Context-Aware Image Encryption via Adaptive Entropy-Oriented Segmentation

Saadia Drissi
Pluridisciplinary Laboratory of Research Innovation (LPRI), Moroccan School of Engineering Sciences (EMSI), Casablanca, Morocco
Saadia.drissi@gmail.com (corresponding author)

Faiq Gmira
Innovative Technology and Computer Science Laboratory, Sidi Mohamed Ben Abdellah University, Fez, Morocco
faiq.gmira@usmba.ac.ma

Meriyem Chergui
Computer Sciences & Smart Systems (C3S), Hassan II University, Casablanca, Morocco
chergui.meriyem@gmail.com

Received: 5 March 2026 | Revised: 29 March 2026, 15 April 2026, and 3 May 2026 | Accepted: 4 May 2026

 DOI: https://doi.org/10.48084/etasr.18560

ABSTRACT

Recently, the demand for secure visual data transmission has increased significantly in applications such as cloud computing, telemedicine, and intelligent surveillance systems. This study presents an adaptive image encryption framework called Adaptive Entropy-Based Segmentation (AESeg), which, unlike conventional segmentation-based encryption approaches that rely on predefined geometric partitions, introduces an entropy-driven segmentation paradigm where the spatial distribution of information directly guides the allocation of cryptographic strength. In the proposed framework, high-entropy regions associated with rich textures and structural details are protected using strong cryptographic mechanisms, whereas low-entropy homogeneous regions are secured using lightweight encryption operations. By integrating entropy-based segmentation with the Dynamic Cipher Composition (DCC) architecture and adjacency-aware cryptographic allocation, AESeg enables context-aware encryption while reducing unnecessary computational overhead. Experimental results show that AESeg achieves entropy values close to 7.99, NPCR above 99.6%, and UACI above 33.4%, while reducing encryption time by 28–35% compared to conventional uniform encryption approaches. These results demonstrate that the proposed method achieves an effective balance between security robustness and computational efficiency.

Keywords-AESeg; image encryption; local entropy; adaptive security; cryptographic algorithms; segmentation

I. INTRODUCTION

With the rapid development of cloud-based technologies, telemedicine, intelligent surveillance systems, and smart monitoring infrastructures, ensuring the security of visual data is an important research problem. Although traditional encryption algorithms, such as AES and DES, are widely used for protecting data, they are not suitable for protecting visual data. The main reason is that, unlike textual data, visual data is characterized by spatial correlations among neighboring pixels, which are highly redundant and voluminous. These characteristics may lead to inefficient use of traditional encryption algorithms, causing unnecessary computational cost when encryption is performed for all pixels of the image. Therefore, considerable research attention has been focused on developing special encryption algorithms for visual data.

Image encryption research has proposed different methods to address these limitations. Chaos-based encryption methods are popular because of their dependence on initial conditions and random behavior, which adds confusion and diffusion to the image encryption process [1, 2]. Advanced chaos-based encryption methods and nonlinear transformation models have shown good security properties, although they might be associated with increased computation and real-time performance issues [3, 4]. In addition, hybrid approaches, using chaotic systems in conjunction with conventional methods and mathematical transformations, have also been proposed [5].

Recently, adaptive image encryption schemes have attracted considerable interest. In such schemes, the encryption operations vary depending on the texture density, pixel variations, or entropy of the images. These feature-aware and entropy-based encryption schemes have shown promising

results in resisting statistical and differential attacks while avoiding redundant encryption operations over homogeneous regions of the images [6]. Survey works have identified emerging trends of adaptive and intelligent encryption schemes, which can modify the encryption strength depending on the complexity of the images [7, 8].

Segmentation-based encryption strategies form another important research area for image encryption schemes. Block-based encryption schemes encrypt the image in blocks of a particular size and adapt the encryption parameters for better diffusion characteristics and efficiency [9, 10]. Chaos-based segmentation schemes incorporate randomness using chaotic functions for better randomness in the encryption process [11]. Hybrid segmentation schemes have also been proposed for better diversity in the encryption process [12]. However, although these schemes have improved the encryption process using segmentation methods, many of them still follow a particular structure or a segmented approach to encryption, which may not efficiently handle complexity changes in the image.

