ISSN:2302-8149
e-ISSN:2540-9719

Enhanced Image Security Through 4D Hyperchaotic System and Hybrid Key Techniques

[1]Muhammad Naufal Erza Farandi*, [2]Sri Winarno, [3]Zahrah Asri Nur Fauzyah
[1,2,3]Department of Informatics Engineering, Dian Nuswantoro University
[1,2,3]Jl. Imam Bonjol No. 207, Semarang, Indonesia
*e-mail: erza.naufal@gmail.com

(***received***: 9 October 2024, ***revised***: 26 October 2024, ***accepted***: 30 October 2024)

Abstract

This study develops a digital image encryption method using a 4D hyperchaotic system combined with a hybrid key to maximize data security. By generating a random and uniform pixel distribution, the method makes decryption significantly harder for unauthorized access. Evaluations are conducted through histogram analysis, robustness tests, NPCR, UACI, and information entropy. The findings reveal that the method effectively breaks pixel correlation, rendering the encrypted image unrecognizable. Histogram analysis confirms a uniform pixel distribution, while robustness tests show the system can maintain image quality despite manipulations or attacks. NPCR and UACI tests highlight the method’s high sensitivity to even minor changes in the original image, further enhancing security. Information entropy demonstrates a higher level of randomness compared to other encryption techniques. This 4D hyperchaotic and hybrid key-based approach holds considerable promise for applications requiring highly secure image transmission and storage, ensuring reliable data protection in sensitive environments.

Keywords: cryptography, digital image security, encryption, hybrid key, 4d hyperchaotic system

1 Introduction

In an era where communication technology is rapidly evolving, 66% of the world’s population actively uses the internet [1]. Modern life has undergone significant changes, including in the way we communicate. Almost all information exchanges today are conducted digitally and transmitted over networks, including sensitive information and personal data [2]. The security of this information is crucial to protect it from unauthorized access, which could potentially result in material, time, or even financial losses [3], [4], [5]. One form of this sensitive information is digital images, and ensuring the security of image data during both transmission and storage has become a hot topic of research.

Cryptography is the science and art of securing information by transforming it into a form that cannot be understood by unauthorized parties. This process is known as encryption, where the original data (plaintext) is converted into an unintelligible form (ciphertext) using a specific algorithm and encryption key. Only parties with the correct decryption key can return the ciphertext to its original plaintext form [6]. Compared to textual data, image data has unique characteristics, such as large volume and interdependency between pixels. Therefore, algorithms used for text encryption, such as DES, IDES, AES, and RSA, are no longer relevant when applied to image encryption due to these unique characteristics [7].

Due to the limitations of these algorithms in encrypting image data, chaotic systems demonstrate advantages with characteristics such as sensitivity to parameters and initial conditions, pseudorandomness, and ergodicity [2]. In recent decades, numerous image encryption techniques based on chaos theory have been introduced [8], [9], [10], [11], [12], [13]. However, low-dimensional chaotic systems have a drawback, as they can experience degradation, resulting in weakened security performance due to a smaller key space. On the other hand, using high-dimensional chaotic systems still has weaknesses, where the encrypted images become vulnerable to known-plaintext attacks or selected-plaintext attacks [14].

Given the weaknesses of chaotic systems in image encryption, the use of hyperchaotic maps can be a solution. Hyperchaotic maps, characterized by having more than one positive Lyapunov exponent, exhibit more complex and diverse dynamics, enhancing the randomness and unpredictability of the associated system [15]. Therefore, when used in image encryption, hyperchaotic systems can create a larger key space and generate more complex random sequences. The application of hyperchaotic systems in the development of encryption algorithms for image data can significantly enhance the security level of these algorithms [16], [17], [18], [19].

One of the popular hyperchaotic algorithms for image encryption is the 4D Hyperchaotic system. The encryption algorithm based on the 4D hyperchaotic system leverages the complexity generated by four interacting variables, producing higher randomness compared to lower-dimensional systems. With a larger key space, this algorithm creates unique random sequences each time encryption is performed, making brute force attacks nearly impossible. Additionally, its sensitivity to initial conditions means that small changes in parameters can result in significantly different ciphertext, enhancing data security and making the algorithm more resistant to cryptanalysis attacks.

This research focuses on the development and implementation of an image encryption technique using a 4D hyperchaotic system with a hybrid key. The hybrid key refers to a combination of the original image and the user-provided key. This approach not only aims to enhance security but also ensures that the encryption and decryption processes run efficiently without compromising the quality of the encrypted image. Thus, the proposed solution is expected to provide optimal protection for digital images in this rapidly advancing technological era.

2 Tinjauan Literatur

Wu, Shi, and Li (2019) [20] introduced a novel approach to image encryption that combines a 4D hyperchaotic system, dynamic filtering at the pixel level, and DNA-level diffusion. The hyperchaotic system was chosen due to its double Lyapunov exponents, which provide a large key space and high sensitivity to initial parameter changes, thereby enhancing encryption security. Histogram analysis shows that the encrypted images have a uniform distribution, eliminating exploitable patterns. With entropy close to the maximum, this method demonstrates a high level of randomness, while NPCR and UACI values close to 100% indicate strong resistance to differential attacks, as small changes in the original image result in significant changes in the encrypted image. Experimental results show that this method effectively safeguards images from various types of attacks.

Hui Liu et al [21] introduced an innovative approach to encrypting remote-sensing images by utilizing DNA bases probability and a two-dimensional logistic map. This method applies DNA encoding rules and chaotic sequences for enhanced security. Remote-sensing images are encoded into DNA, and a DNA mask generated by the two-dimensional logistic map is used in DNA addition. To strengthen resistance to differential attacks, the chaotic sequences are adapted according to DNA base probabilities, allowing for pixel- and DNA base-level rearrangement. Histogram analysis demonstrates a uniform distribution in encrypted images, indicating the elimination of detectable patterns. The approach also exhibits high entropy, while NPCR and UACI values nearing 100% show robust resistance against differential attacks. Experimental results confirm the method's effectiveness in safeguarding images from a range of attacks.

