Griya Journal of Mathematics Education and Application
Volume 6 Nomor 1, Maret 2026
e-ISSN 2776-124X| |p-ISSN 2776-1258
https://mathjournal.unram.ac.id/index.php/Griya/index

A comparative analysis of AES and LWE in digital image encryption

Aisyah Nooravieta Setiawan[1*], Siska Dwi Kumala[1], Aisyah Enggel Luthfiyah[2]

[1] *Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Bengkulu, Bengkulu, Indonesia*
[2] *Student, Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Bengkulu, Bengkulu, Indonesia*

anooravieta.setiawan@unib.ac.id

Received: 05-02-2026; Revised: 08-03-2026; Published: 12-03-2026

Abstract
This study investigates a comparative analysis between two cryptographic algorithms, which are the Advanced Encryption Standard (AES) and the Learning With Errors (LWE), in the case of digital image encryption. The core of the aim is to evaluate the computational performance, output quality, and security of the two algorithms when applied to digital image data. The methods used include measuring the computational performance by recording the encryption and decryption times for both algorithms, as well as performing a detailed analysis of the image quality post-decryption, and comparing the security of the two algorithms. The results of this analysis indicate that AES outperforms LWE in terms of speed, providing faster encryption and decryption processes with minimal impact on image quality. However, LWE offers a stronger level of security against quantum-based attacks, although with a longer processing time. This study provides important insights for selecting the appropriate encryption algorithm based on security and performance requirements in digital image processing.

Keywords: Encryption; Digital_Image; AES; LWE; Decryption

Abstrak
Penelitian ini mengkaji analisis komparatif antara dua algoritma kriptografi, yaitu *Advanced Encryption Standard* (AES) dan *Learning With Errors* (LWE), dalam penerapannya pada enkripsi citra digital. Tujuan utama penelitian ini adalah mengevaluasi kinerja komputasi, kualitas *output*, serta tingkat keamanan kedua algoritma ketika diaplikasikan pada data citra digital. Metode yang digunakan meliputi pengukuran performa komputasi melalui pencatatan waktu enkripsi dan dekripsi pada kedua algoritma, analisis kualitas citra setelah proses dekripsi, serta perbandingan tingkat keamanan masing-masing algoritma. Hasil analisis menunjukkan bahwa AES memiliki performa lebih unggul dari sisi kecepatan dalam proses enkripsi dan dekripsi, dengan dampak minimal terhadap kualitas citra. Namun, LWE menunjukkan tingkat keamanan yang lebih kuat terhadap serangan berbasis komputasi kuantum, meskipun membutuhkan waktu pemrosesan yang lebih lama. Penelitian ini memberikan wawasan penting dalam pemilihan algoritma enkripsi yang sesuai berdasarkan kebutuhan keamanan dan kinerja dalam pengolahan citra digital.

Kata Kunci: Enkripsi; Citra Digital; AES; LWE; Dekripsi

1. INTRODUCTION

The rapid development of digital technology has increased the need for reliable and efficient encryption methods to protect sensitive data, especially visual data. The

important role of digital images in various sectors, ranging from personal communications and social media to critical infrastructure and defense systems, also ensuring the confidentiality and integrity of visual information has become a significant concern. Traditional cryptographic approaches, such as the Advanced Encryption Standard (AES), have long been valued for their high performance, stability, and wide acceptance in various industry standards. 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 (Lafta, 2005).

However, the rapid development of quantum computing technologies introduces new challenges, as many conventional algorithms face potential vulnerabilities against future quantum-enabled attacks. There are evaluation standards for cryptographic systems that can withstand quantum attacks, referred to as Quantum Secure Cryptography. These standards focus on three main aspects: the level of security, cost and performance, and algorithm implementation (Alagic et al., 2022). One recommended approach for developing quantum-resistant cryptographic systems is lattice-based cryptography.

The foundation of lattice problems was first laid by Ajtai (1997), who introduced the concept of Short Integer Solution (SIS), a method aimed at solving lattice-based computing problems, specifically finding the shortest solution to the system of homogeneous linear equations. Regev (2005) expanded on SIS by incorporating complexity and security considerations, known as Learning With Error (LWE), which introduces small errors into linear equations to enhance security. This evolving landscape raises important questions about how classical and post-quantum algorithms compare when applied specifically to the encryption of digital images, where factors such as processing efficiency, preservation of image quality, and algorithmic resilience must all be carefully evaluated.

