



Multiple Random Keys for Image Encryption Based on Sensitivity of a New 6D Chaotic System

Narjes N. Jasem^{1*} Sadiq A. Mehdi¹

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

* Corresponding author's Email: nargesnasifl@gmail.com

Abstract: This research paper introduces a novel encryption algorithm that utilizes a hyper six-dimensional chaotic system to enhance image security. The algorithm incorporates randomization, switching, diffusion, and XOR operations in a series of stages to ensure robust encryption. Two sets of keys are generated using the chaotic system, adding random and unpredictable elements to enhance the algorithm's security. During the encryption process, the image's color values are transformed into red, green, and blue vectors, enabling precise manipulation at the pixel level. Pseudo-random shuffling, guided by chaotic keys, introduces an additional layer of randomness, making the encrypted image resistant to decryption and tampering attempts. XOR operations further modify the pixel values, while interconnecting the color vectors enhances the encryption's complexity and security. Experimental evaluation of the proposed algorithm demonstrates its efficacy. A high PSNR value of 7.9997 indicates preserved image resolution after encryption. The NPCR value of 99.6002 indicates robust resistance to pixel modifications and the UACI value of 35.3623 showcases uniform pixel distribution. The algorithm also offers a substantial key space of 2^{947} , further strengthening its overall security. Notably, its sensitivity of 10^{15} highlights its resilience against potential attacks.

Keywords: Six-dimensional hyper-chaotic system, Image encryption, Multiple random keys.

1. Introduction

In the world where information and communication is the indispensable composition of human activities, where men and technology must communicate or share information in order to make decisions; it therefore behoves that this composite essence of humans should be protected and managed to ensure its sustainability, integrity, accuracy

Encryption techniques have become the immediate solution to protect information against third parties [1, 2]. How to keep the digital image secret has become a new research topic. The digital image has a large amount of data, contains a lot of redundant information, and has a large pixel correlation. Traditional standard methods are typically designed for textual information, which is not suitable for encrypting digital image information. Therefore, it is very important to find a more secure and effective image encryption scheme for information security [3]. Chaos-based cryptography,

since its inception, has become a widely published Subject. [4] Chaos-based cryptography depends on the dynamics of nonlinear maps or systems that are deterministic but simple. As a result, it could offer a fast and secure means for protecting data that is transmitted over communication channels such as the internet. Some researchers proposed chaos-based image encryption algorithm to provide high security and efficiency, chaotic systems have many desirable cryptography features, and can achieve confusion and diffusion properties related with cryptographic system [5, 6].

In addition, a chaotic system would have a large key space, for resistance to brute force attacks [7, 8].

In this paper provides an overview of the novel image encryption technique proposed which is designed to address the critical concern of secure transmission and storage of digital images in various applications. Robust encryption algorithms are essential to ensure the confidentiality of digital images and prevent unauthorized access to sensitive

information. In this context, our proposed algorithm involves a series of critical steps, such as vector conversion, stampede operation for creating a stampede image, and two rounds of encryption using keys generated from a six-dimensional hyper chaotic system with two different initial values. By employing a six-dimensional hyper chaotic system and a complex XOR operation, the proposed algorithm offers an additional layer of security, making it less vulnerable to brute-force attacks. Moreover, the circular shift row and second stampede image improve the robustness of the encryption. Compared to existing image encryption techniques, the proposed algorithm provides several advantages, such as high-level security and computational efficiency. The NPCR and UACI test results for the proposed cryptographic system evaluated using six different images, namely Girl, Peppers, Sailboat on Lake, Bird, House, and Lena. The NPCR values range from 99.6002% to 99.6251%, indicating a high sensitivity to changes in the plaintext input, while the UACI values range from 30.4768 to 36.2788. As such, it can be inferred that the proposed encryption algorithm possesses sufficient strength to thwart differential attacks.

In summary, the proposed system demonstrates excellent performance in terms of image decrypting criteria, with zero MSE values and infinite PSNR values for all tested images, suggesting its suitability for applications that require high-quality image decrypting.

