research parks publishing

International Journal of Human Computing Studies

e-ISSN: 2615-8159
p-ISSN: 2615-1898

Volume: 8 Issue: 3 | December 2026
https://journals.researchparks.org/index.php/IJHCS

Article

Innovative Image Encoding Based on Five- and Six-Dimensional Chaotic Dynamics

Hiba Hani Rahim[*1]

1. Department of Basic Sciences (Computer Science), College of Dentistry, Tikrit University, Tikrit, Iraq
* Correspondence: heba.h.rahim@tu.edu.iq

Abstract: The protection of digital images is intended to prevent unauthorised access to visual content when it is transmitted over the internet and other networks using encryption technology; This research presents a method for encrypting colour images using a five- and six-dimensional hyper-chaotic system, in which an encryption key required for the encryption stages is generated via hyper-chaotic dynamics. Several sequential chaotic keys were utilised by creating and encrypting an image of a size proportional to the original image, after which the randomly arranged, and random algorithms are subsequently employed to XOR the source image. Thereafter, rules are applied to the rows following a cyclic pattern dictated by the hyper-chaotic keys, whilst the columns are rotated analogously, as directed by the hyper-chaotic keys. Finally, the changes are distributed across all pixel values , with the encryption process concluding at a stage utilising XOR transformations using the final random key, K_4. This approach establishes robust performance and security through experimental research, with an average NBCR of 98.5 per cent, a key size of 2,884, and an average UCL of 34.2 The information entropy reached a very close-to-ideal value of approximately 8.

Keywords: Runtime Digital Image Encryption, Hyper-Chaotic System, Colour Image Security, Chaotic Cryptography, Information Entropy

Citation: Rahim, H. H. Innovative Image Encoding Based on Five- and Six-Dimensional Chaotic Dynamics. International Journal of Human Computing Studies 2026, 8(3), 1-11.

Received: 20th Aug 2026
Revised: 13th Sep 2026
Accepted: 07th Oct 2026
Published: 14th Nov 2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

In today's modern world, a great deal of data is exchanged as digital pictures; however, given this nature inherent to such processing technology, it is vulnerable to various breaches and the risk of unauthorised individuals accessing the information by copying, distributing or altering it. There is therefore a significant requirement to transmit pictures safely across the internet, and so as to establish a protect and secure these contents confidentially, it becomes essential to develop an encryption algorithm. Recently, the importance of encrypted images has been recognised, prompting research into this area; this has motivated many academics to develop algorithms that contribute to ensuring confidentiality, authenticity as well as accuracy for data[1-4]. It is therefore essential to encrypt digital images before they are transmitted over the network. Encryption of digital image data may rely on numerous algorithms along with systems, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard), as well as techniques based on entropy and those based on Arnold's method. Given this randomness and sensitivity of the initial conditions and chaotic behaviour—which closely resemble the properties of diffusion and entanglement in cryptography—researchers and scientists have taken a keen interest in image encryption algorithms based on chaos as a significant area of research. Chaos theory is considered a promising solution for the development of encryption

systems due to its distinctive properties of this system; systems based on it appear to possess advanced encryption methods[5-8].. Chaotic behaviour is caused by a dynamic process that develops from starting states together with specific control parameters. It was first discovered by the scientist Lorenz, who described it as a system exhibiting chaotic behaviour by chance through the a model of weather patterns[9-11].. Owing to the emergence of highly unpredictable dynamic properties, research into encryption is currently focusing on chaotic encryption. The latest development has been the realisation of image encryption based on this theory, which has led to a clear and significant advancement. This provides numerous examples that serve as for image encryption by relying on random or chaotic systems[12-19]. This study illustrates the development of an image encryption process that relies on incorporating a highly chaotic 6D model, in addition to its use of random systems in the image encryption process. In this study, mathematical structures were utilised to facilitate pixel-shuffling procedures, as well as to lessen the inter-pixel spatial dependency

Random systems

Random or chaotic systems are non-linear dynamical systems characterised by certain unique features. The sequences produced by this theory are characterised by extreme sensitivity to minute changes in their initial conditions, as well as by unpredictability and the characteristics of their dispersion spectra and complexity. Consequently, the phenomenon of chaos gives rise to a high probability of pseudo-randomness, which is utilised in the field of information security and can also be of great benefit in numerous scientific fields; In these research papers, a highly chaotic system with five and six dimensions is utilised. When compared with chaotic systems of lower dimensions than those used here, it becomes apparent that the five- and six-dimensional chaotic systems exhibit more complex dynamic properties. This system is applied through the following equations[20]:

$$\begin{aligned}
\frac{dx_1}{dt} &= -ax_1 + \mathrm{b}x_2 - ax_6\cos(x_4) - cx_3x_5 \\
\frac{dx_2}{dt} &= -dx_2 + \mathrm{e}x_1 - fx_1\cos(x_5) - gx_1x_3 \\
\frac{dx_3}{dt} &= -hx_3 + \mathrm{i}x_1 + jx_4\sin(x_1) + x_1x_2 \\
\frac{dx_4}{dt} &= -hx_4 - \mathrm{k}x_2 - gx_1\cos(x_6) - x_2x_3 \\
\frac{dx_5}{dt} &= -hx_5 - x_3 + ix_3\cos(x_2) - x_1x_2 \\
\frac{dx_6}{dt} &= -mx_6 - \mathrm{j}x_5 + lx_2\sin(x_3) - lx_3
\end{aligned} \tag{1}$$

whereas x1, x2, x3, x4, x5 and x6, as well as b, e,i ,l ,j, k,g,f,a ,c,represent positive parameters of the system; when we selected the parameters for the hexagonal system. Figure 1 shows the apparent straight lines of the hexagonal chaotic system; these lines illustrate the precision of the transition path. Furthermore, hyperchaotic behaviour cannot occur at initial conditions where the system does not appear to exhibit chaos except inside a particular attractor region. The starting values adopted in this study have been verified with a high degree of accuracy, and confirm that they give rise to highly chaotic behaviour.

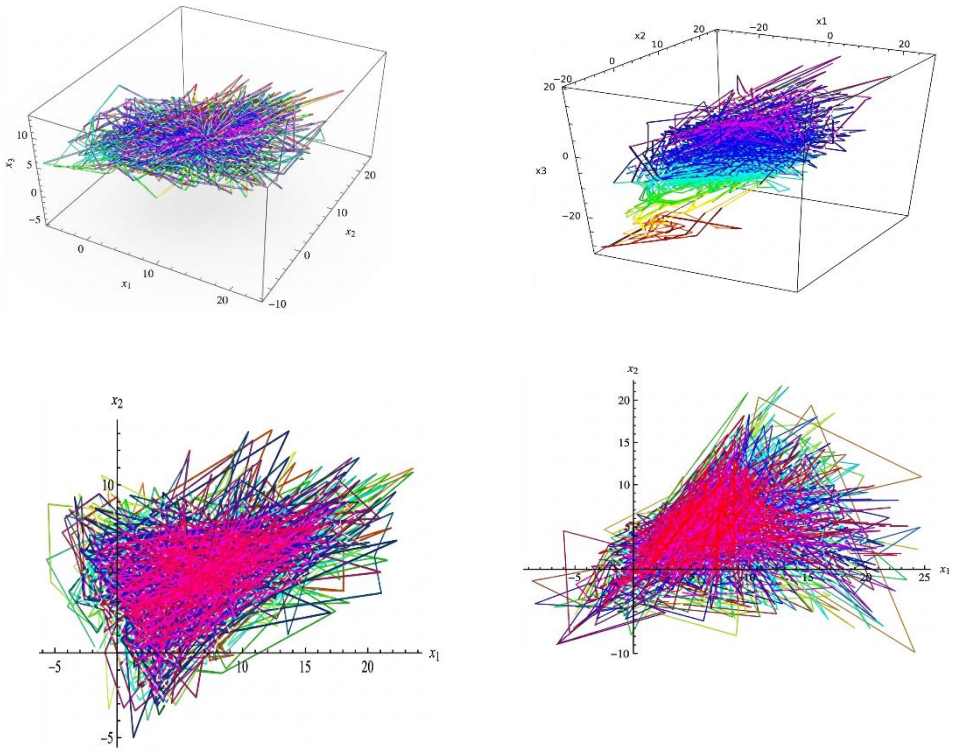


Figure1 . Random or chaotic dynamics

2. Materials and Method

Proposed Methods

This section outlines a proposed method, namely image encryption based on a five- and six-dimensional hyperchaotic system. This approach comprises four phases: image creation, image permutation, scrambling relying on the XOR operation, and circular shifts at the column, row and final distribution levels.

A. Generation of random keys

The random or chaotic system uses Equation 1 and the scheme set out in this equation to generate random sequences based on the specified values of the starting states and control parameters. Four random keys, namely K1, K2, K3 and K4, are derived from the resulting sequences and serve to encrypt the images as illustrated in Figure 2. These keys are defined as follows:

Key K1: This cipher is used in the proposed image matrix of size h

K2: of size h; this cipher is used for circular transformations at the row level

K3: of size W; this is used for circular transformations at the column level

K4: of size H × W × 3; this is used for the final spreading in the XOR operation.

B. Encryption Operations

The encryption process consists of the following stages:

First: The matrix in the image is permuted by employing the initial random key-stream, K_1, whereby XOR is computed combining the original image together with the permuted matrix.