Zhongyun Hua et al [22] introduced a medical image encryption scheme that utilizes high-speed scrambling and pixel-adaptive diffusion. This method includes the insertion of random data around the image, followed by two rounds of scrambling and diffusion to enhance security. The technique involves bitwise XOR and modulo arithmetic operations, providing flexibility for hardware and software implementations. The proposed scheme demonstrates high efficiency, achieving rapid encryption and decryption speeds while being resistant to differential attacks. Experimental results indicate that the encrypted images have uniform pixel distribution and high entropy, making them highly secure against statistical and differential attacks. Furthermore, the scheme shows resilience to data loss and impulse noise, maintaining high visual quality in decrypted images even when the encrypted images are partially corrupted.

Aqeel ur Rehman et al. [23] introduced a color image encryption technique using chaotic systems and DNA rules combined with Exclusive-OR and the SHA-256 hash function to enhance image security. The hyperchaotic Chen system, Lorenz system, and piecewise linear chaotic map (PWLCM) were utilized to generate the random sequences required for pixel shuffling and substitution of pixel values based on complementary DNA rules. Experimental results show that this method is highly sensitive to initial key and control parameter changes, proving its high level of security. Entropy analysis indicates that the encrypted images approach the ideal value of 8, demonstrating a high degree of randomness. Additionally, the algorithm was tested using security analysis parameters such as NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). The results show that the method achieves an NPCR value close to 99.6%, meaning a single-pixel difference in the original image leads to significant changes in the encrypted image. Meanwhile, the average UACI value is around 33.45%, indicating a significant intensity difference between two encrypted images produced from small changes in the original image. These results demonstrate that the proposed algorithm offers strong resistance against differential and brute-force attacks.

3 Research Method

This section will provide a detailed explanation of the working mechanism of the 4D hyperchaotic system, including the principles underlying its generation and how it achieves the high level of chaos required for data encryption. Additionally, it will describe the process of generating the hybrid key and initial value, which play crucial roles in ensuring the security and uniqueness of each encryption session. The discussion will then continue with the integration of the 4D hyperchaotic system and hybrid key in the digital image encryption process. This involves combining the hyperchaotic algorithm with a complex encryption key, resulting in a system capable of producing highly secure image encryption with resilience against attacks and data alterations.

3.1 4D hyperchaotic System

The 4D hyperchaotic system has dynamic characteristics measured through Lyapunov exponents, which indicate the level of divergence or convergence between two closely adjacent points in the system's phase space. In a chaotic system, at least two Lyapunov exponent must be positive, signifying sensitivity to initial conditions, where small changes in initial conditions can lead to significant differences in the system's evolution. However, in systems categorized as hyperchaotic, there are positive, negative, and null Lyapunov exponents, indicating a higher level of complexity. This means the system has two or more directions in which divergence occurs, making the system's behavior more unpredictable, more random, and far more complex than that of a regular chaotic system [24].

The complexity generated by the presence of more than one positive Lyapunov exponent makes hyperchaotic systems more effective in encryption applications, where a high level of unpredictability is crucial for data security. In the research conducted by Zhiqing Dong at all (2024) [25], using a new algorithm based on a 4D hyperchaos system has been proposed by [24] to perform image encryption, and can be formulated in equation 1, which explains the complex interactions between the variables in the system.

$$\begin{cases} \dot{x} = a\,(y - x - w) + byz \\ \dot{y} = c(4x + y) - xz \\ \dot{z} = dx - ez + xy \\ \dot{w} = rx + f(3yz + y^2) \end{cases} \tag{1}$$

Where, $a = 80$, $b = 45$, $c = 22$, $d = 5$, $e = 21$, $f = 8$, and $60 \leq r \leq 322$.

Based on equation 1, if $r = 60$, the Lyapunov exponents are $LE_1 = 0$, $LE_2 = 34.2420$, $LE_3 = 41.2114$, and $LE_4 = -1741.93$. Thus, the system used in equation (1) satisfies the characteristics of a hyperchaotic system, as it has more than one positive Lyapunov exponent (LE_2 and LE_3), which reflects divergence in two different directions in phase space. The negative exponent LE4 indicates contraction in one dimension. The attractor of equation (1) can be seen in Figure 1.