2. Related work

In 2021 Sadiq. A. Mehdi, proposed a novel four-dimensional chaotic system has been created, which has characteristics such as high sensitivity to the initial conditions and parameters. It also has two a positive Lyapunov exponents. This means the system is hyper chaotic. In addition, a new algorithm was suggested based on which they constructed an image cryptosystem. In the permutation stage, the pixel positions are scrambled via a chaotic sequence sorting. In the substitution stage, pixel values are mixed with a pseudorandom sequence generated from the 4D chaotic system using XOR operation. A simulation has been conducted to evaluate the algorithm, using the standardized tests such as information entropy, histogram, number of pixel change rate, unified average change intensity, and key space. Experimental results and performance analyses demonstrate that the proposed encryption algorithm achieves high security and efficiency.[1]

In 2017, Chunhu Li, et al, proposed an algorithm for encrypting images that use a three-dimensional

chaotic logistic map to generate pseudo-random sequences that are independent and approximately uniform. After a series of transformations, the sequences constitute a new pseudo-random sequence uniformly distributed in the value space, which covers the plain-text by executing Exclusive-OR and shifting operations for some rounds to form the cipher. Experiments and safety analysis are carried out to analyze the performance, security and the resistance to differential and linear attack of this cryptographic system by simulation. Simulation results show that the algorithm is efficient and usable for the security of the image encryption system. [9].

Lizhang, et al presents a new scrambling algorithm for image encryption. It combines the Logistic chaotic sequence and the common Rubik's Cube. The algorithm partitions an original image into several blocks and generates some cubes. that this novel scrambling algorithm has good security and robustness.[10]

3. The novel chaotic system

The novel six-dimensional autonomous system is obtained as follows:

$$\begin{aligned} \frac{dx_1}{dt} &= -ax_1 + bx_2 - ax_6 \cos(x_4) - cx_3x_5 \\ \frac{dx_2}{dt} &= -dx_2 + ex_1 - fx_1 \cos(x_5) - gx_1x_3 \\ \frac{dx_3}{dt} &= -hx_3 - ix_1 + jx_4 \sin(x_1) + x_1x_2 \\ \frac{dx_4}{dt} &= -hx_4 + kx_2 - gx_1 \cos(x_6) - x_2x_3 \\ \frac{dx_5}{dt} &= -hx_5 + x_3 - lx_3 \cos(x_2) - x_1x_2 \\ \frac{dx_6}{dt} &= -mx_6 + jx_5 + lx_2 \sin(x_3) - lx_3x_4 \end{aligned} \quad (1)$$

Where $x_1, x_2, x_3, x_4, x_5, x_6$ and $t \in \mathbb{R}^+$ called the states of system and $a, b, c, d, e, f, g, h, i, j, k, l$ and m are positive parameters of the system. The 6-Dimensional system Eq. (1) exhibits a chaotic attractor, when the system parameter values are chosen as: $a=18, b=16, c=0.5, d=5.3, e=32, f=9, g=5, h=2, i=4.1, j=3, k=12, l=4$ and $m=50$. We take the initial conditions as: $x_1(0)=5, x_2(0)=2, x_3(0)=1.5, x_4(0)=0.6, x_5(0)=0.4$ and $x_6(0)=5$. This a novel six-dimensional nonlinear system. Some basic properties of the system have been investigated The novel 6-D chaotic system has one unstable equilibrium points and calculated Lyapunov exponents, the Lyapunov exponents of the system are: $L_1= 10.7223, L_2= 3.4266, L_3= -2.41435, L_4= -10.457, L_5= -28.4043$ and $L_6=-52.0782$. the maximal Lyapunov exponent (MLE) of the novel system is $L_1=10.7223$. In

addition, the Lyapunov dimension of the novel chaotic system is obtained as $DKY = 4.04498$.

3.1 Equilibrium point

We can obtain that the system (1) has equilibrium points:

$$\begin{aligned}
 0 &= -ax_1 + bx_2 - ax_6 \cos(x_4) - cx_3x_5 \\
 0 &= -dx_2 + ex_1 - fx_6 \cos(x_5) - gx_1x_3 \\
 0 &= -hx_3 - ix_1 + jx_4 \sin(x_1) + x_1x_2 \\
 0 &= -hx_4 + kx_2 - gx_1 \cos(x_6) - x_2x_3 \\
 0 &= -hx_5 + x_3 - lx_3 \cos(x_2) - x_1x_2 \\
 0 &= -mx_6 + jx_5 + lx_2 \sin(x_3) - lx_3x_4
 \end{aligned} \tag{2}$$

