Enhancing Image Security through Modified RC4 Algorithm and Chaotic Map-Based Encryption

Thesa Adi Saputra Yusri, Vivin Sativa Putri, Bambang Sumarno Hadi Marwoto, Lusi Harini, Deddy Rudhistiar

Abstract—This study proposes a novel digital image encryption scheme that integrates a modified RC4 algorithm with chaotic map-based encryption. The encryption framework consists of three key stages: diffusion, keystream generation, and confusion. Performance analysis is conducted through encryption and decryption assessments, resistance to statistical and differential attacks (measured via histogram correlation, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI)), entropy calculation, and robustness analysis (Peak Signal-to-Noise Ratio (PSNR) and noise resistance). The proposed algorithm demonstrates enhanced security and computational efficiency, with superior resistance to statistical and brute-force attacks. A comparative analysis with existing encryption methods confirms the robustness of the proposed approach in securing digital images.

Index Terms—Arnold Cat Map, Chaotic Map, Digital Image Encryption, Modified RC4 Algorithm

I. INTRODUCTION

The global landscape is currently experiencing the transformative wave of the Fourth Industrial Revolution, commonly referred to as Industry 4.0. This era is marked by the seamless integration of advanced technologies, leading to the emergence of novel communication channels and sophisticated information manipulation techniques. Consequently, traditional communication modalities are becoming increasingly obsolete [1], [2].

This paradigm shift from conventional to digital communication underscores the paramount importance of data security in information dissemination. Among the various data forms, digital images hold significant value and necessitate robust protection measures. Implementing encryption techniques for digital images serves as a pivotal solution to safeguard them from unauthorized access and potential breaches [3].

Encryption is the process of converting plaintext into ciphertext using a specific key, rendering the message unintelligible to unauthorized parties [4]. This mechanism is fundamental to cryptographic systems, which are categorized based on key usage into symmetric and asymmetric cryptography [5].

Symmetric cryptography employs a single key for both encryption and decryption, whereas asymmetric cryptography utilizes a pair of keys (public and private) for these processes. Within symmetric encryption, two primary techniques are block ciphers and stream ciphers. Block ciphers encrypt fixed-size blocks of data, while stream ciphers encrypt data one bit or byte at a time [6]. Examples of block cipher algorithms include AES, DES, and 3DES, whereas RC4 and A5 are notable stream cipher algorithms.

Rivest Cipher 4 (RC4) is a stream cipher developed by Ronald L. Rivest in 1987. Renowned for its simplicity and speed, RC4 has been widely adopted in various security protocols, including Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP). The algorithm operates by generating a pseudorandom keystream, which is then combined with the plaintext to produce ciphertext, typically through bitwise exclusive OR (XOR) operations. Despite its historical significance and widespread use, RC4 has been found to possess several vulnerabilities, leading to a decline in its usage in favor of more secure encryption methods [7].

RC4 has been extensively implemented across various domains, notably in the encryption of digital images. Its advantages include rapid encryption speed, minimal resource requirements, and straightforward implementation. These attributes make RC4 particularly suitable for applications where computational efficiency and simplicity are paramount [6], [8].

In addition, chaos-based encryption has emerged as a chaos-based cryptography leverages the inherent properties of chaotic systems, such as high sensitivity to initial conditions, nonlinearity, and aperiodicity, to enhance encryption robustness. These characteristics ensure that even minute alterations in the initial parameters lead to vastly different encryption outcomes, thereby bolstering security against potential attacks. Consequently, chaos-based encryption methods are increasingly favored for their ability to provide robust security in image encryption applications [9].

The integration of chaotic maps in digital image encryption is often synergized with other encryption

Manuscript received Jan 2, 2025; revised Apr 20, 2025.

T. A. S. Yusri is a lecturer in Department of Mathematics, Universitas Negeri Yogyakarta, Indonesia (corresponding author e-mail: thesaadisaputrayusri@uny.ac.id).

V. S. Putri is an undergraduate student in the Department of Mathematics, Universitas Negeri Yogyakarta, Indonesia (e-mail: vivinsativa.2020@student.uny.ac.id).

B. S. H. Marwoto is a lecturer in the Department of Mathematics, Universitas Negeri Yogyakarta, Indonesia (e-mail: bambang@uny.ac.id).

L. Harini is a lecturer in the Department of Mathematics, Universitas Negeri Yogyakarta, Indonesia (e-mail: lusi.harini@uny.ac.id).

D. Rudhistiar is a lecturer in the Department of Information Technology, Institut Teknologi Nasional Malang, Indonesia (email: rudhistiar@lecturer.itn.ac.id).

algorithms to optimize performance. For instance, combining chaos-based techniques with traditional cryptographic methods can enhance both the confusion and diffusion properties of the encryption process, leading to improved security and efficiency. Such hybrid approaches leverage the unpredictability of chaotic systems alongside established encryption frameworks to achieve superior protection of digital images [10].