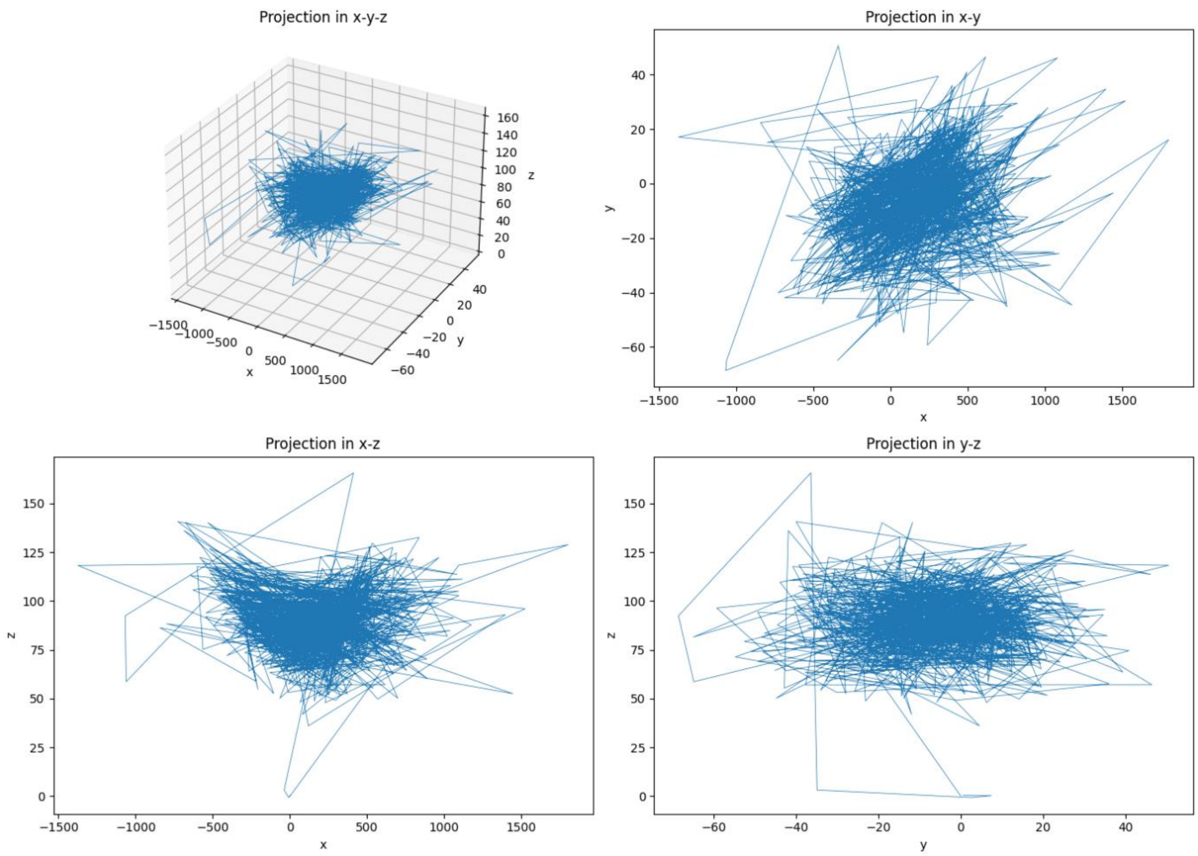


Figure 1. 4D hyperchaotic attractor at r = 60. The projections are as follows: in x−y−z, in x−y, in x−z, and in y−z

In the image, the hyperchaotic attractor is visualized in three projections (x-y-z, x-y, x-z, and y-z). Each projection shows the random and complex behavior of the system, with irregular paths and a spread distribution across each axis. This demonstrates the system's sensitivity to initial conditions, which is a key characteristic of hyperchaotic dynamics. The attractor proves that the algorithm used generates patterns that are difficult to predict, which is crucial for encryption applications.

3.2 Hybrid Key Generation and Initial Values

The Hybrid Key is a key generation technique that utilizes the original image as an integral part of the key generation process, so that any small change in the original image will result in a different key. This key generation process uses the SHA-512 hash algorithm, which is chosen for its ability to enhance the key space and key sensitivity. The use of hash operations in key generation has been widely employed in previous research, such as in [26], [27], [28]. Hash operations are crucial because of their characteristic of producing unique and random outputs from input data, meaning that even small changes in the original image can lead to significant changes in the key. In this Hybrid Key technique, the combination of the original image and the user key will be used in the hashing process to generate a more secure and complex encryption key. The steps to form a Hybrid Key based on the original image and user key in the encryption process are as follows:

1. Take the image to be encrypted and convert it into a one-dimensional form.
2. Hash the image to be encrypted (key_1) and the user key (key_2) using a hash operation, which will produce the hash values.
3. The hash values generated from each key are then converted into an array of 8-bit unsigned integers.
4. Next, both keys are added element-wise, and a modulo 256 operation is performed to obtain the hybrid key. The mathematical form can be seen in equation (2).

ISSN:2302-8149
e-ISSN:2540-9719

$$Hybrid_{key} = (key_1 + key_2) mod\ 256 \tag{2}$$

To calculate the initial values *x*, *y*, *z*, and *w* that will be used in the 4D hyperchaotic system, the standard deviation is employed to measure how far the data spreads from the average key value, providing an indication of the variation within the key. In this context, these values serve as a source of chaos to initialize the initial conditions of the hyperchaotic system. Subsequently, these values are normalized to fall within the range of [0, 1]. For more information, see Equations (3)-(6).

$$x = \frac{\mathrm{std}(\mathrm{hybrid\_key}_1,\ldots,\mathrm{hybrid\_key}_{16})}{10^{n_1}} \tag{3}$$

$$y = \frac{\mathrm{std}(\mathrm{hybrid\_key}_{17},\ldots,\mathrm{hybrid\_key}_{32})}{10^{n_2}} \tag{4}$$

$$z = \frac{\mathrm{std}(\mathrm{hybrid\_key}_{33},\ldots,\mathrm{hybrid\_key}_{48})}{10^{n_3}} \tag{5}$$

$$w = \frac{\mathrm{std}(\mathrm{hybrid\_key}_{49},\ldots,\mathrm{hybrid\_key}_{64})}{10^{n_3}} \tag{6}$$

Where std is the standard deviation function. $\mathrm{hybrid\_key}_\mathrm{i}$ is an element of the hybrid key array at index *i*, with *i* ranging from 1 to 64. In each iteration, the values *x*, *y*, *z*, and *w* will be updated by adding new terms to the total previously calculated, until the conditions x > 1, y > 1, z > 1, and w > 1 terpenuhi. are met. The numbers n_1, n_2, n_3, and n_4 represent how many times the standard deviation exceeds the value of 1 for each key segment. The calculation of these values n can be seen in equation (7).

$$n = \left\lfloor \log_{10}\left(\frac{std(hybrid\_key_{n\_min},\ldots,hybrid\_key_{n\_max})}{1}\right)\right\rfloor \tag{7}$$

3.3 Encryption Process

In this section, we will introduce the encryption method we propose. Our approach emphasizes a 4D hyperchaotic system-based encryption technique that adheres to the principles of confusion by integrating it with a hybrid key, creating a comprehensive and effective solution for image encryption. We will provide a detailed explanation of the method we propose, including a step-by-step process for encrypting the original image into the encrypted image, as well as the main supporting components illustrated in the flowchart in Figure 2.