when the system parameter values are chosen as: $a=18, b=16, c=0.5, d=5.3, e=32, f=9, g=5, h=2, i=4.1, j=3, k=12, l=4$ and $m=50$. The equilibrium point becomes: $E0\{x_1=0, x_2=0, x_3=0, x_4=0, x_5=0, x_6=0\}$ Equilibrium $E0(0,0,0,0,0,0)$ are respectively obtained as follows:

$$\begin{aligned}
 \lambda_1 &= -49.9598, \lambda_2 = -31.9827, \lambda_3 = 8.73031, \\
 \lambda_4 &= -2, \lambda_5 = -2.04392 + 1.91785i \text{ and} \\
 \lambda_6 &= -2.04392 - 1.91785i.
 \end{aligned}$$

Therefore, the equilibrium $E0(0,0,0,0,0,0)$ is a saddle point. So, and the hyper chaotic system is unstable at the point $E0$.

3.2 Lyapunov exponents and lyapunov dimensions

The new Six-Dimension hyper chaotic system has six Lyapunov exponents they are obtained as follows: $L_1 = 10.7223, L_2 = 3.4266, L_3 = -2.41435, L_4 = -10.457, L_5 = -28.4043$ and $L_6 = -52.0782$ Since it has two positive values of Lyapunov exponents and the rest four values of Lyapunov exponents are negative, Consequently, this system is hyper chaotic. The fractional dimension is as well a typical feature of chaos calculated Kaplan-York dimension via the Lyapunov exponents, and D_{KY} for the new system could be obtained as follows :

$$\begin{aligned}
 D_{KT} &= j + \frac{1}{|L_{j+1}|} \sum_{i=1}^j L_i \\
 D_{KT} &= 4 + \frac{1}{|L_{j+1}|} \sum_{i=1}^4 L_i = \frac{l_1+l_2+l_3+l_4}{l_5} \\
 &= 4 + (10.7223 + 3.4266 + -2.4143 + -10.4569) / 28.4043 \\
 &= 4.04498
 \end{aligned} \tag{3}$$

This means that the Lyapunov dimension for system Eq. (1) is fractional nature and that the new system has non-periodic orbits its nearby trajectories diverge. Therefore, there is really chaos in this chaotic system.

4. Proposed encryption algorithm

In this paper illustrates design a strong encryption scheme depends on a hyper-chaotic System to enhance security and efficiency as illustrated in Fig. 1, 2.

4.1 Encryption image stage

The important stage in the proposed system is the encryption stage. After the image to be encrypted is uploaded, we follow the 7 steps below:

4.1.1. 6D Hyper-chaotic system

In this process, a six-dimensional hybrid chaotic system is utilized to generate two sets of keys. The two sets of keys are generated with different initial values of the chaotic system, leading to the production of distinct keys in each set. This approach helps to further increase the level of randomness and unpredictability of the keys used for encryption, thereby enhancing the overall security of the system.

4.1.2. Create vectors

At this stage of the encryption process, three vectors (R, G, and B) are constructed from the two-dimensional image that is to be encrypted. These vectors represent the red, green, and blue colour channels of the image, respectively. The process of constructing these vectors involves extracting the corresponding colour values from each pixel of the image and organizing them into distinct vectors. This step is crucial for the subsequent encryption operations that are performed on the individual colour channels, as it allows for the manipulation of the image data at a granular level.

4.1.3. Scrambled step

This step involves the manipulation of the pixel values in an image by rearranging them in a pseudo-random manner. The aim is to add an element of randomness to the image, which makes it more difficult to decode or reverse engineer. To achieve this, a set of chaotic keys are generated using a Hyper-Chaotic system with different initial conditions. These keys are then used to shuffle the values of the red, green, and blue colour channels of the image. A vector is created with the same size as the colour channels, which contains the chaotic keys arranged in a specific manner. The unique values from this vector are then selected to create a new vector that is used to rearrange the pixel values of each colour channel.

