International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 1009-1017
Journal homepage: http://iieta.org/journals/ijsse

A New Hybrid Lightweight LEA-PRESENT (HLP) Algorithm to Encrypt Color Images

Eman Noori Kadhim*, Khalid Ali Hussein

Department of Computer Science, College of Education, Mustansiriyah University, Baghdad 10052, Iraq

Corresponding Author Email: dcm236@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.160507

Received: 28 March 2026
Revised: 8 May 2026
Accepted: 16 May 2026
Available online: 31 May 2026

Keywords:
chaotic system, counter mode, encryption color images, hybrid algorithm, Internet of Things, LEA algorithm, lightweight algorithm, PRESENT algorithm

ABSTRACT

Protecting digital images has become a challenge with the widespread adoption of Internet of Things (IoT) environments. These environments require encryption algorithms with high computational efficiency and strong security. Traditional algorithms, although secure, are often unsuitable due to their high computational cost. This requires lightweight and efficient solutions for color image encryption. This research presents a hybrid lightweight algorithm for color image encryption that combines the LEA and PRESENT algorithms in counter mode (CTR), supported by a five-dimensional (5D) chaotic system and utilizing the Hash-based message authentication code Key Derivation Function (HKDF) standard key derivation mechanism based on a cryptographically secure pseudo-random number generator (CSPRNG). This methodology encrypts image data first with LEA-128 algorithm for efficiency, followed by a robust encryption stage using PRESENT-128 algorithm, ensuring key independence and preventing insecure reuse of nonces. A key sensitivity measurement mechanism is integrated by holding nonces during testing. The results demonstrated that encrypted images reach an entropy value of 7.999, with a clear decrease in correlation coefficients in horizontal, vertical, and diagonal directions. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) exceed 99% and 33%, respectively, in key sensitivity tests. Mean squared error (MSE) and peak signal-to-noise ratio (PSNR) confirm lossless decryption with suitable encryption and decryption times, demonstrating the algorithm's suitability for resource-constrained environments.

1. INTRODUCTION

Digital images have become an essential part of modern communication systems, which are characterized by their large size and high statistical correlation between adjacent pixels, making the use of traditional encryption algorithms insufficient in many cases, both in terms of efficiency or security level [1]. Consequently, many studies have focused on developing image encryption algorithms based on chaotic systems, taking advantage of their characteristics such as high sensitivity to initial conditions and pseudo-random behavior, which resemble the principles of confusion and diffusion in modern cryptography [1-3]. Although these algorithms achieve strong security performance, their high computational complexity often makes them unsuitable for resource-constrained environments such as Internet of Things (IoT) devices and embedded systems [4]. To address this limitation, lightweight encryption algorithms have emerged with the aim of providing an acceptable security level while maintaining low computational cost and reduced energy consumption.

Among the most prominent examples are the LEA and PRESENT algorithms. LEA is characterized by its high software efficiency on general-purpose processors, whereas PRESENT was specifically designed to operate efficiently in hardware-constrained environments [5-7]. These lightweight block ciphers, however, are not necessarily effective in minimizing statistical correlations between pixels when applied to highly correlated image data, unless proper modes of operation or preprocessing are applied, which may still leave residual statistical correlations [8]. To address these issues, several studies have proposed the use of lightweight algorithms with chaotic techniques or hybrid mechanisms to strike a balanced, secure, and computationally efficient approach. These strategies show that with well-designed hybrid systems, it is possible to increase security features without significant performance degradation. Nevertheless, much of the literature is based on non-standardized or under-specified key generation methods, which may limit their reproducibility and resistance to security attacks [9-11].

The current study proposes a new lightweight hybrid algorithm in the encryption of digital images, through the combination of LEA and PRESENT algorithms, which will work in the counter mode (CTR) of operation. The secret key material is derived using the standardized Hash-based message authentication code Key Derivation Function (HKDF) mechanism in accordance with the RFC5869 [12] guideline, in addition to the use of a cryptographically secure pseudo-random number generator (CSPRNG) to produce the initialization vector (IV). Also, a five-dimensional (5D) chaotic system is included to enhance randomness and strengthen diffusion. The design proposed provides a high degree of security and at the same time low computational

overhead, hence it meets the requirement of secure image transmission in modern communication systems.

1.1 Main contribution

The main contributions of this work can be summarized as follows:

1. A novel hybrid lightweight image encryption framework that integrates LEA and PRESENT block ciphers within a unified CTR mode architecture, enabling a balanced trade-off between computational efficiency and security strength.
2. The incorporation of a 5D hyperchaotic system combined with a standardized HKDF-based key derivation mechanism, ensuring strong key independence, improved randomness, and resistance to key reuse vulnerabilities.
3. A secure and structured key and nonce generation process based on CSPRNG and HKDF, addressing limitations in prior hybrid encryption schemes that rely on non-standardized key generation methods.
4. Comprehensive security and performance evaluation demonstrating high entropy, low correlation, and strong resistance against differential attacks, making the proposed approach suitable for resource-constrained IoT environments.

2. RELATED WORK

The encryption of digital images has gained increasing significance with the increasing necessity of transmitting images and videos safely, particularly when transferring a huge amount of data. The current methods can be broadly categorized according to their mechanisms, security strength, and evaluation metrics such as entropy and correlation coefficient used to assess their effectiveness [1, 13]. Although much research has been carried out, there remains a significant challenge in achieving a balance between computational efficiency and high security.