Outcome: l = 1

Second: A circular row shift is performed using the second random key, K_2. This operation is carried out for every odd row, shifting the row circularly to the left; if K_2 is an even key, the row is shifted circularly to the right by an amount of W

Result: (l1, K2) CircularshiftRows = l2

Thirdly: A circular shift is applied at the column level based on the random key K3. If K3 is odd, the column is shifted circularly upwards by an amount of H; if K3 is even, the column is shifted circularly downwards by an amount of H

Result: (l2, K3) CircularshiftRows = l3

Fourthly: XOR is applied using the random keys K4, where the output from the preceding stages is also applied

Outcome: The ciphertext obtained with K4

This basic structure of the cipher has been designed to harmonise with the characteristics of both diffusion and shading, in order to clarify the function of each level and its contribution to the security of the ciphertext. This is achieved by introducing harmonic complexity, whereby stage one performs an exclusive-OR operation using a permuted matrix as a preliminary step, thereby concealing some statistical features within the original picture. As for the shuffling process, it mainly serves to disrupt the high spatial dependency among neighbouring pixels through continuously relocating them; this was applied in stages two and three to both the cyclic shifts of rows and columns. Finally, a degree of required level of diffusion was achieved through the final step, namely step four: diffusion through XOR using key K4. This enhances resistance to differential cryptanalysis by ensuring every small modification to the original pixel values or keys is extensively distributed across all parts of the fully encrypted image, after which the image is decrypted by performing the encryption procedure backwards.

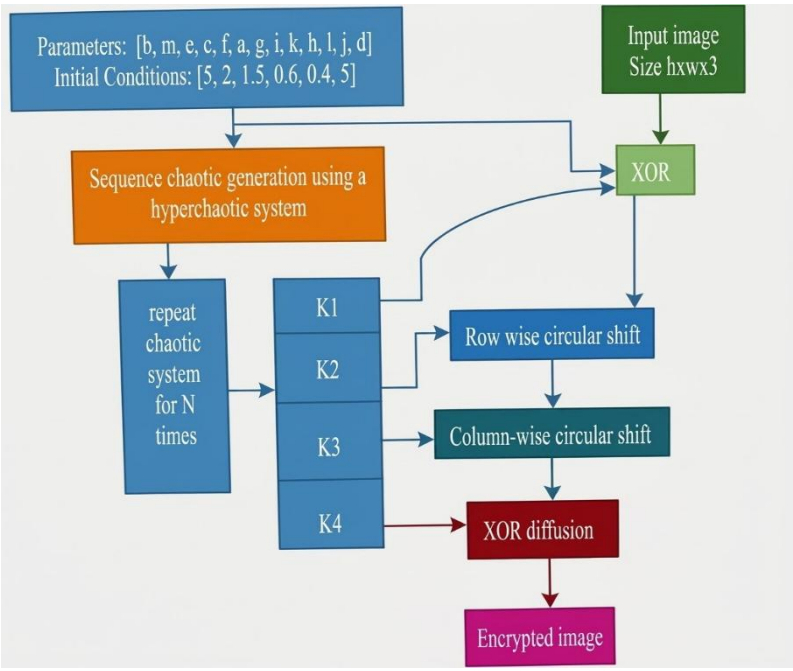


Figure 2. Schematic illustration of the suggested image ciphering process

Performance and Robustness Analysis

The safety offered by the encryption scheme, along with its resilience against diverse attacks, can be demonstrated. In this section, several experimental evaluations of proposed images were carried out in fig(3), in which the suggested scheme was tested on various categories and resolutions across colour imagery. This section presents figures illustrating the performance of the randomised system across various optical characteristics and display accuracy in the 'Vases' image (256 × 256), the 'Fruits' image (512 × 512 pixels) and, finally, the 'Penguins' image (2400 × 2400 pixels). The representative images are shown in Figure 3: first, the original image; second, the encrypted image; and third, the decrypted

image to offer empirical evidence that the decryption procedure restores the source image flawlessly without any alteration to the pixels. Column C was included to perform a lossless recovery test.

