square matrix depended based on a four-dimensional hyper-chaotic approach that achieves a security high level. The sequence chaotic generated by the system is used to diffuse and permute plain images of any size to produce encrypted images. Statistical measures have been used to analysis the Results such as the histogram, coefficient of correlation, and key sensitivity to examine the algorithm's performance. The experimental results show that the encrypted images have uniform histogram and entropy values between 7.99990 and 7.99991. The values of NPCR and UACI are close to ideal, with NPCR at 99.6825 percent and UACI at 33.4778 percent. Moreover, the method is robust against statistical, predictive, differential, and brute-force assaults because of its strong encryption performance, huge key space of 10168, and great sensitivity to small changes in the secret key.

**Keywords**: Four-Dimensional (4D) Hyper-Chaotic Systems, Cryptography, Image Encryption in IoT, Multimedia Security, New Algorithm..

## Introduction

In our culture, the rapid expansion of communication networks has resulted in a greater reliance on digitized information. As a consequence, data is now more vulnerable to misuse [1]. Because of the advancement of network and multimedia technology, the web is now moving toward multimedia data. Image, audio, and video are all examples of multimedia data video, text. [2]. Digital images have evolved into one of the most significant data carriers, with applications in biometric authentication, medical research, military, and online personal image albums, among others [3]. Text encryption is not the same as image encryption [4]. Conventional encryption methods are powerful ways to protect the data of the image. But because of the unique advantage

of image characteristics, like as strong redundancy and the capability of aggregated data, it is not suitable for image coding and shows some shortcomings and weaknesses. This makes the encrypted images weak and facilitates the attack via cryptanalysis [5].

Built on chaos Cryptography is based on the dynamics of non-linear maps or deterministic yet basic systems. As a result, it will have a quick and safe way to protect data sent over communication networks like the internet [6]. To achieve both high security and efficiency, several researchers developed a chaos-based image encryption technique [7]. Because of its great applicability and simplicity, a one-dimensional chaotic map has frequently been employed, such as a logistic map [8]. Furthermore, its disadvantages are its low security and small key size [9].

The sort of a standard square matrix, the set of N x N that's populated is known as a set of components of the N-token, with each image showing up precisely once in each push and column, with a Latin square of arranging N. The number of Latin squares is tremendous [10,11].

**Related Works**

Many four-dimensional hyper-chaotic systems have been implemented, some of which are built on color image encryption. Danial Roohbakhsh and Mahdi Yaghobi published a chaos-encryption algorithm for color images, in which the four-dimensional super chaotic Chen method is used to clutter the image, and the chaos produced by the system is used to clutter the image. The outcomes indicate that the encryption schema is more resistant to various attacks, and the histogram for encrypted images is standardized [12]. Hui Xu, Miao Zhang, Zhu Wang, Xiaojun Tong, and Yang Liu, reported a new autonomous four-dimensional hyperchaotic system to get a chaotic encryption scheme with high dimensions and enhance security. The new hyperchaotic system was constructed based on the Rabinovich chaotic system, and essential properties and dynamic behaviors of the new system are investigated to confirm its chaotic characteristics, depending on the random sequence produced from the new system. A new scheme was implemented in two stages image shuffling and pixel substitution. In the image shuffling stage, the rearrange operation is carried out to pixels of the plain image, while the second stage includes changing the pixel values for the plain image, the two stages are implemented to ensure the desirable security [13]. Jinling Liang, Tiantian Sun, Xia Huang, and Yuxia Li presented an encryption method for color images based on a fractional-order hyperchaotic scheme. The scheme produced four sequences of chaotic as a secret key. The encryption scheme was investigated using various security ..analyses such as statistical analysis, difference analysis, and keys pace [14]. A new encryption algorithm for images was proposed by Jian Zhang, Hong Ren, and Dezhi Hou it relies on DNA coding and the Chen hyperchaotic system. The method has two phases. The experiments show that the proposed scheme has a huge keyspace, is resistant to statistical analysis, and has other desirable properties [15].

