https://dx.doi.org/10.4314/dujopas.v10i2b.21
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490

Review of the Advanced Encryption Standard System Performance on Hidden Data

A.A. Adigun[1], O.I. Adigun[2], M.O. Abolarinwa[3], O.S. Bakare[4], S.O. Folorunso[5], S.O. Adebayo[4], A.I. Oladimeji[6]

[1]Department of Computer Science,
Osun State University,
Osogbo,
Nigeria;

[2]Department of International Mechatronics,
Technical University of Applied Science
Wurzburg -Schweinfurt,
Germany

[3]Department of Cyber Security,
Osun State University,
Osogbo
Nigeria

[4]Department of Computer Science,
Osun State University,
Osogbo
Nigeria.

[5]Department of Mathematical Science,
Olabisi Onabanjo University,
Ago-Iwoye,
Nigeria.

[6]Department of Computer Science,
Aminu Saleh College of Education,
Azare,
Nigeria.

Email: adepeju.adigun@uniosun.edu.ng

Abstract

As the digital landscape continues to rapidly evolve, fueled by the proliferation of multimedia applications, ensuring the security of data transmission has become a paramount concern. Cryptography emerges as a stalwart guardian in this dynamic environment, offering a robust approach to safeguarding sensitive information. Despite significant strides in enhancing security services and processes over the years, the relentless march of technological progress demands a

Author for Correspondence

continual reassessment of strategies for protecting data in transit. Cryptography, with its ability to transform plaintext into ciphertext through encryption procedures, remains a cornerstone of modern data security frameworks. This paper reviews a series of data security methods, focusing on the performance of the Advanced Encryption Standard (AES) system in concealing data. A structured approach is employed to actualize the reviewed methods, with cryptographic techniques scrutinized in the literature. Analysis is conducted to obtain reviewed literature, evaluating the strengths and limitations of different cryptographic methods. The practical application of cryptography techniques is assessed across various literatures, identifying potential implications for enhancing data security in the modern digital environment. It is observed that encryption techniques are utilized to protect data over the internet and other forms of data transmission, yet brute force methods can sometimes easily identify hidden data. This paper suggests that combining two or more algorithms can lead to better data security. Specifically, combining the AES algorithm with other algorithms such as Proxy re-encryption, Honey encryption, and N-th degree Truncated Polynomial Ring Unit (NTRU) can enhance the data encryption and decryption process.

Keywords: Encryption, Decryption, Cryptography, Steganography, Data Transfer

INTRODUCTION

Although security services and processes have achieved significant progress, the trend of the digital world continues to evolve with additional security dangers that seem inevitable. Traditional methods of information security are no longer acceptable in this era. With the rise of multimedia applications, security is becoming more crucial in the transmission of images, text, video, and audio, among other things.

One crucial approach to ensure data security is through Cryptography, which includes symmetric and asymmetric encryption methods. (Tong et al., 2021) Advanced Encryption Standard (AES), Data Encryption Standard (DES) Blowfish, and 3DES are the most well-known symmetric encryption algorithm (Hosseinzad & Navi, 2018).

The asymmetric (public) key cryptosystem, employs the same technique for encryption and decryption with a pair of keys (public and private), which cannot be deduced from the public key computationally (Yang & Hanzo, 2019). The symmetric technique used for the encryption of large data includes AES, Blowfish, DES, MD5, etc. which are faster in processing than the asymmetric techniques(Schoinianakis, 2020). Among all the symmetric algorithms, AES is preferred since it is a little more secure than other symmetric techniques(Cheng et. al., 2020).

Data encryption procedures transform data into cipher text, which is difficult to decipher. Enhance security for various applications, such as online personal photo albums, medical systems, confidential video conferences, and military communications.

Steganography plays a crucial role in securing data transfer over an open network by hiding data from unauthorized access during transmission. Despite the use of Steganography, encryption remains essential to provide additional layers of security, especially in scenarios where Steganographically hidden data could be intercepted and retrieved. Encryption offers effective security by preventing information from being intercepted and used to jeopardize emergency response activities or endanger responders and the general public.