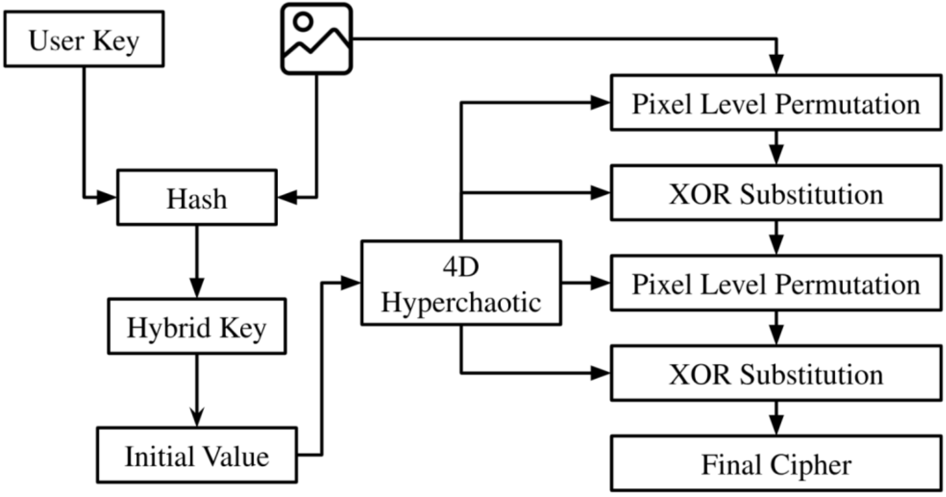


Figure 2. Proposed method

ISSN:2302-8149
e-ISSN:2540-9719

Based on Figure 2, the steps of the encryption process using the 4D hyperchaotic system and Hybrid key on image data are as follows:

1. The encryption stage begins by generating a chaotic sequence based on the Initial Value and the parameters that have been determined. The parameter values used by 4D hyperchaotic are $a = 80,\ b = 45,\ c = 22,\ d = 5,\ e = 21,\ f = 8,$ and $r = 60$. After the function is run, it will form 4 sequences, namely $Sequance_x$, $Sequance_y$, $Sequance_z$, and $Sequance_w$.
2. The image is first converted into a 1-dimensional array, where each element represents the pixel intensity of the image in grayscale (0-255 for 8-bit images). This array is the input to your multi-layer encryption process.
3. Permutation is a process where the order of elements in an array is shuffled or rearranged. In the first layer, the $Sequance_x$, generated from a chaotic system, is used. This sequence is normalized and scaled to match the length of the image array. It determines how the pixels in the array are reordered. The algorithm swaps the pixel positions based on indices defined by $Sequance_x$, where each pixel in the array is moved to a new position determined by its corresponding value in $Sequance_x$. After this permutation, the rearranged image array is referred to as $encL1$.
4. Substitution involves replacing pixel values with new ones based on a specific rule. In the second layer, the chaotic sequence $Sequance_y$ is used to modify each pixel value in $encL1$ using the XOR operation. Each pixel in $encL1$ is XOR-ed with a value derived from $Sequance_y$. Mathematically, each pixel in $encL1$ is XOR-ed with a value calculated using the equation (8).

   $$enrypted\_pixel_i = (encL1_i) \oplus \left(\left\lfloor \frac{255 * y_i}{\max(Sequance_y)} \right\rfloor mod\ 256 \right) \tag{8}$$

   Where, The variable $enrypted\_pixel_i$ represents the encrypted pixel at position *i*, while $encL1_i$ is the previously encrypted pixel at position *i*. The value y_i corresponds to the chaotic sequence $Sequance_y$ at position *i*. The symbol ⊕ represents the XOR operation. The factor 255 is used to scale the pixel values to fit within the range of 0-255. Finally, the modulo 256 operation ensures that the result stays within the 8-bit range (0-255). The result of this substitution forms a new array called $encL2$.
5. The third layer applies another permutation to the array $encL2$, this time using the sequence $Sequance_w$. Similar to the process in the first layer, the pixel positions in $encL2$ are shuffled again based on the values in $Sequance_w$. The result of this process is a new array called $encL3$.
6. In the final layer, another substitution is performed using the chaotic sequence $Sequance_z$. Similar to the second layer, an XOR operation is used to modify the pixel values in $encL3$. Each pixel in $encL3$is XOR-ed with a value derived from $Sequance_z$ using equation (8).
7. The result of the last layer is the final cipher. The decryption process is done in reverse of the encryption process used.

4 Results and Analysis

In this research, experiments were conducted using Python and Google Colab as the text editing platform. We tested the effectiveness of the proposed encryption method using several standard sample images commonly used in various studies. Five grayscale images were utilized in this testing: Lena, Pirate, Cameraman, Baboon, and Boat (on Figure 3). To evaluate the encryption results, we employed encryption metrics such as histogram analysis, information entropy, NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), and robustness test.