**The Proposed Algorithm**

In this section, all details of the proposed algorithm will be presented

The Proposed Four-Dimensional (4D) Dynamic System

The Proposed new hyperchaotic system design characteristic with more complex dynamical behavior. The system uses ten terms, including eight control factors and six terms with quadratic cross-product nonlinear effects and expressed by the following mathematical model in Equation

$$\frac{dx}{dt} = ayz - bxz - cw$$

$$\frac{dy}{dt} = dx - xz - y$$

$$\frac{dz}{dt} = exy - fz$$

$$\frac{dw}{dt} = gxz + hzy$$

Where (x, y, z, w) are real numbers that make up the state variables of a dynamic system. The parameters (a to h) are positive. These variables are chosen after trying several times so that these periods can be reached that fulfill the conditions of the chaotic system. The proposed (4D) system in Equation (1) indicates a chaotic attraction when the beginning circumstances and system parameter values are set to the following values: a∈[18,18.5] , b∈[3.2,3.6] , c∈[2,2.5] , d∈[10,10.5] , e∈[3,3.5] , f∈[2.5,2.8] , g∈[5,5.5] , h∈[13,13.5], x(0)=0.2 , z(0)=0.6 , y(0)=0.4, and w(0)=0.8. The chaotic element behaviors in this nonlinear system are complicated and many of the intriguing attractors are shown in figures (1), (2), and (3).

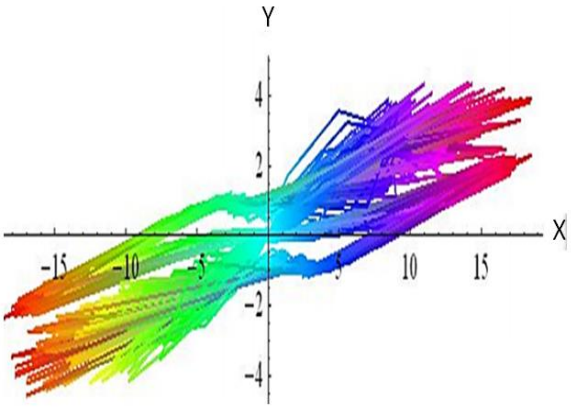


Figure. 1. Hyper chaotic attractors, 2D- view (y-x).

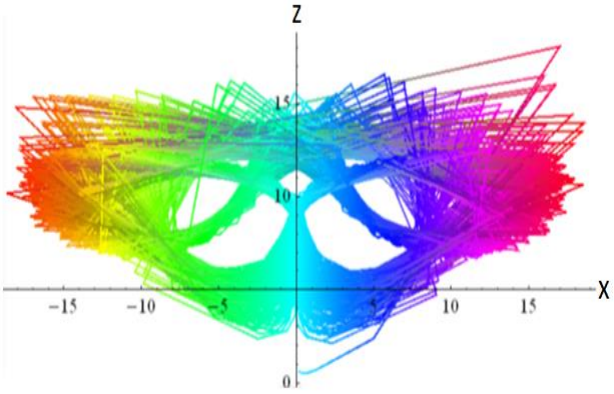


Figure. 2. Hyperchaotic attractors, 2-Dimensional view (z-x).

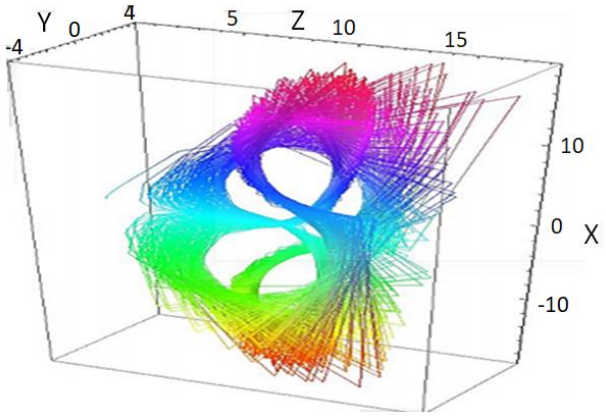


Figure. 3. Hyper chaotic attractors, 3D- view (y-z-x).

The numerical simulation was performed using the mathematics program. This nonlinear system exhibits many, intricate, and complicated chaotic dynamics phenomena.
Figures (1 & 3) display the strange attractors in two dimensions. Figure (2) displays the strange attractors in three dimensions. The topology of figures (1 & 3), for example, resembles the shape of a flying butterfly flapping its wings, hence the name "Butterfly Effect".
Some fundamental system features that have been researched are present in the proposed (4D) system. Three unstable balance points and estimated Lyapunov instances exist in the chaotic 4D system.
The Lyapunov types of the scheme are (Ly1= 1.4924), (Ly2= 1.9362), (Ly3= -2.6176), (Ly4= -31.0624). The maximal Lyapunov of the proposed scheme is Ly2= 1.9362). In expansion, the Lyapunov measurement is gotten as D-K-Y= 3.0243.

