



ENHANCEMENT OF IMAGE ENCRYPTION SECURITY THROUGH CHAOTIC SYSTEM AND KERNEL-BASED DIFFUSION

Hadeel Jabbar Shnaen^{*1}, Sadiq A. Mehdi², Kadhum I. Khalaf³

¹Mustansiriyah University, College of Education, Department of Computer Science, Baghdad, Iraq

²Mustansiriyah University, College of Education, Department of Computer Science, Baghdad, Iraq

³Baghdad University, College of Administration and Economics, Department of Statistics

*Correspondance: a.hadeel.albahadili@gmail.com

Abstract: In this paper a new encryption strategy is introduced by combining Kernel functions with systems and XOR operation to make data more secure and ensure that data can be retrieved accurately. The method creates data obfuscation by placing data in higher dimensional space using Kernel functions. On the hand chaotic models add unpredictable behavior to make the system much stronger against advanced cryptographic attacks. The new system is safer than methods. It hides the information well through complicated mathematical changes. Experiments are set up. Studied to prove that the approach offers a high level of security against difficult attacks while also keeping the flexibility needed to get the original data back. The test outcomes indicate that a high NPCR value of 99.6072 signifies substantial pixel alteration during encryption, which is advantageous for security. The PSNR value (8.0996) is crucial for maintaining image quality. This value shows that little information was lost during the encryption. The optimum UACI score (31.132%–35.215%) indicates that the encrypted image has few visual distortions and artifacts.

Keywords: Encryption, Chaotic System, Kernel Function, Decryption, Initial Conditions, Sensitivity, Correlation

Introduction

The significant increase of digitally recorded images and videos has intensified the need for safeguarding audio-visual content. The purpose of image and video encryption is to obscure sensitive information and prevent breaches of confidentiality [1],[2]. The significant correlation among neighboring pixels renders conventional encryption methods, such as symmetric-key AES and public-key RSA, inadequate in terms of security, failing to achieve the necessary levels of confusion and diffusion for image data.

Image encryption, in particular, divides an image into smaller segments before encrypting each segment independently in a random sequence utilizing a chaotic framework based on fractional-order differential equations, with pixel confusion

achieved through a nonlinear piecewise function. The amalgamation of kernel function with chaotic system update yields a significant degree of diffusion in image data. [3]

Related Works

Review of previous studies is a great help for the research process, which helps to find out the information gaps and to construct a full analysis and a deep understanding. It contributes to the development of a solid theoretical foundation for current research, the identification of strengths and flaws, and the identification of opportunities for additional exploration.

A. S. Budi, A. F. Rochim, and K. T. Martono(2021)

This study concentrated on the utilization of Radial Basis Functions (RBF Kernel) in the context of chaotic systems. Research indicates that the application of the RBF Kernel facilitates intricate nonlinear modifications among the optical elements of pixels, hence enhancing the encryption of vital information and security evaluation with improved resistance to chosen-plaintext assaults [4].

Luoyin Feng, Jize Du, Chong Fu, and Wei Song (2023)

In the present study, the integration of convolutional neural networks (CNN) with chaotic sequence generators was explored. Stochastic convolution kernel and activation output medium were provided by using chaotic sequences as necessary generators. Then the convolution process was used to simultaneously encode and compress the image, resulting in robust encryption for statistical attacks [5].

Shnaen, H. J., & Mehdi, S. A. (2024)

In this paper, a unique color image encryption scheme is proposed to provide high data security by utilizing multi-dimensional chaotic dynamics and high sensitivity to data changes. Alters the basic characteristics of the key generation operation by the use of the "delta feature". Thus, even a small change in the initial image completely changes the resulting encryption keys [6].

Xiaoqiang Zhang, Pengfei Chen, and Xueheng Zhang (2026)

A new two-dimensional chaotic mapping is formulated. In contrast to conventional chaotic systems, it demonstrates enhanced chaotic efficacy and a broader parameter spectrum; additionally, the suggested algorithm aims to transform the original image into three dimensions, succeeded by 3D concurrent scrambling and diffusion; furthermore, a 2D exclusive OR (XOR) operation is executed for additional diffusion; ultimately, the 3D matrix is consolidated to produce the encrypted image [7].