Recent advancements in digital image encryption continue to address the limitations of traditional encryption algorithms, particularly in enhancing security and computational efficiency. Several studies have explored modifications to existing encryption techniques to improve their robustness. For instance, Reference [11] introduced an enhanced RC4 algorithm incorporating chain encryption and bit shifting, demonstrating improved resistance to statistical attacks. Similarly, Reference [12] proposed a hybrid approach that integrates the Arnold Cat Map with DNA encoding, leveraging the strong diffusion and confusion properties of chaotic systems. Furthermore, Mohamed and Jawad combined the RC4 algorithm with a chaos-based encryption mechanism, capitalizing on the randomness and unpredictability of chaotic sequences to strengthen security. While these approaches have contributed to advancing encryption methodologies, challenges remain in achieving a balance between encryption strength, computational efficiency, and adaptability to diverse image datasets [7], [13].

Despite these improvements, existing encryption techniques still face limitations in scalability, key management, and resistance to modern cryptanalysis techniques such as deep learning-based attacks. Many current approaches focus solely on enhancing randomness and diffusion without addressing the trade-offs in processing time and key dependency. This research aims to bridge these gaps by developing a digital image encryption algorithm that synergizes a modified RC4 algorithm with chaos-based encryption. By optimizing keystream generation and integrating adaptive chaotic transformations, the proposed method seeks to achieve a higher level of security while maintaining computational efficiency. The algorithm will be evaluated on various $N \times N$ image datasets to assess its resilience against statistical and differential attacks, providing a comprehensive analysis of its feasibility for real-world applications.

II. Proposed Encryption Algorithm

The proposed algorithm is formed by combining the modified RC4 algorithm and chaos map-based encryption. The chaos function to be used is Arnold Cat Map or ACM. This algorithm has three encryption stages, namely the diffusion stage, keystream formation stage, and confusion stage. There are six keys that will be used in this algorithm, namely p, q, r, s,IV_f , andIV_b . The flowchart of the proposed encryption algorithm is shown in Figure 1.

A. Diffusion Stage

The diffusion stage is done by randomizing the pixels in the plainimage using the ACM equation. The purpose of this randomization is to reduce the correlation between adjacent pixels. Randomization is done by using the ACM equation shown in Equation 1. In the equation, the keys p and q will be substituted for the values of b and c respectively.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N \quad (1)$$

with b and c are positive integers, (x_i, y_i) is the pixel location in the image, (x_{i+1}, y_{i+1}) is the new pixel location after the i-th iteration, and the determinant value of the matrix $\begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}$ is 1 [3].

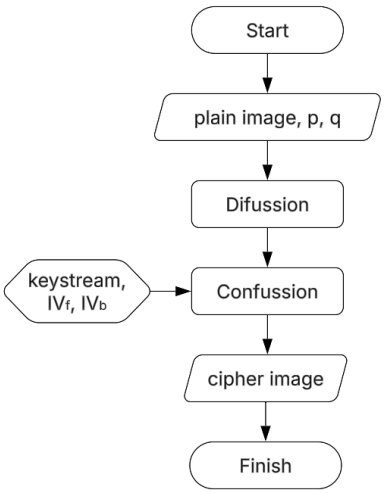


Fig. 1. Flowchart of Digital Image Encryption with Proposed Method

B. Keytream Generation

Keystream generation is done in two stages, namely Key Scheduling Algorithm or KSA and Pseudo Random Generation Algorithm or PGRA. The flowchart of keystream generation is shown in Figure 2.

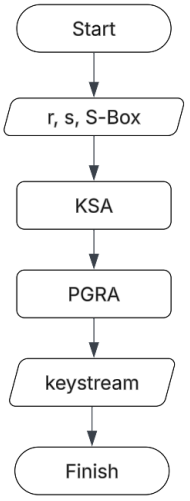


Fig. 2. Flowchart of Keystream Formation

KSA is performed to form the SBox. The first step of this stage is to form an ordered S-Box filled with integers in the interval [0,255]. The S-Box will be randomized by using the ACM equation. To do so, the S-Box will be made into a 16x16 matrix which will later be returned to a 1×256 matrix. This is done because randomization with ACM can only be used on NxN sized matrices. Next, the S-Box is randomized using Equation 1. In the equation, the keys r and s will beustituted to the values of b and c respectively.

Next, the mutated S-Box will be used to form the keystream at the PGRA stage. The number of keystreams formed is equal to the number of pixels to be encrypted. The

following is the PGRA stage psudocode [11].

```
i = 0; j = i
for (i=0; i <=  n_plaintext; i+ +){
  i = (i+1) mod 256
  j = (j + S-Box[i]) mod 256
  Swap(S-Box[i], S-Box[j])
  t = (S-Box[i] + S-Box[j]) mod 256
  Keystream[i] = S-Box[t]
}
```

C. Confusion Stage

The confusion stage is done by substituting the new value at each pixel obtained through the forward encryption and reverse encryption processes. Forward encryption is performed starting from $n = 1, 2, 3, \ldots, N \times N - 1, N \times N$ with N being the image size. The forward encryption function is shown in Equation 2 below.