In addition to segmentation and adaptive encryption, several research studies have proposed improvements to the cryptographic algorithms used for secure image processing. Research on improving AES-based encryption algorithms has shown improved image security in cloud environments while maintaining reasonable computational efficiency [13]. In addition, lightweight cryptography has been proposed to reduce computational overhead in environments such as IoT networks [14]. Advanced cryptographic paradigms such as homomorphic encryption have also been proposed to ensure privacy-preserving image processing. However, such paradigms are computationally complex [15]. Recently, hybrid encryption models have been proposed to ensure improved security of images against sophisticated attacks by utilizing asymmetric cryptography, signal transformations, and learning models [16]. Recent studies have explored advanced image encryption techniques that focus on hybrid models and adaptive security mechanisms. Hybrid approaches that combine deep learning with traditional cryptographic methods have shown improved robustness in protecting medical images in cloud environments [17].

In [18], we proposed the DCC framework, which is a multi-method image encryption scheme that utilizes different encryption algorithms for different regions of the image, employing a register-based approach and a library of cryptographic methods. Although the DCC framework has been shown to be more flexible and secure against certain types of attacks, the method of dividing the image into regions was based on radial segmentation, which does not necessarily take into account the spatial distribution of information.

Unlike conventional entropy-based encryption schemes that typically apply uniform cryptographic mechanisms after entropy estimation, the proposed AESeg framework integrates entropy-driven segmentation with dynamic cryptographic allocation inside the DCC architecture. In addition, AESeg introduces adjacency-aware cipher assignment, ensuring that neighboring regions are protected using different cryptographic methods. This combination enables both context-aware encryption strength allocation and increased spatial cryptographic diversity. Specifically, the proposed framework incorporates a new content-based segmentation strategy that uses local entropy to control region classification and cryptographic strength allocation. By combining entropy-based segmentation with the DCC model and incorporating adjacency-based cryptographic allocation, AESeg offers an intelligent allocation of cryptographic operations over different regions of an image. This not only makes AESeg computationally efficient, but also maximizes spatial diversity in cryptographic strength, thereby improving immunity to statistical and differential attacks. Thus, AESeg expands on the DCC model by making segmentation an entirely adaptive process based on entropy.

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

- Proposes the AESeg entropy-driven segmentation mechanism that transforms image segmentation into a data-driven process controlling adaptive cryptographic allocation.
- Introduces adjacency-aware cryptographic diversity to prevent neighboring regions from using identical encryption methods.
- Integrates AESeg into the DCC framework to dynamically allocate encryption strength according to local image complexity.
- Reduces computational overhead while maintaining strong security metrics such as entropy, NPCR, UACI, and enhanced resistance to statistical and differential attacks through entropy-aware region classification and cryptographic diversity.

II. PROPOSED ASEG MECHANISM

Images are characterized by a highly non-uniform distribution across their spatial regions. Conventional uniform encryption approaches treat all image areas the same, leading to unnecessary computational overhead in regions with low informational value, while neglecting protection in highly detailed regions. To address this limitation, the proposed AESeg mechanism introduces a context-aware protection strategy that dynamically adjusts encryption strength with local image characteristics. Specifically, the proposed framework applies strong cryptographic protection to regions with dense textural information, while lightweight encryption operations are used in areas dominated by redundancy. This strategy ensures a consistent security level across the entire image while significantly improving runtime performance. Operating before the DCC modality assignment stage, the proposed mechanism generates a segmentation map that guides the adaptive selection of encryption algorithms and their corresponding strength levels.

A. Motivation

Although fixed-size block partitioning is used for computational stability and efficiency, the proposed AESeg differs from conventional block-based schemes by employing entropy as a decision driver for both region classification and

adaptive cryptographic assignment within the DCC framework. Additionally, the proposed method introduces adjacency-aware cipher selection to increase spatial cryptographic diversity. AESeg operates before the DCC modality assignment stage and produces a semantic map guiding the selection of encryption strength.

B. Local Entropy Computation

Let the image I be partitioned into non-overlapping blocks of size ($k \times k$). For each block B_i, local entropy is computed as:

$$H(B_i) = -\sum_{j=0}^{255} p_j \log_2 p_j \quad (1)$$

where p_j represents the probability of occurrence of the intensity level j within the block B_i. The collection of entropy values computed for all blocks forms an entropy map, which reflects the spatial distribution of information density across the image. By applying a suitable threshold to this entropy map, the image can be segmented into high-entropy regions, corresponding to areas with rich texture or detail, and low-entropy regions, which typically represent smoother or more homogeneous areas.