3.1.1 Equilibrium Point
The proposed system (4D) in Equation (1), includes three balance focuses when values for system parameters are indicated as takes after {a=18.1, d=10.4, e=3.2, g=5.2, b=3.2, c=2.3, f=2.7, h=13.3} and the nonlinear conditions should be unraveled as follows.

$$\begin{aligned} ayz - bxz - cw &= 0 \\ dx - xz - y &= 0 \\ exy - fz &= 0 \\ gxz + hzy &= 0 \end{aligned} \quad \text{.. (2)}$$

Three equilibrium points for the modern hyperchaotic system are obtained as follows: E1, E2, and E3. At that moment, each of the eigenvalues that compare to equilibrium E1 is obtained as follows: λ1 = -2.6, λ2 =-1, λ3 = 0, λ4 =0. Therefore, the equilibrium E1 could be a point of the saddle, and the hyperchaotic scheme is unsteady at point $E1$. Also, it is simple to show that the balance point $E2$ is additionally an unsteady saddle point.
Therefore, the equilibrium E1 is a saddle focus, and unstable. As the equilibrium point E3 was reached, the eigenvalues were as follows: λ1= -16.2588, λ2= -57.6623, λ3= 4.2047, λ4= 2.6415. Therefore, the equilibrium E3 is a saddle focus, and unstable. Thus, every point of the

equilibrium for the proposed four-dimensional system chaotic is unstable with E1 being the saddle point and E2 and E3 being focus points on the saddle.

3.1.2 Components and Dimensions of Lyapunov

The proposed 4D hyperchaotic scheme includes four Ingredients of Lyapunov (L). Since the proposed hyper-chaotic Lyapunov exponents L1 and L2 are positive, the remainder of the two Lyapunov types are negative. Hence, the suggested structure is hyper-chaotic.

The fractal estimation, which is also a usual feature of chaos, is computed using Lyapunov forms, and (DKY) for the current method can be obtained as follows [16].

$$D_{xy} = j + \frac{1}{\left|L_{j+1}\right|}\sum_{i=1}^{j} L_i$$

$$D_{xy} = 3 + \frac{1}{\left|L_{j+1}\right|}\sum_{i=1}^{3} L_i = 3 + \frac{l_{1+}L_{2+}L_3}{L_4} \qquad ..(3)$$

$$= 3 + \frac{1.4904 + 1.9342 + (-2.6706)}{31.0164} = 3.0243$$

3.1.3 Sensitivity to initial conditions

A chaotic system's greatest defining attribute is its long-term unpredictability. No matter how similar the two beginning circumstances are, they will ultimately diverge, as seen in Figures (4 and 5).

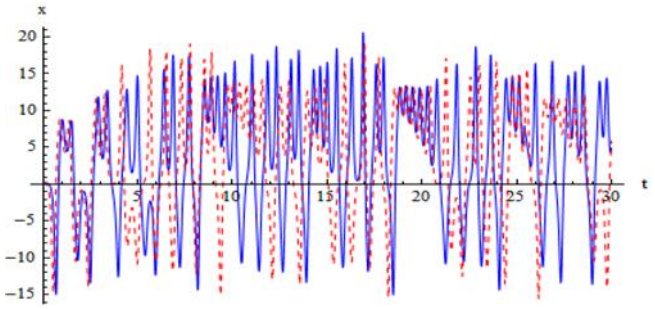


Figure. 4. Tests of sensitivity of the suggested scheme x (t).

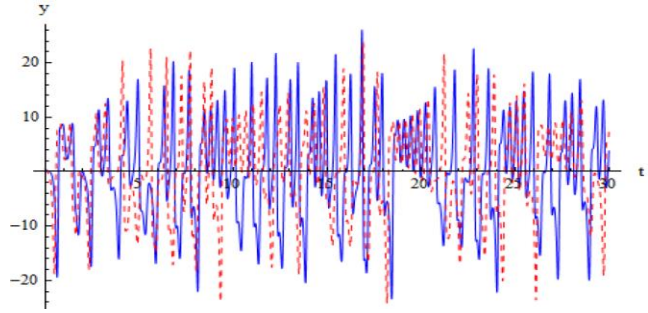


Figure. 5. Tests of sensitivity of the suggested scheme x (t), y (t).

Sensitive dependency on beginning circumstances is a term used to describe the non-periodic waveform of the system in Equation (1) and its increased sensitivity to the initial conditions.

3.2 The Proposed Encryption and Decryption Method

To increase the security and performance of encrypting/decrypting images communicated by IoT devices, this study shows how to construct a potent encryption system that depends on the system as a hyper-chaotic. Assume I have an R*C*3-sized plain image. A novel hyper-chaotic system is used to create chaotic vectors as the first step in the encryption process. The pixel coordinates in the plain image are then changed using these vectors to create a nice permuted image. A sort process in increasing order and swap operations will be used to carry out this task. The suggested encryption system's block diagram is shown in Figure (6).