In a previous study, Setiawan et al. (2024) explored the application of lattice-based cryptography for digital image encryption using the Learning With Errors (LWE) algorithm. The study primarily focused on implementing the LWE algorithm for encrypting digital images and demonstrated its feasibility as a quantum-resistant cryptographic approach. However, the study did not provide a comprehensive evaluation of the algorithm's performance, nor did it compare LWE with widely used classical encryption methods such as AES. Consequently, the relative advantages and limitations of classical and post-quantum cryptographic approaches for image encryption remain insufficiently understood. Therefore, this study conducts a comparative analysis of AES and LWE by examining their computational efficiency, image quality preservation, and statistical security characteristics.

To investigate these aspects, this study adopts a structured evaluation framework that considers three main dimensions: computational efficiency, image quality preservation, and statistical security. The computational aspect is analyzed by measuring the

encryption and decryption times of each algorithm to identify differences in operational efficiency. Image quality is further examined through the analysis of decrypted images to ensure that the encryption process does not introduce distortions or degrade essential visual information. In addition, a statistical security analysis is carried out to evaluate the robustness of encrypted images and to contrast the established reliability of AES in classical cryptographic environments with the theoretical resilience of LWE against potential quantum-based attacks.

Through this framework, the study provides a systematic comparison between AES and LWE for digital image encryption by examining computational efficiency, image quality preservation, and statistical security. The results offer practical insights into the trade-offs between performance and security when selecting appropriate cryptographic techniques for image protection.

2. METHODS

This study employs an experimental comparative methodology to systematically evaluate the computational performance, output quality and security characteristics of the Advanced Encryption Standard (AES) and the Learning With Errors (LWE) algorithm in the context of digital image encryption. To simplify the computational process, all experiments were performed using grayscale images, as their single-channel pixel matrices require significantly lighter processing than RGB images. This choice also reflects the hardware limitations of the testing environment, which is not sufficiently capable of handling the heavier computational load associated with multi-channel color images.

2.1 Theoritical Background

The foundational theories supporting this research will be presented in the following section, with a particular emphasis on modern cryptographic concepts. The main focus will be on encryption and decryption schemes based on the AES and LWE.

2.1.1 Cryptosystem

According to Stinson (2006), a cryptosystem is formally defined as a 5-tupple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, that satisfied the following condition:

i) $\mathcal{P}$ is a finite set of possible plaintext.

ii) $\mathcal{C}$ is a finite set of possible ciphertext.

iii) $\mathcal{K}$, the key space, is a finite set of possible key.

iv) For each $k \in \mathcal{K}$ there is an encryption scheme $e_k \in \mathcal{E}$ and corresponding decryption scheme $d_k \in \mathcal{D}$. Each $e_k: \mathcal{P} \to \mathcal{C}$ and $d_k: \mathcal{C} \to \mathcal{P}$ are function such that $d_k(e_k) = x$ for every plaintext element $x \in \mathcal{P}$.

2.1.2 The Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric block cipher adopted by Dworkin (2001). A block cipher processes the plaintext of a fixed length, knows as the block size. When the plaintext exceeds this size, it must be separated into multiple blocks. In most cases, the final block requires padding so that its length matches the required block size (Almuhammadi & Alhejri, 2017).

2.1.3 The Cipher Block Chaining (CBC)

Dworkin (2001) explains that the CBC mode is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous ciphertext blocks. The CBC mode requires an initialization vector (IV) to combine with the first plaintext block. The IV need not be secret, but it must be unpredictable. Also, the integrity of the IV should be protected. The CBC mode is defined as follows:

CBC Encryption:

$C1 = CIPH_K(P_1 \oplus IV)$;

$Cj = CIPH_K\left(P_j \oplus C_{\{j-1\}}\right)$ for $j = 2 \ldots n$.

CBC Decryption:

$P_1 = CIPH_K^{-1}(C_1) \oplus IV$;

$P_j = CIPH_K^{-1}\left(C_j\right) \oplus C_{j-1}$ for $j = 2 \ldots n$.