$$T_n = P_n \oplus T_{n-1} \oplus K_n \quad (2)$$

with $T_0 = IV_f$. Backward encryption is performed starting from $n = (N \times N), (N \times N - 1), (N \times N - 2), \ldots, 2, 1$ with N being the image size. Backward encryption is performed based on the following conditions.

a. If N is an odd number, the encryption function in Equation 3 is used to encrypt every n that is an odd number; while the encryption function in Equation 4 is used to encrypt every other n.
b. If N is an even number, the encryption function in Equation 3 is used to encrypt every n that is an even number; while the encryption function in Equation 4 is used to encrypt every other n.

$$C_n = T_n \oplus C_{n+1} \oplus K_n \quad (3)$$

$$C_n = (T_n + C_{n+1}) \bmod 256 \oplus K_n \quad (4)$$

with $C_{N \times N+1} = IV_b$.

The encryption algorithm above will be implemented on four images, namely the Lena Color, Peppers, Lena Grayscale, and Cameraman images. The Lena Color and Peppers images are 512×512 RGB images, while the Lena Grayscale and Cameraman images are 256×256 grayscale images. The encryption results of the four images will then be analyzed for performance. The performance analysis includes analysis of encryption and decryption results, analysis of statistical attacks, analysis of differential attacks, analysis of entropy values, analysis of Peak Signal to Noise Ratio or PSNR values between plainimage and cipherimage, analysis of noise resistance, and key space analysis.

III. Results and Discussion

Results

The process of encrypting a digital image using the proposed algorithm and analyzing its performance is done with the help of Python programming language. The results obtained from the process are shown in Table 1. The results will be presented in the following explanation.

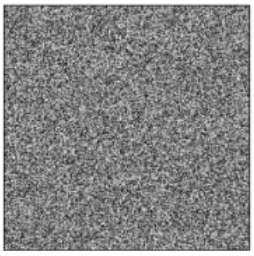
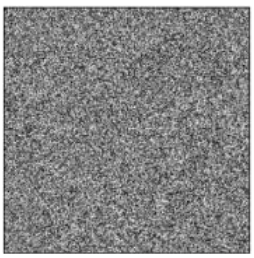
First, the encryption and decryption results. The encryption and decryption results of each image are shown in Table 1.

Second, the results of the analysis of statistical attacks. This analysis was conducted through histogram analysis and correlation analysis. The results of the analysis are shown in Table 2, Figure 3 and Figure 4. The data in Figure 3 and 4 are obtained from correlation analysis of 10,000 randomly selected samples of pixels in the plainimage and cipherimage. The correlation coefficient is calculated based on Equation 5.

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{\mathrm{var}(x) \times \mathrm{var}(y)}} \quad (5)$$

with r_{xy} is the correlation coefficient between variables x and y, $\mathrm{cov}(x, y)$ is the covariance of variables x and y, $\mathrm{var}(x)$ is the variance of variable x, and $\mathrm{var}(y)$ is the variance of variable y.

TABLE I
IMAGE ENCRYPTION AND DECRYPTION RESULTS

Image Name	Encryption Result	Decryption Result
Lena Color		
Pappers		
Lena Grayscale		
Cameraman		

Third, the results of the analysis of the differential attack. This analysis is done by calculating the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values. The resistance of the encryption algorithm to differential attacks is considered good if the NPCR value obtained is higher [14]. NPCR and UACI values are calculated based on Equations 6 and 7 respectively [15]. The results of the calculation of NPCR and UACI values are shown in Table 3.

$$\mathrm{NPCR} = \frac{1}{W \times H} \sum_{i}^{N} \sum_{j}^{M} D(i, j) \times 100\% \quad (6)$$

$$\mathrm{UACI} = \frac{1}{W \times H} \sum_{i}^{N} \sum_{j}^{M} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (7)$$

$$D(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, C_1(i,j) = C_2(i,j) \end{cases} \quad (8)$$

where $W \times H$ is the image size, $C_1(i,j)$ is the pixel value of the cipher image at position (i,j), and $C_2(i,j)$ signifies the pixel value at the same position in the cipher image derived from the original image after a single pixel modification..

Fourth, the results of entropy analysis. The entropy value is calculated based on Equation 9. The results of the entropy value calculation for each image are shown in Table 3 [16].

$$H(x) = -\sum_{i=0}^{2^n-1} P(s_i)\log_2 P(s_i) \quad (9)$$

with n = 8 if the pixel is represented in 8 bits and $P(s_i)$ is the probability of occurrence of the pixel s_i.

Fifth, the results of analyzing the PSNR value between plain image and cipher image. PSNR value is calculated based on Equation 10 [17]. The calculation results of PSNR value between plain image and cipher image are shown in Table 4.