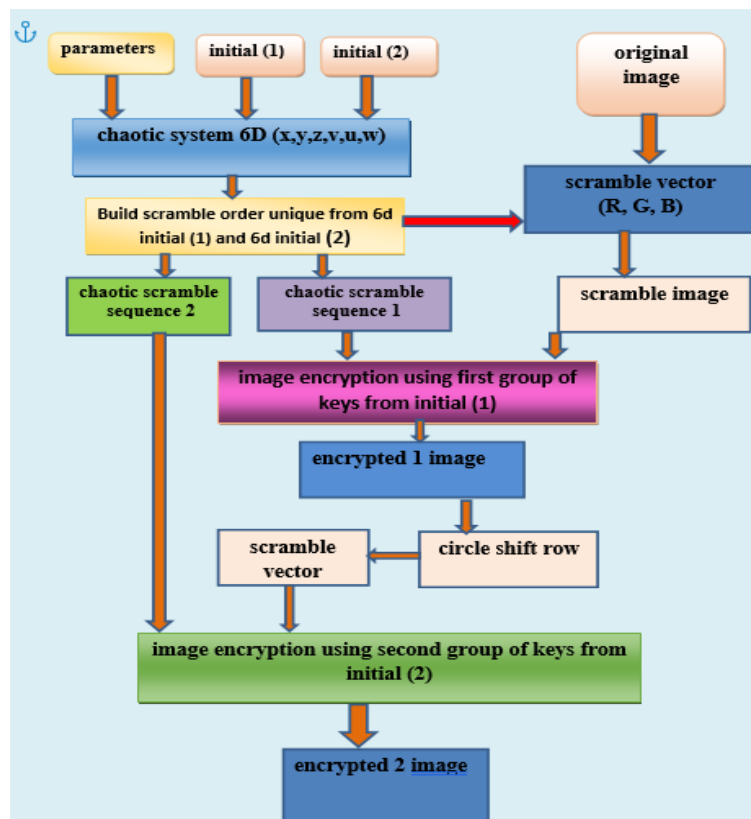


Figure. 1 layout of the proposed system

4.1.4. Image encryption using first key from initial 1

In the proposed image encryption system, the exclusive OR (XOR) operation is used to modify the pixel values in a way that makes it difficult to reverse without knowing the keys used in the encryption process. Specifically, the red (R), green (G), and blue (B) vectors undergo a series of steps that involve XORing them with different keys. The vectors are also interconnected to further enhance the complexity and security of the system.

4.1.5. Circle shift row

In image encryption, a circular shift row is a permutation-based operation that shuffles the positions of pixels within each row of the image. The process involves rotating each row by a fixed number of positions in a circular manner. The purpose of this operation is to achieve diffusion of the image pixels, which enhances the security of the encryption algorithm by making it more difficult for an attacker to determine the relationships between adjacent pixels.

4.1.6. Scramble vector

In the proposed image encrypting algorithm, step 3 involves the scrambling of pixel values using hybrid six-dimensional chaotic systems. After the

circular shift row operation is applied to the image in the previous step, step 3 is re-applied to the resulting image.

4.1.7. Image encryption using second key from initial 2

In the proposed image encryption system, Step 7 represents the final stage of image encryption. In this step, an exclusive OR (XOR) operation is used to modify the pixel values in a way that makes it difficult to reverse them without knowing the keys used in the encryption process. Specifically, the red (R), green (G), and blue (B) vectors undergo a series of steps that involve XORing them with different keys that are generated with different initial values. These keys are used to modify the pixel values in a way that makes it difficult to determine the original pixel values without knowing the keys.

4.2 Decryption image stage

The decryption process is the inverse of the encryption process. It takes as input an encrypted image and two secret keys, where the parameter values and initial conditions are distinct for each key, and outputs the decrypted image. The results of the encryption and decryption process on the images shown in Table 1:

Table 2. The Systems evaluation for encryption criteria of the original images and the encrypted images using proposed system

Image	Correlation Coefficient for Original Encryption			Correlation Coefficient for Image Encryption		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Girl	0.97368	0.96545	0.95124	0.08365	-0.00105	0.00237
Sailboat on lake	0.97368	0.97002	0.95691	0.00755	0.00204	-0.00040
Bird	0.98684	0.98720	0.98043	0.01217	-0.00073	0.00056

uniform due to sturdy presented encryption scheme excellent diffusion stage.