2.1.4 Learning With Error Distribution

Given a vector $\boldsymbol{s} \in \mathbb{Z}_q^n$ called secret. The LWE distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing $\boldsymbol{a} \in \mathbb{Z}_n^q$ uniformly random, choosing error $e \leftarrow \chi$, and outputting $(\boldsymbol{a}, b = \langle \boldsymbol{s}, \boldsymbol{a} \rangle + e \bmod q$ (Peikert, 2016).

2.1.5 Learning With Error Search Problem

Given m independent samples $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ drawn from $A\_\{s, \chi\}$ for a uniformly random $s \in \mathbb{Z}_q^n$, the Search-LWE problem is finding s (Peikert, C., 2016).

2.1.6 Learning With Error Encryption and Decryption Scheme

a. LWE Encryption

The LWE encryption process begins by selecting a private vector $r \in \mathbb{Z}_q^n$. A public matrix $A \in \mathbb{Z}_q^{n \times m}$ is generated, and a public key vector $b = As + e_1$ is computed using a secret vector $s$and a small error term e_1. To encrypt a message x, the algorithm forms two ciphertext components:

$$u = r^T A + e_2,$$

$$v = r^T b + e_3 + x$$

where e_2 and e_3 are additional small error. The ciphertect is the pair (u, v) (Peikert, C., 2016).

b. LWE Decryption

Decryption uses the secret vector s to recover the message. The plaintext is obtained by computing,

$$x = v - (u \cdot s),$$

which removes the LWE-related components and error terms, leaving the original message x. The small noise values ensure security while still allowing correct message recovery (Peikert, C., 2016).

2.2 Evaluation Metrics

The evaluation metrics used in this study are computational performance (time), output quality, and security. The details are as follows.

2.2.1 Computational Performance (time)

a. Encryption Time (in second)
b. Decryption Time (in unit second)

2.2.2 Output Quality (Decrypted Image)

a. Mean Squared Error (MSE)
b. Structural Similarity Index Measure (SSIM)

2.2.3 Security

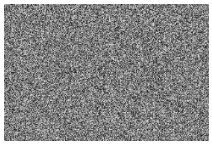
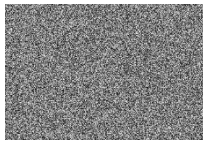
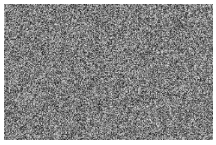
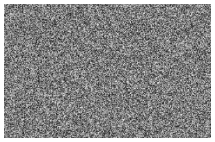
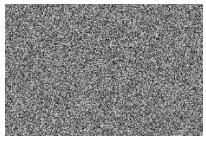
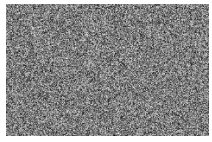
Correlation Coefficient Analysis

3. RESULTS AND DISCUSSIONS

Digital image categorizes into three types based on their color and pixel structure: RGB, grayscale, and binary images. This paper focuses specifically on applying digital image encryption techniques to grayscale images. A grayscale image is mathematically represented as a matrix containing gray intensity values that range from 0 (white) to 255 (black). Picture 1 is the plain image or Original Image which later converted into a matrix whose entries are the pixels of the image. Table 1 presents the encryption and decryption results obtained using AES and LWE, with each experiment performed three times.

Picture 1. Plain Image

Table 1. Encryption and Decryption Output of AES and LWE

Schemes	Trial 1	Trial 2	Trial 3
AES Encryption Output			
AES Decryption Output			
LWE Encryption Output			
LWE Decryption Output			

Moreover, all outputs were evaluated. Computational performance was assessed by measuring the estimated execution time of both the AES and LWE algorithms. Image quality evaluation was conducted using Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM) to determine the degree of similarity between the original and decrypted images. Finally, the security evaluation was performed using correlation coefficient measurements to examine the randomness of the encrypted images produced by each algorithm.

3.1 Computational Performance

The computational performance is evaluated based on the execution time (in second) of the encryption and decryption of AES and LWE. Each experiment was repeated three times to observe the trend in the runtime performance.