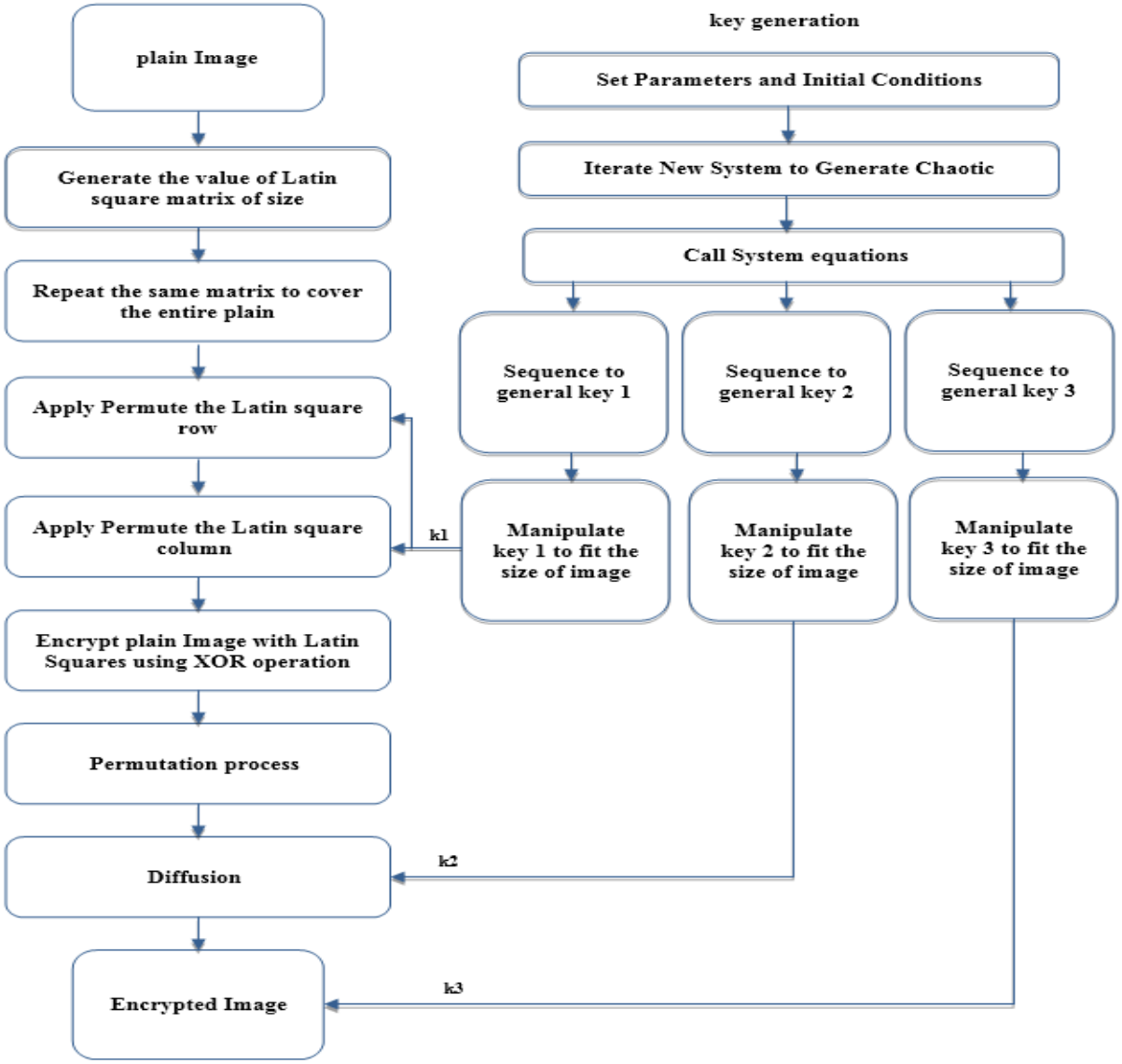


Figure.6. The proposed encryption method block diagram.

The encryption algorithm is divided into four stages: diffusion stage, permutation image pixel stage, Latin square stage, and chaotic sequence creation stage. The colored plain image is converted into an encrypted image with random properties throughout the encryption process to fend off statistical assaults. The plain image is encrypted using a bit-XOR technique and a Latin

square matrix. While the stage of diffusion comprises changing the values of pixels concurrently by employing the (bit-XOR) process. The pixel permutation stage incorporates permuting the positions of encrypted image pixels privately. Decryption is the opposite of encryption. The input here is an encrypted image and a secret key (parameter values and initial condition) and the output here is the decryption image. The suggested decryption system's block diagram is shown in Figure (7).

