An Analysis of Image Encryption Standards: A Brief Performance Comparison of DES vs AES

[1] V.Senthil Balaji, [2.] Dr.R.Priya, [3.]Dr.V.Punitha

[1.]Research Scholar Department of Computer Science Engineering FEAT Annamalai University Chidambaram, Tamilnadu, India. senthilvvrvv@gmail.com
[2.] Professor Department of Computer Science Engineering FEAT Annamalai University Chidambaram, Tamilnadu, India. pryknd n@yahoo.com
[3]Professor and Head Department of Computer Science Engineering Saranathan college of Engineering, Tiruchirapalli, India. cse.hod@saranathan.ac.in

Abstract
The rapid progression of the Internet and communication technologies that have been extensively utilized in images is inevitable. The specific features of the images, like correlation between pixels, high transmission speed with constraint bandwidth, redundancy, and bulk capacity make traditional algorithms unfit for image encryption. Pre-encryption of data is needed for protection as cybercrime has reached the highest level. The information is continuously monitored, which makes encryption paramount from personal information traded on the dark web to application vulnerabilities. With the increasing use of digital images in communication and multimedia systems, efficient image encryption has become essential. This paper presents a brief comparison of the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) for image encryption applications. DES, based on a 56-bit key and Feistel structure, offers low computational complexity but suffers from weak security and vulnerability to statistical and brute-force attacks. AES, using larger key sizes and a substitution–permutation network, provides stronger resistance to cryptanalysis. Reported studies show that AES achieves efficient entropy, encryption and decryption, MSE, PSNR and NPCR. This work confirms AES as a more suitable standard for modern image encryption.

Keywords: Image Encryption; Advanced Encryption Standard; Data Encryption Standard; Digital Image; Secret Key; Private Key

1. Introduction

The rapid expansion of digital imaging technologies and the extensive exchange of images over open and untrusted networks have made image security a critical research concern. Sensitive image data used in applications such as medical diagnostics, military communication, biometric authentication and multimedia cloud services must be protected against unauthorized access, tampering and information leakage. Encryption remains one of the most effective techniques for ensuring confidentiality and integrity during image transmission and storage.

Symmetric-key cryptographic algorithms standardized by the National Institute of Standards and Technology (NIST), particularly the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), have been widely adopted for securing digital data. DES operates on 64-bit data blocks using a 56-bit key and was historically a benchmark in cryptographic security. However, advances in computational power have rendered DES vulnerable to brute-force attacks, significantly limiting its applicability in modern security systems. AES, introduced as DES's successor, employs a 128-bit block size and supports key lengths of 128, 192, and 256 bits, offering enhanced security and improved computational efficiency.

2. Literature Survey

The security of digital images has attracted significant research attention due to the increasing use of images in sensitive applications such as medical diagnostics, surveillance systems, biometric authentication, and cloud-based multimedia services. Unlike textual data, images exhibit high redundancy and strong spatial correlation among pixels, which makes conventional encryption techniques less straightforward when applied directly. As a result, a wide range of image encryption approaches have been proposed in the literature.

A substantial body of work focuses on chaos-based image encryption techniques due to their pseudo-random behaviour and sensitivity to initial conditions. Hybrid chaotic encryption schemes employing optimized substitution boxes and complex chaotic maps were proposed in [1] and [5], demonstrating strong resistance against statistical and differential attacks. Advanced methods combining pixel-level diffusion, DNA encoding, and multidimensional chaotic systems have also been explored to enhance security [3], [9]. Partial image encryption using chaotic systems and transform-domain techniques was investigated in [10]. Comprehensive surveys in [4] and [20] summarized these chaos-based and hybrid techniques, while highlighting challenges such as increased computational complexity and implementation difficulty.

In parallel, conventional cryptographic algorithms have been studied for image encryption. Public-key approaches such as modified ElGamal encryption were examined in [6], and elliptic-curve-based hybrid techniques were proposed in [8]. Hardware-oriented implementations of the Data Encryption Standard (DES) were discussed in

[18], emphasizing performance optimization using FPGA architectures. However, due to its limited 56-bit key size, DES is widely regarded as insecure for modern applications and is primarily used for legacy systems or comparative benchmarking.

