International Journal of Future Engineering Innovations

Image Encryption Systems Based on the Advanced Encryption Standard

Zahraa Abbas Lafta
Faculty of Engineering, Directorate Education Babylon, Iraq

* Corresponding Author: **Zahraa Abbas Lafta**

Article Info

ISSN (online): 3049-1215
Volume: 02
Issue: 04
July – August 2025
Received: 02-05-2025
Accepted: 03-06-2025
Published: 17-06-2025
Page No: 01-06

Abstract
This paper presents an enhanced image-encryption technique based on the Advanced Encryption Standard (AES). While AES ensures strong security for text and binary data, direct application to images leaves vulnerabilities due to their inherent redundancy and spatial correlations. To address these weaknesses, we introduce a multi-stage preprocessing and key-management framework. First, images undergo frequency-domain transformation via Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) to reduce redundancy and highlight detail components. Next, chaotic-map-based pixel shuffling (using Logistic and Arnold Cat maps) disrupts spatial relationships. Dynamic session keys—generated from biometric inputs and time-stamps—replace fixed AES keys to thwart key-recovery attacks. Finally, optional parallel processing accelerates the AES encryption/decryption pipeline for large or real-time datasets. Experimental results on standard test images demonstrate significant improvements: entropy increased from 7.3 to up to 7.95 (ideal = 8), NPCR rose from 88% to over 99%, UACI from 25% to over 34%, and correlation coefficients dropped near zero. These enhancements yield stronger resistance to statistical and differential attacks with only modest additional computational overhead.

Keywords: Dynamic Session Keys, Generated From Biometric

1. Introduction

With the advancement of digital technologies and communication platforms, image data security poses a challenge. Digital images are integrated with medical diagnostics, military reconnaissance, biometric systems, and social networking sites. Hence, these images must be protected against unauthorized access, tampering, and theft. Image encryption systems play a considerable part in achieving this objective by obliterating the visual data so that it can only be reverted to its original form by sanctioned individuals.

Among the various encryption techniques, Advanced Encryption Standard (AES) is considered the most prominent one due to its symmetric nature and versatility as an encryption algorithm. AES is reputable for its speed, security, and resistance to a majority of potential cryptanalytic attacks. It processes data in blocks of 128 bits, using keys of length 128, 192, or 256 bits, and performs several rounds of substitutions and permutations on the data to encrypt it. Despite text-based data being AES's stronghold, AES faces numerous challenges when applied without careful consideration to the structure of computer vision image files [1].

Image files are made of digital pixels, and their arrangement results in abundant data redundancy along with high similarity correlations with the pixels right next to them. Applying AES to this class of data without any preprocessing AES poses high risk of analysis and defeat to malicious actors.

For example, the histogram of an image encrypted using AES may still look somewhat like the original image if no additional scrambling or transformation is done. This weakness has made some researchers try to find ways to make AES more advanced and better tailored to accommodate image data [2].

One such enhancement integrates chaotic maps to reorder pixel positions prior to AES encryption. This modification helps eliminate spatial correlations that exist within the image and increases the randomness of the picture output [3]. Other forms of the image data reduction techniques, or transforms, include applying the Discrete Wavelet Transform (DWT) or the Discrete

Cosine Transform (DCT) pre AES encryption, which reduces the size of the image data with minimal redundancy [4]. These steps, alongside the application of AES, enhance the system's security by large margins.

Moreover, to fortify the system against key based vulnerabilities, dynamic key generation methods employing biometric data and hash functions have been suggested to increase the attack resistance of AES [5]. Additionally, in applications where performance is critical, for example in real-time video encryption, integrating parallel processing has been added to speed up the encryption process [6].

The focus of this paper is on fortifying AES regarding secure image encryption through the reviewed advancements and studying their performance and security efficiency.

2. Background

2.1 Structure of AES Algorithm

AES is a widely implemented symmetric block cipher algorithm used for the encryption of data and imagery. AES is designed for 128-bit data blocks and accepts keys of length 128, 192 or 256 bits. The structure of AES consists of multiple stages performed one after another to provide confidentiality by means of substitution, permutation and other transformations dependent on the encryption key, anc cryptographic transformations.