The research gap lies in addressing the evolving security challenges posed by multimedia applications and open network communication, particularly in reviewing the performance of the Advanced Encryption Standard (AES) system on hidden data. While encryption offers effective security by preventing intercepted information from jeopardizing emergency response activities or endangering responders and the general public, there is a need to assess the system's performance in concealing sensitive data. This paper aims to contribute to this field by evaluating the effectiveness of the AES system in securely hiding data, thereby enhancing our understanding of its capabilities and potential limitations.

Application of advanced encryption standard system

AES diverges from the Feistel cipher paradigm through its adoption of an iterative methodology. This cryptographic algorithm relies upon two fundamental techniques, namely substitution and permutation networks (SPN), for the encryption and decryption of data. SPN entails a series of mathematical operations intrinsic to block cipher algorithms. Notably, AES possesses the capability to process a fixed plaintext block size of 128 bits (equivalent to 16 bytes). These bytes are structured into a 4x4 matrix, forming the operational unit upon which AES operates. Additionally, an essential aspect of AES pertains to its utilization of rounds, a quantity contingent upon the length of the encryption key. AES accommodates three distinct key sizes(128, 192, or 256 bits), thereby facilitating the encryption and decryption of data. The selection of key size dictates the number of rounds employed in the AES algorithm; specifically, AES employs 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Abdullah, 2017).

The Feistel cipher paradigm is a cryptographic structure used in the design of block ciphers. It was proposed by Horst Feistel in 1973. In a Feistel cipher, the plaintext is divided into blocks, typically halves, which undergo a series of iterations called rounds. Each round involves the application of a function that operates on one half of the block while the other half is subjected to various transformations, including permutation and substitution. The output of the function is then combined with the other half through a reversible operation such as XOR. This process is repeated for a fixed number of rounds, after which the resulting Ciphertext is obtained.

The Feistel cipher structure is characterized by its simplicity, efficiency, and security properties. It allows for the construction of secure block ciphers using relatively simple components and operations. Many well-known ciphers, such as DES (Data Encryption Standard), Triple DES, and Blowfish, are based on the Feistel cipher paradigm. However, modern block ciphers like AES (Advanced Encryption Standard) depart from the Feistel structure and employ alternative techniques for encryption.