The Advanced Encryption Standard (AES) has emerged as the dominant symmetric-key algorithm for image encryption. Studies in [2] and [15] demonstrated that AES provides strong security with acceptable computational performance for image data. AES-based encryption has also been applied in constrained environments such as the Internet of Things [19]. Several researchers combined AES with chaotic systems to further improve security and diffusion properties [7], [13], [14]. Comparative analyses involving AES and other encryption algorithms consistently identified AES as a balanced solution in terms of security strength and efficiency [11], [12], [16]. A direct comparison of DES and AES in networking and security contexts was presented in [17], confirming the superiority of AES for modern encryption requirements.

Although extensive research exists on advanced and hybrid image encryption schemes, relatively few studies focus on a concise performance comparison of DES and AES specifically for image encryption. This gap motivates the present work, which evaluates DES and AES using standard performance and statistical metrics to assess their suitability for secure image encryption applications.

3. Prposed Work

The proposed work aims to perform a systematic and objective performance analysis of two symmetric-key encryption standards, namely the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), when applied to digital image encryption. Although DES and AES were originally designed for textual data, this study evaluates their effectiveness and suitability for securing image data, which exhibits high redundancy and strong pixel correlation.

In this work, colour images of fixed dimensions are used as test inputs. Each image is encrypted separately using DES and AES under identical experimental conditions to ensure a fair comparison. AES encryption is implemented with a 128-bit key size, while DES uses its standard 56-bit key. Both algorithms operate in the same block cipher mode to eliminate mode-dependent performance variations.

The outcomes of this proposed work are expected to highlight the relative strengths and limitations of DES and AES in image encryption scenarios. The analysis aims to demonstrate the superior security and performance characteristics of AES while positioning DES as a baseline reference. The results provide practical insights into the selection of appropriate encryption standards for secure image transmission.

3.1. Design of DES Model

The Data Encryption Standard (DES) is a symmetric block cipher that operates on 64-bit data blocks using a 56-bit secret key. In the proposed design model for image encryption, the input digital image is first converted into a binary stream and divided into fixed-size blocks suitable for DES processing. Each block undergoes an initial permutation, followed by 16 rounds of Feistel-based encryption, and a final inverse permutation to produce the encrypted image data.

Each DES round consists of expansion, key mixing, substitution using S-boxes, and permutation operations. The round keys are generated through a key scheduling process involving permutation and left circular shifts. This structure provides basic confusion and diffusion, which are essential for obscuring pixel relationships in image data . After encryption, the cipher blocks are recombined and reshaped to form the encrypted image.

Although the DES model offers simplicity and ease of implementation, particularly in software and FPGA-based systems, its limited key size and weaker resistance to cryptanalytic attacks reduce its effectiveness for modern image security applications. As highlighted in recent studies, DES is mainly used today as a baseline or comparative model rather than a standalone secure solution, especially when compared with AES-based and hybrid encryption approaches.

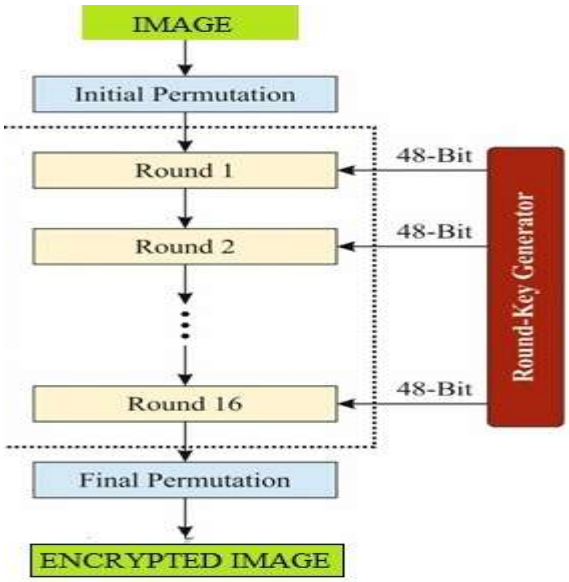

Fig. 1. Structure of DES

The block diagram of the DES-based image encryption model consists of a sequence of functional modules that collectively transform a plain image into its encrypted form. Initially, the input image is acquired and converted into a grayscale or RGB matrix, which is then reshaped into a one-dimensional binary data stream. This binary stream is segmented into 64-bit blocks to match the DES block size requirement.