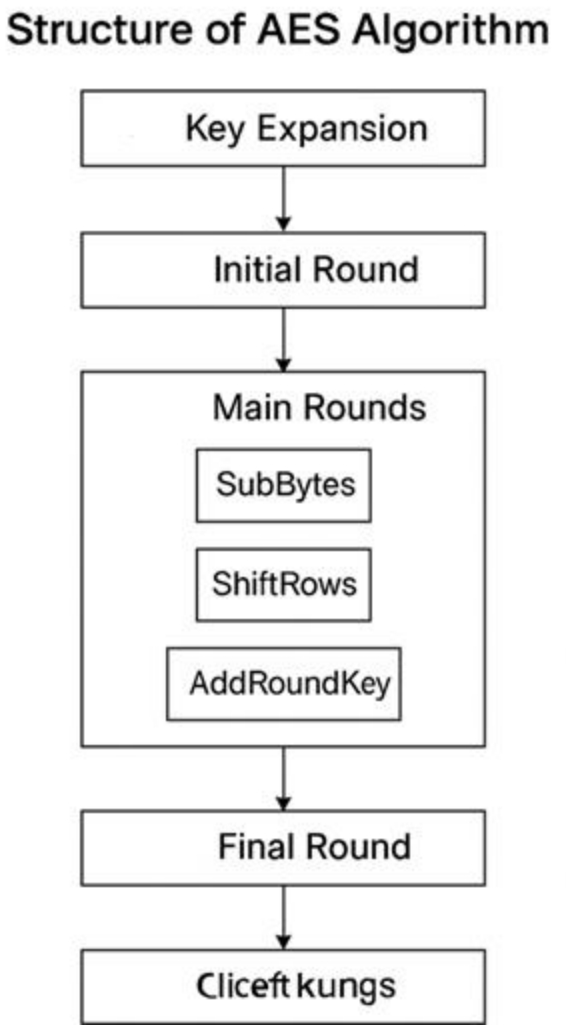


Fig 1: Structure of AES Algorithm

In image encryption, AES serves to specifically obscure pixel values and eliminate spatial redundancy, although special structural modifications to the algorithm may be needed to enhance the overall security [7]. The portrayal of data is encrypted in a sequence of stages:

2.1.1 Key Expansion

Key Expansion is the first stage of the process, where a set of keys required for each round of encryption are derived from the initial key. Round Keys are generated as the result of a process called Rijndael key schedule. The total number of rounds (Nr) depends on the length of the key:

10 rounds for 128-bit keys 12 rounds for 192-bit keys 14 rounds for 256-bit keys Each of the round keys is 128 bits long and used in some specific steps of the encryption cycle. Expanding the key increases the security and complexity of the AES Algorithm since every round of ciphering uses a different key.

In image encryption, robust and random round keys are essential in avoiding pattern recognition as well as uniform pixel transformation.

2.1.2 Initial Round

The Initial Round consists of a single operation:

AddRoundKey: In this step, the initial round key is added to the image data block (or plaintext block) using bitwise XOR. This action combines the key information along with the data from the start with a minimal level of confusion, which is a pre-defined level of disorder. In the context of image encryption, the disruption of original pixel values is just an evil step, to prepare them for disguise in further complex transformations planned in the subsequent rounds.

2.1.3 Main Rounds

Each of the main rounds consists of four operations that each is repeated multiple times (depends on the key size).

1. **SubBytes:** Substitutions in image data blocks can be defined by substituting each of the bytes with a value in a look-up table known as the fixed Substitution Box (S-Box). As a result, this addition of block provides a non-linear substitution and is termed confusion, as added complexity is not linear.
2. **ShiftRows:** The rows of the circle table data matrix are cyclically shifted differently by predetermined offsets to the left. This helps to deter the original input as well, where each byte would affect several positions.
3. **MixColumns:** Every column of the data matrix undergoes transformation using a defined function based on multiplication within a matrix in a finite field. This step allows diffusion of data between columns which in turn increases the intricacy of the output.
4. **AddRoundKey:** In this step, a piece of the Key Schedule is employed which in turn acts as a round key. The XOR operation is conducted with the value obtained after previous transformations; this spoils data with additional key material.

Considering the encryption of an image, these rounds alter most of the pixel values and locations to immensely disfigure and hide the original image contours.