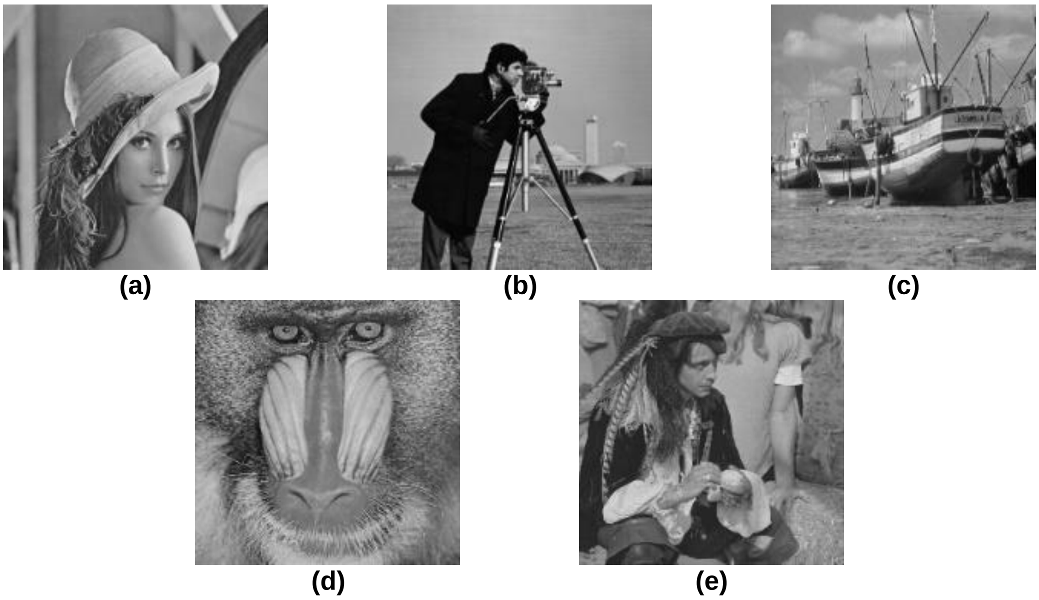
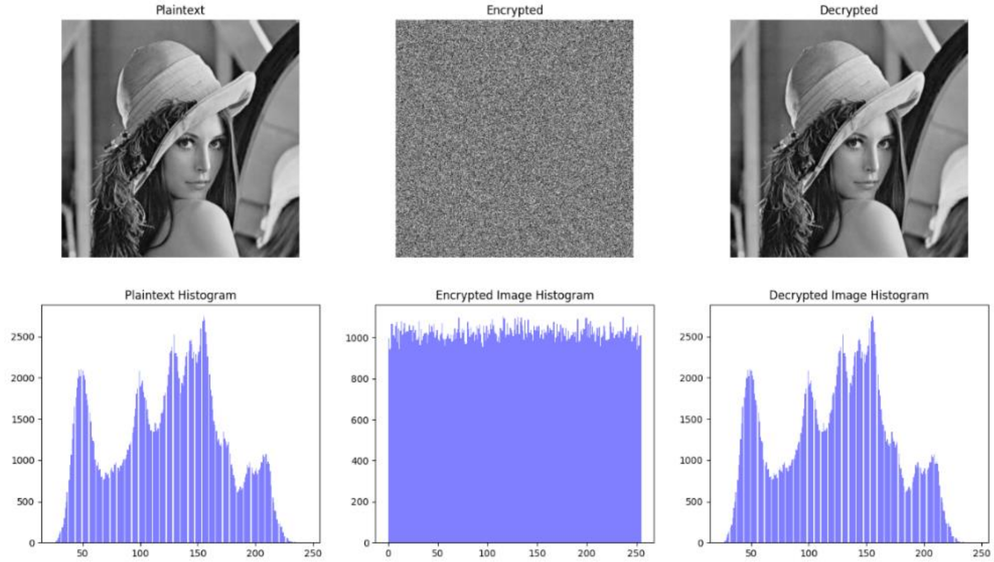