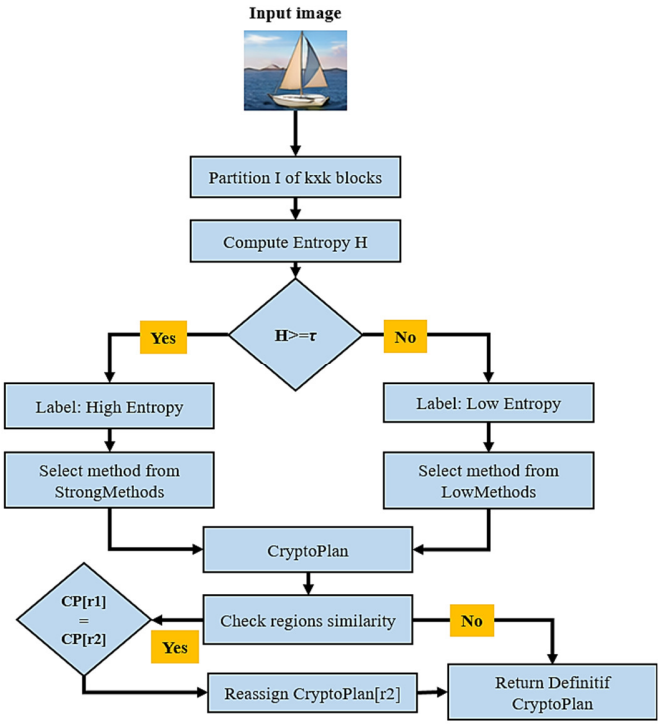


Fig. 1. Flowchart of AESeg mechanism.

The block size $k \times k$ used for image partitioning plays a crucial role, as it directly influences the balance between local feature representation and computational complexity. Smaller block sizes allow a more accurate capture of local spatial variations and texture information, whereas excessively small blocks may lead to unstable estimations due to insufficient pixel statistics. On the other hand, larger blocks reduce computational cost but may smooth out relevant local details.

In this work, the block size was selected based on extensive empirical evaluations conducted on images with different resolutions and characteristics. Experimental results show that block sizes ranging from 8×8 to 16×16 provide a good compromise between accuracy, robustness, and computational efficiency. Therefore, this range was adopted in all experiments. It is worth noting that the proposed framework remains flexible and allows the block size to be adjusted according to the image resolution and application requirements.

C. Region Classification Based on Entropy

Table I describes an entropy-based adaptive encryption scheme where the level of encryption is determined by the level of entropy of a specific region. If the entropy level $H > \tau$, the region has a high level of entropy and strong encryption schemes such as AES-256, AES-128, or chaos-based diffusion from the LIEM library are employed for security purposes.

TABLE I. REGION CLASSIFICATION BASED ON ENTROPY

Local entropy	Region type	Encryption level	Example methods (LIEM Library)
$H > \tau$	High entropy	Strong encryption	AES-256, AES-128, chaos-based diffusion algorithms
$H \leq \tau$	Low entropy	Lightweight encryption	Lightweight permutation–substitution, reduced diffusion methods

If $H \leq \tau$, the region has a low level of entropy, and lightweight encryption schemes are used to reduce computational complexity while providing security. This classification is later used by the DCC model to select appropriate encryption methods from the LIEM library according to the richness of each image area. The entropy threshold τ plays a critical role in the proposed AESeg mechanism, as it determines the boundary between high-information and low-information image regions. In this work, the threshold τ is selected empirically based on the statistical distribution of local entropy values computed across the entire image. Specifically, the entropy values obtained from all image blocks are first analyzed to estimate their global mean entropy. Blocks whose entropy exceeds this reference value are considered information-rich and classified as high-entropy regions, while the remaining blocks are labeled as low-entropy regions.

This strategy is motivated by previous studies showing that entropy values close to the global average effectively distinguish textured regions from smooth areas in natural images, without introducing excessive segmentation granularity or instability [6, 7]. Unlike fixed or heuristic thresholds, this adaptive selection allows the segmentation process to adjust to image content variability while maintaining robustness across different image types and resolutions. Experimental observations further confirm that using a mean-based entropy threshold yields a stable balance between security robustness and computational efficiency, as reflected in the achieved NPCR, UACI, and entropy metrics.