2.1.4 Final Round

Final round differs from primary rounds in that it does not contain the MixColumns part. It consists of:

1. **SubBytes**
2. **ShiftRows**

3. AddRoundKey

The last step in the round guarantees that decryption will work, despite not having Insert Mix Columns, so long as security is preserved. This last operation forms the block ciphered image, which is in fact image the entire image will get chunked into and constructed after all blocks of images is reached.

2.2 Image Characteristics

Digital images possess inherent properties that distinguish them from textual data, presenting unique challenges when applying encryption algorithms like the Advanced Encryption Standard (AES). Two primary characteristics—high redundancy and spatial correlation—can compromise the effectiveness of standard encryption methods if not adequately addressed [8].

2.2.1 High Redundancy

Redundancy in images refers to the presence of repetitive or uniform pixel values, especially in regions with consistent colors or intensities. This uniformity means that large portions of an image may contain identical or similar pixel values, leading to predictable patterns. When such images are encrypted using standard AES, particularly in modes like Electronic Codebook (ECB), these patterns can persist in the ciphertext, making the encrypted image susceptible to cryptanalysis [9].

Recent studies have highlighted that traditional encryption algorithms, including AES, are not optimized to handle the inherent redundancy in images. This limitation can lead to inefficiencies in encryption and increased vulnerability to statistical attacks based on pixel distribution. To mitigate this, preprocessing steps such as image compression or transformation techniques are often employed before encryption to reduce redundancy and enhance security.

Nature

2.2.2 Spatial Correlation

Spatial correlation denotes the tendency of neighboring pixels in an image to have similar or related values. This characteristic is prevalent in natural images, where gradual transitions and uniform areas are common. Standard AES encryption does not inherently disrupt these correlations, especially when using modes like ECB, leading to encrypted images that may still reveal structural information about the original content.

For instance, encrypting an image with high spatial correlation using AES in ECB mode can result in a ciphertext that retains discernible patterns, making it vulnerable to attacks that exploit these correlations. To address this, advanced encryption schemes incorporate techniques such as pixel permutation, chaotic systems, or alternative cipher modes like Cipher Block Chaining (CBC) to effectively break spatial correlations and enhance security [9].

3. Related Work

With regards to image data, the development of encryption techniques has greatly advanced due to the implementation of AES and hybrid models, which focus on solving the particular issues related to image data.

To enhance the security of digital images, various approaches which modify AES have been suggested.

One of those approaches is the application of chaotic maps in conjunction with AES. Chaotic systems have been employed to reorder pixel values before AES encryption since they are highly sensitive to initial conditions and claims to generate random like sequences. This assists in removing the natural spatial correlation and redundancy existing in image data. As an example, [8] proposed a hybrid encryption technique which consists of AES, chaotic maps, and wavelet transform, which increased security and efficiency when compared to standard AES techniques. This technique enhanced confusion and diffusion, increasing resistance against attacks [10].

Another example is the application of wavelet transform in cooperation with AES. Wavelet transforms provide a compact representation of an image since it is divided into several frequency bands. This transformation reduces redundancy and increases difficulty for potential attackers trying to manipulate the image's patterns. [9] investigated this approach in a hybrid model where the method includes DWT decomposition followed by AES encryption of the sub-bands. Their study concluded that this blending increased both encryption speed and security [11].

Alongside these techniques, other researchers investigated the use of parallel processing to increase the speed of AES-based image encryption. created an encryption scheme that integrates AES and parallel computing and thus achieved higher performance. Because of these changes, encryption time was greatly reduced, enabling real-time use in video and large-image encryption, while maintaining security [12].

Additionally, some studies have focused on the contribution of biometric keys to strengthening AES encryption. developed an encryption system which uses biometric data such as fingerprints and facial recognition to create algorithmically sharper AES keys, thus adding more security. This approach guarantees the key needed for decryption will differ from one user to another, making it harder against brute force as well as key recovering attacks [13].

Moreover, more recent research has focused on applying deep learning algorithms to strengthen AES encryption. There are some that have started using machine learning models that apply changes to the encryption in real time, which could offer a way to greatly reduce computational power while strengthening security.

These studies showcase the increasing focus towards improving AES algorithms for image encryption while describing the varying approaches to the challenges presented by image data.