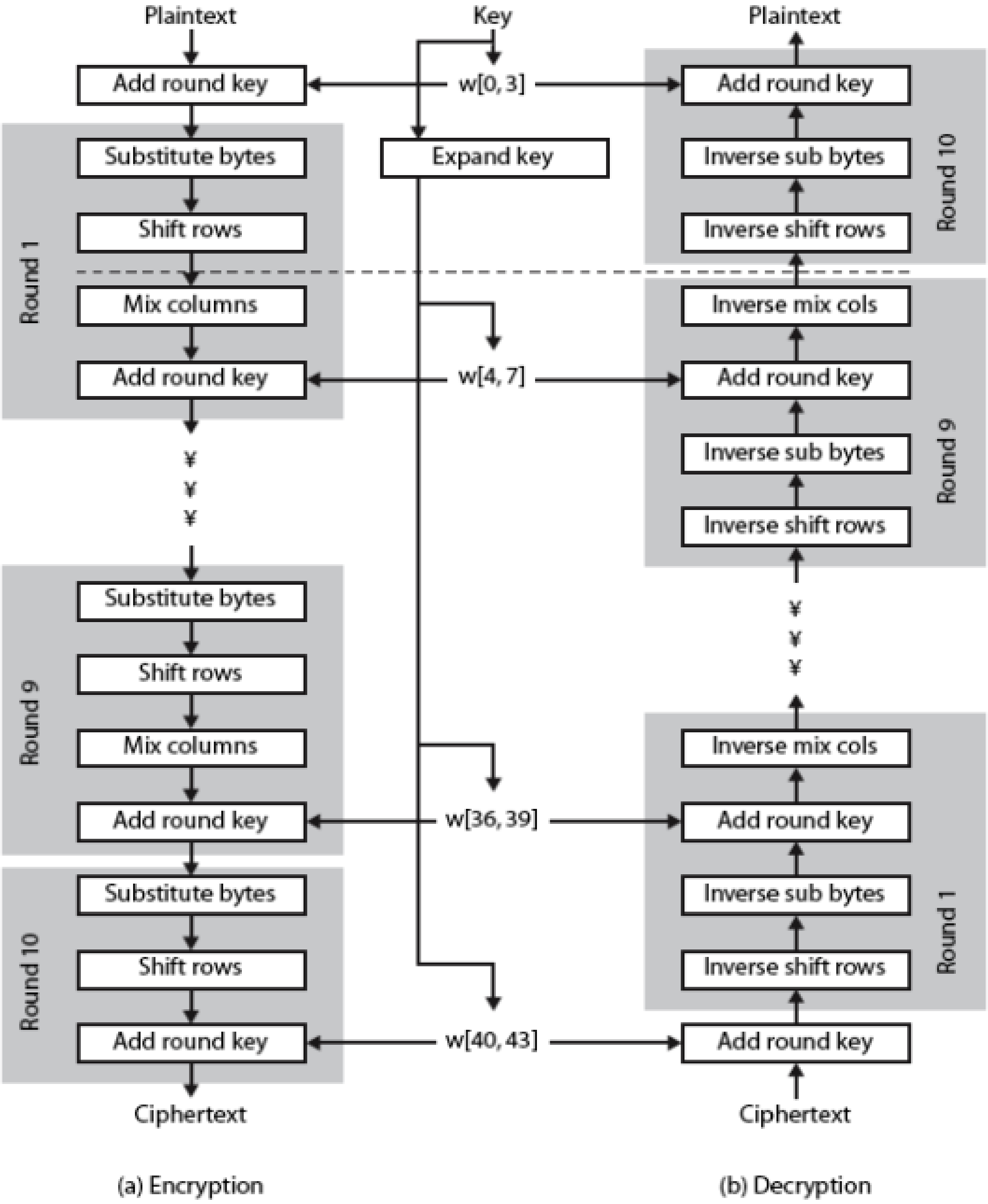

Figure 1: AES Basic Algorithm (Abdullah, 2017)

a. Encryption Process:

Among the most widely used methods for securing data from hackers is encryption. For optimal security, the AES algorithm encrypts data using a specific structure. It uses several rounds, with four sub-processes in each cycle, to accomplish it. To encrypt a 128 bit block, each round consists of the following four processes.

i. **Substitute Bytes Transformation:** The Sub Bytes transformation is the initial step in every round. This step uses a nonlinear S-box to replace a state byte with a different byte. Diffusion and confusion Shannon's principles state that in order to achieve significantly higher security, cryptographic method design plays a crucial role.

ii. **ShiftRows Transformation :** ShiftRow is the action that comes after SubByte that modifies the state. This step's basic notion is to move the state's bytes cyclically to the left in each row instead of starting at row zero. The bytes from row zero stay in this process, and no permutation is performed. There is only one circular shift to the left in the first row of bytes. There is a two-byte shift to the left of the second row. Three bytes are moved to the left of the final row. The position of the bytes in the state has been altered, but the size of the new state has remained unchanged at 16 bytes.

iii. **Mix Column Transformation:** MixColumn is another essential stage in the state process. The process of multiplication is done outside of the state. In matrix transformation, every byte in a row is multiplied by every value (byte) in the state column. Stated differently, the matrix transformation requires that each row be multiplied by each state column. These multiplication results are combined using XOR to create a new set of four bytes for the following state. The state's initial 4 by 4 dimensions are maintained in this phase.

iv. **AddRoundkey Transformation:** The most important step in the AES algorithm is AddRoundKey. A 4x4 matrix of bytes makes up the structure of both the key and the input data, commonly known as the state. When encrypting data, AddRoundKey can offer significantly higher security. Establishing a connection between the encrypted text and the key is the foundation of this process. The text in cipher originates from the earlier phase. The key that users select determines exactly what the AddRoundKey output will be. Additionally, the Subkey and state are integrated into the stage.