The use of the mean entropy value as the segmentation threshold provides a simple and computationally efficient mechanism to distinguish between information-rich and homogeneous image regions. However, alternative threshold

selection strategies such as percentile-based thresholds, adaptive statistical models, or clustering-based segmentation can also be considered to further refine the classification of image regions. A detailed comparative analysis of these thresholding strategies is considered an interesting direction for future research to further optimize the segmentation accuracy and cryptographic allocation of the AESeg framework.

D. Integration with DCC Framework

The integration of AESeg enhances spatial unpredictability while preserving the lightweight character of DCC. In the first step, AESeg interfaces with the DCC by performing entropy computation and region classification, after which strong or lightweight encryption labels are propagated. In the second step, the appropriate cryptographic methods are determined. The image is divided into fixed-size blocks, and entropy is employed as a statistical measure that distinguishes homogeneous and textured regions. Algorithm 1 summarizes the steps of the proposed method.

Algorithm 1:
Input: Image I $(L \times W)$, block size k, threshold τ
Output: EntropyMap, Labels
1. Divide I into $N = (L/k) \times (W/k)$ non-overlapping blocks $\{B_i\}$.
2. Initialize $EntropyMap$ and $Labels$.
3. For each block B_i:
   Compute histogram and probability distribution.
   Compute entropy H_i.
   Assign label:
   High-Entropy if $H_i \geq \tau$,
   otherwise Low-Entropy.
4. Return $EntropyMap$ and $Labels$.

The proposed method carries out block-wise entropy analysis to assess the information content of the image. The input image is divided into non-overlapping blocks of uniform size, ensuring that local texture variations can be captured efficiently. Entropy is then calculated using the normalized intensity histogram of each block. The output is saved in the form of an entropy map that represents the information content in terms of spatial location. Each block is then assigned either a high or low entropy label according to a predetermined threshold. In summary, entropy-based region classification allows distinguishing textured areas from homogeneous parts. After classifying the image into regions, an adaptive encryption method is employed to provide appropriate protection measures. The allocation method considers not only the entropy value of each region but also neighboring regions. Algorithm 2 outlines the allocation algorithm.

Algorithm 2:
Input: $Labels[]$, $StrongMethods$, $LightMethods$
Output: $CryptoPlan[]$
1. Initialize $CryptoPlan$ with a size equal to the number of regions.
2. For each region r:
   If $Labels[r] = High - Entropy$
   Select a method m from $StrongMethods$
   otherwise
   select m from $LightMethods$.
   Assign $CryptoPlan[r] \leftarrow m$.
3. Repeat
   For each pair of adjacent regions (r_1, r_2):
   If $CryptoPlan[r_1] = CryptoPlan[r_2]$,
   reassign $CryptoPlan[r_2]$ to another method,
   Until no neighboring regions share the same method,
4. Return $CryptoPlan$.

In the proposed framework, the cryptographic methods are chosen from a library of predefined methods based on the DCC architecture. For strong encryption, high-security symmetric algorithms, such as AES-256 and AES-128, and chaos-based diffusion-confusion algorithms for image encryption are considered to offer high resistance against statistical and differential attacks and applied to high entropy regions. For lightweight encryption, various computationally efficient operations such as lightweight permutation-substitution and reduced complexity diffusion algorithms are considered and applied to low entropy regions where image redundancy is high, improving computational efficiency while providing adequate security protection. The cryptographic key sizes are based on standard sizes of the considered cryptographic algorithms, such as 128-bit or 256-bit symmetric algorithms, and the final assignment of cryptographic methods is dynamically performed based on the AESeg classification and the DCC method selection mechanism.

In addition to the first algorithm, the second assigns cryptographic methods to image regions based on their entropy classification. High-entropy regions are protected using stronger cryptographic techniques, while low-entropy regions employ lighter methods. An adjacency constraint is further applied to prevent neighboring regions from using identical methods, thereby increasing cryptographic diversity and resistance to attacks. This adaptive assignment enhances overall security without impacting performance.