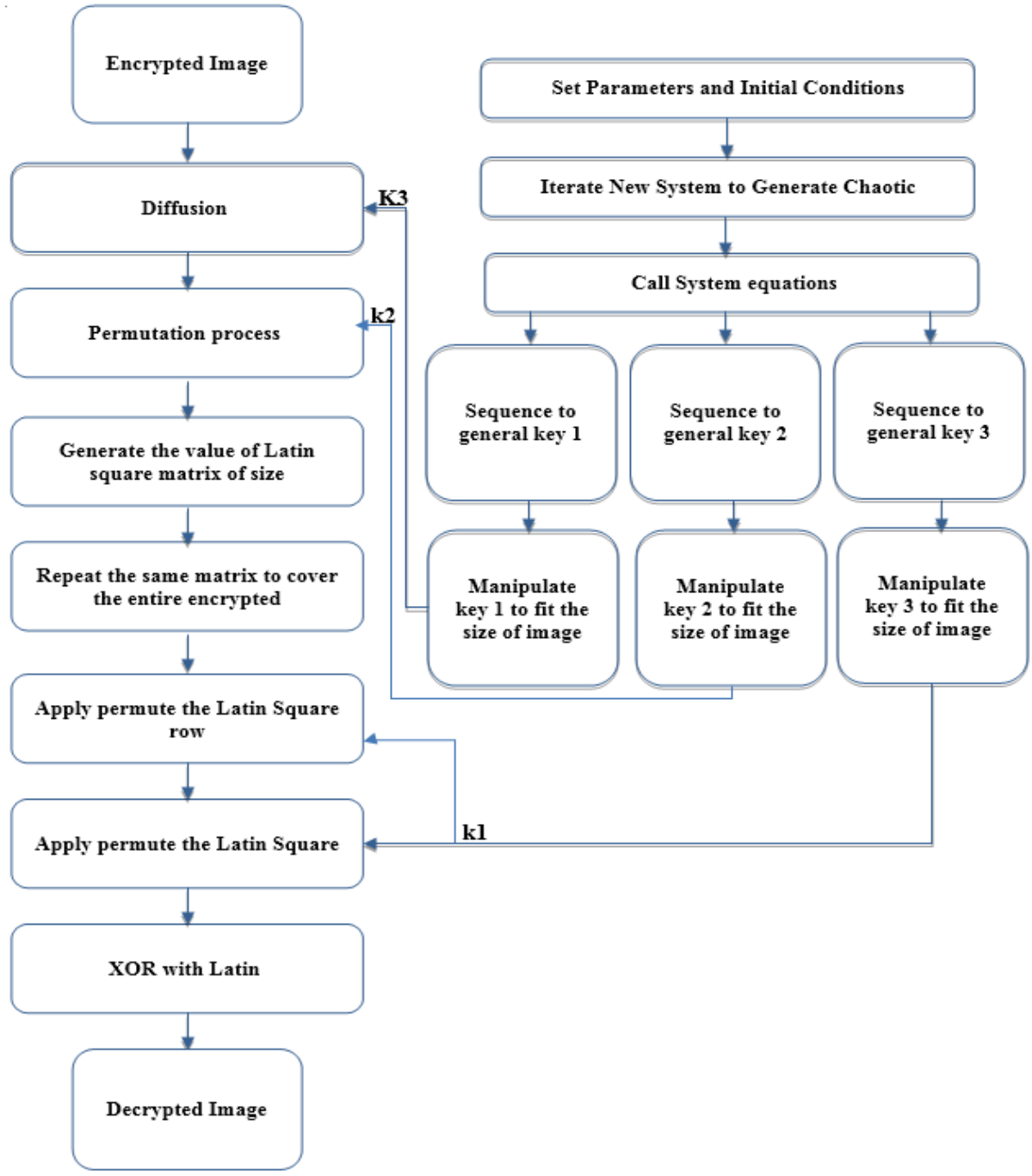


Figure.7. The proposed decryption method block diagram.

**Analysis and Results**

Several images have been processed using the proposed method. The proposed algorithm, on the other hand, can be used on any image of any size pixel.

Figure (8) shows a collection of color images of different sizes from the set used to evaluate this algorithm.

Figure. 8. An image from the set used to evaluate this algorithm. The original, encrypted, and decrypted image is in the first, second, and third columns from left to right, respectively.

The proposed algorithm will be checked for security and statistical analysis in the subsections that follow, and its efficacy will be demonstrated.

To demonstrate the encryption algorithm's security, the secret key must be extremely sensitive, and the keyspace length should be greater than 2128 to avoid brute force attacks Sensitivity Analysis, and correlation analysis is performed to illustrate that the proposed method is very effective against statistical attacks.

4.1 Security Analysis

In this section, the analytical operations performed on the proposed algorithm will be explained.