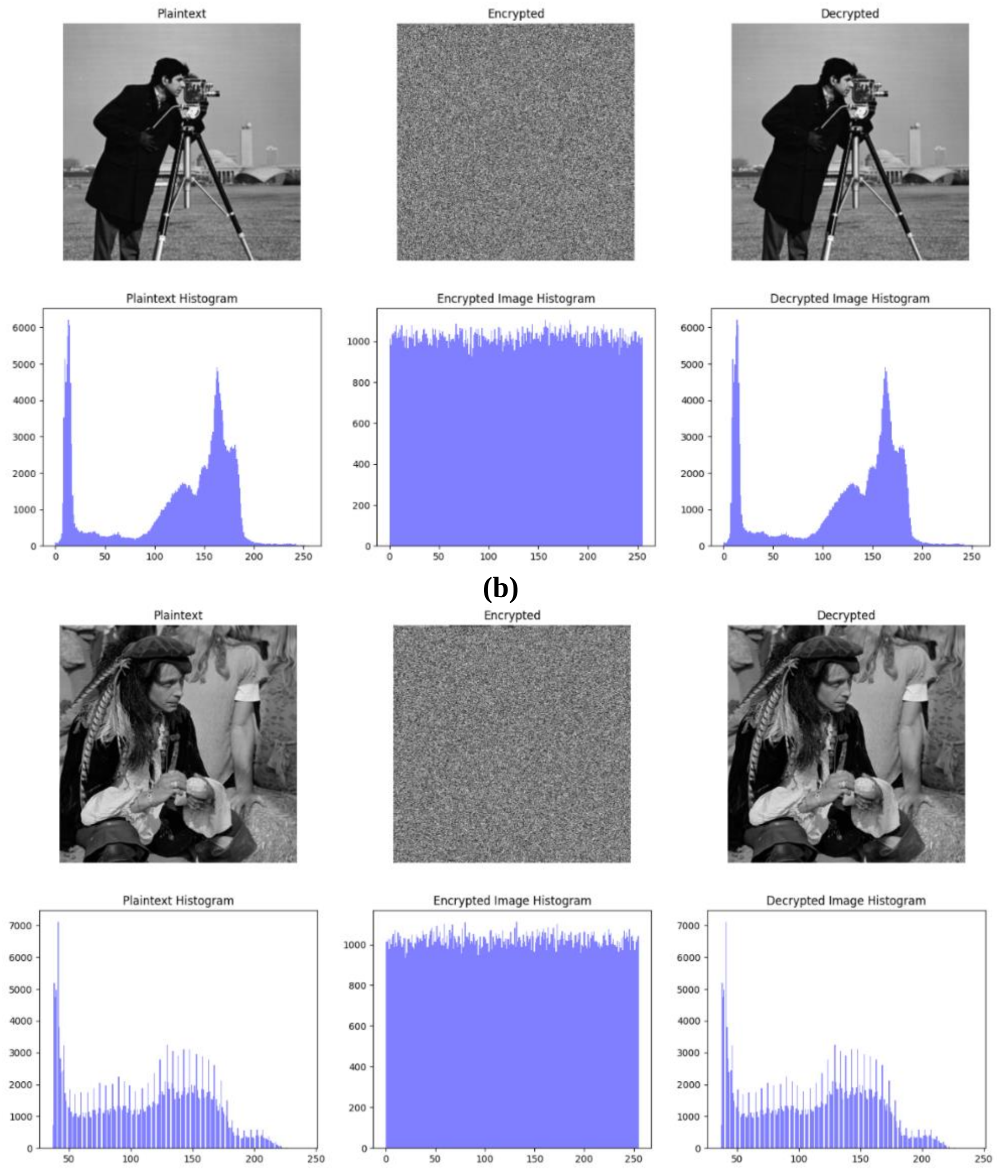
Figure 3. A sample of the standard test image was used for testing. (a) Lena (b) Cameraman (c) Boat (d) Baboon (e) Pirate

4.1 Histogram Analyst

The histogram of an image is a graph that displays the distribution of pixel intensities within that image. In the histogram, the horizontal axis (x) represents the pixel intensity values, while the vertical axis (y) shows the number of pixels with a specific intensity [19]. The importance of the histogram in image encryption lies in its ability to reveal the distribution of pixel intensities. The results of the encryption, decryption, and the histogram of the proposed method can be seen in Figures 4-6.



(a)



(b)

(c)

Figure 6. histogram original, enkripsi, dan dekripsi dari; (a) Lena, (b) Pirate, (c) Baboon

Pixel intensity will be evenly distributed as a result of the encryption process and will resemble the original histogram after the decryption process. The proposed method appears to succeed in this regard, as visually, the histogram of the encrypted image is relatively uniform.

4.2 Information Entropy

Information entropy measures the level of uncertainty or randomness in data. In cryptography, entropy is used to assess how random the encrypted data is. The higher the entropy, the more difficult it is for unauthorized parties to predict the data [29]. The calculation of Information Entropy can be seen in equation (9), and the results of the calculations from the proposed method are presented in table 1.

$$H(x) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \quad (9)$$

Where H(x) represents the Information Entropy of random variables x, and P(x_i) is the probability of occurrence of a value x_i of random variable x, and n the total number of possible values of random variable x.

ISSN:2302-8149
e-ISSN:2540-9719

Tabel 1. IE results and comparison

Image	**Size**	**Method** [30]	**Proposed**
Lena	512 x 512	7.9973	7.9992
Pirate	512 x 512	-	7.9993
Cameraman	512 x 512	7.9974	7.9992
Baboon	512 x 512	-	7.9992
Boat	512 x 512	-	7.9993

4.3 Differential analysis

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are two metrics commonly used in image cryptography analysis, particularly to measure the effectiveness of image encryption schemes. These two metrics are used to assess how well an encryption algorithm scrambles an image, especially when there are small changes to the original image [31].

NPCR measures the percentage of pixel changes between two images, specifically the encrypted image derived from two original images that differ by only one pixel. In other words, NPCR calculates the extent of change that occurs in the encrypted image when one pixel of the original image is altered. Ideally, a high NPCR value indicates that the encryption algorithm is very sensitive to small changes in the original image, which is a desirable characteristic in encryption systems. The optimal value for NPCR is 99.6094%; however, if the NPCR value is around 99%, it still indicates very good performance [32]. The mathematical expression for NPCR can be seen in equation (10).

$$NPCR = \left[\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\delta(i,j)\right] \times 100\%, \delta(i,j) \begin{cases} 0 \; if \; E_1(i,j) = E_2(i,j) \\ 1 \; if \; E_1(i,j) \neq E_2(i,j) \end{cases} \tag{10}$$

UACI (Unified Average Changing Intensity) measures the average intensity difference between two encrypted images, which are derived from two original images that differ by only one pixel. This helps evaluate the extent of average intensity change in the encrypted image when one bit of the key changes. A higher UACI value indicates a greater intensity difference between the two encrypted images, meaning that the encryption algorithm provides good diffusion. The optimal value for UACI is 33.4615%; however, similar to NPCR, if the resulting value is around 33%, it still indicates very good performance [32]. The mathematical expression for UACI can be seen in equation (11).