2.1 Chaos-based image encryption

Image encryption schemes based on chaos have attracted considerable attention because of their inherent properties, including high sensitivity to initial conditions and pseudo-random behavior. These properties enable their use in the creation of secure encryption schemes [14-16]. A number of works have utilized complex chaotic systems and multi-layer chaotic maps to improve security by reducing statistical relationships among adjacent pixels and increasing randomness [2, 17]. However, these techniques are often computationally intensive, which limit their applicability in real-time systems and resource-constrained environments such as IoT devices [3, 4].

2.2 Lightweight block ciphers for image encryption

Lightweight block ciphers have been proposed to overcome performance constraints and provide efficient solutions for resource-constrained devices. These lightweight ciphers, such as PRESENT, are designed for low computational cost and minimal hardware requirements [5, 8, 18]. Similarly, LEA has been shown to be highly efficient in software implementations due to its ARX-based design, making it suitable for general-purpose processors [6, 7, 19].

Although they perform well in conventional cryptographic applications. However, when applied directly to image encryption, they may not perform well in reducing pixel correlation. This limitation stems from the underlying structural design and modes of operation. Hence, more improvement mechanisms are needed in order to enhance their effectiveness.

2.3 Hybrid and chaotic-enhanced encryption schemes

Hybrid encryption schemes that combine chaotic system and block ciphers have been proposed to leverage the strength of each technique. These techniques typically use chaotic systems in their permutation and diffusion operations, with block ciphers providing robust cryptographic security and key management.

Despite the fact that these approaches show enhanced security performance, many lack standardization and reproducibility. Also, the vulnerability might exist in the case of improper way of handling the initial parameters and key generation procedures, making the encryption scheme susceptible to prediction [9-11].

2.4 Motivation and research gap

From the above discussion, a research gap emerges. Chaos-based algorithms offer strong diffusion properties, but are computationally intensive. On the other hand, lightweight block ciphers are efficient; however, they may be sensitive to configuration and parameter selection, which can limit their ability to fully exploit the statistical properties of image data.

Also, the current hybrid designs often lack standardization and sufficient cryptographic robustness, especially in terms of key derivation, nonce management, and randomness control. This may adversely affect security and reproducibility.

Therefore, a systematic hybrid image encryption strategy that integrates lightweight block ciphers within a secure mode of operation (like CTR mode) and employs a standardized key derivation and randomness generation mechanism is required. The use of multidimensional chaotic systems can further enhance diffusion properties while maintaining efficiency, which motivates the proposed approach.

3. METHODOLOGY

The suggested methodology was formulated in accordance with the goals of the National Institute of Standards and Technology (NIST) lightweight cryptography standardization process, aiming to achieve a balance between security and efficiency in resource-constrained environments. Thus, a Hybrid Lightweight LEA-PRESENT (HLP) algorithm is proposed, which combines LEA as a preprocessing encryption phase and PRESENT as the main encryption layer to provide enhanced security measures. Finally, a 5D hyperchaotic system is used to generate initial keys and parameters according to the PILEA model [10].

3.1 LEA block cipher algorithm

LEA is a lightweight block cipher specifically designed to achieve high performance in software implementations while maintaining low resource consumption. It is based on the ARX (Addition, Rotation, XOR) structure, which relies exclusively on simple arithmetic and logical operations without the use of

S-boxes. LEA operates on 128-bit data blocks and supports key sizes of 128,192 and 256 bits. In this research, LEA-128 is adopted, which performs (24) encryption rounds. Each round consists of modular addition modulo 2^{32}, cyclic bitwise rotations and XOR operations, ensuring efficient diffusion and confusion properties. Due to its ARX-based design, LEA has demonstrated high execution speed and strong software efficiency compared to many conventional lightweight block ciphers, particularly on general-purpose processors [6, 20]. The operations of LEA algorithm are shown in Figure 1.

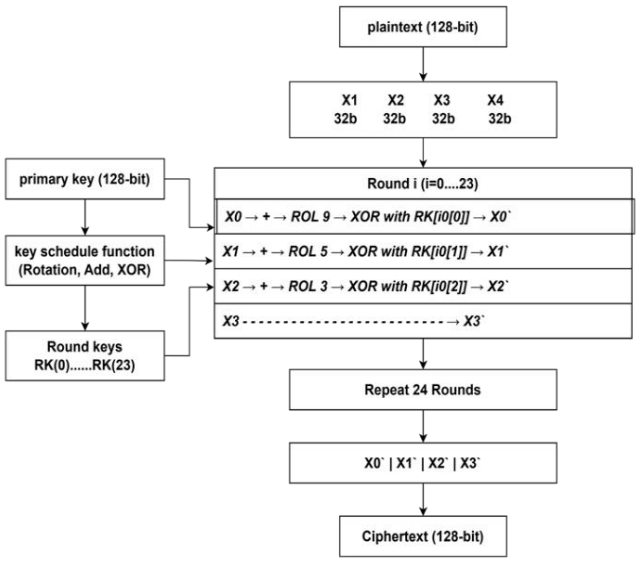

Figure 1. LEA encryption round structure

3.2 PRESENT block cipher

PRESENT is a lightweight block cipher designed for hardware-constrained environments, such as smart cards and IoT devices. It operates on 64-bit data blocks and supports 80-bit and 128-bit secret keys. In this study, PRESENT-128 was adopted to enhance security [5].