4.1.1 Histogram Analysis

Any statistical association between the plain image and the encrypted image can be prevented to prevent the retrieval of sensitive details from the plain image. Figure (9) and (10) displays the histogram of the original and associated encrypted images respectively.

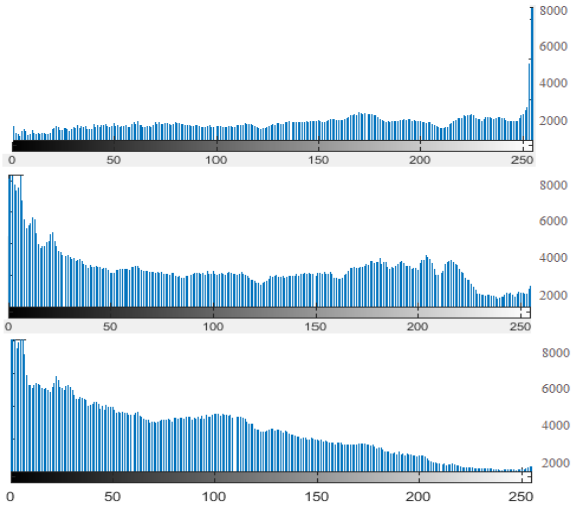


Figure. 9. The histogram for the plain images. The Red, Green, and Blue images are in the first, second, and third rows respectively.

The histogram of the encoded image must be fully smooth and distinct from the regular image to deter statistical attacks, which implies a consistent distribution over a random and full image scale [17].

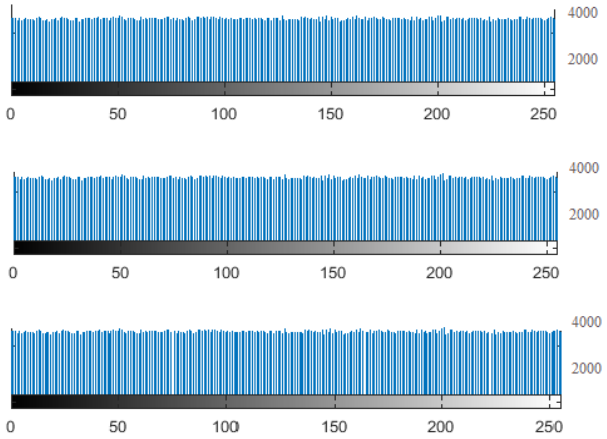


Figure. 10. The histogram for the encrypted images. The Red, Green, and Blue images are in the first, second, and third rows respectively.

4.1.2 Correlation Analysis Coefficient

Each pixel in a plain image is closely connected to its neighbors in either the diagonal or vertical, horizontal diagonal orientation, which is one of the fundamental properties of a plain image. To defend the system from statistical assaults, the correlation coefficients between pixels near the encoded image must be close to zero. These are the correlation coefficients that were calculated [18].

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})^2)(\frac{1}{N}\sum_{i=1}^{N}(Y_i - \bar{Y})^2)}} \quad ..(4)$$

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad , \quad \bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i$$

The analysis correlation between the images original and their cipher image for 2- adjacent pixels is shown in Table (1).

Table (1): The analysis correlation between the images and their cipher images.

| Image | plain images | | | encrypted image | | |
|---|---|---|---|---|---|---|
| | Hori-zontal | Vert-ical | Dia-gonal | Hori-zontal | Vertical | Diagonal |
| Fruit | 0.995 | 0.995 | 0.982 | -0.001 | 0.001 | -0.008 |
| Baby | 0.978 | 0.997 | 0.976 | 0.001 | 0.003 | 0.008 |
| Tree | 0.978 | 0.969 | 0.953 | -0.001 | -0.001 | 0.001 |

4.1.3 Information Entropy Evaluation Analysis

The most crucial aspects of randomization and their analysis of the encryption scheme. The following formula can be used to determine the source n's entropy [19]:

$$m = -\sum_{i=0}^{N-1} p(m_i) \log_2[p(m_i)] \quad ..(5)$$

The value of entropy must be near (9) Show from table (2) that encrypted image entropy values are extremely near to (9) and that the proposed encryption technique is robust and resistant to entropy attack.

