IJEMD-CSAI, 3 (1) (2024), 1 – 9 https://doi.org/10.54938/ijemdcsai.2024.03.1.268

International Journal of Emerging Multidisciplinaries:
Computer Science and Artificial Intelligence

Research Paper
Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2791-0164 ISSN (online): 2957-5036

Performance Analysis of symmetric and asymmetric Encryption Algorithms Based on File, Image and Video

Aisha Atib Tijjani [1], Abdullahi Isa [1*]

1.Department of Computer Science, Faculty of Physical Sciences, University of Maiduguri, Nigeria

** Corresponding Author*

Abstract

The rapid evolution of digital technology has exponentially amplified the generation and sharing of diverse digital data, notably files, images, and videos, over the internet, intensifying the critical need for enhanced security measures to safeguard these prevalent data types. This research presents a comprehensive analysis of various encryption algorithms applied to different data types - files, images, and videos. The study categorizes encryption algorithms into symmetric and asymmetric types, with examples including AES, DES, Triple DES, RSA, Diffie-Hellman, and ECC. The paper further explores specific algorithms used for file, image, and video encryption. A comparative analysis is conducted based on parameters such as encryption and decryption speed, key size, data blocks, and data types. The objective is to identify the most efficient encryption algorithm for each data type, thereby enhancing data security in the digital age. The paper emphasizes that while encryption is a crucial tool for data security, it should be used in conjunction with other security measures for comprehensive protection.

Keywords: encryption algorithms, file encryption, image encryption, video encryption, AES, DES, RSA.

Introduction

The rapid advancement of digital technology has led to an exponential increase in the generation and sharing of digital data. Among these data, files, images, and videos are the most common forms that are shared over the internet. As such, the security of these data types has become a paramount concern. However, due to cyber threats and digital vulnerabilities of various data types, the critical need for robust data protection mechanisms has propelled encryption algorithms to the forefront of information security research. This paper presents a meticulous examination of the performance attributes of both symmetric and asymmetric encryption algorithms in the context of securing diverse data types such as files, images, and videos. As emphasized by [10], encryption serves as a fundamental tool to safeguard sensitive information from unauthorized access, providing a secure channel for data transmission. The

Email Addresses: aishaatib86@gmail.com (AISHA) , isaabdullahi@unimaid.edu.ng (ABDULLAHI).

significance of encryption in bolstering network security is underscored by the works of [4], who highlights the indispensability of cryptographic techniques in thwarting potential cyber threats.

Encryption algorithms can be broadly categorized into two types: symmetric and asymmetric. Symmetric encryption, also known as secret key encryption, uses a single key for both encryption and decryption. Examples of symmetric encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES. On the other hand, asymmetric encryption, also known as public-key encryption, uses a pair of keys - a public key for encryption and a private key for decryption. RSA, DSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are examples of asymmetric encryption algorithms.

When it comes to file encryption, several algorithms like TripleDES, Twofish, Blowfish, AES, IDEA, MD5, and HMAC are commonly used . For image encryption, algorithms such as AES, RSA, Chaotic System, DCT, and DWT have been proposed and used [6] , [7]. Video encryption, on the other hand, often employs advanced algorithms to encode video data, making it unreadable to unauthorized individuals [9], [11]