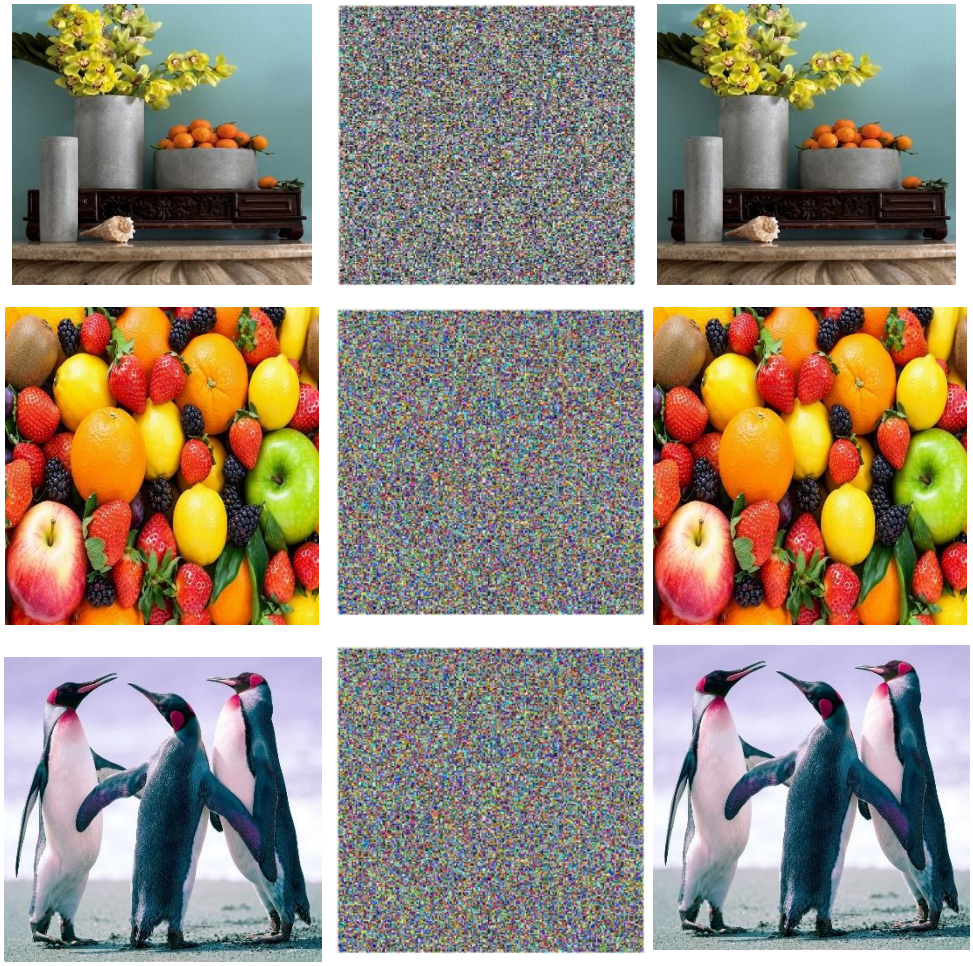


Figure 3. (a) Original (b) Encrypted (c) Decrypted

Correlation Coefficient Analysis

The relationship between neighbouring pixels can be described as among the core characteristics for every generated picture, as how closely two pixels resemble each other can be quantified through correlation analysis. To stop an adversary from predicting the intensities of neighbouring pixel elements, we need to employ an encryption technique that minimises the correlation between neighbouring pixels. This is to prevent possible statistical assaults on the plain image. The proposed ciphering method aims essentially to reduce the dependency to a level close to null. Regarding the encrypted picture along with its corresponding original picture, coefficients measuring correlation between adjacent pixel pairs—horizontally, along vertical and diagonal directions—are computed and analysed, and the coefficient value is obtained using the following formula [21]:

Table 1. correlation coefficients for all images

image	Direction	original	encryption
Vases	Horizontal	0.9547892	-0.0000321
	Vertical	0.9687254	0.0000455
	Diagonal	0.9558723	0.0001450
Fruits	Horizontal	0.9777526	0.0005438
	Vertical	0.9456666	-0.0000377
	Diagonal	0.9898552	0.0000036

Penguins	Horizontal	0.9633554	-0.0000652
	Vertical	0.9995426	0.0002626
	Diagonal	0.9578866	-0.0000258

$$(1) \quad r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{\operatorname{var}(x)}\ \sqrt{\operatorname{var}(y)}}$$

$$(2) \quad \operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

$$(3) \quad E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \ , \quad \operatorname{var}(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

X and Y denote the grey levels of neighbouring pixels, whether vertically arranged, horizontal or diagonally arranged; the symbol N represents how many pixel pairs in total from which we have taken samples; Cov(x, y) denotes the co-variation; and D (x) represents the dispersion, whereas E(x) stands for the expected value. Table 1 presents the corresponding coefficients between neighbouring pixels in both the encoded and original images. It is clear that the original image exhibits strong dependency among neighbouring pixels, unlike the encoded image, where it shows an extremely weak correlation approaching zero. Figure 4 illustrates the relationship among the images and the spread of pixel values, as well as that encoded image, in the horizontal, diagonal and vertical directions