Tabel 2. The execution time (in second) of AES and LWE

Skema	Trial 1	Trial 2	Trial 3
AES Enkripsi	0,136	0,103	0,192
AES Dekripsi	0,137	0,202	0,208
LWE Enkripsi	83,518	81,682	83,867
LWE Dekripsi	4,173	4,124	4,099

As shown in Table 2, the execution time for AES encryption and decryption ranges from 0.1 to 0.2 seconds. In contrast, LWE requires significantly longer execution time, requiring around 81–83 seconds for the encryption process. This is due to the fact that each pixel in the image generates a pair of cipher pixels. Furthermore, the decryption process in LWE takes approximately 4 seconds.

3.2 Output Quality (Decrypted Image)

The analysis of image quality was performed to assess whether there were any changes in the resolution or structural characteristics of the original image following the decryption process. To evaluate this, Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM) were employed as the assessment methods.

3.2.1 Mean Squared Error (MSE)

Mean Squared Error (MSE) is one of the most widely used quantitative metrics for evaluating the quality of decrypted images in image encryption systems because it measures the average squared difference between the original image and the decrypted result. In the context of encryption and decryption, MSE indicates whether the reconstruction process is lossless, meaning that all visual information is fully restored after the original image has been transformed into an unintelligible encrypted form. MSE computes the average squared discrepancies between corresponding pixels in the original and cipher images. The calculation formula for MSE in this study follows the approach presented by Elmenyawi et al. (2024). A lower MSE values reveal a lower level of distortion, implying that the cipher image closely resembles the original ((Zhang & Hu, 2021). A smaller MSE value reflects a higher level of pixel similarity between the two images, and an MSE approaching zero signifies that no distortion occurred during the decryption phase.

Table 3. MSE Analysis of AES and LWE

Trial	AES	LWE
1	0.0	0.0
2	0.0	0.0
3	0.0	0.0

Table 3 presents the results of the MSE analysis of image quality between AES and LWE decrypted images obtained in this experiment. The results show that in all trials, the comparison between the original image and the decrypted image for both AES and LWE yields an MSE value of zero, indicating that the decrypted images are identical to the original

3.2.2 Structural Similarity Index Measure (SSIM)

The Structural Similarity Index Measure (SSIM) is a perceptual image quality metric used to evaluate the structural fidelity between an original image and its decrypted version. It plays an essential role in image encryption research because it assesses luminance, contrast, and structural similarity, providing a more human-perceptual evaluation compared to purely numerical measures such as MSE. Within the context of decryption, an SSIM value in Table 4 both of AES and LWE is equal to 1, which indicates the spatial patterns of the image, including textures, edges, and local structural relationships, are preserved after the encryption and restoration process.

In addition, numerous image encryption studies show that symmetric algorithms such as AES often yield SSIM values of 1.0 because their decryption process restores the image without altering its structural content (Alexan et al, 2025). Consequently, SSIM is essential not only for evaluating numerical accuracy but also for confirming that the structural characteristics of the image remain intact during encryption and decryption.

Tabel 4. SSIM Analysis of AES and LWE

Trial	AES	LWE
1	1.0	1.0
2	1.0	1.0
3	1.0	1.0

3.3 Security

To evaluate the security of the image encryption process, a correlation coefficient analysis will be conducted on the AES and LWE cipher images. Both analyses aim to verify that the pixels of the image have been encrypted in uniformly random.

3.3.1 Correlation Analysis

A correlation coefficient analysis aim to verify that the pixels of the image have been encrypted in uniformly random. Pixel-correlation analysis evaluates how much statistical

dependence remains between adjacent pixels in a cipher-image. In natural images, neighboring pixels typically have very high correlation (0.95–0.99), reflecting spatial continuity. A secure encryption system must drastically reduce this correlation so that adjacent pixels in the cipher-image appear statistically independent (Bashir Abugharsa et al., 2012)

