International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2025.6.5

Volume 11, Issue 6
June - 2025

Subject Review: Comparison of Data Encryption Algorithms

Wedad Abdul Khuder Naser[1], Amal Abbas Kadhim[2], and Safana Hyder Abbas[3]

[1,2] Assistant Professor, and [3]Professor

Department of computer science

University Al Mustansiriyah

Baghdad, Iraq

ABSTRACT

Data encryption protects data by converting it into an unreadable format, ensuring confidentiality, integrity, and security during transmission and storage. There are several encryption algorithms, each with its own distinct characteristics, strengths, and weaknesses. This study compares the most widely used encryption algorithms: AES, DES, RSA, and ECC, analyzing their strengths, weaknesses, and ideal use cases.

Keywords: Cryptography, Data Security, Data security, Encryption, Encryption Algorithms.

1. INTRODUCTION

Encryption is essential processes in securing data in today's digital world. Encryption refers to the conversion of data into a coded format, making it unreadable to unauthorized users. This ensures that sensitive information, such as financial transactions, personal details, and confidential communications, is protected from potential threats. The encryption process uses algorithms and keys to transform plain text into cipher text. The use of encryption enhances data security, privacy, and integrity . Various encryption methods, such as symmetric key encryption, where the same key is used for both encryption and decryption, and asymmetric key encryption, which uses a pair of public and private keys, are employed depending on the use case and security requirements. Symmetric encryption is faster and is often used for large volumes of data, while asymmetric encryption is more secure and typically used in activities like digital signatures and secures communications. in this paper has proposed various encryption techniques, including traditional cryptographic techniques and modern chaotic-based approaches, and compares between them, analyzing their strengths, weaknesses, and ideal use cases. For instance, traditional algorithms like AES and RSA are highly secure but may not be suitable for real-time image encryption due to their slower speeds. On the other hand, specialized algorithms designed for image encryption often address these challenges by optimizing for the unique characteristics of image data, such as redundancy and pixel correlation [1].

2. COMMON DATA ENCRYPTION ALGORITHMS

Traditional cryptographic algorithms play a crucial role in data encryption, ensuring confidentiality and security during transmission and storage. Some common encryption techniques include:

2-1- AES (Advanced Encryption Standard):

It is a widely used encryption algorithm that ensures data security by encrypting information with a symmetric key. It was established by the U.S. National Institute of Standards and Technology (NIST) in 2001, replacing the older DES (Data Encryption Standard). AES is known for its efficiency, security, and speed, making it a go-to choice for encrypting sensitive information across various applications . AES encrypts data using a process called the

Substitution-Permutation Network (SPN), which consists of multiple rounds of transformations. The number of rounds depends on the key size:

- **AES-128** → 10 rounds
- **AES-192** → 12 rounds
- **AES-256** → 14 rounds

Each round involves:

- **SubBytes** – Byte substitution using an S-Box (non-linear transformation).
- **ShiftRows** – Rows of the state matrix are shifted.
- **MixColumns** – Column mixing for diffusion (not in the last round).
- **AddRoundKey** – XOR operation with a round key.

AES operates on fixed-size blocks of data (128 bits). It supports three key sizes—128, 192, and 256 bits—which determine the level of security. It uses a series of mathematical transformations, including substitution (S-box), shifting rows, mixing columns, and key addition, to scramble data effectively [1] .

It is resistant to all known practical attacks, including brute-force and differential cryptanalysis. It has High security with strong cryptanalysis resistance and Suitable for both software and hardware implementations but Block-based encryption can introduce patterns in image encryption and High computational cost for large images [2].

2-2 DES (Data Encryption Standard) : is a symmetric-key encryption algorithm that was widely used for securing sensitive data. Developed in the early 1970s by IBM and later adopted by the U.S. It was widely used for securing electronic data in the past. Developed in the 1970s, DES operates on blocks of data, typically 64 bits in size, and uses a 56-bit key for encryption and decryption. The steps below show the works of it at a high level:

- **Key Generation:** A 56-bit key is used as the foundation for encryption. (Initially, 64 bits are provided, but 8 bits are used for error detection.)
- **Initial Permutation:** The input data block goes through an initial permutation to rearrange its bits.
- **Rounds of Encryption:** DES performs 16 rounds of encryption. Each round involves substitution, permutation, and mixing the data with portions of the key through a process called the Feistel network.
- **Final Permutation:** After completing the rounds, the block undergoes a final permutation, resulting in the encrypted output[3] .