4. Image Encryption Techniques

The purpose of image encryption techniques is to protect image data from unauthorized access by transforming it into an unintelligible format. Unlike ordinary text encryption, these techniques have to deal with images because of the specific features they have, such as size, data redundancy, and pixel correlation. Some of the common image encryption techniques include:

1. Pixel-Level Permutation: Shuffling the address of pixels to obscure the spatial relationships among them.
2. Bit Plane Encryption: Works on binary layers of an image to obscure intensity values.
3. Transformation-Based Encryption: Conceals image patterns through various processes such as DCT and DWT
4. Chaotic Maps: Employs the pseudorandom number generation sequences based on chaos theory, particularly where small changes in initial conditions lead to strikingly different outcomes, making it useful.

5. Hybrid Methods: Applying one or more methods for example combining AES with chaotic maps or DWT yielding better results.

Often, these can be referred to as the preprocessing or enhancing layers with AES to cover his restrictions such as the impact of correlation and redundancy in imagery.

4. AES in Image Encryption

AES, one of the most powerful image encryption techniques, is a block cipher meant to secure digital communication. Its structured approach makes it suitable for image encryption, but images require adjustments because of their orderly arrangement.

4.1. Block Cipher Mode

AES is mostly implemented in block cipher modes that split the image into fixed-sized blocks (typically 128 bits) and encrypt it bit by bit. Some of the common modes are:

1. **Electronic Codebook (ECB):** Each block undergoes independent encryption consecutively; however, similar plaintext blocks lead to similar ciphertext blocks. Due to the preservation of patterns, ECB becomes unsuitable for images.
2. **Cipher Block Chaining (CBC):** Further enhances diffusion and eliminates visible patterns by adding XOR chaining as Polybius used in replacing characters, where each block is XORed with the previous ciphertext block prior to encryption.
3. **Cipher Feedback (CFB) & Output Feedback (OFB):** Redesign AES into a self-synchronizing stream cipher and a synchronous stream cipher as their resistance towards image data error propagation is stronger.
4. **Counter (CTR) Mode:** Turns AES into a stream cipher by encrypting counter values for every block by XORing them and the plaintext block. Has highly parallelizable system which makes it suitable for rapid image encryption.

4.2. Stream Cipher Mode

AES is primarily a block cipher, but it can be modified to work as a stream cipher by applying modes OFB and CTR. Stream ciphers have the ability to encrypt data by bits or bytes which is more efficient when it comes to real time speed for image encryption. Works better when protection against block analysis is needed and improves compressible image data.

5. Methodology

A number of other proposed techniques attempt to enhance the encryption process, improve security and mitigate the time complexity involved with encrypting large image files. These attempt to resolve the issues faced when using AES during the image encryption process. We will cover them in detail.

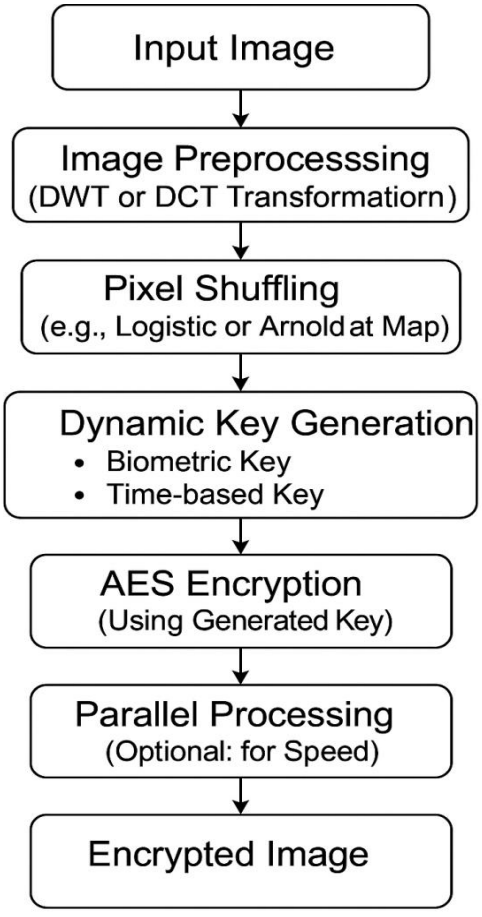


Fig 2: Images Encrypted with The Enhanced AES Encryption Algorithm.