E. Advantages of the AESeg Extension

The proposed segmentation mechanism introduces several advantages, such as:

- Contextual encryption, where security is applied proportionally to information density.
- Reduced computational cost in flat regions, improving real-time performance.
- Enhanced diffusion and confusion in highly detailed areas.
- Improved resistance to structural attacks, as segmentation is content-dependent.

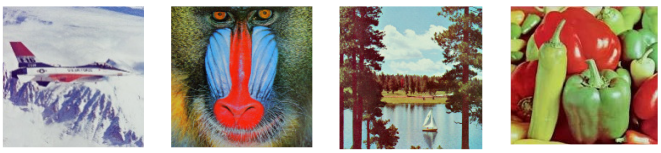
Therefore, AESeg enables further robustness against several types of attacks, such as statistical and differential, compared to current models.

III. EXPERIMENTAL STUDY

The experimental evaluation was conducted using standard grayscale benchmark images obtained from the USC-SIPI Image Database [19]. All selected images are publicly available and are commonly used as standard benchmarks in image processing and encryption research, ensuring reproducibility of the experimental results. Specifically, the following images were used:

- Baboon (512×512), characterized by highly textured regions and complex spatial details.
- Peppers (512×512), containing smooth regions and moderate texture variations.
- Sailboat (512×512), representing natural scenes with mixed textures, edges, and water reflections.
- Airplane (512×512), featuring structured objects with sharp edges and relatively uniform background regions.

These images (Figure 2) were selected because they provide diverse entropy distributions, including high-frequency textures, smooth regions, and structured patterns, enabling a comprehensive evaluation of the proposed adaptive encryption scheme under different image characteristics. In addition, these standard images are commonly used for image encryption techniques, and they provide a fair comparison with existing techniques.



Airplane Baboon Sailboat Peppers

Fig. 2. Image dataset.

A. Experimental Configuration

All experiments were performed on a workstation with an Intel i7 processor and 16 GB RAM using MATLAB and Python. Standard grayscale images of size 512×512 pixels were used for all experiments to ensure a fair comparison with existing image encryption methods. Although the proposed AESeg framework can be extended to color images by applying entropy analysis independently to each RGB channel, experimental validation on color images is left for future work. The runtime performance of all algorithms was compared in a unified environment. Since the runtime of an algorithm depends on several factors, all algorithms were implemented on the same platform, and the image size was kept constant across all experiments. All algorithms were compared based on the same set of images, image resolutions, and evaluation criteria. In some cases, the algorithms were implemented in the same environment for a fair comparison of the results. The reported results correspond to the average of 10 independent runs to ensure stability and reproducibility.

B. Computational Efficiency

AESeg shows a performance advantage compared to the proposed DCC framework, achieving an average reduction in encryption time of approximately 28–35%. To better understand the computational behavior of the proposed framework, the overall runtime can be conceptually divided into two stages: the preprocessing stage, which includes local entropy computation and region classification, and the encryption stage, where cryptographic methods are applied according to the AESeg allocation strategy. In practice, the entropy computation introduces only a small preprocessing overhead compared with the encryption operations. The observed runtime improvement is primarily due to the reduced computational cost of the encryption stage, as lightweight cryptographic methods are selectively applied to low-entropy regions while stronger encryption is reserved for information-rich regions. This improvement results from applying lightweight encryption mechanisms in low-entropy regions, which effectively reduces computational overhead.

C. Security Metrics

The encrypted images appear random and conceal all recognizable patterns. Neighboring pixels are not related (≈0.002), indicating high randomness in the encrypted image, and the entropy is very high (≈7.99), demonstrating strong diffusion properties. Security tests show NPCR above 99.6% and UACI above 33.4%, which indicate strong resistance to statistical and differential attacks under the evaluated conditions.

D. Adaptive Segmentation Impact

High-entropy regions receive stronger cryptographic protection, while low-entropy regions leverage lightweight encryption to reduce computational overhead. In addition, the enforcement of adjacency constraints introduced cryptographic diversity across adjacent regions, effectively preventing localized weaknesses and reinforcing the robustness of the encryption scheme. For a fair and consistent comparison, DCC [18] and a chaos-based method [12] were re-implemented and evaluated under the same experimental conditions as the proposed AESeg framework. All algorithms were tested using a set of benchmark images with identical image resolution and evaluation metrics. The reported results correspond to the average values obtained over 10 independent runs to ensure statistical reliability. Furthermore, the implementations of the compared methods strictly follow the configurations and parameter settings described in their original publications to ensure consistency and fairness in the evaluation. As shown in Table II, AESeg has similar or even better security performance compared to previous methods in terms of security metrics, as its entropy results are close to ideal. Meanwhile, AESeg significantly reduces the encryption time. This indicates that AESeg has better computation efficiency.