Although DES was a significant milestone in cryptography, it is now considered insecure because modern computing power can break its 56-bit key using brute-force attacks. DES has been largely replaced by more secure algorithms like the Advanced Encryption Standard (AES) and Triple DES (3DES), an extended variant of DES [4].

2-3 Triple DES (3DES) : is an encryption algorithm that strengthens the original Data Encryption Standard (DES) by applying encryption three times to each data block. It's designed to provide improved security over traditional DES, which became vulnerable to modern attacks. The steps below show the works of it:

- **First Encryption** – The data is encrypted with the first key.
- **Decryption** – The output is decrypted with the second key (not the same as reversing the process, since it's done with a different key).
- **Final Encryption** – The data is encrypted again with the third key.

The triple DES is More secure than standard DES due to multiple encryption layers and Widely used in financial and security applications but it Slower than modern encryption methods like AES (Advanced Encryption Standard) and Vulnerable to brute-force attacks as computational power increases [5] .

Though 3DES was widely used, it has largely been replaced by AES, which is faster and more secure. In fact, organizations are phasing out 3DES due to security concerns [6] .

2-4 Blowfish : is a symmetric key block cipher designed by Bruce Schneier in 1993. It's known for being fast, secure, and highly flexible , making it popular for protecting data in various applications. It used 64-bit blocks and key length can range from 32 bits to 448 bits . making it highly adaptable . It uses a Feistel network, which allows easy

DOI: 10.31695/IJASRE.2025.6.5

encryption and decryption and Typically 16 rounds of processing for enhanced security. The steps below show the works of it:

- **Key Expansion:** The algorithm generates subkeys from the provided key, filling up the P-array and S-boxes, which are crucial for encryption.
- **Feistel Function:** Blowfish uses a nonlinear function that involves substitution boxes (S-boxes) to process plaintext.
- **Encryption:** The algorithm splits plaintext into two halves and applies several rounds of transformations, ensuring data security [7].

It extremely fast on large processors and suitable for applications requiring high-speed encryption but it less ideal for modern applications compared to AES because it uses fixed 64-bit block size and also Vulnerable to certain cryptographic attacks if used improperly [8].

2-5 - RC4 (Rivest Cipher 4) : is a stream cipher widely used for encryption due to its simplicity and speed. It was designed by Ron Rivest in 1987 and became one of the most commonly used encryption algorithms in applications such as wireless security (WEP and WPA) and SSL/TLS.

RC4 operates as a stream cipher, meaning it encrypts data one byte at a time using a continuously generated keystream . the steps below show the works of it :

a. - RC4 starts with a secret key, which is used to initialize a 256-byte array (S-box).
- The array is scrambled using the key to create the initial permutation.

b. - RC4 generates a keystream by continuously modifying the S-box using pointer indices.
- It selects a byte from the S-box and XORs it with each byte of the plaintext, producing ciphertext.

c. - Since RC4 is symmetric, the same keystream can be XORed with the ciphertext to retrieve the original plaintext[8].

The RC4 is Simple and fast , Requires minimal computational resources and Can encrypt data streams efficiently but it is no longer considered secure due to biases in its output and It has weaknesses like key leakage and predictability, leading to attacks on SSL/TLS implementations [9].

2-6 Chaos-based image encryption: is a cryptographic technique that leverages the principles of chaos theory to secure digital images. It relies on chaotic systems, which exhibit sensitivity to initial conditions, pseudo-randomness, and topological transitivity, making them ideal for encryption purposes [10].

Chaos-based image encryption offers strong security features such as high randomness , sensitivity to initial conditions and fast encryption suited for real-time image applications , but it also faces several challenges:

– Chaotic systems are highly sensitive to initial conditions, meaning even a tiny change in the encryption key can lead to completely different results. While this enhances security, it also makes key management more complex.

– Some chaos-based encryption algorithms require significant computational resources, which can slow down encryption and decryption processes, especially for high-resolution images.

– While chaotic encryption is unpredictable, certain attacks, such as differential and statistical attacks, can still exploit weaknesses in poorly designed chaotic encryption schemes [11].

2-7 Pixel-based Encryption (Permutation-Substitution): is a method used to secure digital images. It involves two main steps:

- **Permutation**: The pixel positions in the image are shuffled based on a predefined algorithm, making it difficult to recognize the original image structure.
- **Substitution**: The pixel values are altered using mathematical operations, such as XOR with a generated keystream, to further obscure the image [12].

This approach enhances security by making it resistant to various attacks, including statistical and brute-force attacks. Researchers have explored different chaotic functions, such as logistic maps, to improve the randomness of the encryption. It high efficiency for image encryption and eserves

DOI: 10.31695/IJASRE.2025.6.5

image structure while making it unreadable but may have weak security if not combined with trong substitution techniques [13].