Structure of 4D Chaotic System

A four-dimensional hyperchaotic system characterized by 10 positive parameters is introduced. It possesses more intricate characteristics than chaotic systems of lesser dimensions. A completely novel 4D autonomous system can be derived from the subsequent differential equation within the system (1).

$$\begin{aligned}\frac{dx}{dt} &= -ax - bw + cyz + ze^y \\ \frac{dy}{dt} &= dy + ex - fxz - xe^z \\ \frac{dz}{dt} &= -gz + hxy\end{aligned}\quad (1)$$

$$\frac{dw}{dt} = -bw + ixz + jyz$$

The states of system are x, y, z , and $w, t \in \text{real number}$ and the positive parameters are $b, d, a, c, g, e, h, f, j, i$ which displays a chaotic attractors in the new 4-D chaotic system by the initial conditions of: $x_0 = 0.2, y_0 = 0.4, z_0 = 1.5$, and $w_0 = 0.8$ and parameter values of: $a = 3.1, b = 2.1, c = 15.8, d = 1.1, e = 16.5, f = 1.5, g = 2.4, i = 5.1, h = 26.6$, and $j = 12.9$. [8]

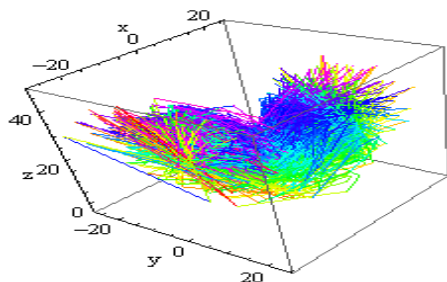


Figure 1. View of chaotic attractors in three dimensions (x-y-z)

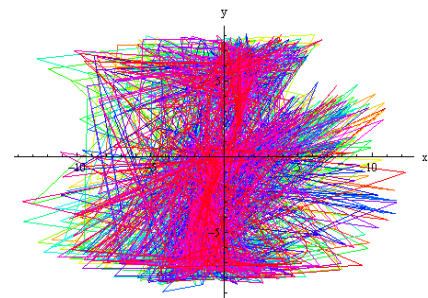


Figure 2. Chaotic attractors, x-y phase plane

The sensitivity to initial conditions of the chaotic system

Prolonged uncertainty is arguably the most essential trait of a chaotic system. This arises from the sensitivity of the solution's dependence on beginning factors. Two distinct initial conditions will ultimately diverge significantly, even if they commence in proximity. Consequently, for each initial condition possessing a limited degree of precision, there will eventually arise a moment when valid forecasts regarding the system's state become unattainable [8].

Proposed encryption algorithm

There are strict rules in several areas about keeping data safe and protecting privacy of people especially in relation to sensitive information. Image encryption is used to comply with numerous laws and regulations. It protects data transfers, be it over the Internet or internal networks. This protects photographs from modification or theft during transfer. The encryption of color images has many challenges especially the file size increase and the compatibility with different image applications and software. Therefore, our proposed system is to provide a balance between strong security and best performance especially for high resolution images.

1. Image Encryption Stage

The encryption stage of the suggested system is a crucial component comprising the following distinct procedures.

2. Image loading

Various color image types and sizes are uploaded to the proposed method, where the images to be encrypted are submitted.

3. Applying the Kernel Function to the Image:

A kernel function is a nonlinear transformation designed to elevate data into a higher-dimensional space, hence complicating decryption. A kernel function (such a Gaussian function or an analogous function) is utilized on the complete image to

convert the data into a different space. Kernel functions may be employed to enhance the intricacy of the encrypted information.

$$= \frac{1}{nh} \sum_{i=1}^n k\left(\frac{x_i - x}{h}\right)$$

4. Calculating the variance of the encoded image:

Subsequent to the application of the kernel function on the image, the variance of the encoded image is determined.

5. Applying XOR to the encrypted image:

After calculating the variance, a series of XOR operations is performed on the encrypted image using a secret key (generated randomly or via a 4D chaotic function).

6. Generating Random Keys from 4 Hyper- Chaotic System

This methodology use a hyper 4D chaotic system to produce the image flipping and encryption keys. As demonstrated in the subsequent equations:

$$\begin{aligned} \frac{dx}{dt} &= -ax - bw + cyz + ze^y \\ \frac{dy}{dt} &= dy + ex - fxz - xe^z \\ \frac{dz}{dt} &= -gz + hxy \end{aligned} \quad (1)$$

$$\frac{dw}{dt} = -bw + ixz + jyz$$

Decryption Image Stage

A decryption algorithm retrieves the original information from the encoded data. The proposed image encryption method demonstrated the process of encrypting an input image through a hyperchaotic system and the XOR operation. In this instance, the decryption technique is the inverse of the encryption procedure and involves reversing the operations performed during encryption to retrieve the original image [9]. Thus, the proposed decryption method aims to retrieve the original image from the encrypted data by employing the identical hyperchaotic system and XOR operation utilized in the encryption procedure.