b. Decryption Process

The process of getting the original, encrypted data is called decryption. The key that was obtained from the sender for network security and cryptography is the foundation of this procedure. With the same key used by both the sender and the recipient to encrypt and decrypt data, the encryption process of an AES is comparable to the encryption process in reverse order. Three stages, such as InvShiftRows, InvSubBytes, and AddRoundKey, make up the final round of a decryption stage. The illustration is showed below:

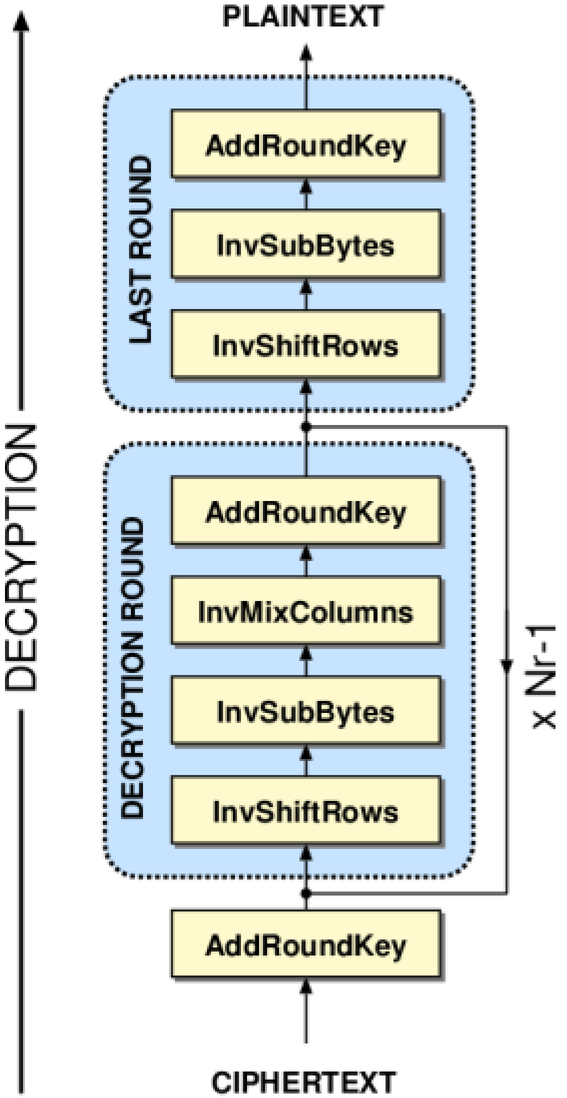

Figure 1: Decryption process (Abdullah, 2017)

Some recent works on advanced encryption standards, steganography, and cryptography spanning from 2018 to date were reviewed and the following eight (8) research works stand out:

a. Dutta et al. (2023) proposed a multi-layered approach to securing data in the cloud by combining various encryption techniques, including Advanced Encryption Standard (AES), proxy re-encryption, Honey encryption, and N-th degree Truncated Polynomial Ring Unit (NTRU). Additionally, a comparison study with other encryption algorithms is provided, evaluating factors such as encryption/decryption speed, key size, memory usage, and network latency. The author demonstrates a comprehensive understanding of encryption techniques and their applications in cloud security. The proposed method addresses the limitations of individual encryption methods by combining them into a multi-layered approach, thereby enhancing data security. The inclusion of Pseudocode and implementation examples adds clarity to the proposed algorithm. However, further clarification on the purpose and implementation of certain steps, such as the use of the proxy server and honey encryption, would improve understanding. Additionally, the paper could benefit from a more detailed discussion on the potential vulnerabilities and limitations of the proposed method, as well as future research directions. Overall, the paper presents a valuable contribution to the field of cloud security and encryption techniques.