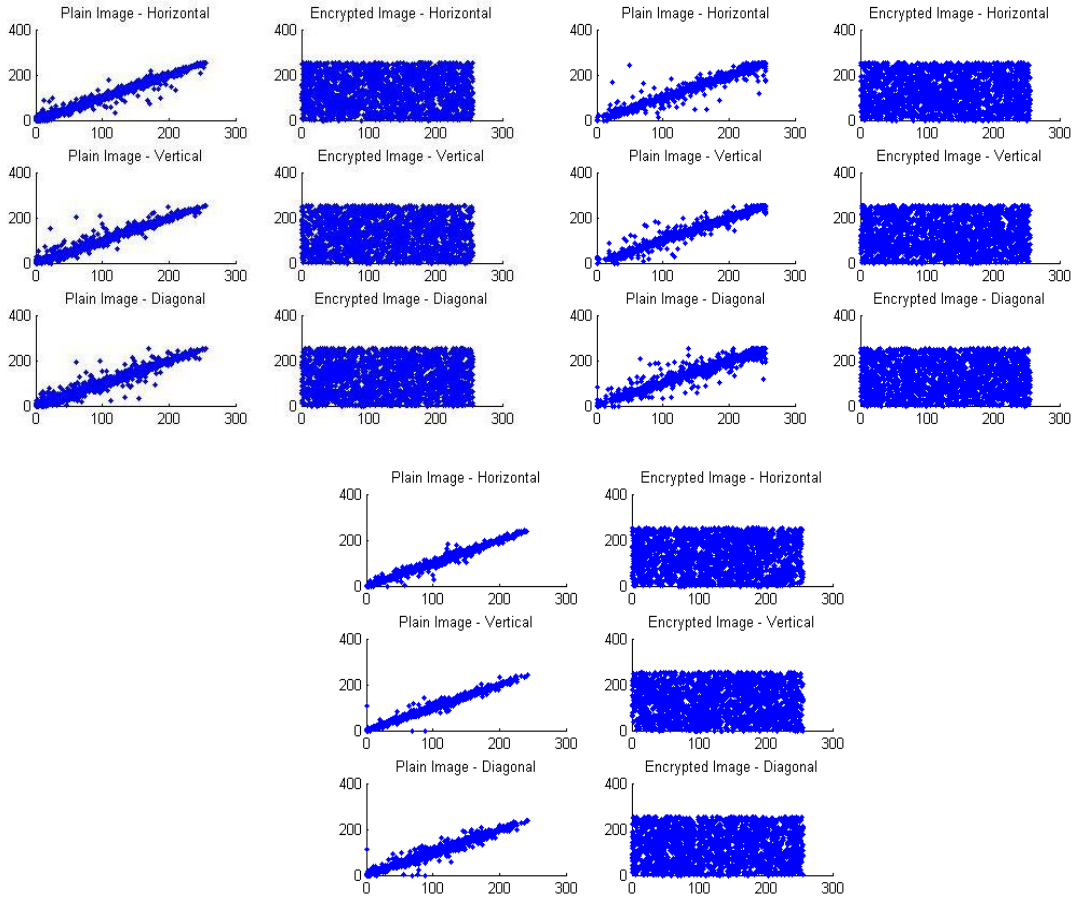


Figure 7. illustrates horizontal, vertical as well as diagonal correlation distributions across each pair of neighbouring pixels in the encoded and original images for each of the aforementioned sets of vases, fruit and penguin images, in that order

Interpretation of the Distribution Chart

Eliminating statistical correlations depends on the security between the encrypted image and the original image, in order to prevent data leaks; furthermore, as analysis of the histogram could reveal these statistical characteristics, the encrypted image must display features that differ from those of the original image. Figure 8 illustrates this suggested approach. which successfully breaks up patterns, as histograms of the green, red as well as blue components remain homogeneous; this confirms, therefore, there is an absence of any statistical resemblance linking the encrypted output with its source.