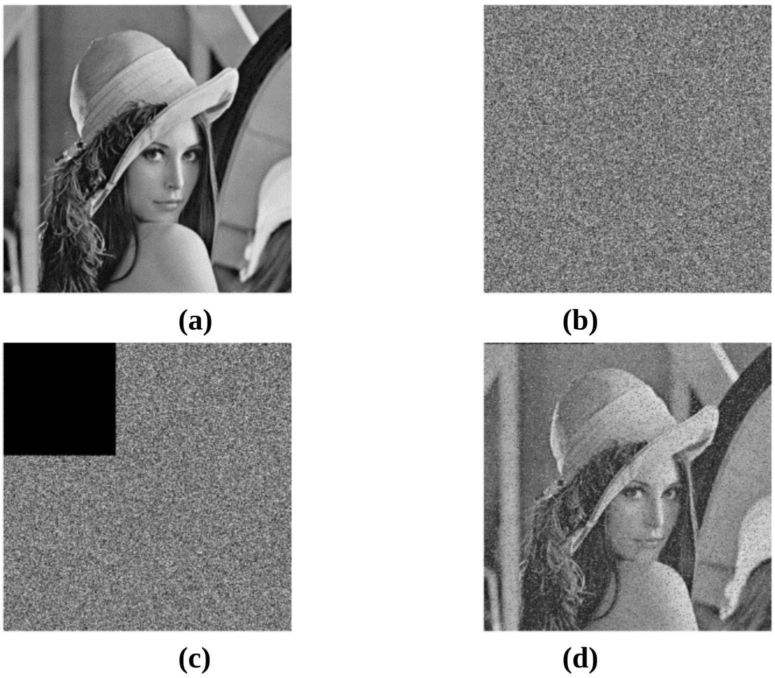
$$UACI = \left[\frac{1}{N\times M}\sum_{i=1}^{N}\sum_{j=1}^{M}\frac{|E_1(i,j)-E_2(i,j)|}{255}\right] \times 100\% \tag{11}$$

Tabel 2. Comparison NPCR and UACI: user key only and hybrid key

Image	**User key Only**		**Hybrid Key**	
	NPCR	**UACI**	**NPCR**	**UACI**
Lena	0.0071 %	137.628 %	99,5613 %	33,3263 %
Pirate	381.469 %	448.787 %	99,5647 %	33,3667 %
Cameraman	381.469 %	747.979 %	99,5788 %	33.3143 %
Baboon	381.469 %	448.787 %	99,5670 %	33.3136 %
Boat	381.469 %	149.595 %	99,5613 %	33.3627 %

4.4 Robustness Test

The Robustness Test in image encryption aims to assess how well the encryption system withstands attacks or modifications by unauthorized parties. This testing is essential for evaluating security and ensuring the system can protect data from various threats. In this study, the proposed method was tested by attacking the image through the deletion of a 200 × 200 pixel area, and the results are displayed in Figure 7.



(a) (b)

(c) (d)

Figure 7. Robustness test using 200×200 pixels attack (a) the original Image of lena; (b) the encrypted images; (c) attacked encrypted image; (d) decrypted attacked image.

The results show that even though the image was manipulated, decryption remained possible and the image still appeared clear, indicating a good level of robustness in the proposed method.

5 Conclusion

The results of this research on the digital image encryption method using a 4D hyperchaotic system combined with a hybrid key highlight several key points. First, this method significantly enhances image encryption security by generating a random and uniform pixel distribution, making the encrypted image nearly unrecognizable to unauthorized parties. Histogram analysis confirms that pixel intensities are evenly distributed, indicating successful encryption without recognizable patterns. Second, the method shows strong resistance to attacks, as demonstrated by the robustness test, where portions of the encrypted image were deleted but could still be effectively decrypted, preserving the clarity of the original image. Third, the system's sensitivity to small changes in the original image is high, as evidenced by NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) values approaching ideal metrics. A high NPCR value means that small changes in the original image lead to significant changes in the encrypted version, ensuring algorithm sensitivity, while a high UACI value indicates substantial intensity changes between encrypted pixels, ensuring excellent diffusion. Fourth, entropy analysis shows that the encrypted images achieve high randomness levels, making them unpredictable and difficult to decipher without the decryption key. Overall, this 4D hyperchaotic system with a hybrid key provides robust security for digital images, combining strong encryption with resilience against attacks and efficient decryption, making it ideal for secure image transmission and storage in cyber-attack-prone environments.

Reference

[1] B. Mahardhika, P. Waseso, and N. A. Setiyanto, "Web Phishing Classification using Combined Machine Learning Methods," *Journal of Computing Theories and Applications*, vol. 1, no. 1, pp. 11–18, Aug. 2023, doi: 10.33633/JCTA.V1I1.8898.

[2] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn*, vol. 105, no. 2, pp. 1859–1876, Jul. 2021, doi: 10.1007/s11071-021-06663-1.

[3] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, “UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection,” *Journal of Computing Theories and Applications*, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: 10.33633/JCTA.V1I2.9462.

[4] J. Kolapo Oladele *et al.*, “BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange,” *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 231–242, Jan. 2024, doi: 10.62411/JCTA.9509.

[5] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, “IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System,” *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 273–283, Feb. 2024, doi: 10.62411/jcta.9541.

[6] V. Manikandan, V. Raj, S. Janakiraman, R. Sivaraman, and R. Amirtharajan, “Let wavelet authenticate and tent-map encrypt: a sacred connect against a secret nexus,” *Soft comput*, vol. 28, no. 9–10, pp. 6839–6853, May 2024, doi: 10.1007/S00500-023-09580-0.

[7] T. Li, J. Shi, X. Li, J. Wu, and F. Pan, “Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin Cubes,” *Entropy*, vol. 21, no. 3, Mar. 2019, doi: 10.3390/e21030319.