TABLE II. PERFORMANCE COMPARISON

Method	Entropy	NPCR (%)	UACI (%)	Time (ms)
DCC	7.98	99.4	33.1	120
Chaos Based	7.99	99.5	33.2	185
AESeg	7.99	99.6	33.4	85

E. Parameter Sensitivity Analysis

Table III shows that block sizes between 8×8 and 16×16 provide stable security metrics while maintaining good computational efficiency, which justifies the parameter adopted in the proposed AESeg framework.

TABLE III. PARAMETER SENSITIVITY ANALYSIS

Block size	Entropy	NPCR (%)	UACI (%)	Time (ms)
8×8	7.99	99.6	33.4	87
12×12	7.99	99.6	33.4	86
16×16	7.98	99.5	33.3	85

DISCUSSION

The proposed AESeg framework is an extension of the previously introduced DCC framework, but it replaces traditional geometric segmentation with an entropy-based adaptive segmentation method. This enables the encryption operation to make more efficient use of the information contained within the image. Thus, AESeg is more computationally efficient and secure. As shown in Table IV, the proposed method achieves a trade-off between security robustness and computational performance.

TABLE IV. SEGMENTATION MODELS COMPARISON

Model	Segmentation Basis	Adaptivity	Key Objectives	Limitations
[7]	Entropy-guided but fixed blocks	Medium	Introduces adaptivity, better security	Basic segmentation; lacks adjacency constraints
[9, 10]	Fixed-size non-overlapping blocks	Low	Captures local variations	Uniform encryption, high overhead for large images
[11]	Chaotic maps for random partition	Medium	High unpredictability, strong randomness	Computationally heavy, no entropy awareness
[12]	Chaos + geometric or block	Medium	Combines diversity and complexity	Still lacks full content adaptivity, complexity trade-off
[18]	Radial partition (8 regions)	None	Simple, low complexity	Predictable, ignores image content, vulnerable to structural attacks
AESeg	Local entropy-driven segmentation	High	Context-aware encryption, 28–35% faster, strong security	Requires an entropy computation step

As shown in Table II, AESeg achieves entropy values close to 7.99 and high NPCR and UACI values, and a reduction in encryption time compared to the original DCC framework and other chaos-based encryption methods. In addition, it differs from previous segmentation-based encryption schemes by introducing entropy-driven adaptive segmentation combined with adjacency-aware cryptographic allocation, which enables context-aware encryption. Although the comparison includes representative baseline methods such as the DCC framework and chaos-based encryption schemes, future work will extend the evaluation to include additional recent adaptive and learning-based image encryption methods to provide a broader benchmark.

From a computational perspective, AESeg reduces the average encryption time to 85 ms by applying lightweight encryption selectively in low-entropy regions. This is mainly due to the selective use of lightweight encryption techniques in low-entropy regions. Homogeneous regions contain limited structural information and therefore do not require computationally intensive cryptographic operations. This reduces encryption time without impacting security metrics. Although entropy computation introduces a preprocessing step, this overhead remains relatively small compared to the encryption stage. The additional preprocessing cost is compensated by the reduced cryptographic workload in low-entropy regions, which results in the overall reduction in execution time observed in the experiments.

Furthermore, entropy-driven region classification also enhances the distribution of cryptographic strength within the image, where regions with high information content receive stronger encryption, whereas smooth regions receive weaker encryption mechanisms. In addition, the adjacency constraint, which is considered during the assignment of the cryptographic method, ensures that the regions with adjacent locations are not given the same encryption method, thereby increasing the diversity of the encryption method and eliminating possible structural patterns in certain region-based encryption mechanisms.