TABLE II
CORRELATION COEFFICIENT VALUE OF LENA COLOR IMAGE

Type	Layer	Correlation Coefficient Value		
		Horizontal	Vertical	Diagonal
Plain image	R	0.978854	0.988675	0.969047
	G	0.966972	0.982149	0.953902
	B	0.933252	0.957114	0.918471
Cipher image	R	0.001764	0.008497	-0.028045
	G	-0.001518	-0.014409	0.001677
	B	-0.002083	0.003423	-0.010360

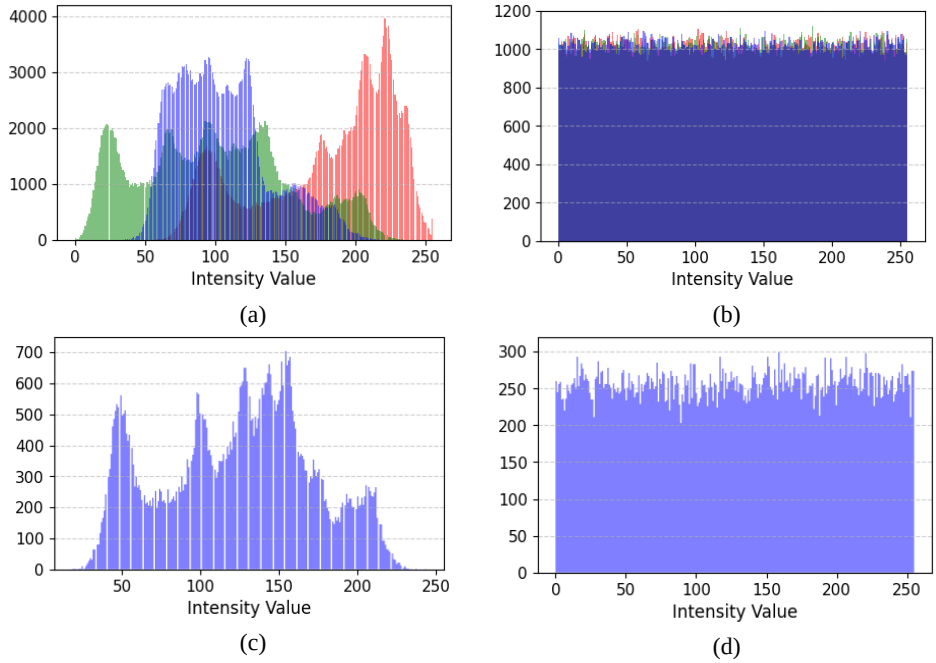


Fig 3. Histogram of pixel intensity distribution (a) plain image of lena color, (b) cipher image of lena color, (c) plain image of grayscale, (d) cipher image of lena grayscale

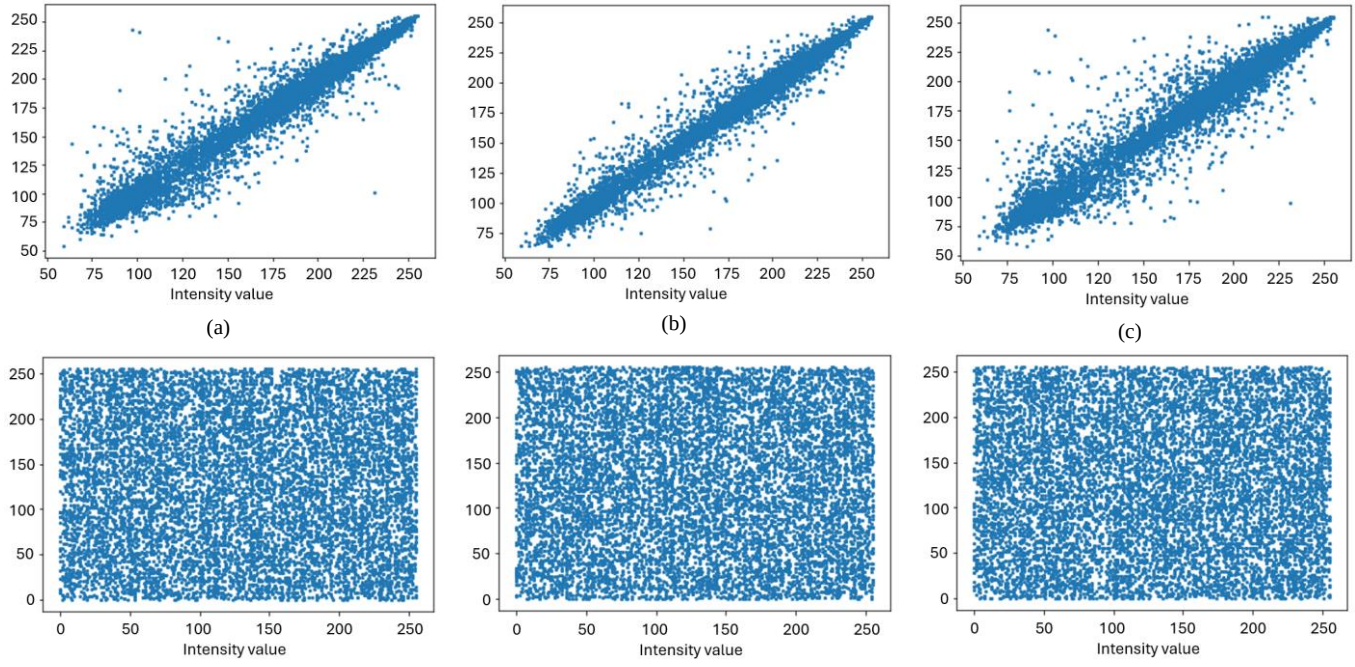


Fig 4. Correlation of adjacent pixels (a) Horizontal direction of the plain, (b) Vertical direction of the plain, (c) Diagonal direction of the plain, (d) Horizontal direction of the cipher, (e) Vertical direction of the cipher, (f) Diagonal direction of the cipher