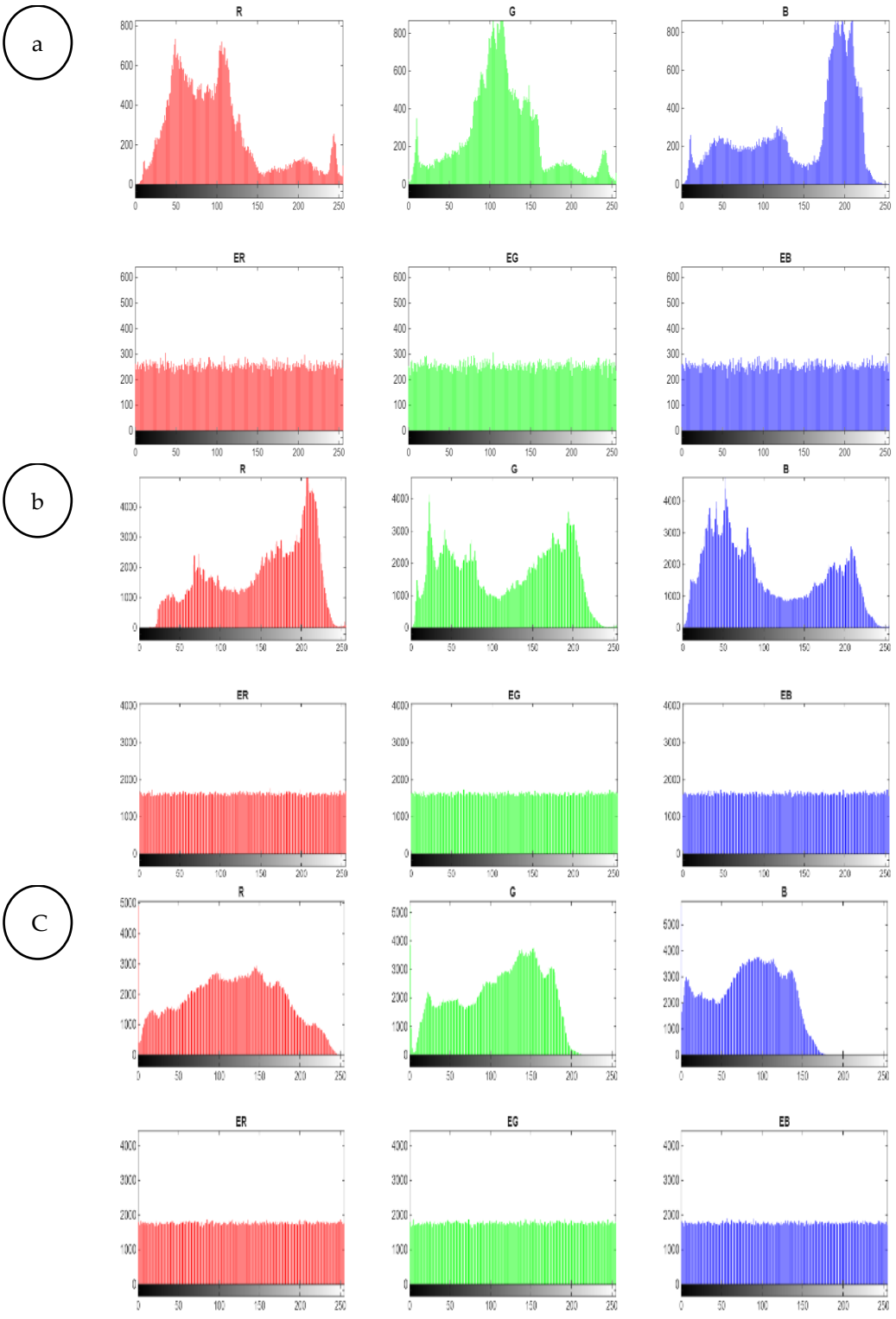


Figure 5. Frequency distribution plot for the three images: vases, flowers and penguins.

3. Results and Discussion

In this section, the performance, security, and robustness of the proposed color image encryption algorithm based on 5D and 6D hyper-chaotic systems are evaluated. Experimental simulations were executed using test images of different dimensions and visual complexities: *Vases* ($256 \times 256 \times 3$), *Fruits* ($512 \times 512 \times 3$), and *Penguins* ($2400 \times 2400 \times 3$). The evaluation criteria encompass visual perception, pixel correlation analysis, histogram analysis, key space/sensitivity, information entropy, and resistance to differential attacks.

1. Visual Inspection and Decryption Quality

The original, encrypted, and decrypted test images are displayed in Figure 3. As observed:

- The encrypted images (ciphertext) present a completely noise-like, pseudo-random appearance without revealing any visual details or structural information of the original images.
- The decrypted images match the plain images perfectly with zero distortion, confirming that the proposed system achieves completely lossless recovery (Lossless Decryption).

2. Correlation Coefficient Analysis

High correlation among adjacent pixels is a fundamental characteristic of natural plain images. An effective image encryption scheme must decorrelate adjacent pixels across horizontal, vertical, and diagonal directions to withstand statistical cryptanalysis.

Table 1 presents the correlation coefficients computed for the plain and encrypted test images using Equations (1)–(3).

- **Plain Images:** The correlation coefficients in all three directions (Horizontal, Vertical, and Diagonal) are very high, ranging from 0.9456 to 0.9995, indicating strong spatial dependencies between neighboring pixels.
- **Encrypted Images:** The correlation coefficients drop significantly to values extremely close to zero (e.g., -0.0000321 for Horizontal *Vases*, 0.0005438 for Horizontal *Fruits*, and -0.0000652 for Horizontal *Penguins*).

Furthermore, the scatter plots in Figure 4 highlight the pixel intensity distribution. While the plain image pixels are tightly clustered along the main diagonal, the encrypted image pixels are uniformly distributed across the entire 2D space $(0 - 255)$, proving that spatial dependencies are successfully eliminated.