Table 1: Comparison of Encryption Techniques (Dutta et al., 2023)

Algorithm	Encryption/Decryption speed	Key Size	Memory Usage	Network Latency
Proposed	Fast	Small	Moderate	Low
AES	Fast	Large	Low	Low
RSA	Slow	Large	Low	Low
Bluefish	Fast	Small	Low	Low
ChaCha20	Fast	Small	Low	Low

The proposed method by Dutta et al. (2023) demonstrates efficiency with fast Encryption/Decryption Speed and small Key Size, alongside moderate Memory Usage and low Network Latency compared to slower alternatives.

b. Riya et al. (2023) discussed the Analysis and Implementation of Image Steganography by using the AES algorithm. Advanced Encryption Standard (AES) enables secure data transfer over the internet, mobile phone encryption, and encryption of extremely sensitive data. It operates in terms of blocks, or chunks, of data. Steganography is the process of hiding data in another sort of data, such as a digital image. This study analyzed the possibility of hiding data inside digital photos by utilizing encryption techniques like AES. The performance comparison of AES and Data Encryption Standard (DES), a full Python implementation of the AES for image steganography is also presented. The Advanced Encryption Standard can be programmed in software or built with pure hardware.

Table 2: Comparison of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) (Riya et al., 2023)

Parameter	DES	AES
Key length	56 bits	128, 192, 256 bits
Block Size	64 bits	128 bits
Types of rounds	Expansion XOR operation with round key. Substitution and Permutation	Byte Substitution, Shift Row, Mix Column and Key Addition
Processing speed	Slower than AES	Faster than DES
Security	Less secure	More secure
H/W or S/W	Efficient only with hardware	Efficient with both hardware and software

The work done and efforts of Riya et al. (2023) established the possibility of hiding data inside digital photos by utilizing encryption techniques like AES method and Data encryption standard. AES proof much more efficiency and standard in data protection than DES.

c. Nahom & Samuel, (2022), introduced an Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm. In AES, among the four stages that are used for encryption and decryption, Sub Bytes and Mix Column produce more delay. From the two, the mix column accounts for 60% of the whole delay. To overcome these challenges, in the designed symmetrical cryptography algorithm, the mix column stage is replaced by the bitwise reverse transposition technique. This helps to improve the speed efficiency of the existing Advance Encryption Standard (AES) and Modified Advance Encryption Standard (MAES) algorithm. Simulation of the Bitwise Reverse Transposition technique resulted in better encryption and decryption speed time compared with the original Advance Encryption Standard (AES) and Modified Advance Encryption Standard (MAES): 128.953% and 115.4% encryption and decryption speed performance. Taking an average of ten trials; 140.8% increased the throughput because of bitwise reverse transposition. Hence, the Enhanced-Efficiency Advanced Encryption Standard (EE-AES) has better encryption and decryption speed performance and throughput compared to the original Advance Encryption Standard (AES) and Modified Advanced Encryption Standard (MAES).
The efforts of Nahom & Samuel, (2022), resulted in better encryption and decryption speed performance and throughput compared to the original Advance Encryption Standard (AES) and Modified Advanced Encryption Standard (MAES).

d. Nahom & Samuel, (2022), proposed an Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm. Four stages are used for encryption and decryption Sub Bytes and Mix Column produce more delay. Shift Rows stage contributes to less security level of AES because it uses easy operation that is linear. The designed symmetrical cryptography algorithm shift row stage of AES is replaced by a symmetrical transposition technique to advance security. The simulation result of the Symmetrical Transposition technique showed better security achievement, with a greater than 50% avalanche effect, which means the proposed algorithm makes better confusion and diffusion. Hence, the proposed Enhanced Security of Advanced Encryption Standard (ES-AES) algorithm has better security compared to the original Advance Encryption Standard (AES) algorithm. The outcomes demonstrate the suggested technique is powerful and adds Security levels for information transfer.