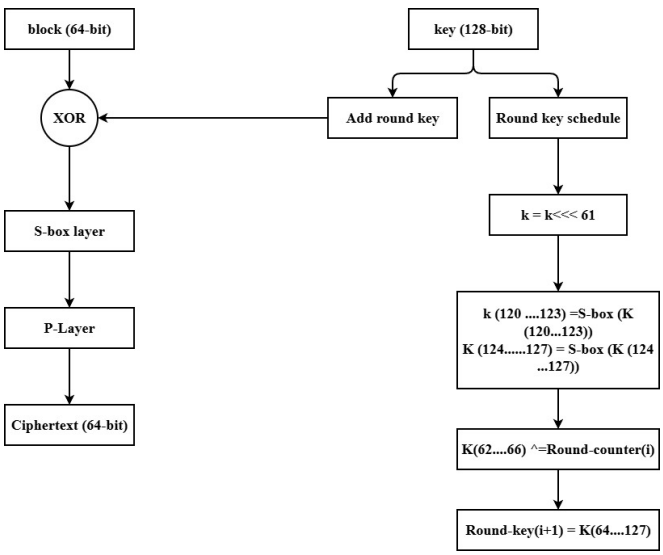

Figure 2. One round of the PRESENT algorithm

PRESENT follows a Substitution–Permutation Network (SPN) architecture consisting of 31 rounds. Each round includes a substitution layer implemented using 4-bit S-boxes, followed by a permutation layer (P-layer) that performs bitwise permutation to achieve diffusion. Despite its compact structure and minimal hardware footprint, PRESENT provides adequate security strength when properly configured within a secure mode of operation [18]. The operations of the PRESENT algorithm are shown in Figure 2.

3.3 Chaotic key generation

The chaotic system adopted in this research is inspired by the PILEA hybrid algorithm, which is characterized by being very sensitive to initial conditions and parameters, which is a fundamental property for enhancing the system's resistance to statistical and differential attacks [10]. It provides an effective ability to generate numerical sequences, making it suitable for use in an image encryption system that requires masking spatial patterns and reducing statistical correlation between pixels. Despite these good random properties provided by the chaotic system, chaotic systems alone are not cryptographically secure random number generators due to their deterministic nature [20].

Recent studies have proposed enhanced color image encryption methods based on pseudorandom affine functions to improve confusion and diffusion properties [21]. Other work has introduced a DNA-level enhanced Vigenère encryption approach that secures color images by combining chaotic maps with DNA operations [22].

The 5D chaotic system is described by the following mathematical model:

$$\frac{dx}{dt} = -ax + bz^2 - y$$

$$\frac{dy}{dt} = d\ sin\ z - y - xz + v$$

$$\frac{dz}{dt} = ey - fz + gxy$$

$$\frac{du}{dt} = hu + i \sin z$$

$$\frac{dv}{dt} = -jz$$

The system exhibits hyperchaotic behavior characterized by multiple positive Lyapunov exponents. The system parameters are defined as: $a = 11$, $b = 1.27$, $d = 13$, $e = 2.5$, $f = 5$, $g = 5$, $h = 12.3$, $i = 2$ and $j = 8$, while the initial conditions are: $x(0) = 10$, $y(0) = 2$, $z(0) = 0.5$, $u(0) = 8$, and $v(0) = 3$.

4. PROPOSED ALGORITHM

This study proposes a lightweight hybrid algorithm for digital image encryption that combines the LEA and PRESENT block ciphers in counter CTR mode with a 5D chaotic system and a CSPRNG for key and nonce management. This design aims to achieve an effective balance between computational efficiency and statistical security, making it suitable for image encryption in resource-constrained environments. The encryption process consists of two consecutive stages. In the first stage, the image is encrypted using LEA-128 in CTR mode to achieve high speed

and reduce the statistical correlation of adjacent pixels. In the second stage, the intermediate output is processed using PRESENT-128 in CTR mode to further enhance diffusion and increase ciphertext complexity.

4.1 Key and nonce generation

The key generation process begins with a 256-bit master key is generated using the Python secrets library, which relies on an operating-system-based CSPRNG seeded from entropy sources such as /dev/urandom, ensuring a non-deterministic cryptographic key.

To enhance randomness, a 5D chaotic system is employed for entropy diversification. The system parameters remain identical to those defined in the mathematical model adopted from the PILEA Algorithm, while only the initial state variables (X, Y, Z, U, V) are derived from the master key using HKDF. The system is solved numerically using the fourth-order Runge–Kutta (RK4) method. The RK4 numerical integration is performed using a fixed step size (dt = 0.001) over 2000 iterations to eliminate transient behavior and ensure numerical stability. The final state is hashed using SHA-256 to produce a 32-byte chaotic seed.

This seed is used as the salt in the HKDF-Extract phase, while the master key acts as the Input Keying Material (IKM) according to RFC 5869. HKDF then derives independent parameters, including a 128-bit key for LEA-128, a 128-bit key for PRESENT-128, and independent nonces for each encryption stage, ensuring proper key separation. The nonces used in CTR mode are deterministically derived using the HKDF expansion phase from the master key and the chaotic seed. The nonce size is selected according to the block size of each cipher (128 bits for LEA and 64 bits for PRESENT). Separate nonce values are generated for each encryption stage (LEA and PRESENT), ensuring independence between keystreams.

This design eliminates the risk of nonce reuse and guarantees that each encryption process operates with unique and securely derived parameters, preserving the security properties of CTR mode. The counter value is incremented sequentially for each processed block, ensuring that each input to the encryption function is unique and maintaining the correctness and security of CTR mode operation.

4.2 Encryption and decryption process

After loading the image and converting it into a byte array and dividing it into 128-bit blocks (b_i), if the image size is not a multiple of 128 bits, zero padding is applied to complete the final block. The following steps are performed.