3. COMPARATIVE ANALYSIS

Each algorithm has its strengths and weaknesses, and the choice depends on factors like security needs, speed, and computational resources

Algorithm	Type	Key Size (bits)	Speed	Security	Use case
AES	Symmetric	128, 192, 256	Fast	Very High	Secure communications, file encryption
DES	Symmetric	56	Moderate	Weak	Legacy systems
3DES	Symmetric	112, 168	Slow	Moderate	Banking, financial transactions
Blowfish	Symmetric	32 - 448	Fast	High	Password hashing, VPNs
RC4	Symmetric	40 - 2048	Very Fast	Weak	Not recommended due to weak security
RSA	Asymmetric	1024 - 4096	Very Slow	Very High	Digital signatures, secure key exchange
Chaos-Based	Nonlinear	Varies	Moderate	High	Suitable for real-time and lightweight applications
Pixel-Based	Scrambling	Varies	Fast	Moderate	Efficient but needs additional security measures

4 CONCLUSION

This survey provides a review of different data encryption techniques due to their importance in data encryption and a comparison between them to know its strengths and weaknesses. Choosing the right image encryption algorithm depends on several factors, including security requirements, computational efficiency , speed , Efficiency and Application-Specific Needs The review concluded the following:

- AES is the best option for high-security applications.
- Blowfish offers a good balance between security and speed.
- Chaos-based encryption is effective for real-time image protection.
- RSA is not suitable for direct image encryption but is valuable for key management.

ACKNOWLEDGMENT

The authors would like to thank the Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad, Iraq for supporting this work.

REFERENCES

1. T. A. Brown and S. Kumar, "A Comparative Analysis of AES, Triple DES, RSA, SHA, and Blowfish Encryption Algorithms," Journal of Computer and Communications, vol. 7, no. 3, pp. 33-40, 2019.

2. James Nechvatal, Elaine Barker , “Report on the Development of the Advanced Encryption Standard (AES)”., Journal of Research of the National Institute of Standards and Technology, Volume 106, Number 3, May–June 2001

3. S. Gautam, S. Singh, and H. Singh, ―”A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH”,‖ Int. J. Res. Electron. Comput. Eng., vol. 7, no. 1, 2019, [Online]. Available: https://www. researchgate.net/publication/ 334724160.

4. Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, M.Shabbir, “New Comparative Study Between DES, 3DES and AES”. Journal of Computing, VOL.2,No.3,pp 15-64,March 2010.

5. Majithia Sachin, Dinesh Kumar, “Implementation and Analysis of AES, DES and Triple DES on GSM Network”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1,pp 133-138, January 2010.

DOI: 10.31695/IJASRE.2025.6.5

6. Mohit Kumar Malviya, 2Prof. Manish Kumar Singhal ." A Literature Survey on Different Data Encryption and Decryption Techniques " , Journal of Emerging Technologies and Innovative Research (JETIR)., Volume 11, Issue 9 September 2024 .

7. T. Nie, C. Song, and X. Zhi, ―Performance evaluation of DES and Blowfish algorithms,‖ 2010 Int. Conf. Biomed. Eng. Comput. Sci. ICBECS 2010, pp. 16–19, 2010, doi: 10.1109/ICBECS.2010.5462398.

8. M. Anand Kumar and S. Karthikeyan, ―Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms,‖ Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 2, pp. 22–28, 2012, doi: 10.5815/ijcnis.2012.02.04.

9. Prachi Goyal , " The Importance of Data Encryption in Data Security". Journal of Nonlinear Analysis and Optimization, Vol. 13, No. 1, (2022).

10- Kwok-Wo Wong, Bernie Sin-Hung Kwok," An efficient diffusion approach for chaos-based image encryption" , Chaos, Solitons & Fractals , Volume 41, Issue 5, Pages 2652-266 , 15 September 2009.

11. Sobhy, M.I.; Shehata, A.-E." Chaotic algorithms for data encryption". In Proceedings of the 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Proceedings (Cat. No. 01CH37221), Salt Lake City, UT, USA, 7–11; pp. 997–1000. May 2001.

12. Shahna KU, Mohamed A "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map". Appl Soft Comput 90:106162. ISSN 1568-4946 , 2020.

13. W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and H. Kiya, ''Privacy preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain,'' in Proc. IEEE Int. Conf. Image Process. (ICIP), pp. 674–678, 2019

DOI: 10.31695/IJASRE.2025.6.5