A comprehensive literatures assessment has been conducted on both symmetric and asymmetric encryption algorithms, focusing on their performance across different data types such as files, images, and videos. The evaluation criteria encompass critical aspects such as time efficiency, resource usage, and privacy considerations. For instance, the study by [1] does not analyze symmetric encryption algorithms. It only evaluates the performance of two asymmetric encryption algorithms (RSA and ElGamal) on mixed data such as binary, text, and image files. Therefore, it does not provide information on the performance analysis of symmetric encryption algorithms on file, image, and video data. Also, the paper by [5] does not analyze the performance of encryption algorithms based on file, image, and video. It focuses on evaluating the performance of symmetric encryption algorithms (3DES, AES, Blowfish, and IDEA) based on time, resource, and privacy criteria using MCDM methods. The paper by [3] discusses a comparative analysis of symmetric and asymmetric encryption algorithms, including AES, MAES, RSA, DES, 3DES, and BLOWFISH, for securing image and video data in mobile computing. The research by [8] centered on conducting a comparative examination of symmetric algorithms, namely AES, DES, Ceaser Cipher, and Stream Cipher, alongside asymmetric algorithms such as Diffie Hellman and RSA. Additionally, it explores the application of symmetric algorithms in the encryption of both files and images. The investigation by [8] delves into the distinctions between symmetric and asymmetric algorithms, conducting an assessment of their respective efficiencies. The study employs three algorithms—RSA, AES, and DES—for this purpose. In their simulation, the parameters considered include the original file size, encryption time, and decryption time. The simulation accommodates various file formats, including jpeg, mp3, and mp4, as well as pdf and docx documents. The approach advocated in this paper [2]involves employing a blend of symmetric and asymmetric encryption algorithms and subsequently assessing its performance against established systems. The process entails dividing the file into n-parts based on its size, after which each segment undergoes encryption using either the AES, DES, or RSA algorithms. The outcomes of this hybrid technique exhibit enhanced security measures. The comparison is conducted by evaluating the time taken, measured in milliseconds, by both the proposed and existing systems to encrypt varying amounts of text and image data bytes.

Against this backdrop, the current research endeavors to contribute to the field by conducting a comprehensive performance analysis of key encryption algorithms to identify the most efficient encryption algorithm for each data type, thereby contributing to the enhancement of data security in the digital age, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), and Digital Signature Algorithm (DSA). The evaluation will delve into the speed, Memory, and Time consumption and resource utilization of these algorithms during both encryption and decryption processes, shedding light on their applicability in safeguarding file, image, and video data. The findings of this research aim to inform practitioners and policymakers about the strengths and weaknesses of symmetric and asymmetric encryption techniques, facilitating informed decisions for optimizing digital data protection in a rapidly evolving digital landscape.

Methodology

This section presents the methodology used to assess the performance of the selected encryption algorithms for file, image and video. The overall approach employed in this study presented first, the dataset utilized, and the performance evaluation metrics.

Approach employed

This paper employs operational modeling, as the research involves developing a functional system to extract and analyze data for interpretation and insights. Operational analysis is employed to measure and evaluate the actual system in operation. The performance metrics considered include speed, memory consumption, and time consumption. To serve as an experimental environment, a prototype system is created using the PYTHON programming language.

Dataset Utilized

This section presents the dataset utilized in this research. The dataset consists of one file, one image and one video as listed in table 1 below.