5.2 Correlation coefficient analysis

Table 2 display the correlation coefficients for horizontal, vertical, and diagonal directions of the Original, and encrypted images. Correlation coefficient values range from -1 (perfect negative correlation) to 1 (perfect positive correlation), with 0 indicating no correlation. The results reveal that all images and directions have very low correlation coefficients, indicating that the encryption process has randomized the pixel values effectively and removed any linear relationships between them.

The scatter plots in figures depict the correlation values between the original and encrypted images for various tested images in the horizontal, vertical, and diagonal directions, respectively. The correlation values represent the degree of similarity between the original and encrypted images. The scatter plots show that the proposed encryption systems are successful in generating encrypted images that are not easily recognizable as the original images, as there is a very low correlation between the two. This indicates that the proposed encryption systems can effectively protect the privacy and confidentiality of the images.

5.3 Entropy analysis

Table 3 displays the MSE, PSNR, Entropy values of the original and encrypted images for the two test images using the proposed encryption system. A higher MSE value implies a better encryption outcome, while a lower PSNR value indicates higher encryption quality. A higher entropy value implies a better encryption outcome, indicating that the encryption process maintains the randomness and unpredictability of image data, which is a desired feature for secure encryption. This ensures that even

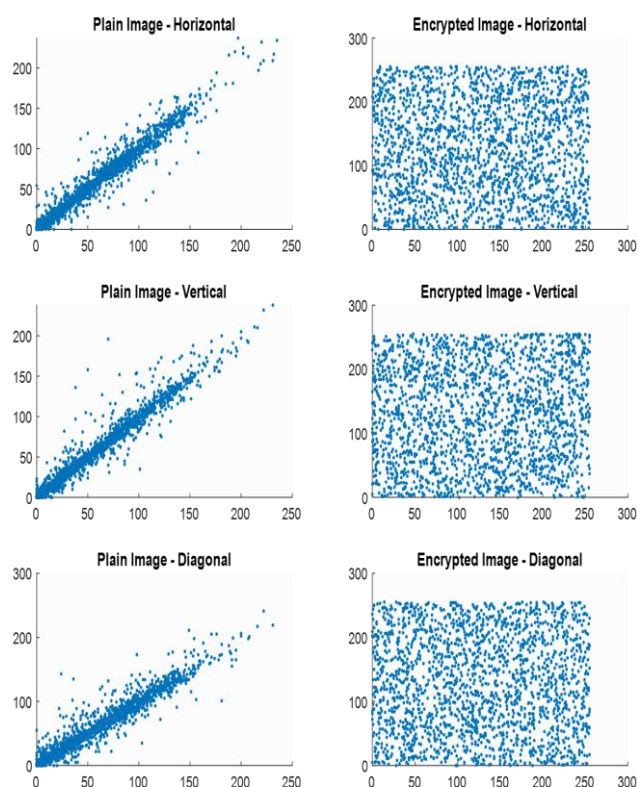


Figure. 3 A Diagram describes horizontally, vertically and diagonally correlation for two adjacent pixels in plain and encrypted image (Girl)

if an attacker has knowledge of the encryption algorithm, the encrypted data cannot be easily guessed or predicted. [12]

5.4 PSNR and MSE analysis

The proposed system for image decoding criteria is evaluated using the widely accepted Peak Signal-to-Noise Ratio (PSNR) as the primary metric [11]. PSNR is considered one of the most crucial criteria for assessing the quality of image encoding, as it measures the signal-to-noise ratio between standard test images and their corresponding decrypted images.

Table 3. The systems evaluation for encryption criteria of the original images and the encrypted images using proposed system

Image	MSE	PSNR	Entropy	
			Plain	Encrypt
Girl	48.7788	7.2960	7.1835	7.9991
Sailboat on lake	112.7681	8.1071	7.7675	7.9997
Bird	90.4795	7.3737	7.7995	7.9997