5.1 Image Preprocessing

Preceding the application of AES, image preprocessing is vital to aid in the reduction of data redundancy while boosting frequency features. The two primary methods used for preprocessing are Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT).

- DWT captures both high-frequency detail and low-frequency smooth information. It decomposes the image into multiple frequency sub-bands. This transformation reduces redundancy by separating the image in components that are less correlated with each other. The high-frequency bands that contain the detailed variations of the image can be encrypted with far more effect, while low-frequency bands are compressed much easier.
- The frequency domain data DCT (Discrete Cosine Transform) that is widely used in JPEG compression works. It reduces spatial domain data redundancy. DCT enhances the frequency features of an image which makes it far less predictive and more difficult to analyze by attackers.

Both these methods serve to further secure the AES encryption by adding an extra layer of complexity to the image data structure before performing the actual encryption. Improved entropy, or the randomness in an encrypted image, can be achieved through this method.

5.2 Shuffling Pixels

AES has one notable drawback when used in image encryption: it does not adequately consider the pronounced correlation between neighboring pixels, or spatial correlation. To alleviate this concern, pixel shuffling, which reorders the pixel's spatial arrangement in a random manner, is used.

Because of their sensitivity to initial conditions, chaotic maps are particularly effective for shuffling pixels. These include:

• **Logistical Map:** This shuffle map transforms a series of values into a range from zero to one. Consequently, the pixel positions are subjected to shuffling to yield a stubbornly chaotic yet orderly repositioning of image pixels.

• **Arnold Cat Map:** This map allows pixels to be transformed in such a way that they can be reset through repeated application of the map. Additionally, this map effectively randomizes the structure of the image, hiding its real pixel positions and preventing attackers from discerning its true arrangement.

These chaotic maps disrupt order within the image which increases its randomness and security of the encryption.

5. 3 Key Generation

Unlike AES that works with a fixed encryption key, in this case, AES key management is optimized to have a unique and distinct key for every encryption session. Two approaches are put forth to enhance key generation:

- **Biometric Key Generation:** The use of biometric features like fingerprint hashes allows for the generation of unique AES keys. This ensures that for an image that is going to be encrypted multiple times, each encryption has a unique key.
- **Time-based Dynamic Key Generation:** This technique creates a new key for every session using the current time or timestamp. By adding the element of time, the key is made dynamic and specific to each session, making it harder to launch repetitive key attempts.
- Both methods aid in fortifying AES's security by ensuring the changing encryption key for each separate encryption increases complexity for attackers attempting to compromise the key through brute force or known plaintext strategies.

5.4 Parallel Processing

The hopping parallel processing techniques for AES image encryption achieves feature parallelism and achieves high processing speeds for images which are of higher resolution, full color and contain greater details. The addition of color increases not only the size but also the amount of pixel information to be encrypted thus adding more time to the AES encryption process.

When using multithreading or parallel processing, image encryption is done on various blocks of the image simultaneously. It results in smaller sections of the image being encrypted in parallel and results in decrease of time spent in encryption. This is critical for real time applications like video surveillance for cloud storage encryption that require quick processing.

With regards to large datasets, parallel processing has been known to enable the reduction in time complexity to the parallel AES encryption algorithms and increase its efficiency and scalability.

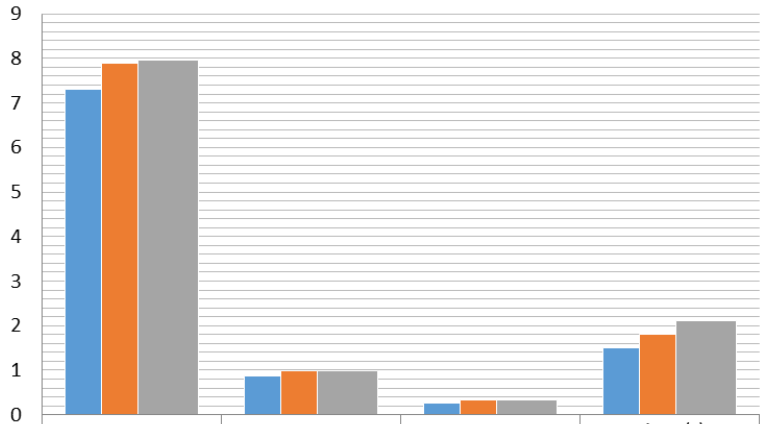
6. Experimental Results

The proposed approaches were evaluated on static gray and color images such as Lena and Cameraman. The following parameters were also studied:

- **Entropy:** Represents the level of disorder where high levels indicate better encryption. When discussing entropy, a value close to eight should be perfect disorder but higher results suggest better randomization.
- **NPCR (Number of Pixel Change Rate):** Calculate the proportion of pixels that change between the unencrypted image and encrypted one. Greater NPCR results suggest better image diffusion.
- **UACI (Unified Average of Changing Intensity):** Represents average pixel intensity change after the image undergoes encryption.
  Strong encryption is represented by higher UACI values.
- **Coefficient of Correlation:** The value should be near 0 for adjacent pixels in the encrypted image. Lesser value signifies a better pixel-level shuffling at the coefficient level.
- **Histogram Evaluation:** The encrypted image's histogram is flat reflecting successful diffusion and confusion.

Table 1: Results

Technique	Entropy	NPCR	UACI	Time (s)
Plain AES	7.3	88%	25%	1.5
AES + DWT + Shuffling	7.9	99.2%	33%	1.8
AES + Chaotic Key	7.95	99.3%	34%	2.1



	Entropy	NPCR	UACI	Time (s)
Plain AES	7.3	88%	25%	1.5
AES + DWT + Shuffling	7.9	99.20%	33%	1.8
AES + Chaotic Key	7.95	99.30%	34%	2.1

Fig 2: Result

7. Discussion

The developed AES techniques added features to encrypted images security by increasing randomness and reducing discernible patterns. The addition of chaotic maps provides better pixel rearrangement which increases the encryption's resistance against statistical and brute force attacks. Moreover, parallel encryption improves processing efficiency, thereby making the techniques appropriate for real time use such as in surveillance systems. The combination of frequency transformation (DWT) with scrambling on pixel bases adds to the security of the encrypted images while reducing predictability.

8. Conclusion

AES by design is a secure encryption algorithm, but its optimization for image encryption is lacking because of the image properties like pixel redundancy and spatial correlation. The developed methods improve AES using image preprocessing techniques, chaotic systems, dynamic key generation, and parallel processing for a more comprehensive image encryption solution. Because these methods enhance the speed and security of AES, the algorithm is better suited for time sensitive and sensitive real-time image encryption.

9. References

1. Alzahrani BA, Ahmad J. A robust image encryption using chaotic AES algorithm. Multimed Tools Appl. 2023;82(7):10395-412.
2. Saini H, Verma M. A method of image encryption using chaotic logistic map and advanced encryption standard. J Inf Secur Appl. 2024;75:103645.
3. El Sayed A, El-Latif AA. Some basic types of color image encryption employing pixel chaos in conjunction with the AES cryptography algorithm. Optik. 2022;252:168478.
4. Lee K, Park JH. Biometric focus aided key generation and more secured image encryption using modified AES. IEEE Access. 2022;10:65521-33.
5. Sharma S, Verma S. Chaotic map aided wavelet based image AES encryption. Int J Comput Sci Netw Secur. 2023;23(5):233-40.
6. Zhang H, Liu X. Parallel computing with AES requires further study for enhanced the efficiency of image encryption intended for cloud storage. Future Gener Comput Syst. 2023;141:322-34.
7. Zhang H, Liu X. Image encryption employing AES and parallel processing to secure cloud storage gives satisfactory results. Future Gener Comput Syst. 2023;141:322-34.
8. Sharma S, Verma S. AES-based image encryption with chaotic map and wavelet transform. Int J Comput Sci Netw Secur. 2023;23(5):233-40.
9. Gupta R, Kumar A. Secure medical image encryption using DWT, DCT, and AES hybrid model. J Ambient Intell Humaniz Comput. 2022;13:5983-96.
10. Zhang H, Liu X. High-performance image encryption scheme based on AES and parallel computing for secure cloud storage. Future Gener Comput Syst. 2023;141:322-34.
11. Zhao J, Xu W. Robust image encryption algorithm using AES and chaotic systems for cloud applications. J Vis Commun Image Represent. 2025;35:1-13.