Table 3: The comparison Table between ES-AES and AES Algorithm (Nahom & Samuel, 2022)

Metric	ES-AES Algorithm	AES Algorithm
Hamming Distance	Better	Low
Avalanche Effect	> 50%	49.2%
Diffusion	Better	Low
Randomness of Output	Better	Low
Throughput	Increased by 114.3%	Low

Nahom & Samuel, (2022), show that the simulation result of the Symmetrical Transposition technique generated better security achievement compared to the original Advance Encryption Standard (AES) algorithm.

e. Manjula & Mohan, (2020), proposed a Secure Framework For Medical Image Encryption Using Enhanced AES Algorithm. This paper was based on using an enhanced AES algorithm to encrypt patient data hide medical images and transmit it over the communication medium. In this paper, an overall evaluation of the organization of the Rijndael AES algorithm and a new dynamic S-Box is spawned using a Hash function to provide robust security. Henceforth very intelligent and secure encryption techniques should be used to transmit information via medical images. Embedding vital information of the patient and doctor must be transmitted without degrading the eminence of the cover image. Decoding the data at the receiver side and the processing time are also important. The proposed security framework attempts to attain enhanced performance by dropping the encryption processing time and enhancing the quality of the stego image.
Manjula & Mohan, (2020) attempt to attain enhanced performance by dropping the encryption processing time and enhancing the quality of the Stego image.

f. Malik et al. (2019) presented a Performance Enhancement of the Advanced Encryption Standard via Pipelined Implementation. This paper studies one of the most important and widely used secret key encryption/decryption algorithms, namely the Advanced Encryption Standard (AES). The implementation of the AES algorithm involves complex computational steps that have made the implementation of these steps slow and time-consuming. The proposed AES implementation does not require dedicated equipment, it works with any kind of computers that are available to the public, such as Intel-based computers. A comparison of CPU performance is performed on both pipelined and sequential implementations on different file sizes. The pipelined implementation outperforms the sequential one, without the use of any special equipment. Using state-of-the-art multi-core architecture, a pipelined implementation of the AES algorithm was proposed to reduce both computation complexity and elapsed computation time.
Malik et al. (2019) indicated that AES implementation does not require dedicated equipment, it works with any kind of computer that is available to the public.

g. Omar & Shawkat (2018) established an Enhancing Performance of Advanced Encryption Standards for Data Security. The research target is to tackle the Advanced Encryption Standard (AES), comparing and contrasting it with prominent valid algorithms to enhance the security range by minimizing processing time, taking five rounds instead of ten, and preserving the maximum security. The comparison in terms of efficiency, key size, complexity, and time consumed was evaluated and tested via a comparison of different cryptographic algorithms such as DES, AES, and RSA, based on throughput for various numbers of words. The tests are conducted using Intel-R, Core-TM i5, CPU 2.40-GHz,128-bit processor with 8GB of RAM.

Omar & Shawkat (2018) targeted test and evaluation of efficiency, key size, complexity, and time consumed via different cryptographic algorithms. The tests were conducted using Intel-R, Core-TM i5, CPU 2.40-GHz,128-bit processor with 8GB of RAM but no evaluation was conducted.

h. Devishree et al. (2018) presented a Data Hiding using a Meaningful Encryption Algorithm to Enhance Data Security. This paper discussed the enhancement of communication security by embedding secret messages into an inconspicuous carrier and thereby transmitting them to receivers. The scheme aims to encrypt any confidential information to another meaningful text that does not convey its true meaning thus maintaining the authenticity of the information without compromising its security. The meaningful encrypted text is in the form of a report of a specific domain. The domain of the report depends on the key being used in this cipher. This key is a set of databases containing attributes used for generating the report. These attributes are numbered starting from zero in the databases. Two prominent parts of the algorithm are the first database for target data mapping and data to be encrypted that is given as input to the system, another is Key Generation, here the database used for mapping that is shuffled randomly using the Fisher-Yates Shuffle algorithm and is encrypted using any standard encryption algorithm such as RSA, DES. After these two processes, the database is ready to be implemented for Cryptography.

Devishree et al. (2018) use a Meaningful Encryption Algorithm to Enhance Data Security by embedding secret messages into an inconspicuous carrier and transmitting them to receivers.