Security Analysis

The examination of an image encryption technology includes its capacity to safeguard private image information from illegal access or modification. Test the algorithm's encryption strength so that the adversary even having the access to the encrypted image is not able to decode the contents without the correct decryption key. We need to estimate the computing efficiency of the algorithm. Strong security is vital, but the technique must be simple and user-friendly; complexity may prevent practical use [10].



Figure 3. illustrates the histogram for each the Original /Encryption image and Decryption Image using the proposed algorithm.

1. Histogram analysis

In an effort to reduce the probability of acquiring key information from the raw image, it is important to remove any statistical correlation between the raw image and the encrypted version of the image. Moreover, to enhance security against statistical attacks, the histogram of the encrypted image should be uniform and different from the histogram of the unencrypted image [11].

Table 1. Correlation coefficients between the original images and the encrypted images utilizing the proposed methodology.

Image		Correlation Coefficient for Original Image			Correlation Coefficient for Encryption image		
		H.	V.	D.	H.	V.	D.
Girl	256x256	0.9746	0.9653	0.9522	0.0023	0.001	0.0015
Lena	512x512	0.9668	0.9751	0.9530	-0.0001	-0.0006	0.0012
Peper	512x512	0.9656	0.9678	0.9644	-0.0014	0.0011	0.0001
Bboon	512x512	0.8826	0.75386	0.72134	-0.0016	0.0032	0.00004

2. The correlation coefficient

It is a statistical metric utilized to evaluate the correlation between two random variables or data sets and to quantify the similarity between two images. In table (1), a correlation coefficient nearing 1 signifies a robust positive association. In the realm of image encryption, this implies that an enhancement in one variable (such as encryption strength or security) corresponds with an improvement in the other variable (such the quality of the encrypted image). A favorable association indicates that stronger encryption leads to enhanced image security. When the result of the calculation is 0, a definitive correlation between the encryption robustness and the caliber of the encrypted image is absent. A correlation value nearing -1 signifies a strong inverse association [12].

3. Key Sensitivity Analysis

A slight change to any single parameter, without any other adjustments, will modify the encrypted image. The elucidation of this concept can be obtained by examining the fluctuations in pixel values between the encrypted image and its original version on an individual pixel level. The principal element affecting the

strength of a cryptographic method is its ability to endure a vast array of possible key variations, particularly around 10^{15} , prior to the opponent's expected proficiency in determining the accurate key with considerable confidence [13].

Table 2. Entropy values to the original / encrypted and decrypted images using the proposed system.

Image	Entropy_Original image	Entropy _Encryption Image	Entropy_Deryption image
Girl 256x256	7.1834	7.9991	7.1825
Lena 512x512	7.4871	7.9997	7.4882
Peppers 512x512	7.7153	7.9997	7.7252
Baboon 512x512	7.7649	7.9998	7.7649

4. Information Entropy Analysis

Entropy quantifies the degree of unpredictability or informational density inside an image [14]. Table (2) illustrates that the entropy of the original image ranges from 7.4871 to 7.7649. In this instance, the initial image seems to have a moderate to high level of information density, potentially encompassing a variety of pixel values or patterns. The entropy of the encrypted image (7.9991 to 9.9998) is markedly greater than that of the original image. This indicates that the encryption procedure has introduced a significant degree of randomness or intricacy to the image. A substantial entropy value in the encrypted image is frequently advantageous as it signifies enhanced security and complicates the efforts of unauthorized individuals to scrutinize or decode the image.

Table 3. Elapsed time to generate keys/Encryption and Decryption images using the proposed system.

Image	Elapsed time to create keys	Elapsed time to Encryption	Elapsed time to Decryption
Girl 256x256	0.379063	0.468104	0.469214
Lena 512x512	1.642138	2.082405	1.946376
Peppers 512x512	0.964617	1.945104	1.954841
Baboon 512x512	1.012612	1.969175	1.982390

5. Time Analysis

Temporal assessment within the realm of encryption methods refers to quantifying the computing duration necessary for executing encryption and decryption processes .Table 3 displays the duration of encryption for the image, which ranges from (0.46810 to 1.9691)seconds. The durations inside this interval seem to be sensible and fairly effective for image encryption, with the decryption duration likewise aligning with the encryption time. This implies that the decryption procedure mirrors the encryption process regarding computing complexity and duration. Resilient encryption techniques ought to necessitate an unfeasible duration

for decryption in the absence of the appropriate key, rendering it computationally unviable for adversaries to compromise the encryption [6],[15].