Table (2) the encrypted image's information entropies.

| Images | Entropy |
|---|---|
| Fruit (1024 ×1024) | 7.99990 |
| Baby (576 ×1024) | 7.99991 |
| Town (462 ×462) | 7.99990 |

4.1.4 NPCR and UACI Analysis

Following is a summary of the two key quantifiers that were utilized to determine how sensitive the cryptographic system was to changes in the plain images in these two investigations [20].

$$\frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\%$$

$$UACI(c_1,c_2) = \frac{100}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} \frac{|c_1(i,j) - c_2(i,j)|}{255} \quad .. (6)$$

Table (3) demonstrates that all NPCR values of more than (99.6%) and UACI values between (33.4718) and (33.4778) are near the optimal value.

| NPCR | UACI | The Image |
|---|---|---|
| Fruit (**1024 ×1024**) | 33.4718 | 99.6315 |
| Baby (**576×1024**) | 33.4778 | 99.6147 |
| Town (**462 ×462**) | 33.4761 | 99.6825 |

The results for NPCR and UACI presented in table (3) show that all UACI and NPCR scores are close to the optimum score which is (99. 6825 percent) for NPCR and (33.4778 percent) for UACI. This indicates that the suggested encryption algorithm is strong enough to thwart the difference attack.

4.1.5 Peak Signal-to-Noise Ratio Analysis and Mean Squared

PSNR (Peak Signal-to-Noise Ratio) is a measure of encryption standards. The error of cumulative squared between the decrypted image and the original is known as the mean square

error (MSE). MSE with a lower value indicates less error. The lower PSNR score indicates a higher level of encryption accuracy [21]. Table (4) presents the results.

Table (4) the MSE and PSNR results.

| The Image | MSE | PSNR |
|---|---|---|
| Fruit(**1024 ×1024**) | 0 | 9.256838794 |
| Baby (**576×1024**) | 0 | 6.556829166 |
| Town (**462 ×462**) | 0 | 8.625879960 |

The PSNR and MSE result values accurately represent the suggested encryption algorithm's high level of security and are particularly suited for safe encryption systems.

4.1.6 Key Space Analysis

The keyspace makes sure that all feasible key sizes should be used for encryption. The keyspace size can reach the 〖(10^14)〗 ^12=10^168≈2^554 [19]. In this method, the initial parameters and conditions: (x0, y0, z0, w0), (a to h) were used as the secret key. If the precision is 10-14, the keyspace size can reach 10168 □ 2554], it is bigger than 2128 and it's big enough to withstand attacks [22].

4.1.7 Key Sensitivity Analysis

A good cryptosystem should be extremely sensitive to even minor changes in the key, as even a single bit change will result in a major change. Key sensitivity has two aspects: (A) sensitivity to encryption, where a small change in the encryption key results in a completely totally cipher image when utilized to the same plain image, and (B) sensitivity to decryption, where a tiny alter in the decryption key results in the cipher image becoming completely different when utilized to the same plain image. The encrypted image cannot be decrypted with a minor adjustment in the key. To test the key sensitivity, alter the beginning condition (x0) from having a value of (0.1) to (0.10000000000001), where extremely tiny variations in the key prevent the accurate recovery of the encrypted image [20]. Figure (11) shows the results in images that are very different from plain images, showing that the encryption system is capable of withstanding exhaustive assaults and has good key sensitivity [23].

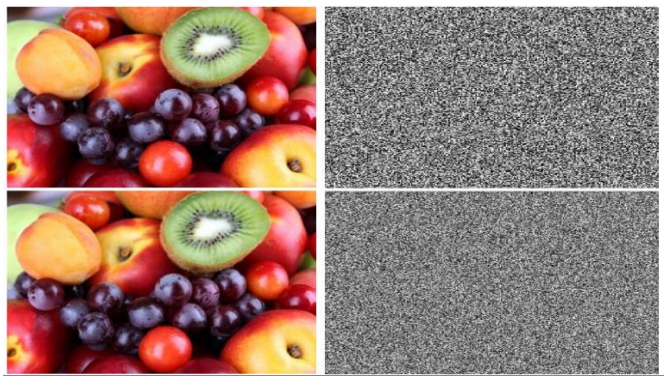

Figure. 11. Sensitivity analysis of Fruit Images. The image in the first row is the plain image and is encrypted from left to right, respectively. The image in the second row is a decrypted image and decrypted with the wrong key from left to right, respectively

## Conclusion

This paper presents the algorithm for encrypting colored images for image encryption/decryption schemes that are sent over IoT devices based on a proposed 4D hyperchaotic system. This algorithm can be used for both encryption and decryption. As opposed to other algorithms, the encrypted images have outstanding misunderstanding and diffusion properties. Signal-to-Noise Ratio (PSNR) and the algorithm's output (UACI) were assessed using analysis (Correlation Coefficient, Histogram, Information Entropy, Key Space, Pixels Number Change Rate (NPCR), Key Sensitivity, and Unified Average Changing Intensity). The outcomes of the experiment show that the encrypted images have a uniform histogram and the entropy values were between 7. 99990 and 7. 99991, and the NPCR and UACI scores are close to the perfect value (99.6093 percent for NPCR and 33. 4778 percent for UACI). As a result of these findings, the proposed algorithm has a high level of security.