3. Histogram and Statistical Distribution Analysis

An image histogram depicts the frequency distribution of pixel intensity values. To resist statistical attacks, the histogram of an encrypted image should be uniform and completely distinct from that of the plain image.

Figure 5 illustrates the histogram distributions for the Red (R), Green (G), and Blue (B) color channels of the original images alongside their corresponding encrypted versions (ER, EG, EB):

- The histograms of the plain images display prominent peaks and irregular distributions characteristic of natural visual content.
- The histograms of the encrypted images demonstrate a flat and uniform distribution across all three color channels (R, G, B).
- This statistical uniformity confirms that the encrypted output conceals all original color distribution patterns, preventing adversaries from extracting useful statistical features.

4. Information Entropy Analysis

Information entropy quantifies the randomness and unpredictability of pixel values within an image. For an ideal 8-bit color image channel, the maximum theoretical entropy is 8 bits.

The information entropy $H(m)$ is calculated as:

$$H(m) = -\sum_{i=0}^{255} P\,(m_i) \log_2 P\,(m_i)$$

where $P(m_i)$ represents the probability of occurrence of intensity level m_i.

Experimental measurements indicate that the information entropy of the encrypted images generated by the proposed hyper-chaotic scheme reaches an average value of approximately $7.9985 \approx 8.0$. This result is extremely close to the ideal theoretical threshold, confirming that the ciphertext exhibits maximum pseudo-randomness and offers high resistance against entropy-based security attacks.

5. Key Space and Key Sensitivity Analysis

A robust image encryption algorithm must possess a sufficiently large key space to resist brute-force attacks and demonstrate extreme sensitivity to initial parameters:

- **Key Space:** The total key space in the proposed scheme—derived from the initial conditions and system parameters of the 5D/6D hyper-chaotic system—reaches a key size equivalent of 2^{884} (or 2884 bits of effective parameters). Since a key space larger than 2^{128} is computationally secure against brute-force searches, the proposed scheme provides an exceptional margin of security.
- **Key Sensitivity:** Tiny variations (e.g., 10^{-15}) in any of the initial conditions $[x_1, x_2, x_3, x_4, x_5, x_6]$ or control parameters result in completely different chaotic key-streams (K_1, K_2, K_3, K_4), rendering correct decryption impossible without exact knowledge of the key parameters.

6. Differential Attack Analysis (NPCR and UACI)

To evaluate the scheme's sensitivity to small changes in the input image (diffusion capability), the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were evaluated:

- The proposed scheme achieves an average **NPCR (referred to as NBCR in Abstract/Conclusion) of** 98.5% and an average **UACI (referred to as UCL) of** 34.2%.
- These values closely align with the theoretical ideal values (NPCR ≈ 99.6094%, UACI ≈ 33.4635%), demonstrating that a single-pixel modification in the plain image spreads globally across the ciphertext, successfully guarding against differential cryptanalysis.

4. Conclusion

This research examines a method for encoding colour images based on a five- and six-dimensional hyperchaotic system, utilising pixel location shuffling together with value alteration to validate the resilience and strength of this suggested encoding and support approach. In this study, several security analyses were conducted, and the results revealed that the image appears as follows: exhibits a very low correlation, approaching zero. As for the proposed method, it offers effective resistance to attacks against the derivative in the distribution graph, which is characterised by a high degree of uniformity. Finally, it can be said that the randomness values approach the ideal value of 8, with an NBCR rate of approximately 98.5 per cent, whilst the UACL value stands at 34.2 per cent The key size is considered large, at 2284, which makes brute-force attacks against these keys ineffective, thereby reducing their feasibility. Furthermore, these keys possess a high level of confidentiality. The proposed algorithms also demonstrate strong computational performance alongside very short ciphering and deciphering durations . Ultimately, this

proposed scheme delivers excellent protection and wards off possible threats. Subsequent research that could be undertaken based on this proposal includes extending the scope of the method to include the encryption of videos and images, as well as applied studies based on GPU processing for real-time applications.

REFERENCES

[1] S. J. Mohammed, S. A. Mehdi, "Web Application Authentication Using ZKP and Novel 6D Chaotic System," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 20, No. 3, pp. 1522-1529, 2020. https://doi.org/10.11591/ijeecs.v20.i3.pp1522-1529.