Preparation of Advance encryption standard system

Based on the available literature, the following parameters were used by some researchers who recently worked on advanced encryption standards, steganography, and cryptography to evaluate the performance of the advanced encryption standard system on hidden data:

a. Overview of information security challenges.
b. Role of cryptography
c. Classification of cryptography
d. Prominence of symmetric encryption algorithms
e. Preference for AES
f. Application of Encryption
g. Introduction of Steganography
h. Integration of encryption and Steganography
i. Importance of Security in Emergency Response Activities

The research reviewed in the realm of data transfer security over the Internet from 2018 to date has significantly elevated the level of security in data exchange and communication among users.

Table 4: Summary of parameters used to evaluate the performance of the advanced encryption standard system on hidden data

Method	Encryption/Decryption Speed	Key Size	Memory Usage	Network Latency
Dutta et al. (2023)	Fast	Small	Moderate	Low
Riya et al. (2023)	Fast	Small	Moderate	Low
Nahom & Samuel (2022)	Faster	Smaller	Less	Lower
Nahom & Samuel (2022)	Better	Smaller	Less	Lower
Manjula & Mohan (2020)	Enhanced	N/A	N/A	
Malik et al. (2019)	Performance Enhancement	N/A	N/A	N/A
Omar & Shawkat (2018)	Enhancing Performance	N/A	N/A	N/A
Devishree et al. (2018)	N/A	N/A	N/A	N/A

Note: N/A (Not Available)

CONCLUSION

The evaluation of the reviewed literature indicates significant advancements in the field of data encryption and concealment. Dutta et al. (2023) employ a multi-layered approach to securing cloud data, combining various encryption techniques such as Advanced Encryption Standard (AES), proxy re-encryption, Honey encryption, and N-th degree Truncated Polynomial Ring Unit (NTRU). Their work includes a comprehensive comparison study with other encryption algorithms, evaluating factors like encryption/decryption speed, key size, memory usage, and network latency. Meanwhile, Riya et al. (2023) demonstrate the practical application of encryption techniques by concealing data within digital photos, showcasing the potential for securely embedding sensitive information within images. Nahom & Samuel (2022) contribute enhancements to the AES algorithm, resulting in improved speed performance, throughput, and security achievement, thereby enhancing the effectiveness and robustness of AES-based encryption systems. Manjula & Mohan (2020) focus on optimizing encryption processes to enhance stego image quality while reducing encryption processing time, addressing key challenges in data concealment. Additionally, Malik et al. (2019) highlight the accessibility and versatility of AES implementation, emphasizing its operability on commonly available computers without specialized equipment. Lastly, Devishree et al. (2018) contribute to enhancing communication system security through innovative encryption algorithms, underscoring the importance of robust encryption techniques in safeguarding sensitive information during data transmission. These findings collectively illustrate the multifaceted advancements in AES technology and its pivotal role in ensuring data security and privacy in modern communication networks.

With a plethora of encryption methods discussed, discerning the optimal approach requires a thorough assessment across various dimensions. Nahom & Samuel's (2022) ES-AES algorithm enhances the Advanced Encryption Standard (AES) by substituting the shift rows stage with symmetrical transposition, purportedly resulting in improved security metrics and throughput. Riya et al. (2023) delve into image steganography utilizing AES's established security and efficiency for concealing data within digital images. Meanwhile, Dutta et al. (2023) present a multi-layered approach to cloud data security, integrating AES among other techniques, although specific AES performance metrics are not outlined. Additionally, Nahom & Samuel (2022) introduce the Enhanced Efficiency of AES (EE-AES) Algorithm to enhance AES speed efficiency, while Malik et al. (2019) propose a pipelined AES implementation to streamline computational complexity. Omar & Shawkat (2018) aim to enhance AES performance by minimizing processing time, albeit without a detailed comparison to other encryption methods. Devishree et al. (2018) concentrate on data hiding rather than directly comparing with AES, whereas Manjula & Mohan (2020) target medical image encryption using an enhanced AES algorithm. Ultimately, the selection of a method depends on specific requirements such as security, efficiency, and suitability for distinct use cases.