Table 4. PSNR and MSE Values between the original and the decrypted image

Image	MSE	PSNR
Girl	0	∞
Sailboat on lake	0	∞
Bird	0	∞

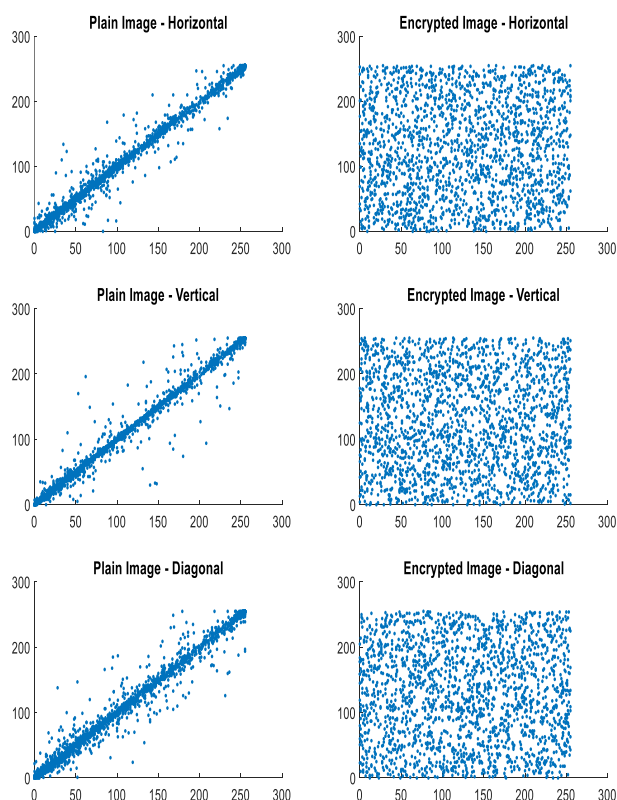


Figure. 4 A Diagram describes horizontally, vertically and diagonally correlation for two adjacent pixels in plain and encrypted image (Bird)

the mean square error (MSE) is another important metric used to evaluate the proposed system's performance, representing the cumulative square error between the original and the decrypted image. The resulting MSE and PSNR values for the proposed system are presented in Table 4.

5.5 Key space analysis

The key space is defined as the range of possible keys that can be generated by a key generation system.

The size of the key space is an important factor in the security of the keys, as a larger key space means that there are more possible keys and therefore a higher level of security. The key space size can reach the $(10^{15})^{19} = 10^{285} \approx 2^{947}$. This value is significantly greater than the recommended minimum key space size of 2128 for secure encryption. Thus, the encryption system is highly resistant to brute force attacks due to the large key space.

5.6 Key sensitivity analysis

Key sensitivity is a measure of the cryptographic algorithm's resilience against brute force attacks where the attacker attempts to guess every possible key until finding the correct one. For cryptographic algorithm, the key sensitivity of 10^{15} implies its capacity to withstand 10^{15} possible key combinations before the attacker is likely to discover the correct key. This magnitude of key sensitivity is regarded as robust and sufficient for safeguarding the confidentiality of image data in various applications. As show in tables.

6. Proposed system and another system comparison

Table 6 displays the results of a performance evaluation of a proposed method for encryption, as compared to previous methods. We compared proposed algorithm with six other systems as follows:

Algorithm number (1) is for researchers A. Kadhim, S. Mehdi, published in 2022[13]. Algorithm number (2) is for researchers B. Ahuja, R. Doriya, S. Salunke, published in 2023 [14]. Algorithm number (3) is for researchers S. Mehdi, Z. Ali, published in 2020 [15]. Algorithm number (4) is for researchers D. Zhang, L. Chen, T. Li, published in 2021 [16]. Algorithm number (5) is for researchers H. Mohamed, D. ElKamchouchi, K. Moussa, published in

Table 5. Key sensitivity




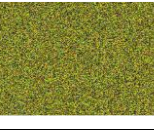




Images	Encrypted image with $x_0 = 5$	Decrypted image with $x_0 = 5$	Encrypted image with $x_0 = 5.000000000000001$
			
			

Table 6. Proposed system and another system comparison

Measurements	Proposed	[1]	[2]	[3]	[4]	[5]	[6]
entropy	7.9999	7.9992	7.9012	7.99990	7.9971	7.9974	7.9993
horizontal correlation	0.00068	0.0011345	0.0012	-0.0019	-0.0004	0.0013	-0.0195
vertical correlation	-0.01001	-0.0000458	-0.0122	-0.0019	0.0031	0.0025	-0.0101
diagonal correlation	-0.00228	0.0003442	-0.0007	0.0013	0.0057	0.0010	-0.0109

Table 7. Comparison among the suggested algorithm and the algorithms in literature based on NPCR and UACI