Table 5. Scatter Plot AES

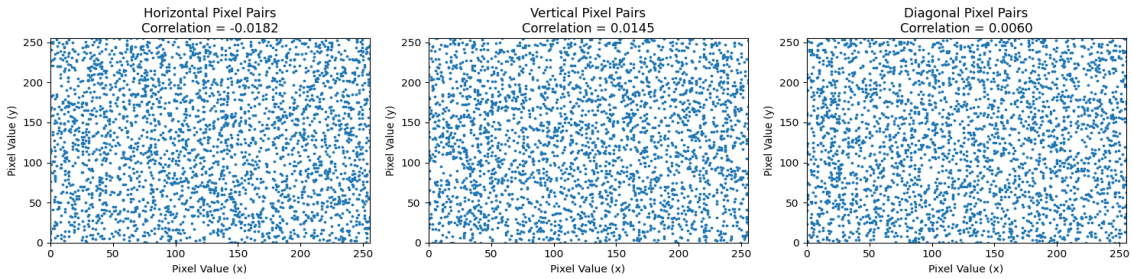
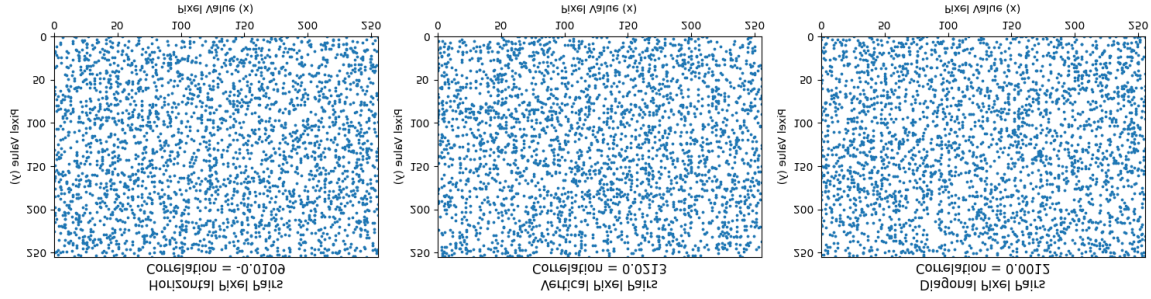
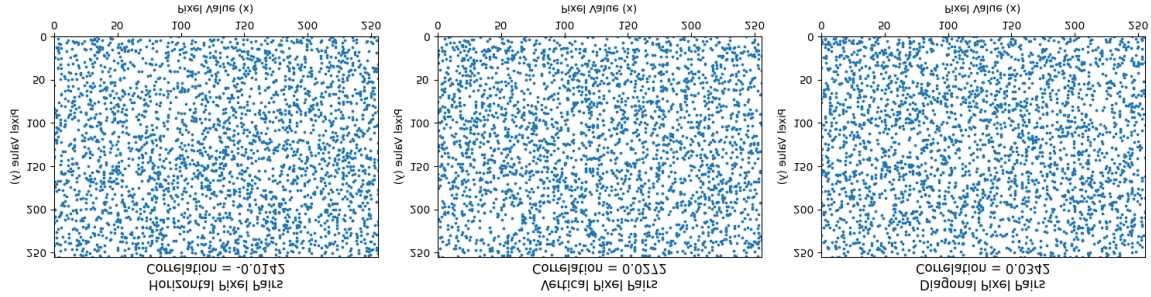
Scatter Plot AES
Trial 1