Each 64-bit block is passed through an **Initial Permutation (IP)** unit, which rearranges the bit positions to enhance diffusion. The permuted data is then divided into two 32-bit halves and processed through **16 Feistel rounds**. In each round, the right half undergoes expansion, XOR operation with a round key generated by the **Key Scheduling Module**, substitution using fixed **S-boxes**, and permutation before being combined with the left half.

After completing all rounds, the output halves are swapped and fed into the **Final Permutation (FP)** module, producing encrypted 64-bit cipher blocks. These blocks are concatenated and reshaped to reconstruct the encrypted image. The same structure, with reversed round keys, is used for decryption, ensuring correct image recovery.

3.2. Design of AES Model

The AES is similar to the Rijndael algorithm [19]. The only dissimilarity is that the key and packet lengths are varied. The Rijndael algorithm has a variable key and packet lengths fixed to 32 bits, ranging between 16 to 32 bytes. The AES sets the key length to 16, 24, and 32 bytes and the packet length to 16 bytes. AES has easy software and hardware implementation, high speed, and high security.

The SubBytes, ShiftRows, MixColumns, and AddRoundKey are the four different stages of the AES architecture algorithm. Each work on the entire 16-byte plaintext packet is rotated right by 16 bits, and the 4th line is rotated as state of the algorithm. An algorithm state involves right by 8 bits. The effects of 128 bits, which is generally illustrated as a matrix of 4 row shift transform improves the diffusion rate of the rows and four columns.

A. Byte substitution

This is a nonlinear operation and also plays a significant role in ensuring security. AES exploits 16 similar S-boxes, each containing 8-bit input, 8-bit output, and the S-box work simultaneously. All the bytes are replaced non-linearly with new byte using byte substitution. The S box generation can be implemented in two different stages:

- Transform a byte to its multiplicative inverse in GF (2^8). Note that the multiplication of AES 0 element is mapped inversely to itself, however, the multiplication inverse of 0 element doesn't exist.
- The linear conversion can be done on the results of the initial stage and is represented by $b = f(a)$, viz, all the bytes are initially multiplied by the constant matrix, and then add 1-byte hexadecimal value {63}.

$$\begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} a_7 \\ a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad (1)$$

B. Line shift

The line shift is a process of periodically shifting all the rows based on the displacement amount. The 1st line should remain unchanged, the 2nd line can be rotated right by 24 bits, the 3rd line can be rotated right by 16 bits, and the 4th line can be rotated right by 16 bits. The effects of line shift transform increase the diffusion rate of the algorithm, ensuring AES security.

C. Column mixing

A column mixing is used to separately perform a blending transformation on all the columns as a polynomial with the coefficient on $GF(2^8)$, multiplied by the modular polynomial$(x^4 + 1)$, and a fixed polynomial$c(x)$,

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \quad (2)$$

Where the coefficients {01}, {02}, and {03} are hexadecimal values representing elements of {GF^8).Next, all the bytes are mapped to additional values and 32 bits of the column.

Each column of the AES state matrix is treated as a polynomial of degree three and multiplied modulo x^4+1 with the fixed polynomial c(x). This operation ensures strong diffusion by mixing the bytes within each column, such that a change in one input byte affects all four output bytes.

The multiplication by {02} and {03} is performed using finite-field arithmetic. Specifically, multiplication by {02} corresponds to a left bit shift followed by conditional reduction using the AES irreducible polynomial $x^8+x^4+x^3+x+1$ while multiplication by {03} is equivalent to multiplying by {02} and then adding the original byte.

The Mix Columns transformation significantly enhances the diffusion property of AES, contributing to its resistance against linear and differential cryptanalysis. Notably, this operation is omitted in the final encryption round to maintain inevitability during decryption

D. Round key addition

This is an XOR operation of a 128-bit and a 128-bit subkey. The subkey can be attained using the key expansion through the first key.