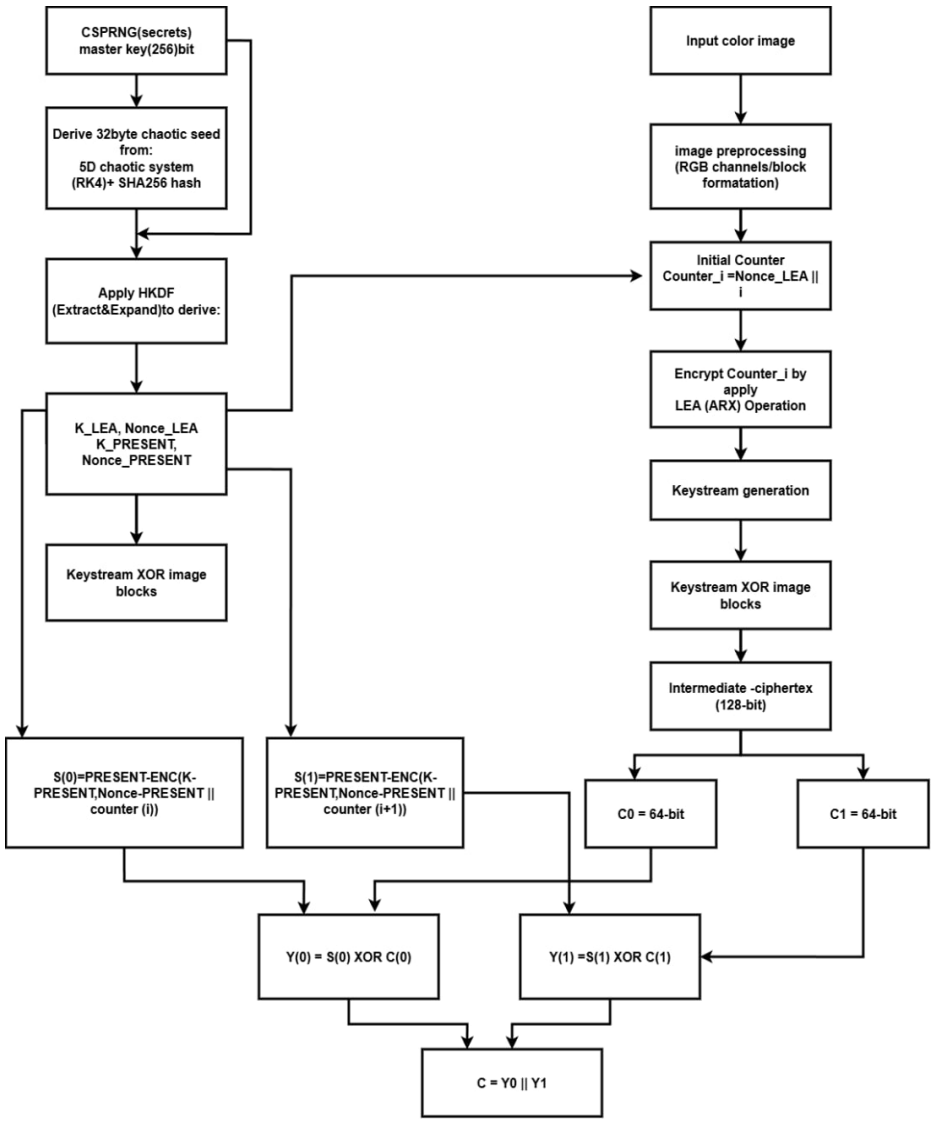

Figure 3. The proposed Hybrid Lightweight LEA-PRESENT (HLP) algorithm

Algorithm 1: The proposed HLP algorithm

Input: Color image I, 256-bit master key K
Output: Cipher image C
1: Derive chaotic seed:
- Generate initial state from K using HKDF
- Apply RK4 integration (dt = 0.001, 2000 iterations)
- Hash final state using SHA-256
2: Key and nonce derivation:
- Apply HKDF (Extract and Expand)
- Generate:
K_LEA (128-bit), K_PRESENT (128-bit)
N_LEA, N_PRESENT (nonces)
3: Convert image I into byte array and divide into 128-bit blocks (b_i)
4: // Stage 1: LEA-CTR Encryption
5: for each block b_i do
6: CTR_i = N_LEA || counter_i
7: k_i = LEA_Encrypt(K_LEA, CTR_i)
8: CT_i = b_i XOR k_i
9: end for
10: Intermediate ciphertext CT = concatenate (CT_i)
11: // Stage 2: PRESENT-CTR Encryption
12: for each 128-bit block in CT do
13: Split block into C0, C1 (64-bit each)
14: Generate counters: ctr0 = 2j, ctr1 = 2j+1
15: S0=PRESENT_Encrypt(K_PRESENT, N_PRESENT || ctr0)
16: S1=PRESENT_Encrypt(K_PRESENT, N_PRESENT || ctr1)
17: Y0 = C0 XOR S0
18: Y1 = C1 XOR S1
19: end for
20: Construct final ciphertext C = Y0 || Y1
21: return C

1- Encrypting the image data using LEA-128 in CTR mode based on the derived key and nonces. The output of this stage is (128-bit) intermediate ciphertext.

2- Passing the output of the first stage to PRESENT-128 in CTR mode using an independent key and nonces. Where the intermediate ciphertext is divided into two halves each of (64-bit) as plaintext, and then apply PRESENT operations on the nonce and the counters. Then, the output XORed with the plaintext.

3- Reconstructing the final output into an encrypted image.

The decryption process follows the same computational structure in reverse order. Since CTR mode operates by generating a keystream independent of the plaintext, encryption and decryption are performed using identical operations, relying on XOR with the same keystream blocks. The proposed HLP is shown in Figure 3.

4.4 Theoretical security analysis

From a theoretical perspective, the security of the proposed HLP algorithm relies on the combined effects of confusion and diffusion achieved through both the block cipher structure and the chaotic system. The use of CTR mode enables stream-like encryption, preventing pattern leakage across identical plaintext blocks.