Trial 2

Trial 3


Table 6. Scatter Plot LWE

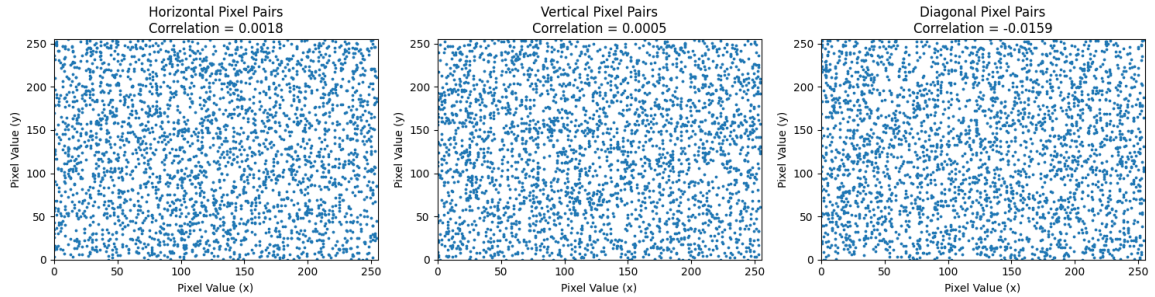
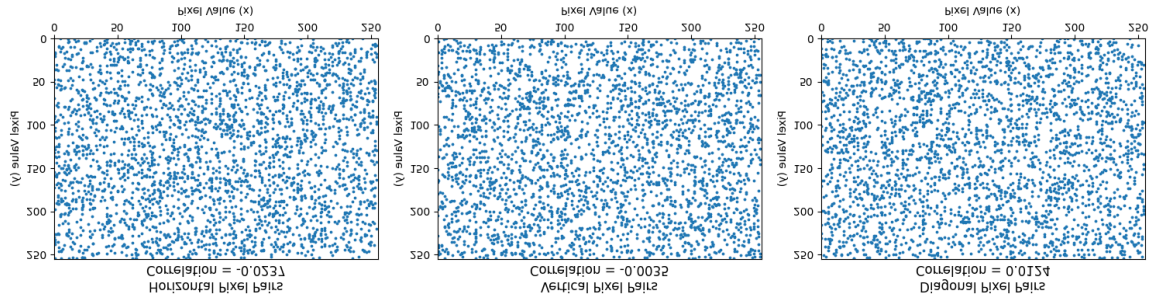
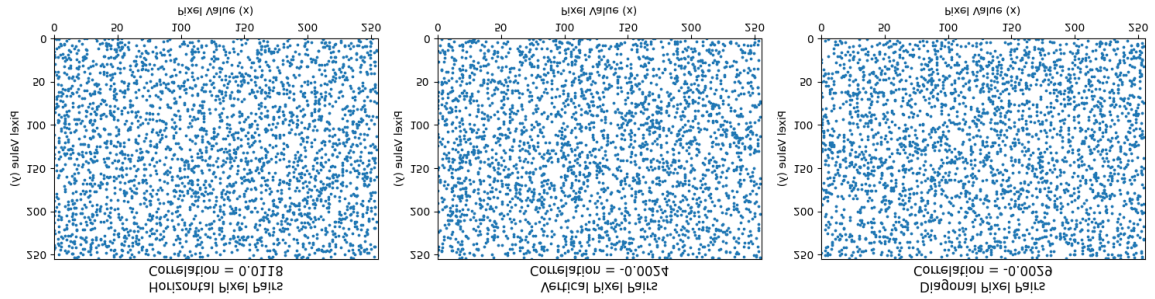
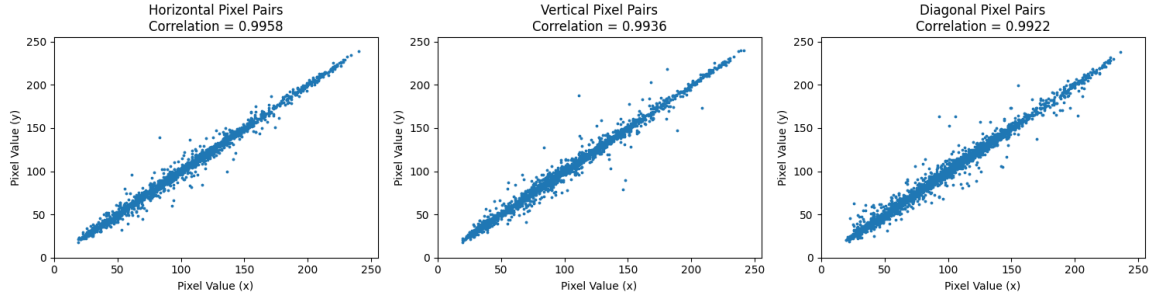
Scatter Plot LWE
Trial 1

Trial 2

Trial 3

Scatter Original Image


Table 7. Correlation Coefficients of Adjacent Pixels for Plain-Image, AES, and LWE

Method	Direction	Correlation Value
Plain Image	Horizontal	0.9958
	Vertical	0.9936
	Diagonal	0.9922
AES	Horizontal	–0.0182
	Vertical	0.0145
	Diagonal	0.0060
LWE	Horizontal	0.0018
	Vertical	0.0005
	Diagonal	–0.0159

Table 5, Table 6, and Table 7 show all values fall well within the secure threshold ($|r| < 0.03$), indicating that both algorithms successfully eliminate spatial dependencies from the plaintext. However, LWE consistently achieves lower correlation values than AES for all three directions. The correlations for LWE are extremely close to zero 0.0018 and 0.0005 for horizontal and vertical directions, respectively and slightly negative for diagonal pairs.