TABLE III
NPCR, UACI, AND ENTROPY VALUE OF EACH IMAGE

Image Name	Layer	NPCR	UACI	Entropy
Lena Color	R	99.69%	33.48%	7.99942
	G	99.65%	33.38%	7.99933
	B	99.67%	33.56%	7.99931
Peppers	R	99.67%	33.58%	7.99937
	G	99.69%	33.56%	7.99928
	B	99.67%	33.44%	7.99934
Lena Grayscale	-	99.73%	33.41%	7.99700
Cameraman	-	99.81%	33.71%	7.99680

where L is the depth of the image, H is the length of the image, W is the width of the image, and P and D are the two pieces of data being compared.

$$\text{PSNR} = 10 \log_{10} \frac{(2^{L}-1)^{2}}{\text{MSE}} \text{(dB)} \quad (10)$$

$$\text{MSE} = \frac{1}{W \times H} \sum_{r=1}^{H} \sum_{c=1}^{W} (P(r,c) - D(r,c))^{2} \quad (11)$$

TABLE IV
PSNR OF EACH IMAGE

Image Name	Layer	PSNR (dB)
Lena Color	R	7.847
	G	8.548
	B	9.607
Peppers	R	9.092
	G	7.610
	B	7.654
Lena Grayscale	-	9.240
Cameraman	-	8.393
Lena Grayscale		

TABLE V
IMAGE ENCRYPTION AND DECRYPTION RESULTS WITH NOICE

Image Name	Var = 0.0001	Var = 0.001
Lena Color		
Pappers		
Lena Grayscale		
Cameraman		

Sixth, the results of the noise robustness analysis. Noise robustness analysis is performed by adding gaussian noise with variance 0.001 and 0.0001 to the cipher image and then decrypting it. The robustness of the encryption algorithm against noise can be measured through the PSNR value between the plain image and the decryption result of the cipher image that has been given noise. The decryption results of the cipher image that has been given noise and the resulting PSNR value are shown in Table 5 and Table 6.

Discussion

The initial analysis focuses on evaluating the encryption and decryption outcomes. As demonstrated in Table 1, the proposed encryption algorithm successfully generates a highly random and unrecognizable cipher image. Moreover, the decryption process accurately reconstructs the original image from the cipher image, indicating the algorithm's effective applicability to digital images.

TABLE VI
PSNR BETWEEN PLAIN IMAGE AND CIPHER IMAGE DECRYPTION RESULT GIVEN NOISE

Type	Layer	PSNR (db)	
		Var = 0.0001	Var = 0.001
Plainimage	R	15.60	12.07
	G	16.29	12.78
	B	17.84	14.31
Cipherimage	R	17.01	13.49
	G	15.35	11.72
	B	15.38	11.89
Lena grayscale	-	17.18	13.74
Cameraman	-	16.04	12.62

Subsequently, a statistical attack analysis was conducted, beginning with histogram analysis. Figure 3 illustrates that the histogram of the cipher image is uniformly distributed, signifying that each pixel value occurs with nearly equal frequency. This uniformity contrasts sharply with the histogram of the plain image, where certain pixel values predominate. An effective image encryption algorithm should produce a cipher image histogram with a uniform distribution, thereby obfuscating statistical properties and enhancing security [18].

These findings align with previous research emphasizing the importance of uniform histogram distribution in encrypted images to resist statistical attacks [19]. For instance, studies have demonstrated that a flat histogram in the cipher image indicates a robust encryption process, effectively concealing the original image's features [20].

TABLE VII
COMPARISON OF CORRELATION COEFFICIENT VALUES OF LENA COLOR IMAGE

Algorithm	Layer	Correlation Coefficient		
		Horizontal	Vertical	Diagonal
Proposed Algorithm	R	0.001764	0.008497	-0.028045
	G	-0.001518	-0.014409	0.001677
	B	-0.002083	0.003423	-0.010360
RC4	R	0.000400	0.016780	-0.000600
	G	-0.011600	-0.000320	0.003700
	B	0.004010	-0.005650	-0.010870
Ref [16]	R	-0.004000	0.001500	0.002500
	G	0.007400	-0.001600	-0.002400
	B	-0.000200	-0.004100	0.001100

Recent studies have underscored the importance of analyzing the correlation between adjacent pixels to evaluate the robustness of image encryption algorithms against statistical attacks. A lower correlation coefficient between neighboring pixels signifies a more effective encryption scheme [17]. For instance, a comprehensive survey on image

encryption algorithms highlights that effective confusion and diffusion processes are essential to reduce pixel correlation, thereby enhancing security [21].