REFERENCES

Aziz, A. and Ikram, N. (2007), Memory Efficient Implementation of AES S-boxes on FPGA, *Journal of Circuits, Systems and Computers (JCSC)*, vol. 16, no. 4, pp. 689– 694.

Biham, E. and Shamir, A. (2018), Differential cryptanalysis of the data encryption standard. Springer Science & Business Media.

Devishree Naidu, Shubhangi Tirpude, Kanak Kalyani, Vrushali Bongirwar, Tejasvee Sharma (2020), Data Hiding using Meaningful Encryption Algorithm to Enhance Data Security. *International Journal of Advanced Trends in Computer Science and Engineering*. Vol 9. No. 2, pp 2408 – 2413.

Dutta, A., Bose, R., Roy, S., & Sutradhar Sh. (2023). Hybrid Encryption Technique to Enhance Security of Health Data in Cloud Environment. *Archives of Pharmacy Practice*, 14(3), 41-7. https://doi.org/10.51847/raeh8fHBt6

Federal Information Processing Standards Publication (FIPS 197), Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/ fips/fips197/fips-197.pdf.

May Hattim Abood, Zahraa Khudhair Taha (2019), Secure and Hidden Text using AES Cryptography and LSB Steganography. *Journal of Engineering Science and Technology.* Vol 14, No. 3, pp 1434 – 1450.

Majula G, Mohan H.S. (2020), A secure framework for Medical Image Encryption Using Enhanced AES Algorithm. *International Journal of Scientific & Technology Research*. Volume 9, Issue 02. ISSN 2277-8616

Manjula G, Mohan H S. (2018), Improved Dynamic S-Box generation using Hash function for AES and its Performance Analysis, 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT).

Nahom Gebeyehu Zinabu, Samuel Asferaw (2022). Enhanced Efficiency of Advanced Encryption Standard (EE-AES) Algorithm. *American Journal of Engineering and Technology Management*. Vol. 7, No. 3, pp. 59-65. doi: 10.11648/j.ajetm.20220703.13

Nahom Gebeyehu Zinabu, Samuel Asferaw (2022). Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm. *American Journal of Computer Science and Technology*. Vol. 5, No. 2, pp. 41-48. doi: 10.11648/j.ajcst.20220502.13

Omar G. Abood, Shawkat K. Guirguis (2018), Enhancing Performance of Advanced Encryption Standard for Data Security. *International Journal of Engineering and Information Systems (IJEAIS).* Vol. 2. Issue 11, pp 32 – 38.

Patel, F. R. and Cheeran, A. (2015), Performance evaluation of steganography and AES encryption based on different formats of the image, *Performance Evaluation*, vol. 4, no. 5.

Pandya, D. and Narayan, K. R. (2018), "Brief History of Encryption, *Int. J. Software Engineering and its Application.*, vol. 131, no. 9, pp. 28–31.

Riya Kedia, Biresh Kumar, Pallab Banerjee, Pooja Jha, Tannisha Kundu, Mohan Kumar Dehury (2023). Analysis and Implementation of Image Steganography by using AES algorithm. Proceedings of the 7th International Conference on Trends in Electronics and Informatics. IEEE Xplore Part Number: CFP23J32-ART; ISBN: 979-8-3503-9728-4

Singh, G. (2013), A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 975–8887.

Thulasimani, M. M. (2015), Design and Implementation of Reconfigurable Rijndael Encryption Algorithms For Reconfigurable Mobile Terminals, *Int. J. Comput. Sci. Eng.,* vol. 02, no. 04, pp. 1003–1011.

Zakaria, N. H., Mahmod, R. Udzir, N. I. and Zukarnain, Z. A. (2015), Enhancing Advanced Encryption Standard (AES) S-Box Generation Using Affine Transformation., *J. Theor. Appl. Inf. Technol.*, vol. 72, no. 1.