E. Key expansion algorithm

This represents how to produce sub-key of all the rounds through the first key. Note that the subkeys are not equivalent to the rounds, however, it is essential to add 1 to all the rounds. The preliminary key is 16 bytes, 24

bytes, and 32 bytes, and their rounds are 10, 12, and 14 correspondingly. Similar to the three AES key lengths, the key expansion algorithm has specific similarities.

The subkey is recursively evaluated in the AES algorithms, viz., if the subkey w_i is to be produced, the pre-condition is that the subkey w_{i-1} is needed. Furthermore, the fundamental element is a 4-byte word. The input is taken as 4 words, and 1D array of 44 words is taken as an output.

Firstly, the initial key is utilized as the 32-bit words of the key expanded array. Then, add the new 32-bit key words to the other portions of the key expanded array. The new key words w_i generation relies on w_{i-1} and w_{i-4}. Fig. 2 illustrates the architecture of AES.

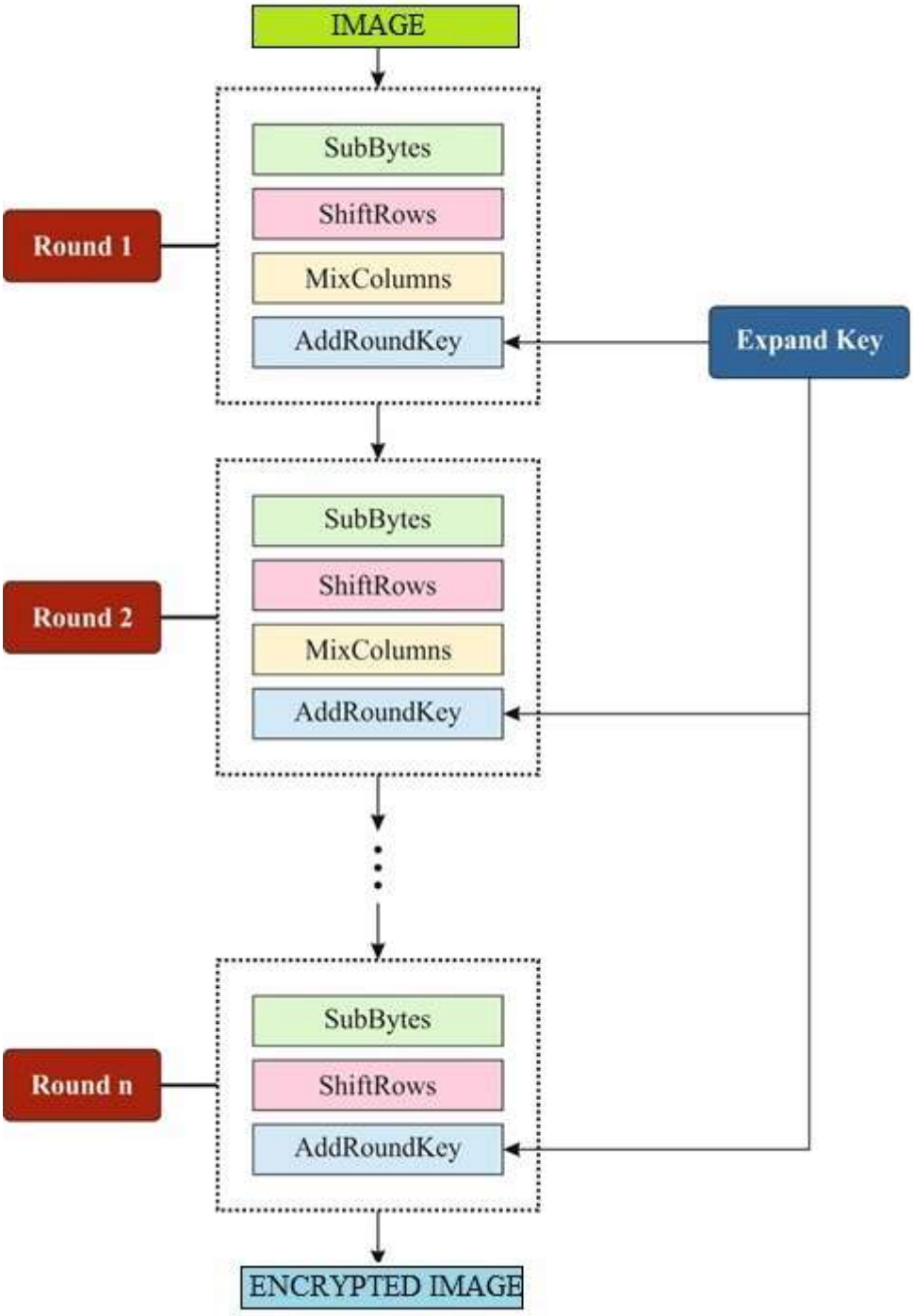

Fig. 2. Architecture of AES

Simultaneously, it makes use of function g to evaluate the key words whose array index is a multiple of 4.

- When i mod $4 \neq 0$, $w_i = w_{i-4} \oplus w_{i-1}$;
- When i mod $4 = 0$, $w_i = w_{i-4} \oplus g(w_{i-1})$;

The function $g()$ is a nonlinear function of 32-bit inputs and outputs. In the $g()$ function, the 4 input bytes are first rotated left by 8 bits; next, the 4 S-boxes carry out byte substitution on the shifted 32 bits; lastly, they are replaced. The round constant is a 32-bit word, and the others are 0 except that the leftmost bytes are not 0. Note

that the round constant of all the rounds is not the same, described as $con[j] = (Rc[j],0,0,0)$, where $Rc[1] = 1$, $Rc[j] = Rc[j-1] * 2\ (GF(2^8))$.

4. Result Analysis and Discussion

This section inspects the performance analysis of the DES and AES models. Fig. 3 demonstrates the sample of original, histogram, encrypted, and decrypted images.