The security of CTR mode depends on the uniqueness of nonces and counter values. Reusing a nonce with the same key may lead to keystream reuse and potential plaintext leakage. In the proposed HLP algorithm, nonces are securely derived using HKDF and assigned independently for each encryption stage, eliminating the risk of reuse. The counter is incremented for each block to ensure unique inputs, preserving the security properties of CTR mode.

Furthermore, the adoption of HKDF for key derivation ensures cryptographic separation between keys and nonces, reducing the risk of key-related attacks and preventing parameter reuse across encryption stages. The integration of a 5D chaotic system enhances randomness and introduces high sensitivity to initial conditions, strengthening resistance against statistical and differential attacks.

The proposed design also improves resistance against known-plaintext and chosen-plaintext attacks. The use of unique nonces ensures that identical plaintext blocks produce different ciphertexts, while the combined effect of HKDF-based derivation and chaotic randomness makes it difficult for attackers to infer key-related information.

Finally, the dual-layer encryption process (LEA followed by PRESENT) increases the overall complexity of the system, making it more difficult to analyze or reconstruct the original image without full knowledge of all cryptographic parameters.

5. RESULTS AND SECURITY ANALYSIS

This section aims to evaluate the security strength of the proposed hybrid algorithm through a set of standard security metrics adopted in digital image encryption, in order to measure its ability to resist statistical attacks and achieve confusion and propagation characteristics.

5.1 Experimental setup

The performance of the proposed algorithm was evaluated by measuring the quality of the encrypted and decrypted images using several statistical metrics, including histogram analysis, entropy, correlation coefficient, number of pixels change rate (NPCR), unified average changing intensity (UACI), mean squared error (MSE), peak signal-to-noise ratio (PSNR), encryption time, and decryption time.

All experiments were performed using Python in the Visual Studio Code environment on Microsoft Windows 11 Pro. The experiments were conducted on a Dell Vostro 15 3515 laptop equipped with an AMD Ryzen 5 5500U CPU at 2.10 GHz and 6 GB of RAM. This software and hardware environment was used to perform the encryption and decryption operations and calculate the security and performance metrics adopted in this study. The dataset used in the experiments is summarized in Table 1.

Table 1. Data set image

Image Name	Tajmahal.png	Barbara.jpg
Size	256 × 256	256 × 256
	512 × 512	512 × 512
	1024 × 600	1024 × 600

5.2 Histogram analysis

The histogram is one of the key indicators for measuring the resistance of image encryption algorithms to statistical attacks. In original images, the distribution of color values is irregular and reflects the image content, while the histogram of an encrypted image is supposed to be homogeneous and close to a regular distribution. The results obtained from the proposed algorithm show that the histogram of the encoded images in the three RGB color channels has a quasi-regular distribution without any clearly exploitable peaks or patterns, as shown in Figure 4.

5.3 Correlation analysis

Correlation coefficients between adjacent pixels in the three directions (horizontal, vertical, and diagonal) were calculated for both the original and encoded images. The results showed that the original images had high correlation coefficients, while these values decreased significantly in the encoded images, approaching zero. This indicates the effectiveness of the algorithm in breaking statistical correlation. All results of the encrypted and decrypted images are shown in Tables 2 and 3.

5.4 Information entropy analysis

Entropy is a measure of the degree of randomness and uncertainty in encoded data. The optimal value for the entropy of an 8-bit image is close to 8. The entropy of the original and encoded images was calculated, and the results are shown in Table 4 that the entropy values of the encoded images approach optimal values, indicating an efficient random distribution of pixel values. This reflects the important role of the 5D chaotic system in generating highly sensitive initial values, in addition to key separation using HKDF, prevent key prediction or reuse.