The encryption algorithm eliminates spatial correlation in the original image. Compared to other segmentation schemes, AESeg provides a more adaptive mechanism for image segmentation. Fixed geometric-based segmentation schemes, such as radial partitioning in the traditional DCC model, do not take into account the spatial distribution of image information. Similarly, block-based image segmentation schemes take into account local changes but apply uniform encryption across all blocks, which may lead to increased computational cost. Chaos-based and hybrid image segmentation schemes improve randomness, but also increase complexity. AESeg balances efficiency and security.

Besides entropy, NPCR, and UACI, the statistical properties of the encrypted images were also investigated. The histogram analysis of the encrypted images shows a nearly uniform distribution of pixel intensities, which indicates strong randomness and effective diffusion properties. This uniform distribution demonstrates that the proposed encryption scheme effectively eliminates the statistical patterns present in the original image. Although the current evaluation includes widely used statistical and differential metrics such as entropy, NPCR, UACI, histogram distribution, and pixel correlation, further cryptographic validation can strengthen the security assessment of the AESeg framework. In particular, additional analyses such as key sensitivity evaluation, key space analysis, and resistance against various attack models will be investigated in future work to provide a more comprehensive security evaluation of the proposed encryption scheme. Further cryptographic evaluation, such as key sensitivity and key space analysis, can provide additional insights into the robustness of the encryption scheme.

Parameter analysis indicates that the proposed method is relatively stable with respect to block size and entropy threshold selection. Experiments show that block sizes between 8×8 and 16×16 provide a good compromise between segmentation accuracy and computational efficiency. Similarly, moderate variations in the entropy threshold do not significantly affect the reported security metrics, suggesting that the method is not highly sensitive to parameter tuning.

Although the experiments were conducted using grayscale images, the proposed AESeg framework can be extended to color images by applying entropy analysis independently to each color channel or through multi-channel entropy estimation. However, experimental validation on RGB images remains an important direction for future work to further demonstrate the effectiveness of the framework in real-world multimedia applications. In such cases, entropy analysis can be performed independently on each color channel or using multi-channel entropy estimation. Although this extension increases computational workload, the adaptive nature of AESeg still enables efficient allocation of encryption operations.

Overall, the results demonstrate that AESeg improves the efficiency of adaptive image encryption while maintaining strong statistical security properties. By combining entropy-driven segmentation with adaptive cryptographic assignment, the proposed method provides a practical and flexible encryption strategy suitable for applications such as cloud computing, telemedicine, and intelligent surveillance.

IV. CONCLUSION

AESeg enhances the DCC model by utilizing content-aware segmentation, which allows applying strong and light encryption algorithms based on the local features of the image. Results obtained using a set of benchmark grayscale images (Baboon, Peppers, Sailboat, Airplane) show that AESeg provides excellent security metrics, with near-ideal entropy values (≈7.99), NPCR more than 99.6%, and UACI higher than 33.4%. At the same time, this approach greatly minimizes processing time, achieving up to 35% speedup compared to other approaches. Therefore, the proposed method is effective in providing both security and efficient performance of cryptographic processing, and can be applied in real-life scenarios, such as cloud computing, telemedicine, and intelligent surveillance systems. However, this study used only benchmark grayscale images as input. In the future, the proposed approach will be evaluated based on large-scale datasets that include colored images as well as real-world cases. Security analysis will also be extended by evaluating key sensitivity, key space, and resistance to attack models.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests.

ACKNOWLEDGMENT

No external funding was received for this research.

DATA AVAILABILITY

This study used some images from the USC-SIPI database [19]. No other data were generated or analyzed during this study.

REFERENCES

[1] W. Alexan, N. H. E. Shabasy, N. Ehab, and E. A. Maher, "A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations," *Scientific Reports*, vol. 15, no. 1, Aug. 2025, Art. no. 31246, https://doi.org/10.1038/s41598-025-15794-z.

[2] 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, Aug. 2022, https://doi.org/10.1007/s10207-022-00588-5.

[3] H. Zhiqiang, A. Rauf, A. Nazir, F. Tchier, A. Aslam, and K. A. Tola, "Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support," *Scientific Reports*, vol. 15, no. 1, Nov. 2025, Art. no. 39951, https://doi.org/10.1038/s41598-025-23592-w.

[4] J. Gao, Y. Shen, S. Li, and J. Zhang, "An enhanced hybrid chaotic system and its application in image encryption," *Journal of King Saud University Computer and Information Sciences*, vol. 37, no. 9, Nov. 2025, Art. no. 295, https://doi.org/10.1007/s44443-025-00320-y.