Measurements	Proposed	[1]	[2]	[3]	[4]	[5]	[6]
NPCR	99.6002	99.9353	99.65	99.9759	99.63	99.617	99.6075
UACI	35.3623	33.4815	33.38	33.4862	33.64	33.42	3.3801

Table 8. Comparison of key space and key sensitivity in different literatures

Measurements	Proposed	[1]	[2]	[3]	[4]	[5]	[6]
Key Space	2^{947}	2^{753}	2^{847}	2^{554}	2^{256}	2^{356}	2^{197}
Sensitivity	10^{15}	10^{14}	10^{16}	10^{14}	-	10^{13}	-

2020 [17]. Algorithm number (6) is for researchers R. Lin, S. Li, published in 2021 [18]. The table shows four performance evaluation metrics: entropy, horizontally correlation, vertically correlation, and diagonally correlation. The suggested method achieved better results than previous methods across all four metrics. Specifically, the proposed method achieved an entropy value of 7.9999, higher than the others, indicating its superior ability to generate unpredictable output. Additionally, the proposed method achieved lower values for all three correlation measurements compared to previous methods, indicating that its output is less correlated or more independent. Specifically, the proposed method achieved a horizontal correlation of 0.00068, a vertical correlation of -0.01001, and a diagonal correlation of -0.00228.

The Table (7) presents a comparison of a proposed algorithm with six algorithms from literature based on two performance metrics: NPCR and UACI. The proposed algorithm achieved an NPCR value of 99.6002, which is slightly lower than

Algorithm [1] (99.9353), but higher than Algorithms [2-6] (ranging from 99.65 to 99.617). The proposed algorithm also achieved a higher UACI value of 35.3623, as compared to all six previous algorithms (ranging from 33.38 to 33.64). These results suggest that the proposed algorithm is more effective at achieving a higher degree of randomness and uniformity of pixel values, as compared to the previous algorithms.

Table 8 provides a comparison of key space and key sensitivity for a proposed encryption algorithm and algorithms from six different literature sources.

7. Conclusions

In this study, a unique 6D hyper chaotic system-based color image encryption algorithm is presented. Using this approach, image encryption and decryption can be done. When compared to other techniques, the encrypted images offer superior confusion and diffusion properties. Statistics such as histogram analysis, correlation coefficient analysis,

information entropy analysis, key space analysis, key sensitivity analysis,

Number of pixels change rate (NPCR), unified average changing intensity (UACI),

Peak signal to noise ratio(PSNR), and others have been used to analysed the algorithm's performance.

The experimental results demonstrate the method's strong encryption capabilities, huge key space, and ability to fend off statistical attacks; as a result, the provided encryption algorithm, which depends on a novel hyper chaotic system, is more safe against statistical and differential attacks.

The proposed hyperchaotic system is based on color image encryption and decryption strength the encryption scheme presented can be concluded and achieve more advantages from the analysis tests are obtained as follows:

1. For encrypted images, the histogram is fairly uniform and the correlation values between the adjacent pixels are very small and close to the theoretical value (zero), while the entropy values close to ideal value (eight), which confirm the robustness and capability of the encryption scheme to thwart statistical attacks.
2. The proposed algorithm is more secure against different types of attacks because it has a large key space equal to , and can frustrate brute-force attacks.
3. The NPCR values range from 99.6002% to 99.6251%, indicating a high sensitivity to changes in the plaintext input, while the UACI values range from 30.4768 to 36.2788. As such, it can be inferred that the proposed encryption algorithm possesses sufficient strength to thwart differential attacks.
4. The encryption and decryption time for all tested images are in real time, this means that the proposed algorithm is effective and secure.
5. The PSNR values between the standard test images and their corresponding decrypted image are infinity and the Mean square error values (MSE) between the plain and decrypted image are zero(MSE = 0)
6. Comparison the novel system with a six-dimensional discrete chaotic system (2018), using the same encryption scheme, the result of security tests refers that the novel system has high complexity and efficiency.

Conflicts of interest

We want to reaffirm that this publication is free of any known conflicts of interest. We further affirm that all named authors have read and approved the article, and that no other individuals who meet the requirements for

authorship but are not listed have contributed to the work.