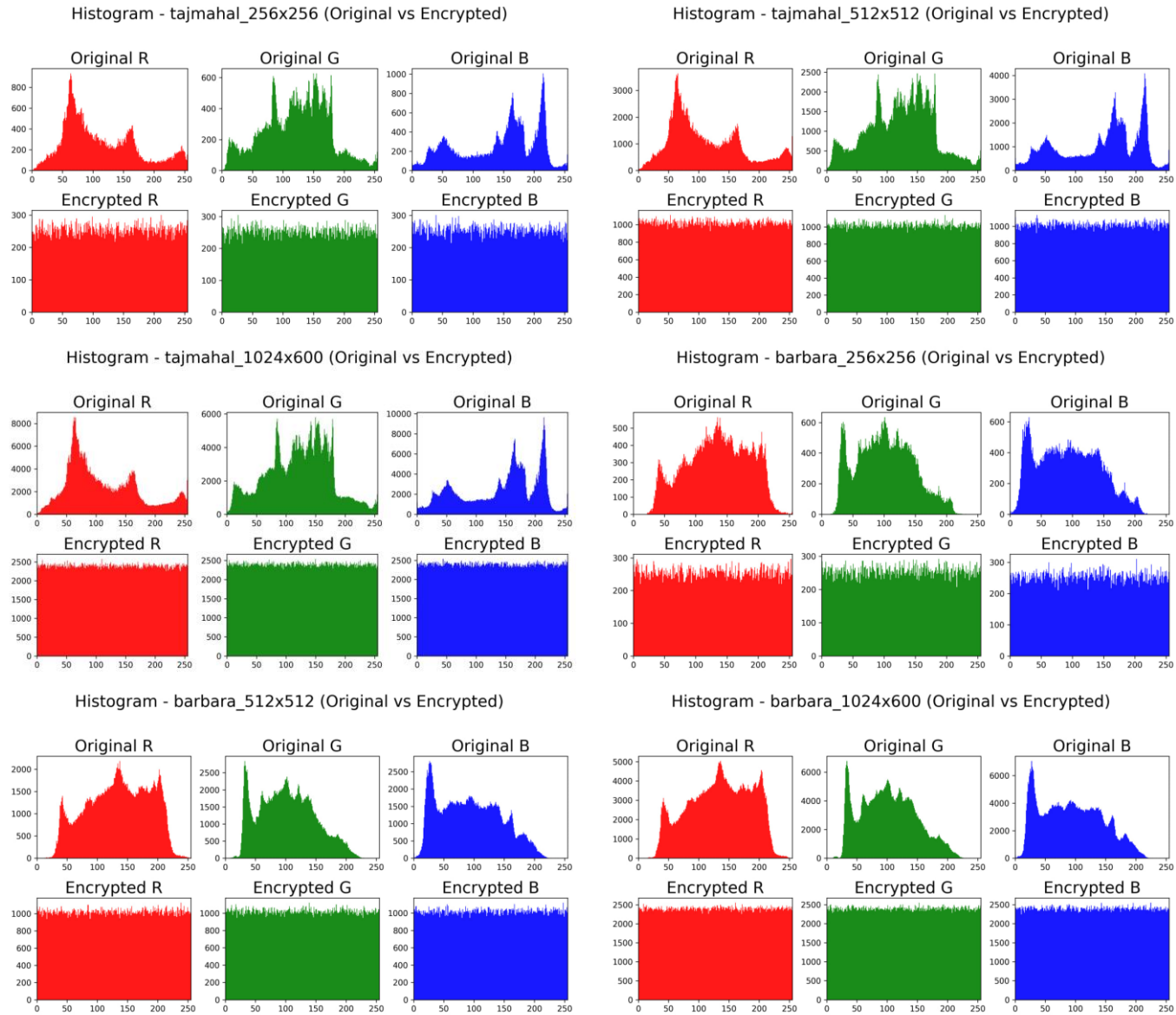

Figure 4. Histogram analysis

Table 2. Correlation of original image

Image	Size	Correlation		
		Original (H)	Original (V)	Original (D)
Tajmahal.png	256 × 256	0.925443	0.959289	0.900423
	512 × 512	0.966668	0.984889	0.956248
	1024 × 600	0.989747	0.989911	0.977456
Barbara.jpg	256 × 256	0.937675	0.950325	0.898717
	512 × 512	0.926336	0.964875	0.911434
	1024 × 600	0.981979	0.980708	0.960229

Table 3. Correlation of encrypted image

Image	Size	Correlation		
		Enc (H)	Enc (V)	Enc (D)
Tajmahal.png	256 × 256	-0.008238	0.016139	-0.011137
	512 × 512	0.037643	0.001776	0.004909
	1024 × 600	0.022350	-0.009595	0.002352
Barbara.jpg	256 × 256	0.011616	-0.016825	-0.002189
	512 × 512	-0.004783	0.000439	-0.016973
	1024 × 600	-0.112708	0.009245	-0.010521

Table 4. Information entropy

Image	Size	Entropy Original	Entropy Encryption
Tajmahal.png	256 × 256	7.811093	7.999763
	512 × 512	7.819783	7.999769
	1024 × 600	7.819937	7.999912
Barbara.jpg	256 × 256	7.632419	7.999581
	512 × 512	7.646069	7.999778
	1024 × 600	7.637515	7.999891

5.5 Differential attack analysis

To measure the algorithm's resistance to differential attacks, the NPCR and UACI indices were used. These indices measure the impact of a slight change in the original image on the encrypted image. High NPCR values and values close to the standard limits for UACI indicate the algorithm's strength against this type of attack. The proposed algorithm showed, in Table 5, high NPCR values and appropriate UACI values, indicating that any small change in the original image leads to a large-scale change in the encrypted image. These results reflect the effectiveness of the hybrid design, especially the combination of the two encryption phases and the use of independent initial keys and values derived in a standardized way.

Table 5. Number of pixels change rate (NPCR) and unified average changing intensity (UACI)

Image	Size	NPCR	UACI
Tajmahal.png	256 × 256	99.617513%	30.748269%
	512 × 512	99.612554%	30.737507%
	1024 × 600	99.605360%	30.765256%
Barbara.jpg	256 × 256	99.611410%	29.652941%
	512 × 512	99.606832%	29.747717%
	1024 × 600	99.613336%	29.759118%

5.6 Key sensitivity analysis

Key sensitivity was evaluated by flipping a single bit in the secret key and re-encrypting the same image. NPCR and UACI were then computed between the two ciphertext images. The results show that NPCR values exceed 99.6% and UACI values are approximately 33%, indicating a strong avalanche effect and high sensitivity to minor key modifications. These findings confirm that even a one-bit change in the secret key produces significant changes in the ciphertext, enhancing resistance against brute-force and key-related attacks. Table 6 presents key sensitivity results for the tested images.

5.7 Encryption and decryption time

The encryption and decryption times for each image were measured using a high-precision timer. The results showed that the encryption and decryption times are similar, which is expected behavior when using the CTR pattern, as both operations rely on the same computational architecture, as shown in Table 7.