[5] Y. Huang, Q. Zhang, and Y. Zhao, "Color image encryption algorithm based on hybrid chaos and layered strategies," *Journal of Information Security and Applications*, vol. 89, Mar. 2025, Art. no. 103921, https://doi.org/10.1016/j.jisa.2024.103921.

[6] 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, Feb. 2024, https://doi.org/10.3390/jcp4010007.

[7] O. P. Singh, K. N. Singh, A. K. Singh, and A. K. Agrawal, "Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions," *Neurocomputing*, vol. 612, Jan. 2025, Art. no. 128714, https://doi.org/10.1016/j.neucom.2024.128714.

[8] S. Rohhila and A. K. Singh, "Deep learning-based encryption for secure transmission digital images: A survey," *Computers and Electrical Engineering*, vol. 116, May 2024, Art. no. 109236, https://doi.org/10.1016/j.compeleceng.2024.109236.

[9] S. Khan and H. Peng, "A secure and adaptive block-based image encryption: a novel high-speed approach," *Nonlinear Dynamics*, vol. 112, no. 18, pp. 16445–16473, Sept. 2024, https://doi.org/10.1007/s11071-024-09870-8.

[10] J. Ahmad, "Secure Image Encryption Using Dynamic Block Segmentation and Adaptive Pixel Modification with Chaotic Masking," in *2024 International Conference on Engineering and Emerging Technologies (ICEET)*, Dec. 2024, pp. 1–6, https://doi.org/10.1109/ICEET65156.2024.10913959.

[11] T. Umar and M. Nadeem, "Chaos-based image encryption techniques: A comprehensive analysis and novel approach," *AIP Conference Proceedings*, vol. 3260, no. 1, July 2025, Art. no. 020017, https://doi.org/10.1063/5.0259015.

[12] R. Zhou, "Attack an image cipher algorithm combined new DNA operation with chaotic map," *The European Physical Journal Plus*, vol. 140, no. 9, Sept. 2025, Art. no. 817, https://doi.org/10.1140/epjp/s13360-025-06759-2.

[13] Z. A. Mohammed, H. Q. Gheni, Z. J. Hussein, and A. K. M. Al-Qurabat, "Advancing Cloud Image Security via AES Algorithm Enhancement Techniques," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12694–12701, Feb. 2024, https://doi.org/10.48084/etasr.6601.

[14] M. Alnabhan, A. El-Qasass, M. Atoum, Q. A. Al-Haija, and A. Habboush, "A Lightweight Cryptographic Solution for Enhanced Image Security," *Engineering, Technology & Applied Science Research*, vol. 15, no. 5, pp. 27052–27059, Oct. 2025, https://doi.org/10.48084/etasr.11707.

[15] Q. Chen, H. Li, S. B. Ariffin, and N. A. B. Mustapa, "A Comprehensive Study on the Homomorphic Encryption for Secure Image Data Processing," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21783–21790, Apr. 2025, https://doi.org/10.48084/etasr.10007.

[16] R. Padma and V. Yendapalli, "Hybrid Asymmetric Cryptography and Modified Cosine Wavelet Transform-Based Steganography Using Convolutional Autoencoder for Secure Data Sharing," *Engineering, Technology & Applied Science Research*, vol. 16, no. 1, pp. 32753–32760, Feb. 2026, https://doi.org/10.48084/etasr.15047.

[17] Y. Alslman, E. Alnagi, A. Ahmad, Y. AbuHour, R. Younisse, and Q. A. Al-haija, "Hybrid Encryption Scheme for Medical Imaging Using AutoEncoder and Advanced Encryption Standard," *Electronics*, vol. 11, no. 23, Nov. 2022, https://doi.org/10.3390/electronics11233967.

[18] S. Drissi, F. Gmira, J. Belkadid, M. Chergui, and M. E. Kamili, "Image-Type Data Security via Dynamic Cipher Composition from Method Libraries," *Technologies*, vol. 13, no. 10, Oct. 2025, https://doi.org/10.3390/technologies13100460.

[19] "USC-SIPI Image Database." [Online]. Available: https://sipi.usc.edu/database.