Table 4. PSNR and MSE Using Proposed System.

Image	Encryption Image		Decryption Image	
	MSE	PSNR	MSE	PSNR
Girl 256x256	9456.4218	7.3128	0	Inf.
Lena 512x512	6331.1517	8.3974	0	Inf.
Peppers 512x512	7364.1514	8.0996	0	Inf.
Baboon 512x512	5526.7531	8.8126	0	Inf.

6. Peak Signal-to-Noise Ratio (PSNR)

PSNR assesses image quality by contrasting it with an ideal reference image. When PSNR reaches infinity, the decrypted image exhibits no noise or distortion relative to the original. MSE (Mean Square Error): quantifies the mean squared disparity between the original image and the encrypted image on a pixel-by-pixel level. When the Mean Squared Error (MSE) is 0, it indicates that there is no disparity between the original and decrypted images, signifying flawless reconstruction, as shown in Table (4) [16].

Table 5. NPCR and UACI using the proposed system

Image		NPCR	UACI
Girl	256x256	99.6098	35.2159
Lena	512x512	99.5997	31.1323
Peppers	512x512	99.6035	33.1772
Baboon	512x512	99.6072	32.8194

7. Unified Average Changing Intensity (UACI)

It measures the average intensity change between the original and encrypted images. It is used for the evaluation of the resilience of the encryption mechanism. The UACI values for image encryption are shown in Table (5) from 31% to 35% reflecting different degradation levels of quality relative to the original images. The exact impact on image quality will depend on the encryption algorithm, compression settings, and the nature of the image itself. Lower UACI values indicate better quality and higher values indicate great quality loss. But it is robust for various attacks. NPCR measures the percentage of the pixels changed after one bit change to the plaintext (original image) before encryption. A NPCR grade of (99.6098) means that if a single bit in the original image is changed and then the altered image is encrypted using the evaluated encryption system, then about 99.6098% of the pixels of the encrypted image are different from the original encrypted image [17].

8. Key space analysis

The key space for cryptography is the number of possible keys used in the cryptographic process. It plays an important role in the protection of encrypted data. A larger key space makes it more difficult for adversaries to use exhaustive search

attack (brute-force attack) to find the correct key [18].

$$\text{Key Space} = (10^{15})^{14} = 10^{210}$$

So, the key space for this cryptographic system is $10^{210} \sim 2^{697}$, which is a considerable number, making it highly secure against brute-force attacks.

Conclusions

Efficiency and security of the color image encryption algorithm based on 4D chaotic system. The entropy value of 7.9998 shows that the encrypted image has a high degree of randomness and complexity, which is good for algorithms used for encryption. The correlation coefficient is 0.00141, which means a very low correlation, hence the encrypted image has very low redundancy. This feature, therefore, becomes a major hurdle for potential attackers, as it prevents them from exploiting patterns or forming links in the encrypted data. The NPCR is found to be 99.6098. The high value of NPCR indicates that a small modification in the source image will be changed to a great extent in the encrypted image, which in turn increases the security. The value of the Unified Average Changing Intensity (UACI) is 33.1772. A large UACI value means that the algorithm is able to spread the impact of the encryption key throughout the whole image and so ensure good diffusion. The key space is huge of size 2^{697} . The vast key space ensures a very high number of viable encryption keys, which makes brute-force attacks computationally infeasible for potential attackers. Encryption time for 256×256 image is 0.468104, compared with 512×512 image, which shows that the encryption method may be used for higher image size. Finally, the technique shows robustness, and it is suited for image encryption with a good level of security, minimal correlation, and significant diffusion. The large key space and the proper temporal rate increase the functionality of the system and its resistance to attacks.

Challenges and Future Directions

The proposed algorithm has a great potential in improving security. However, there are some issues about system performance when the kernel function and chaotic system are used. These factors may increase the computational complexity and increase the time of decryption and encryption tasks. Additional testing and assessment may be required to evaluate the operational effectiveness of the algorithm in real-world scenarios. In addition, the implementation of chaotic systems may need more accuracy on critical calculations for the accurate data retrieval.