[8] J. Li, J. Wang, and X. Di, “Image encryption algorithm based on bit-level permutation and ‘Feistel-like network’ diffusion,” *Multimed Tools Appl*, vol. 81, no. 30, pp. 44335–44362, Dec. 2022, doi: 10.1007/S11042-022-12736-Z/TABLES/12.

[9] X. Wang and S. Gao, “Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,” *Inf Sci (N Y)*, vol. 507, pp. 16–36, Jan. 2020, doi: 10.1016/J.INS.2019.08.041.

[10] S. C. Wang, C. H. Wang, and C. Xu, “An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm,” *Opt Lasers Eng*, vol. 128, p. 105995, May 2020, doi: 10.1016/J.OPTLASENG.2019.105995.

[11] Y. He, Y. Q. Zhang, X. He, and X. Y. Wang, “A new image encryption algorithm based on the OF-LSTMS and chaotic sequences,” *Scientific Reports 2021 11:1*, vol. 11, no. 1, pp. 1–22, Mar. 2021, doi: 10.1038/s41598-021-85377-1.

[12] X. Wang and Y. Su, “Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform,” *Sci Rep*, vol. 10, no. 1, Dec. 2020, doi: 10.1038/S41598-020-75562-Z.

[13] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, “A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2,” *Nonlinear Dyn*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016, doi: 10.1007/S11071-015-2392-7.

[14] H. Wen, S. Yu, and J. Lü, “Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos,” *Entropy 2019, Vol. 21, Page 246*, vol. 21, no. 3, p. 246, Mar. 2019, doi: 10.3390/E21030246.

[15] H. Liu, Y. Zhang, A. Kadir, and Y. Xu, “Image encryption using complex hyper chaotic system by injecting impulse into parameters,” *Appl Math Comput*, vol. 360, pp. 83–93, Nov. 2019, doi: 10.1016/J.AMC.2019.04.078.

[16] S. Zhu, X. Deng, W. Zhang, and C. Zhu, “Construction of a New 2D Hyperchaotic Map with Application in Efficient Pseudo-Random Number Generator Design and Color Image Encryption,” *Mathematics*, vol. 11, no. 14, Jul. 2023, doi: 10.3390/math11143171.

[17] X. Gao, “Image encryption algorithm based on 2D hyperchaotic map,” *Opt Laser Technol*, vol. 142, Oct. 2021, doi: 10.1016/j.optlastec.2021.107252.

[18] Y. Shen, J. Huang, L. Chen, T. Wen, T. Li, and G. Zhang, “Fast and Secure Image Encryption Algorithm with Simultaneous Shuffling and Diffusion Based on a Time-Delayed Combinatorial Hyperchaos Map,” *Entropy*, vol. 25, no. 5, May 2023, doi: 10.3390/e25050753.

[19] M. N. E. Farandi, A. Marjuni, N. Rijati, and D. R. I. M. Setiadi, “Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level,” *Imaging Science Journal*, 2024, doi: 10.1080/13682199.2024.2398954.

[20] J. Wu, J. Shi, and T. Li, “A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion,” *Entropy*, vol. 22, no. 1, p. 5, Jan. 2020, doi: 10.3390/e22010005.

[21] H. Liu, B. Zhao, and L. Huang, “A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map,” *IEEE Access*, vol. 7, pp. 65450–65459, 2019, doi: 10.1109/ACCESS.2019.2917498.

[22] Z. Hua, S. Yi, and Y. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion,” *Signal Processing*, vol. 144, pp. 134–144, Mar. 2018, doi: 10.1016/j.sigpro.2017.10.004.

[23] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, “A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2,” *Optik (Stuttg)*, vol. 159, pp. 348–367, Apr. 2018, doi: 10.1016/J.IJLEO.2018.01.064.

[24] L. Chen, S. Tang, Q. Li, and S. Zhong, “A new 4D hyperchaotic system with high complexity,” *Math Comput Simul*, vol. 146, pp. 44–56, Apr. 2018, doi: 10.1016/J.MATCOM.2017.10.002.

[25] Z. Dong, Z. Zhang, H. Zhou, and X. Chen, “Color image compression and encryption algorithm based on 2d compressed sensing and hyperchaotic system,” *Computers, Materials and Continua*, vol. 78, no. 2, pp. 1977–1993, 2024, doi: 10.32604/cmc.2024.047233.

[26] G. A. Gakam Tegue *et al.*, “A Novel Image Encryption Scheme Combining a Dynamic S-Box Generator and a New Chaotic Oscillator with Hidden Behavior,” *Arab J Sci Eng*, vol. 48, no. 8, pp. 10653–10672, Aug. 2023, doi: 10.1007/S13369-023-07715-X.

[27] A. Hasheminejad and M. J. Rostami, “A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map,” *Optik (Stuttg)*, vol. 184, pp. 205–213, May 2019, doi: 10.1016/J.IJLEO.2019.03.065.

[28] Z. W. Huang and N. R. Zhou, “Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion,” *Opt Laser Technol*, vol. 149, p. 107879, May 2022, doi: 10.1016/J.OPTLASTEC.2022.107879.

[29] Y. S. Najaf and M. K. Mahmood Al-Azawi, “Public key cryptosystem based on multiple chaotic maps for image encryption,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, pp. 1457–1466, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1457-1466.

[30] S. Zhu and C. Zhu, “Secure image encryption algorithm based on hyperchaos and dynamic DNA coding,” *Entropy*, vol. 22, no. 7, Jul. 2020, doi: 10.3390/e22070772.

[31] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, “A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images,” *Inform Med Unlocked*, vol. 20, p. 100396, Jan. 2020, doi: 10.1016/J.IMU.2020.100396.

[32] S. A. Jassim and A. K. Farhan, “Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System,” *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 1, pp. 176–187, 2022, doi: 10.22266/IJIES2022.0228.17.