In our analysis, Figure 4 illustrates the correlation plots for adjacent pixels in both plaintext and ciphered images. The plaintext image exhibits a strong linear relationship among neighbouring pixels, indicating high correlation. Conversely, the cipher image displays a dispersed pattern, suggesting that the encryption process has effectively reduced the correlation between adjacent pixels.

Table 2 quantifies these observations by presenting the correlation coefficients. The plain image shows coefficients approaching 1, indicative of high correlation, whereas the cipher image's coefficients are near 0, demonstrating the encryption algorithm's efficacy in decorrelating adjacent pixels.

The comparison of the correlation coefficient values of adjacent pixels in the cipher image of the Lena Color image between the proposed encryption algorithm and other algorithms is shown in Table 3. From the table, it can be seen that of the 9 values compared, 5 of them show that the correlation coefficient value of the proposed encryption algorithm is better than the standard RC4 algorithm. In addition, the correlation coefficient value of the proposed encryption algorithm is also not much different from the results obtained using the encryption method used in [16].

The next analysis is the analysis of differential attacks in terms of NPCR and UACI values. Reference [22] stated that the critical value of NPCR at a significance level of 0.001 for grayscale images with sizes 256×256 and 512×512 is 99.5341% and 99.5717%, respectively, while the critical value of UACI at a significance level of 0.001 for grayscale images with sizes 256×256 and 512×512 is in the interval (33.1594%, 33.7677%) and (33.3115%, 33.6156%), respectively.

The NPCR and UACI values obtained in Table 3 show that each tested image can survive the differential attack at 0.001 level of significance. In addition, the comparison of the NPCR and UACI values of the Lena Color image in Table 10 shows that the proposed encryption algorithm has higher NPCR and UACI values when compared to the standard RC4 algorithm and is not much different when compared to the encryption algorithm used in [16]. The NPCR and UACI values listed in Table 8 are the average values of the R, G, and B leyers.

TABLE VIII
COMPARISON OF NPCR, UACI, AND ENTROPY VALUE OF LENA COLOR

Algorithm	NPCR (%)	UACI (%)	Entropy
Proposed Algorithm	99.67	33.47	7.99935
Ref [16]	99.60	33.49	7.99937
Ref [23]	99.41	33.30	7.99930
Ref [24]	99.61	33.45	7.99911
Ref [25]	99.60	33.48	7.93320
Ref [26]	99.61	33.46	7.98970
Ref [27]	-	-	7.98120
Ref [28]	99.63	33.46	7.99936

Next is the entropy value analysis. The calculation results obtained in Table 3 show that the proposed encryption algorithm is able to produce entropy values that are very close to the ideal value for each tested image. In addition, the comparison of entropy values generated from the proposed encryption algorithm is not much different from the results obtained using the standard RC4 algorithm and the encryption method used in [16]. The entropy values listed in Table 8 are the average values of all layers.

Next, analyze the PSNR value between plain image and cipher image. The PSNR value can be used to measure the level of similarity between two data. The higher the PSNR value indicates the more similar the two data being compared. A good encryption algorithm produces a low PSNR value between plain image and cipher image. This indicates that the cipher image produced is very random and different from the original image. The data in Table 4 shows a low PSNR value between plain image and cipher image. This means that the resulting cipher image is very different from the original image. In addition, based on the results in Table 9, the comparison of the PSNR value of RGB images from the proposed algorithm with other algorithms shows results that are not much different.

TABLE IX
COMPARISON OF PSNR VALUE OF RGB IMAGE

Image Name	PSNR Value				
	Proposed	Ref. [29]	Ref [30]	Ref [31]	Ref [32]
Lena Color	8.67	8.67	8.68	-	9.05
Peppers	8.19	8.11	8.13	8.73	8.13

The next parameter to be analyzed is resistance to noise attacks. This is done because there is often interference or noise when an image is sent through a channel. Therefore, this test is important. The test results in Table 3 show that the original image decryption results can still be recognized even though when the noise variance value increases, an increasingly blurry image will be obtained. The PSNR value comparison results obtained in Table 10 show better results at a variance value of 0.0001. However, worse results are obtained at a variance value of 0.001. The value shown in Table 12 is the average value of all layers.

TABLE X
COMPARISON OF RESISTANCE TO NOISE

Image Name	PSNR value (db)			
	Proposed Algorithm		Ref [16]	
	0.001	0.0001	0.001	0.0001
Lena Color	16.57	13.05	16.90	12.39
Peppers	15.91	12.37	16.63	12.20

Finally, key space analysis. Key space analysis is used to determine the strength of the keys used in an encryption algorithm against brute force attacks. Key spaces that are less than 2^{56} will be vulnerable to brute force attacks [33].