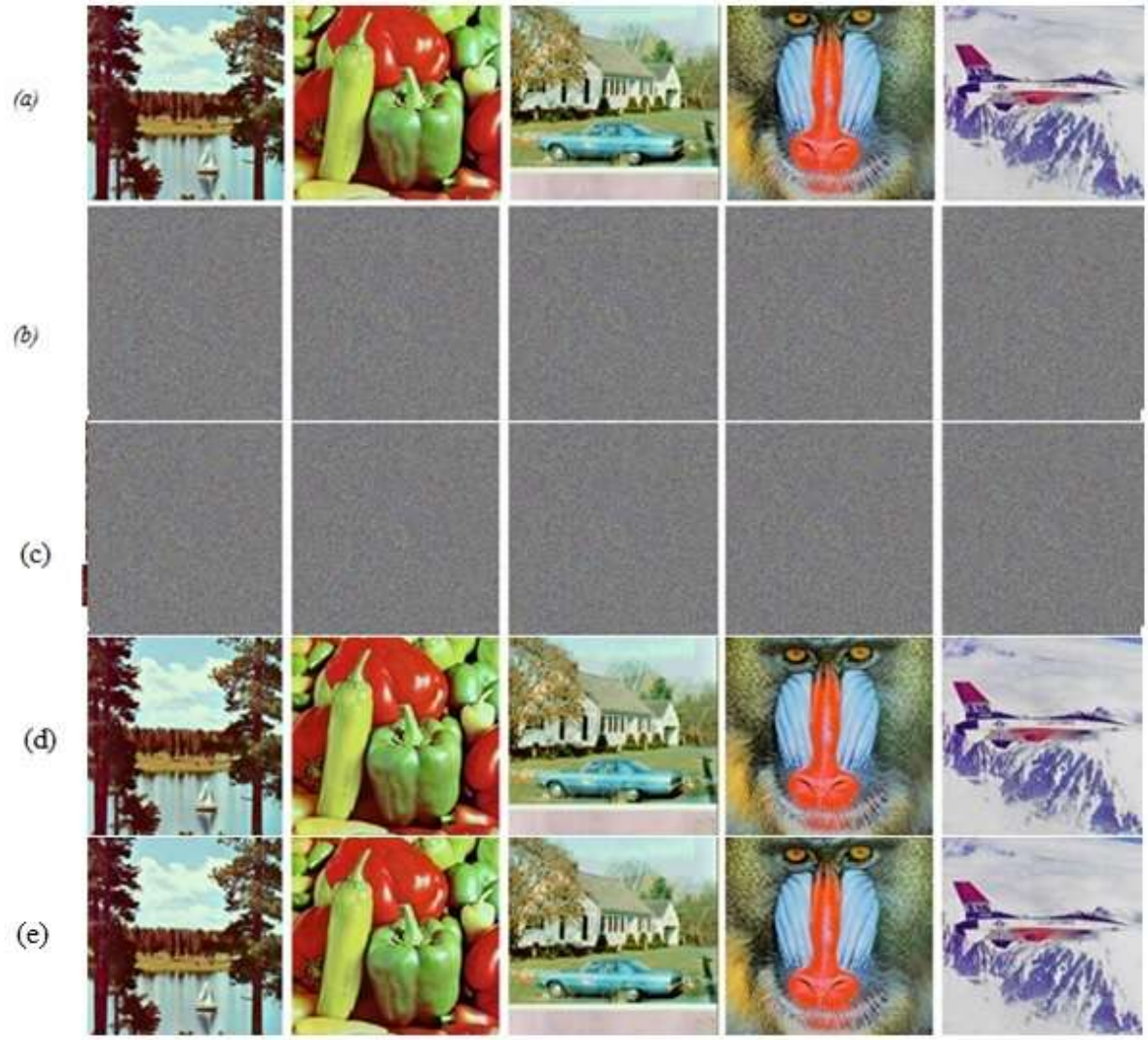

Fig. 3. a) Original Images b) DES Encrypted Images c) AES Encrypted Images (d) AES Decrypted Image (e) DES Decrypted Image

Table 1 inspects detailed encryption time (ECRT) and decryption time (DCRT) results of the AES, DES. The results indicate that the AES model attains reduced ECRT value of 2.49o. On Img-1 (Lake).

Table 1 ECRT and DCRT analysis of encryption models under different images

Test Images	**Encryption Time (sec)**		**Decryption Time (sec)**	
	AES	**DES**	**AES**	**DES**
LAKE	2.49	5.51	1.72	2.86
VEGETABLES	4.15	6.77	2.64	5.4
CAR	4.26	5.89	3.63	5.13
BABOON	4.4	8.18	2.01	4.78
FLIGHT	5.27	9.13	1.62	3.28

Table 2 reports a brief entropy (ENT) and MSE results of the different encryption approaches. The table stated the AES model accomplishes reasonable performance with higher ENT of 7.96 and the AES technique accomplishes minimum MSE of 0.491.

Table 2 Entrospy and MSE analysis of encryption models under different images

Test Images	Entropy		MSE	
	AES	DES	AES	DES
LAKE	7.96	6.8	0.4	2.74
VEGETABLES	7.98	5.89	0.48	4.9
CAR	7.91	5.79	0.39	3.84
BABOON	7.97	6.7	0.455	2.86
FLIGHT	7.95	6.84	0.491	1.81

Table 3 reports a brief PSNR and NPCR results of the different encryption approaches. The table stated that, the AES technique obtains considerable performance with maximum PSNR of 52.110dB.

Table 3 PSNR and NPCR analysis of encryption models under different images

Test Images	PSNR (dB)		NPCR (%)	
	AES	DES	AES	DES
LAKE	52.11	49.438	99.15	90.09
VEGETABLES	51.318	48.588	99.18	90.98
CAR	52.22	48.888	99.03	90.95
BABOON	51.551	48.786	98.6	90.96
FLIGHT	51.22	49.046	98.65	90.95

In table 3, the comparative NPCR outcomes of different encryption approaches are given. the AES algorithm achieves reasonable performance with maximum NPCR of 99.15% . These results ensured that the AES model outperforms the other encryption standards.

5. Conclusion

This paper presented a brief performance comparison of the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) for image encryption applications. The analysis indicates that although DES offers low computational complexity and ease of implementation, its limited key size and weak resistance to cryptanalytic and statistical attacks make it unsuitable for modern image security requirements. Encrypted images produced using DES may retain detectable statistical patterns, increasing vulnerability to attacks.