REFERENCES

- D. Fang, S. Sun, "A new secure image encryption algorithm based on a 5D hyperchaotic map", *JOURNAL PLOS ONE (Vol.15 Iss.1)*, November 2020, pp 1-13, [Doi.org/10.1371/journal.pone.0242110](https://doi.org/10.1371/journal.pone.0242110)
- for "Data Security," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 9, pp. 34-47, 2020. <https://doi.org/10.3991/ijim.v14i09.14173>
- M. Vijayakumar, A. Appathurai, "An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map", *Ain Shams Engineering Journal (Vol.15 Iss.4)*, April 2024, pp.1-15, doi.org/10.1016/j.asej.2023.102620.
- Budi, A. S., Rochim, A. F., & Martono, K. T. (2022). *Image Encryption using Double Layer Chaos with Dynamic Iteration and Rotation Pattern*. *International Journal of Intelligent Engineering and Systems*, 15(2), 58-68. [DOI: 10.22266/ijies2022.0430.06]
- Feng, L., Du, J., Fu, C., & Song, W. (2023). *Image Encryption Algorithm Combining Chaotic*

- Image Encryption and Convolutional Neural Network. *Electronics*, 12(16), 3455. [DOI: 10.3390/electronics12163455]
- Shnaen, H. J., & Mehdi, S. A. (2024). "Enhancing Data Security with a New Color Image Encryption Algorithm Based on 5D Chaotic System and Delta Feature for Dynamic Initialization". *Communications in Computer and Information Science*, 2096 CCIS, 90–105. https://doi.org/10.1007/978-3-031-62814-6_7
- Xiaoqiang Zhang, Pengfei Chen, and Xueheng Zhang(2026). Image Encryption Algorithm Based on a Novel Hyperchaotic Map and 3D Histogram Model. <https://doi.org/10.3390/e28050576>
- H.R Shakir, S.A Mehdi, AA Hattab. A new four-dimensional hyper-chaotic system for image encryption, *International Journal of Electrical and Computer Engineering* 13 (2), 1744–1756
- H. J. Shnaen, S. A. Mehdi, "Enhancing Key Exchange Security: Leveraging RSA Protocol in Encryption Algorithm Based on Hyperchaotic System", *International Journal of Safety and Security Engineering*, (Vol.13 Iss.6), December 2023, pp. 1127–1134, doi.org/10.18280/ijssse.130616.
- S. S. Ahmed, & S. A. Mehdi (2022). Image Encryption Algorithm based on A Novel 5D Chaotic System. 2022 8th International Conference on Contemporary Information Technology and Mathematics, ICCITM 2022, 249–255. <https://doi.org/10.1109/ICCITM56309.2022.10031883>
- M. T. Gatta, & S. T. A. Al-Latief, (2018). Medical image security using a modified chaos-based cryptography approach. *Journal of Physics: Conference Series*, 1003(1). <https://doi.org/10.1088/1742-6596/1003/1/012036>
- X. Wang, H. Zhao, L. Feng, X. Ye. "High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices", *Optics and Lasers in Engineering*, (Vol.122), November 2019, pp.225-238, doi.org/10.1016/j.optlaseng.2019.04.005.
- S. Bazzi, J. Ebert, N. Hogan, & D. Sternad (2018). Stability and predictability in human control of complex objects. *Chaos*, 28(10). <https://doi.org/10.1063/1.5042090>
- O. A. Jasim, K. A. Hussein, "A hyper-chaotic system and adaptive substitution box (S-Box) for image encryption", *International Conference on Advanced Computer Applications*, December 2021, pp. 144-149, doi.org/10.1109/ACA52198.2021.9626793.
- X. Wang, Y. Su, C. Luo, and Ch. Wang," A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling", *JOURNAL PLOS ONE* (Vol.15 Iss.7), July 2020, pp.1- 16, [doi.org/ 10.1371/journal.pone.0236015](https://doi.org/10.1371/journal.pone.0236015).
- Z. Wang, J. Ma, Z. Chen, &Q. Zhang (2015). A new chaotic system with positive topological entropy. *Entropy*, 17(8), 5561–5579.
- Z. Liang, Q. Qin, Ch. Zhou, and N. Wang," Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation", *JOURNAL PLOS ONE* (Vol.16 Iss.11), November 2021, pp.1-32, [doi.org./10.1371/journal.pone.0260014](https://doi.org/10.1371/journal.pone.0260014).
- R. Lin, Sh. Li, "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm", *Security and Communication Networks*, (Vol.2021 Iss.1), 21 April 2021, pp. 1-18, doi.org/10.1155/2021/5586959.