## Acknowledgments

The authors thank the Department of Computer Science, College of Science, Mustansiriyah University, for supporting this work.

## References

[1] J. Sekar & C. Arun, "Comparative performance analysis of chaos-based image encryption techniques". Journal of critical reviews, 7(9), 2020.

[2] A. R. W. Sait, J. Uthayakumar, K. Shankar, & K. S. Kumar, "Introduction to multimedia tools and applications". In Handbook of multimedia information security: Techniques and applications (pp. 3-14). Springer, Cham, 2019.

[3] M. S. Mahdi & Z. L. Ali, “A lightweight algorithm to protect the web of things in IOT,” in Proc. of Int. Conf. on Emerging Technology Trends in Internet of Things and Computing, pp. 46-60, 2022.

[4] X. Wang, Y. Li, & J. Jin, “A new one-dimensional chaotic system with applications in image encryption”, Chaos, Solitons & Fractals, 139, 110102, 2020.

[5] M. Alawida, J. S. Teh, D. P. Oyinloye, M, Ahmad, & R. S. Alkhawaldeh. “A new hash function based on chaotic maps and deterministic finite-state automata”, IEEE Access, vol. 8, pp. 113163-113174, 2020.

[6] M. Kaur, & V. Kumar, “A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering”, Archives of Computational Methods in Engineering, vol. 27, no. 1, pp. 15-43, 2020.

[7] W. Feng, Y. G. He, H. M. Li, & C. L. Li. “Cryptanalysis of the integrated chaotic systems-based image encryption algorithm”, Optik, vol. 186, pp. 449-457, 2019.

[8] D. Lambić, “A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design”. Nonlinear Dynamics, vol. 100 no. 1, pp. 699-711, 2020.

[9] F. Özkaynak, “Brief review on application of nonlinear dynamics in image encryption”, Nonlinear Dynamics, vol. 92, no. 2, pp. 305-313, 2018.

[10] M. S. Mahdi, & S. N. Alsaad, "Detection of Copy-Move Forgery in Digital Image Based on SIFT Features and Automatic Matching Thresholds", In International Conference on Applied Computing to Support Industry: Innovation and Technology, Springer, Cham, pp. 17-31, 2019.
[11] R. J. Stones "K-plex 2-erasure codes and Blackburn partial Latin squares ". IEEE Transactions on Information Theory, vol. 66, no. 6, pp. 3704-3713, 2020.
[12] D. Roohbakhsh & M. Yaghoobi, "Color Image Encryption using Hyper Chaos Chen", International Journal of Computer Applications, vol. 110, no. 4, 2015.
[13] X. Tong, Y. Liu, M. Zhang, H. Xu, & Z. Wang "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", Entropy, vol 17, no. 1, pp. 181-196, 2014.
[14] X. Huang, T. Sun, Y. Li, & J. Liang, "A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System", Entropy, vol.17, no. 1, pp. 28-38, 2014.
[15] J. Zhang, D. Hou & H. Ren, "Image Encryption Algorithm Based on Dynamic DNA Coding and Chen's", Mathematical Problems in Engineering, Article ID 6408741, 2016.
[16] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, & M. F. Ijaz. "Analytical study of hybrid techniques for image encryption and decryption", Sensors, vol. 20, no. 18, pp. 5162, 2020.
[17] B. Zhang, B. Rahmatullah, S. L. Wang, A. A. Zaidan, B. B. Zaidan, & P. Liu, "A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations", Multimedia Tools and Applications, PP. 1-40, 2020.
[18] D. Zhang, L. Chen, & T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation". Entropy, 23(3), 361, 2021.
[19] R. M. Kumar & M. K. Viswanath, "A symmetric medical image encryption scheme based on irrational numbers", Biomedical Research, Special Issue, 2018.
[20] R. C. Barik & S. Changder, "A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps". Multimedia Tools and Applications, vol. 80, no. 7, pp. 10723-10760, 2021.
[21] L. Zhu, D. Jiang, J. Ni, X. Wang, X. Rong, & M. Ahmad "A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map". Information Sciences, 607, 1001-1022, 2022.
[22] A. Kifouche, M. S. Azzaz, R. Hamouche, & R. Kocik, "Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications", International Journal of Information Security, 1-16, 2022.
[23] N. Chaudhary, T. B. Shahi, & A. Neupane, "Secure Image Encryption Using Chaotic", Hybrid Chaotic and Block Cipher Approach. Journal of Imaging, 8(6), 167, 2022.