Author contributions

Conceptualization, Narjes N. Jasem, Sadiq A. Mehdi; methodology and implementation, Narjes N. Jasem, Sadiq A. Mehdi; writing original draft preparation, Narjes N. Jasem.; writing, review and editing, Narjes N. Jasem ; supervision and funding acquisition , Sadiq A. Mehdi, Narjes N. Jasem.

Acknowledgments

This work was supported by Mustansiriyah University.

References

- [1] S. A. Mehdi, "Image encryption algorithm based on a novel 4D chaotic system", *International Journal of Information Security and Privacy*, Vol. 15, No. 4, pp. 118-131, 2021.
- [2] A. Onwutalobi, "Overview of Cryptography", *SSRN Electronic Journal*, pp. 1-10, 2011.
- [3] S. Mehdi and Z. Ali, "A New Six-Dimensional Hyper-Chaotic System", In: *Proc. of Fifth International Engineering Conference on Developments in Civil*, Erbil, Iraq, pp. 211-215, 2019.
- [4] J. Teh, M. Alawida, and Y. Sii, "Implementation and practical problems of chaos-based cryptography revisited", *Journal of Information Security and Applications*, Vol. 50, No.1, pp. 1-42, 2020.
- [5] S. Mehdi, H. Shakir, and A. Hattab, "A dynamic S-box generation based on a hybrid method of new chaotic system and DNA computing", *TELKOMNIKA Telecommunication Computing Electronics and Control*, Vol. 20, No. 6, pp. 1230-1238, 2022.
- [6] S. Zhu and C. Zhu, "Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system", *Multimedia Tools and Application*, Vol. 77, pp. 29119–29142, 2018.
- [7] S. Mehdi and A. Kadhim, "Image Encryption Algorithm Based on a New Five-Dimensional Hyper Chaotic System and Sudoku Matrix", In: *Proc. of Fifth International Engineering Conference on Developments in Civil*, Erbil, Iraq, 2019.
- [8] S. Mehdi and S. Ahmed, "Image Encryption Algorithm based on A Novel 5D Chaotic System", In: *Proc. of 8th International Conference on Contemporary Information*

Technology and Mathematics, Mosul University, Mosul, Iraq, pp. 249-255, 2022.

- [9] C. Li and G. Luo, "An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map", *International Journal of Network Security*, Vol. 21, No. 1, pp. 22-29, 2019.
- [10] L. Zhang, X. Tian, and S. Xia, "A Scrambling Algorithm of Image Encryption Based on Rubik's Cube Rotation and Logistic Sequence", In: *Proc. of International Conference on Multimedia and Signal Processing*, Guilin, China, pp. 312-315, 2011.
- [11] A. Rashid and K. Hussein, "Image encryption algorithm based on the density and 6D logistic map", *Int. J. Electr. Comput. Eng.*, Vol. 13, No. 2, pp. 1903–1913, 2023.
- [12] A. Rashid and K. Hussein, "A Lightweight Image Encryption Algorithm Based on Elliptic Curves and Chaotic in Parallel", In: *Proc. of 3rd Information Technology to Enhance E-Learning and Other Application*, Baghdad, Iraq, pp. 24-30, 2022.
- [13] A. Kadhim and S. Mehdi, "A New Image Encryption Algorithm Based on Six Dimension Hyper Chaotic System and KEN KEN Puzzle", *Journal of Optoelectronics Laser*, Vol. 41, No. 3 pp. 312-321, 2022.
- [14] B. Ahuja, R. Doriya, and S. Salunke, "high dimensional color image encryption architecture using five-dimensional Gauss-logistic and Lorenz system", *Connection Science*, Vol. 35, No. 1, pp. 1-35, 2023.
- [15] S. Mehdi and Z. Ali, "Image encryption algorithm based on a novel six-dimensional hyper-chaotic system", *Al-Mustansiriyah Journal of Science*, Vol. 31, No.1, pp. 54-63, 2020.
- [16] D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation", *Entropy Journal*, Vol. 23, No. 3, pp. 361-384, 2021.
- [17] H. Mohamed, D. ElKamchouchi, and K. Moussa, "A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences", *Entropy Journal*, Vol. 22, No. 2, p. 158, 2020.
- [18] R. Lin and S. Li, "An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm", *Security and Communication Networks*, Vol. 2021, pp. 1-18, 2021.