The proposed encryption algorithm has six key parameters, namely p, q, r, s,IV_f andIV_b . The keys p, q, r, and s are arbitrary positive integers, while IV_f and IV_b are integers between [0,255]. The cryptographic system in this research was created using the Python programming language with the NumPy library. NumPy supports maximum unsigned integer up to 64 bits so that the number of possible integers is around 2^{64} . Therefore, the number of possible keys used is shown in Equation 12.

$$H(p, q, r, s, IV_f, IV_b) = 2^{64} \cdot 2^{64} \cdot 2^{64} \cdot 2^{64} \cdot 2^8 \cdot 2^8 = 2^{272} \quad (12)$$

The results in Equation 12 show the key space of the proposed encryption algorithm is large enough to survive a brute force attack. For an image encryption system to achieve high speeds in both encryption and decryption, the key space

should be no less than 100^2. Considering that $2^{10} \approx 10^3$, the key space utilized in this study is approximately 2^{272}. This extensive key space demonstrates that the proposed algorithm is highly effective in resisting brute force attacks.

TABLE XI
COMPARISON OF KEY SPACE FOR DIFFERENT ALGORITHMS

Algorithm	Proposed	Ref [23]	Ref [24]	Ref [34]	Ref [25]	Ref [35]	Ref [36]
Keyspace	10^{81}	10^{58}	10^{59}	10^{79}	10^{69}	10^{56}	10^{38}

Table 11 compares the key space of the proposed algorithm with those of several existing algorithms referenced from prior studies [23]-[25],[34]-[36]. An encryption algorithm is considered robust if its key space exceeds 2^{100}, approximately 1.27×10^{30} [37]. The key space, representing the total number of possible keys in an encryption system, is crucial in determining the algorithm's resilience against brute-force attacks. A larger key space exponentially increases the difficulty for an attacker to successfully guess the correct key, thereby enhancing the security of the encrypted data. The proposed algorithm features a key space of 10^{81}, which is significantly larger than the key spaces of the other algorithms. In comparison, [23] and [24] have key spaces of $10^{58}$and 10^{59}, respectively, indicating much lower resistance to brute force attacks. Ref [34] has a key space of 10^{79}, which is closer to the proposed algorithm but still slightly less secure. The substantially larger key space of the proposed algorithm demonstrates its superior capability to withstand brute force attempts, highlighting its robustness in encryption security.

IV. CONCLUSION

The findings of this study demonstrate that the proposed encryption algorithm is highly effective for securing digital images, exhibiting strong resilience against statistical and differential attacks while maintaining high-security standards. The entropy values are near the theoretical ideal, indicating the effectiveness of the confusion and diffusion processes, while consistently low PSNR values between plaintext and cipher images reinforce its ability to generate highly randomized encrypted outputs. Additionally, the algorithm maintains robustness against noise attacks, though increased noise variance affects image clarity upon decryption. The extensive key space further enhances security, making the algorithm resistant to brute-force attacks. Comparative analysis with existing encryption methods confirms that the proposed approach achieves performance levels comparable to state-of-the-art techniques while maintaining computational efficiency. These results highlight the algorithm's potential for real-world applications, particularly in scenarios requiring both image security and efficiency. Future research could focus on optimizing execution speed, improving key management strategies, and expanding the algorithm's adaptability to various image formats and real-time encryption systems.

REFERENCES

[1] D. Andriany, "Communication in the era of industrial revolution 4.0," Jurnal Signal, vol. 10, no. 2, p. 312-326, 2022.

[2] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: volume 1, overview," Gaithersburg, MD, 2017.

[3] R. Munir, "Chaos-based digital image encryption algorithm with the combination of permutation techniques and substitution techniques using Arnold cat map and logistic map," Jurnal Nasional Pendidikan Teknik Informatika, vol. 1, no. 3, p. 166, 2012.

[4] D. R. Stinson, Cryptography: Theory and practice. Chapman and Hall/CRC, 2005.

[5] S. Ramadani, Diana, and S. Sauda, "Application of AES and DSA algorithms using hybrid cryptosystem for data security," JURIKOM (Jurnal Riset Komputer), vol. 7, no. 4, pp. 523-529, 2020.

[6] R. Mohammed and L. M. Jawad, "Secure image encryption scheme using Chaotic Maps and RC4 algorithm," Solid State Technology, vol. 63, no. 3, 2020.

[7] E. J. Madarro-Capó, C. M. Legón-Pérez, G. Sosa-Gómez, and O. Rojas, "New weak keys with parity patterns in the RC4 stream cipher," Cryptography, vol. 8, no. 4, p. 54, 2024.

[8] R. U. Ginting and R. Y. Dillak, "Digital color image encryption using RC4 stream cipher and chaotic logistic map," in 2013 International Conference on Information Technology and Electrical Engineering (ICITEE), IEEE, pp. 101-105, 2013.

[9] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," Mathematics, vol. 11, no. 11, 2023.

[10] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on Julia Set of Fractals and 3D Lorenz Chaotic Map," Entropy, vol. 22, no. 3, p. 274, 2020.

[11] T. Zebua and E. Ndruru, "Digital image security based on modified RC4 algorithm," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 4, no. 4, p. 275, 2017.