Table 6. Key sensitivity analysis between number of pixels change rate (NPCR) and unified average changing intensity (UACI)

Image	Size	NPCR	UACI
Tajmahal.png	256 × 256	99.657513%	33.418269%
	512 × 512	99.622554%	33.543757%
	1024 × 600	99.615360%	33.465256%
Barbara.jpg	256 × 256	99.601410%	33.322941%
	512 × 512	99.526832%	33.217717%
	1024 × 600	99.613336%	33.559118%

Table 7. Encryption and decryption time

Image	Size	Encryption Time	Decryption Time
Tajmahal.png	256 × 256	2.755029 s	2.316736 s
	512 × 512	11.051277 s	11.037330 s
	1024 × 600	31.494734 s	29.906701 s
Barbara.jpg	256 × 256	2.750560 s	2.657767 s
	512 × 512	12.471285 s	12.946769 s
	1024 × 600	28.556915 s	28.881389 s

The results in Table 7 show that the execution time increases with image size, reaching higher values compared to some existing methods.

This HLP algorithm is proposed based on lightweight cryptographic principles, which are inherently suitable for IoT system. However, the current implementation is implemented in Python for experimental and validation purposes and does not represent an optimized or production-level implementation.

The anticipated improvement in efficiency for optimized versions is reinforced by the fact that both LEA and PRESENT rely on simple and efficient operations (addition, rotation, XOR, and bitwise permutation) that are efficient for hardware and low-level implementation (C/C++ or embedded system). Moreover, the CTR mode enables parallel processing of blocks, thereby significantly enhancing computational efficiency.

This approach achieves a balanced trade-off between security and performance, with potential use in IoT systems for optimized implementations.

5.8 Mean square error and peak-signal-to-noise-ratio

In the context of image encryption, MSE and PSNR are used to evaluate the level of distortion between the original and encrypted images. A high MSE value indicates a significant difference between the original and encrypted images, which

reflects strong encryption performance.

Similarly, low PSNR values indicate a high level of visual distortion, meaning that the encrypted image reveals minimal information about the original image. Therefore, lower PSNR values are desirable in encryption applications, as shown in Table 8.

The obtained results confirm that the proposed method produces a high level of distortion, making the encrypted images visually unrecognizable and resistant to statistical analysis.

Table 8. Mean square error (MSE) and peak-signal-to-noise-ratio (PSNR)

Image	Size	MSE	PSNR
Tajmahal.png	256 × 256	9137.994949	8.522294
	512 × 512	9145.943915	8.518518
	1024 × 600	9157.789931	8.512897
Barbara.jpg	256 × 256	8431.397196	8.871808
	512 × 512	8506.382507	8.833355
	1024 × 600	8500.843917	8.836183

6. COMPARATIVE ANALYSIS AND DISCUSSION

To verify the efficiency of the proposed HLP algorithm, it is compared with other image encryption algorithms, such as DES-PRESENT and PILEA. These techniques were chosen because they are closely related to hybrid and lightweight image encryption schemes that incorporate block ciphers with chaotic maps or multiple rounds of encryption.

Specifically, DES-PRESENT is a hybrid method that combines block ciphers, similar to the proposed method, and thus is appropriate for comparison in terms of cryptographic security performance. On the other hand, PILEA is a recent hybrid lightweight encryption algorithm that utilizes chaotic systems, providing a reliable benchmark for evaluating randomness and security improvements.

Therefore, these methods are selected to compare with the latest approaches that follow similar design principles and implementation strategies and are suitable for resource-constrained environments and IoT applications. All results shown in Table 9.

Some values are not reported in the referenced studies. The results in Table 9 indicate that all methods achieve entropy values close to the ideal value, reflecting strong randomness. The proposed HLP method shows a slight improvement in entropy compared to others.

All algorithms achieve high NPCR values above 99%, indicating effective diffusion, with the proposed method providing a marginal improvement.

The UACI value of the proposed method is noticeably higher, suggesting better sensitivity to small changes in the plaintext and stronger resistance to differential attacks.

PSNR values are similar across all methods, indicating comparable levels of visual distortion.

Overall, the proposed method demonstrates consistent performance with modest improvements in key security metrics compared to existing approaches.

Table 9. Comparison of performance metrics

Method	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	Correlation
Proposed HLP	7.9999	99.61	30.75	8.53	≈ -0.01 to 0.04
DES-PRESENT [11]	7.9991	99.45	22.00	8.61	≈ 0.01 to -0.03
PILEA [10]	7.9982				≈ 0.003 to -0.005

Note: Hybrid Lightweight LEA-PRESENT (HLP); number of pixels change rate (NPCR); unified average changing intensity (UACI); peak signal-to-noise ratio (PSNR)

7. CONCLUSIONS

This paper proposed a hybrid lightweight algorithm for digital image encryption that integrates the LEA and PRESENT block ciphers in CTR mode, supported by a 5D chaotic system and a secure key derivation mechanism. The design aims to achieve a balance between security and computational efficiency for resource-constrained environments.

Experimental results indicate that the proposed algorithm effectively reduces the statistical properties of the original images. The correlation coefficients of adjacent pixels in the encrypted images approach zero, ranging from −0.026 to 0.037 in different directions. The entropy values of the encrypted images ranged between 7.999063 and 7.999912, which are very close to the ideal value of 8, reflecting high randomness.

The differential attack analysis showed NPCR values between 99.605% and 99.617% and UACI values between 29.65% and 30.76%, indicating good resistance to differential attacks. Key sensitivity analysis also showed NPCR values above 99.52% and UACI values around 33%, this confirms that even a one-bit change in the secret key leads to significant differences in the ciphertext. In addition, the execution time increases with image size and reflects the computational overhead of the dual encryption process and the implementation environment. This suggests a practical trade-off between enhanced security and computational cost.

The experimental results indicate stable performance across standard evaluation metrics and provide a structured approach to combining lightweight encryption with controlled randomness. The method is potentially suitable for resource-constrained environments when implemented using optimized platforms.