These results demonstrate that LWE exhibits stronger pixel decorrelation than AES. This suggests that LWE provides a more effective dispersion of error or noise throughout the cipher-image, a property supported by prior research showing that lattice-based encryption has strong noise propagation due to the injected Gaussian error term by (Lepoint & Naehrig, 2014). This enhanced decorrelation makes statistical attacks based on pixel adjacency significantly more difficult.

4. CONCLUSION

This study presents a comparative analysis of the Advanced Encryption Standard (AES) and the Learning With Errors (LWE) algorithms in the context of digital image encryption. Based on the experimental results, AES demonstrates superior computational performance, offering significantly faster encryption and decryption times while maintaining high output image quality after decryption. On the other hand, LWE delivers more uniformly random for security level, particularly in providing resistance to quantum-based attacks, although it requires longer processing time.

From a practical perspective, these findings indicate that AES remains more suitable for applications requiring real-time processing and computational efficiency, such as multimedia transmission and cloud-based image storage. Meanwhile, LWE-based encryption may be more appropriate for scenarios where long-term security against future quantum threats is a primary concern.

However, this study has several limitations. The evaluation focuses mainly on computational performance, image quality, and basic statistical characteristics, while other factors such as scalability, memory usage, and resistance to advanced cryptanalytic attacks were not extensively examined. Future research may explore optimized

implementations and broader evaluation metrics to provide a more comprehensive assessment of LWE-based image encryption.

5. RECOMMENDATION

Future work may explore possible approaches to improve the computational efficiency of LWE-based encryption, particularly through algorithmic optimization or hardware-supported implementations. Further investigations could also consider evaluating the method using a wider range of image datasets and additional performance indicators, such as memory usage, scalability, and resistance to more advanced cryptanalytic attacks. These efforts would help provide a more comprehensive understanding of the practical potential of post-quantum cryptographic techniques for digital image encryption

6. REFERENSI

Alagic, G., et al. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413-upd1

Ajtai, M. (1996). Generating hard instances of lattice problems. *Quaderni di Matematica, 13*, 1–32. https://doi.org/10.1145/237814.237838

Alexan, W., El Shabasy, N. H., Ehab, N., Maher, E. A., & Gabr, M. (2025). A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations. *Scientific Reports, 15*, 31246. https://doi.org/10.1038/s41598-025-15794-z

Almuhammadi, S., & Alhejri, I. (2017). A comparative analysis of AES common modes of operation. In *Proceedings of the IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*. https://doi.org/10.1109/CCECE.2017.7946655

Bashir Abugharsa, A., et al. (2012). A new image encryption approach using the integration of a shifting technique and the AES algorithm. *International Journal of Computer Applications, 42*, 36–45. https://doi.org/10.5120/5723-7785

Dworkin, M. (2001). Recommendation for block cipher modes of operation (NIST Special Publication 800-38A). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-38A

Elmenyawi, M. A., Abdel Aziem, N. M., & Bahaa-Eldin, A. M. (2024). Efficient and secure color image encryption system with enhanced speed and robustness based on binary tree. *Egyptian Informatics Journal, 27*, 100487. https://doi.org/10.1016/j.eij.2024.100487

Hua, Z., & Zhou, Y. (2016). Image encryption using 2D logistic map. *Information Sciences*. https://doi.org/10.1016/j.ins.2016.01.017

Lafta, Z. A. (2005). Image encryption systems based on the advanced encryption standard. *International Journal of Future Engineering Innovations, 2*, 1–6.

Lepoint, T., & Naehrig, M. (2014). A comparison of the LWE-based homomorphic encryption schemes. *Cryptology ePrint Archive*. https://eprint.iacr.org/2014/062

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*. https://doi.org/10.1561/0400000074

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM, 56*(6), 1–40. https://doi.org/10.1145/1568318.1568324

Setiawan, A. N., et al. (2024). Learning with error for digital image encryption. *Journal of Fundamental Mathematics and Applications,* 7(2), 149–162. https://doi.org/10.14710/jfma.v7i2.21073

Stinson, D. R. (2006). *Cryptography: Theory and practice* (3rd ed.). CRC Press.

Zhang, X., & Hu, Y. (2021). Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding. *Optics & Laser Technology, 141*, 107073. https://doi.org/10.1016/j.optlastec.2021.107073