[12] T. A. S. Yusri and D. Rudhistiar, "Digital image encryption based on a combination of modified Arnold cat map and DNA encoding," Jurnal Mnemonic, vol. 5, no. 2, pp. 173-177, 2022.

[13] H. Kolivand, S. F. Hamood, S. Asadianfam, M. S. Mohd Rahim, and W. Hurst, "Image encryption framework based on multi-chaotic maps and equal pixel values quantization," Multimedia Tools Application, 2024.

[14] U. Zia et al., "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," International Journal of Information Security, vol. 21, no. 4, pp. 917-935, 2022.

[15] S. M. Kareem and A. M. S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," Journal of Information Security and Applications, vol. 50, p. 102410, 2020.

[16] M. Demirtaş, "A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos," Optik., vol. 265, p. 169430, 2022.

[17] K. K. Butt, G. Li, S. Khan, and S. Manzoor, "Fast and efficient image encryption algorithm based on modular addition and SPD," Entropy, vol. 22, no. 1, p. 112, 2020.

[18] S. Bhattacharjee, M. Gupta, and B. Chatterjee, "Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified Chaos-based Logistic Map," Applied Biochemistry and Biotechnology, vol. 195, no. 4, pp. 2395-2413, 2023.

[19] Y. Wu, "Image encryption using the two-dimensional logistic chaotic map," Journal of Electronic Imaging, vol. 21, no. 1, p. 013014, 2012.

[20] Y. Chen, T. Lu, C. Chen, and Y. Xiang, "A novel image encryption method based on improved two-dimensional logistic mapping and DNA computing," Frontiers in Physics, vol. 12, 2024.

[21] Y. Alghamdi and A. Munir, "Image encryption algorithms: A survey of design and evaluation metrics," Journal of Cybersecurity and Privacy, vol. 4, no. 1, pp. 126-152, 2024.

[22] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," Cyberjournals.Com, 2011.

[23] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," Nonlinear Dynamics., vol. 94, no. 2, pp. 1319-1333, 2018.

[24] Y. Chen, C. Tang, and Z. Yi, "A novel image encryption scheme based on PWLCM and standard map," Complexity, vol. 2020, pp. 1-23, 2020.

[25] Y. Han, Y. Tao, W. Zhang, W. Cui, and T. Shi, "Perceptron neural network image encryption algorithm based on chaotic system," IAENG International Journal of Computer Science, vol. 50, no. 1, pp. 42-50, 2023.

[26] R. Zhang, R. Zhou, and J. Luo, "Nonequal-length image encryption based on bitplane chaotic mapping," Scientific Reports, vol. 14, no. 1, p. 9075, 2024.

[27] W. Wu and Q. Wang, "Quantum image encryption based on Baker Map and 2D Logistic Map," International Journal of Theoretical Physics, vol. 61, no. 3, p. 64, 2022.

[28] N. Yassin, "Image encryption technique based on a binary combination of multiple Chaotic Maps and DNA sequence

operations," Jordanian Journal of Computers and Information Technology, p. 1, 2024.
[29] O. Elnoamy et al., "Enhanced image encryption using the Hénon Map, the LCG and the Lorenz System," in 2023 6th International Conference on Signal Processing and Information Security (ICSPIS), IEEE, pp. 93-98, 2023.
[30] E. Moya-Albor, A. Romero-Arellano, J. Brieva, and S. L. Gomez-Coronel, "Color image encryption algorithm based on a chaotic model using the Modular Discrete Derivative and Langton's Ant," Mathematics, vol. 11, no. 10, p. 2396, 2023.
[31] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, "Analytic study of a novel color image encryption method based on the chaos system and color codes," Complexity, vol. 2021, no. 1, 2021.
[32] A. Al-Daraiseh, Y. Sanjalawe, S. Fraihat, and S. Al-E'mari, "Novel, fast, strong, and parallel: A colored image cipher based on SBTM CPRNG," Symmetry (Basel)., vol. 16, no. 5, pp. 593, 2024.
[33] A. Siswanto, "Chaotic-based encryption algorithm using Henon and Logistic Maps for fingerprint template protection," International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 1, 2022.
[34] Y. Tao, W. Cui, J. Zhao, W. Zhang, and Z. Zhang, "A snake encryption algorithm for image with multiple chaos fusion," Engineering Letter., vol. 30, no. 3, pp. 1034-1043, 2022.
[35] L. Shi, X. Li, B. Jin, and Y. Li, "A chaos-based encryption algorithm to protect the security of digital artwork images," Mathematics, vol. 12, no. 20, p. 3162, 2024.
[36] A. Panwar, G. Biban, R. Chugh, A. Tassaddiq, and R. Alharbi, "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images," Heliyon, vol. 10, no. 11, p. e31618, 2024.
[37] M. Akraam, T. Rashid, and S. Zafar, " A chaos-based image encryption scheme is proposed using multiple Chaotic Maps, " Mathematical Problems in Engineering, vol. 2023, no. 1, 2023.