Future work will investigate hardware implementation on FPGA platforms or embedded systems, as well as evaluating resistance against advanced attacks such as side-channel attacks.

ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Science, Mustansiriyah University, Baghdad, Iraq, for supporting this research.

DATA AVAILABILITY

The images used in this study are obtained from publicly

available sources on the Internet. The data are available from the corresponding author upon reasonable request.

STATEMENT ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

AI tools were used only for language editing and proofreading. No AI tools were used to generate the research content or results.

REFERENCES

[1] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 21: 917-935. https://doi.org/10.1007/s10207-022-00588-5

[2] Güvenoğlu, E. (2024). An image encryption algorithm based on multi-layered chaotic maps and its security analysis. Connect Science, 36(1): 2312108. https://doi.org/10.1080/09540091.2024.2312108

[3] Huang, D.Q., Zhang, Z.H., Tu, Y.T., Xie, L.R. (2024). Colour image encryption system based on four-dimensional memristor hyperchaotic. IEEE Access, 12: 161530-161544. https://doi.org/10.1109/ACCESS.2024.3439191

[4] Bhagat, V., Kumar, S., Gupta, S.K., Chaube, M.K. (2022). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications, Concurrency and Computation. Pracice and Experience, 35(1): e7425. https://doi.org/10.1002/cpe.7425

[5] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In International Conference on Cryptographic Hardware and Embedded Systems - CHES 2007, Taipei, Taiwan, China, pp. 450-466. https://doi.org/10.1007/978-3-540-74735-2_31

[6] Jang, W., Lee, S.Y. (2020). A format-preserving encryption FF1, FF3-1 using lightweight block ciphers LEA and, SPECK. In SAC '20: Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, pp. 369-375. https://doi.org/10.1145/3341105.3373953

[7] Seo, H., Liu, Z., Choi, J., Park, T., Kim, H. (2016) Compact implementations of LEA block cipher for low-end microprocessors. In Information Security Applications, pp. 28-40. https://doi.org/10.1007/978-3-319-31875-2_3

[8] Katuk, N., Chiadighikaobi, I.R. (2021). An enhanced block pre-processing of PRESENT algorithm for fingerprint template encryption in the Internet of Things environment. International Journal of Communication Network and Information Security, 13(3): 474-481. https://doi.org/10.17762/ijcnis.v13i3.5101

[9] Hoomod, H.K., Naif, J.R., Ahmed, I.S. (2020). A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system. Periodicals of Engineering and Natural Sciences, 8(4): 2333-2345. https://doi.org/10.21533/pen.v8.i4.1401

[10] Mohammed, Z.A., Hussein, K.A. (2024). PILEA, an advanced hybrid lightweight algorithm utilizing logical mathematical functions and chaotic systems. Engineering, Technology and Applied Science Research, 14(5): 16260-16265. https://doi.org/10.48084/etasr.7799

[11] Husam, S., Hoomod, H.K., Hussein, K.A. (2024). Hybrid algorithm (DES-present) for encryption image color using 2D-chaotic system. Mustansiriyah Journal of Pure Applied Sciences, 3(1): 49-63. https://doi.org/10.47831/mjpas.v3i1.119

[12] Krawczyk, H., Eronen, P. (2010). HMAC-based extract-and-expand key derivation function (HKDF) (No. RFC5869). Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc5869.

[13] Alghamdi, Y., Munir, A. (2024). Image encryption algorithms: A survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1): 126-152. https://doi.org/10.3390/jcp4010007

[14] Shakir, H.R., Mehdi, S.A., Hattab, A.A. (2023). A new four-dimensional hyper-chaotic system for image encryption. International Journal of Electrical and Computer Engineering (IJECE), 13(2): 1744-1756. https://doi.org/10.11591/ijece.v13i2.pp1744-1756

[15] Ahmed, S.S., Mehdi, S.A. (2022). Image encryption algorithm based on a novel 5D chaotic system. In 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), Mosul, Iraq, pp. 249-255. https://doi.org/10.1109/ICCITM56309.2022.10031883

[16] Kadhim, A., Mehdi, S. (2022). A new image encryption algorithm based on six dimension hyper chaotic system and KEN KEN puzzle. Journal of Optoelectron Laser, 41(3): 312-321.

[17] Setiadi, D.R.I.M., Rijati, N. (2023). An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations. Computation, 11(9): 178. https://doi.org/10.3390/computation11090178

[18] Imdad, M., Ramli, S.N., Mahdin, H. (2022). An enhanced key schedule algorithm of PRESENT-128 block cipher for random and non-random secret keys. Symmetry, 14(3): 604. https://doi.org/10.3390/sym14030604

[19] Mohammed, Z.A., Hussein, K.A. (2023). Lightweight cryptography concepts and algorithms: A survey. In 2023 Second International Conference on Advanced Computer Applications (ACA), Misan, Iraq, pp. 1-7. https://doi.org/10.1109/ACA57612.2023.10346914

[20] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

[21] El Bourakkadi, H., Chemlal, A., Tabti, H., Kattass, M., Jarjar, A., Benazzi, A. (2024). Enhanced color image encryption utilizing a novel Vigenere method with pseudorandom affine functions. Acadlore Transactions on AI and Machine Learning, 3(1): 36-56. https://doi.org/10.56578/ataiml030104

[22] Chemlal, A., Tabti, H., El Bourakkadi, H., Hicham, R., Jarjar, A., Benazzi, A. (2024). DNA-level enhanced Vigenère encryption for securing color Images. Acadlore Transactions on AI and Machine Learning, 3(2): 119-136. https://doi.org/10.56578/ataiml030205.