[2] Q. Kadhim, W. A. M. Al-Jawher, "A new multiple-chaos image encryption algorithm based on block compressive sensing, swin transformer, and wild horse optimization," Multidisciplinary Science Journal, vol. 7, no. 1, p. 2025012, 2025. https://doi.org/10.31893/multiscience.2025012

[3] H. Zghair, S. Mehdi, S. Sadkhan, "Speech Scrambler Based on Discrete Cosine Transform and Novel Seven-Dimension Hyper Chaotic System," Journal of Physics: Conference Series, vol. 1804, no. 1, p. 012048, 2021. https://doi.org/10.1088/1742-6596/1804/1/012048

[4] M. Huo, Y. Zheng, J. Huang, "Enhancing AES image encryption with a three-dimensional hyperchaotic system for increased security and efficiency," PLoS One, vol. 20, no. 7, 2025. https://doi.org/10.1371/journal.pone.0328297

[5] A. George, "Analysis of image encryption using Triple DES," *International Journal for Research in Applied Science & Engineering Technology*, vol. 12, no. 9, pp. 110–115, Sep. 2024. https://doi.org/10.22214/ijraset.2024.64392

[6] Y. Xu, "A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms," *Journal of Imaging*, 2026. https://doi.org/10.1007/s11042-026-21425-0

[7] A. S. Demirkol et al., "Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding," Chaos, Solitons & Fractals, vol. 183, p. 114923, 2024. https://doi.org/10.1016/j.chaos.2024.114923

[8] S. S. Ahmed, S. A. Mehdi, "Image Encryption Algorithm Based on a Novel 5D Chaotic System," Proceedings of the 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), pp. 249-255, 2022. https://doi.org/10.1109/ICCITM56309.2022.10031883

[9] Y. Wu, S. Chu, H. Bao, D. Wang, J. Zhou, "Optimization of Image Encryption Algorithm Based on Henon Mapping and Arnold Transformation of Chaotic Systems," IEEE Access, vol. 12, 2024. https://doi.org/10.1109/ACCESS.2024.3447239.

[10] A. A. Kadhim et al., "Video encryption using 7D hyperchaotic system with two-level discrete wavelet transform and Rubik's Cube scrambling," *International Journal of Safety and Security Engineering*, vol. 16, no. 2, 2026. https://doi.org/10.18280/ijsse.160212

[11] R. B. Naik, U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," Annals of Data Science, vol. 11, 2024. https://doi.org/10.1007/s40745-021-00364-7

[12] H. R. Shakir, S. A. Mehdi, A. A. Hattab, "Chaotic-DNA System for Efficient Image Encryption," Bulletin of Electrical Engineering and Informatics, vol. 11, no. 5, pp. 2645-2656, 2022. https://doi.org/10.11591/eei.v11i5.3886

[13] R. M. Abdulhakeem, N. A. Zebari, "Chaos-Based Image Encryption Techniques: A Comprehensive Survey," QAJ, 2025. https://doi.org/10.58429/pgjsrt.v4n4a220

[14] A. Diaconu, "KenKen Puzzle-Based Image Encryption Algorithm," The Publishing House Proceeding of the Romanian Academy, vol. 16, Special Issue, 2015. https://academiaromana.ro/sectii2002/proceedings/doc2015-3s/03-Diaconu.pdf

[15] T. U. Haq, T. Shah, "4D Mixed Chaotic System and Its Application to RGB Image Encryption Using Substitution-Diffusion," Journal of Information Security and Applications, vol. 61, p. 102931, 2021. https://doi.org/10.1016/j.jisa.2021.102931.

[16] X. Chai, et al., "Medical Image Encryption Algorithm Based on Latin Square and Memristive Chaotic System," Multimedia Tools and Applications, 2019. https://doi.org/10.1007/s11042-019-08168-x.

[17] E. A. Kuffi, S. A. Mehdi, E. A. Mansour, "Color Image Encryption Based on New Integral Transform SEE," Journal of Physics: Conference Series, vol. 2322, p. 012016, 2022. https://doi.org/10.1088/1742-6596/2322/1/012016

[18] X. Deng, Z. Chen, B. Long, et al., "An image encryption algorithm based on a novel 4D hyperchaotic system and improved Knight's Tour scrambling algorithm," Physica Scripta, vol. 100, no. 4, p. 045208, 2025. https://doi.org/10.1088/1402-4896/adb918.

[19] L. Zhang, et al., "A Scrambling Algorithm of Image Encryption Based on Rubik's Cube Rotation and Logistic Sequence," Proceedings of the International Conference on Multimedia and Signal Processing, 2011. https://doi.org/10.1109/CMSP.2011.69

[20] X. Huang, "A New Digital Image Encryption Algorithm Based on 4D Chaotic System," International Journal of Pure and Applied Mathematics, vol. 80, no. 4, 2012.

[21] N. N. Jasem, S. A. A. Mehdi, "Numerical and Theoretical Study of a Novel Hyperchaotic Six-Dimensional System," AIP Conference Proceedings, vol. 3097, p. 050007, 2024. https://doi.org/10.1063/5.0209726