Future work will focus on enhancing AES-based image encryption through hybrid approaches, chaotic systems, and hardware-accelerated implementations to further improve security and efficiency.

References

[1] Farah, M.B.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn. 2019, 99, 1–24.

[2] Nahta, R.; Jain, T.; Narwaria, A.; Kumar, H.; Gupta, R.K. Image Encryption Decryption Using Simple and Modified Version of AES. In Smart Systems and IoT: Innovations in Computing; Springer: Singapore, 2020; pp. 641–653.

[3] Li, T.; Shi, J.; Li, X.; Wu, J.; Pan, F. Image encryption based on pixel-level diffusion with dynamic filtering and DNA-level permutation with 3D Latin cubes. Entropy 2019, 21, 319.

[4] Kaur, M.; Kumar, V. A comprehensive review on image encryption techniques. Arch. Comput. Methods Eng. 2020, 27, 15–43.

[5] Jin, X.; Duan, X.; Jin, H.; Ma, Y. A Novel Hybrid Secure Image Encryption Based on the Shuffle Algorithm and the Hidden Attractor Chaos System. Entropy 2020, 22, 640.

[6] Hashim, H.R.; Neamaa, I.A. Image encryption and decryption in a modification of ElGamal cryptosystem in MATLAB. arXiv 2014, arXiv:1412.8490.

[7] Arab, A.; Rostami, M.J.; Ghavami, B. An image encryption method based on chaos system and AES algorithm. J. Supercomput. 2019, 75, 6663–6682.

[8] Dawahdeh, Z.E.; Yaakob, S.N.; Bin Othman, R.R. A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. J. King Saud Univ. Comput. Inf. Sci. 2018, 30, 349–355.

[9] Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. Inf. Sci. 2019, 480, 403–419.

[10] Belazi, A.; Abd El-Latif, A.A.; Diaconu, A.V.; Rhouma, R.; Belghith, S. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt. Lasers Eng. 2017, 88, 37–50.

[11] Varshney, A., Routh, P. and Sujatha, G., 2024, February. Comparison of Image Encryption Techniques Using Chaotic Maps and Conventional Cryptographic Techniques. In *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)* (pp. 1-7). IEEE.

[12] Yeow, S.Q. and Ng, K.W., 2023. Neural Network Based Data Encryption: A Comparison Study among DES, AES, and HE Techniques. *JOIV: International Journal on Informatics Visualization*, *7*(3-2), pp.2086-2094.
[13] Sun, F. and Lv, Z., 2022. A secure image encryption based on spatial surface chaotic system and AES algorithm. *Multimedia Tools and Applications*, pp.1-21.
[14] Sun, J.Y., Cai, H. and Zhang, H., 2024. A novel image encryption algorithm combined complex order chaotic system and modified aes. *Multimedia Tools and Applications*, *83*(14), pp.40361-40376.
[15] Inam, S., Kanwal, S., Firdous, R., Zakria, K. and Hajjej, F., 2023. A new method of image encryption using advanced encryption Standard (AES) for network security. *Physica Scripta*, *98*(12), p.126005.
[16] Muhammed, R.K., Aziz, R.R., Hassan, A.A., Aladdin, A.M., Saydah, S.J., Rashid, T.A. and Hassan, B.A., 2024. Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption. *Kurdistan Journal of Applied Research*, *9*(1), pp.52-65.
[17] Balodi, A., Malik, P., Rawat, P., Das, P., Singh, K. and Manjul, M., 2023, November. Enhancing Data Security in Networking Through AES Encryption and Steganography: A Comparative Analysis of DES and AES Algorithms. In *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)* (pp. 927-932). IEEE.
[18] Oukili, S. and Bri, S., 2015, December. FPGA implementation of Data Encryption Standard using time variable permutations. In *2015 27th International Conference on Microelectronics (ICM)* (pp. 126-129). IEEE.
[19] Su, N., Zhang, Y. and Li, M., 2019, March. Research on data encryption standard based on AES algorithm in internet of things environment. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (pp. 2071-2075). IEEE.
[20] Chowdhary, C.L., Patel, P.V., Kathrotia, K.J., Attique, M., Perumal, K. and Ijaz, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, *20*(18), p.5162.