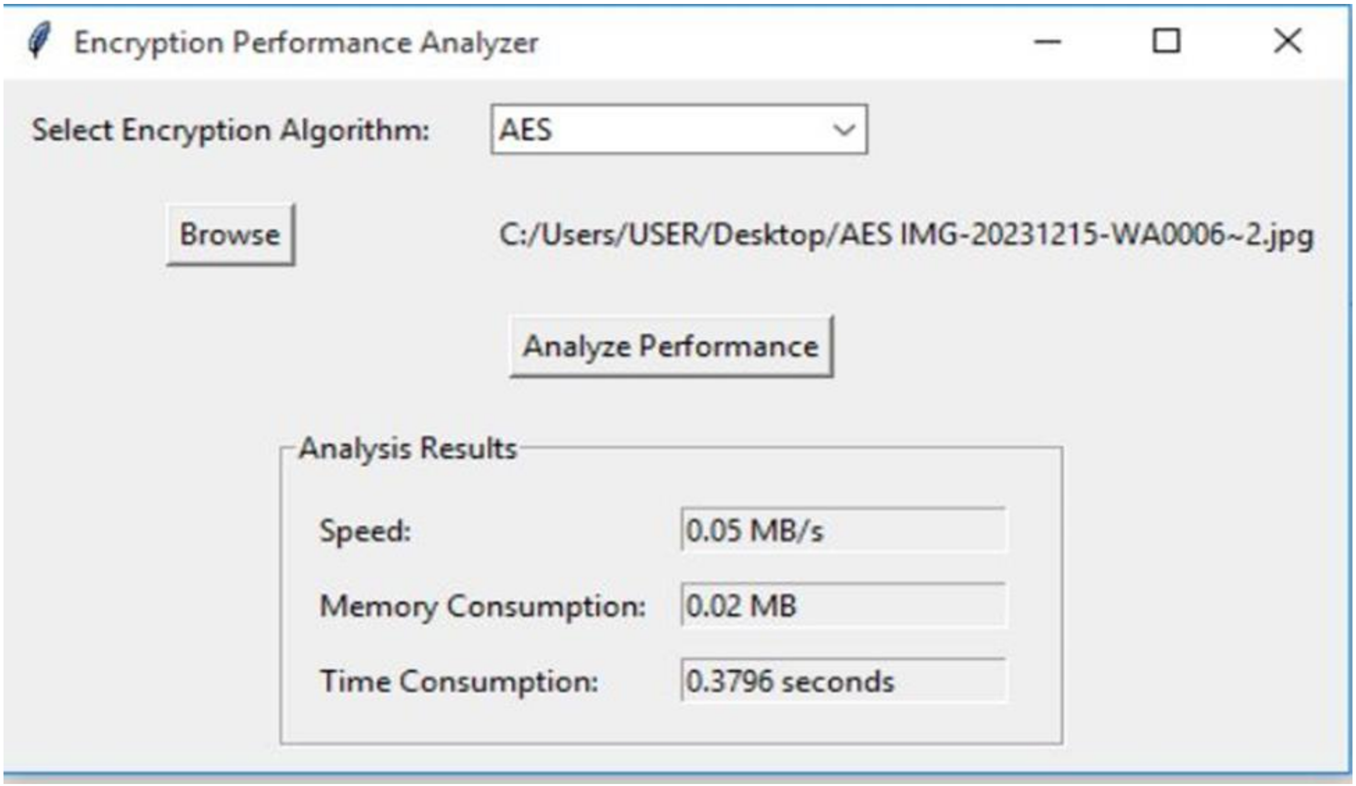
Table 1: Datasets Used

Name	Size	File type
A.ATIB	Size: 25.5 KB	Microsoft Word Document (.docx)
IMG_3728	Size: 13.5 MB	JPG File
Rayuwata	Size: 60.7 MB	MP4 Video File (VLC)

Results and Discussion

The experimentation involved the evaluation of encryption algorithms utilizing three distinct data types: files, images, and videos. This comparative analysis focused on Symmetric encryption algorithms, namely AES and DES, and Asymmetric encryption algorithms, namely RSA and DSA. The assessment criteria included speed, memory consumption, and time consumption for each data type, as visually represented in Figure 1 on the system interface.

To initiate the analysis, users select the desired algorithm type and input the file type for encryption. Upon pressing the designated button, the system commences the evaluation process specific to the chosen algorithm and the file type provided. The outcomes of the analysis are then promptly displayed on the user's screen, mirroring the interface showcased in Figure 1 for a comprehensive and accessible presentation of the results. This user-friendly approach facilitates seamless interaction with the encryption system, enabling users to make informed decisions based on the performance metrics tailored to their selected algorithm and file type.



Encryption Performance Analyzer

Select Encryption Algorithm: AES

C:/Users/USER/Desktop/AES IMG-20231215-WA0006~2.jpg

Analysis Results

Speed: 0.05 MB/s

Memory Consumption: 0.02 MB

Time Consumption: 0.3796 seconds

Figure 1: System interface

A. FILE

Table 2 below presents the results obtained for the following encryption algorithms (AES, DES, RSA, and DSA) with a focus on file-based assessments.

Table 2: File Results

Algorithms	Speed (MB/S)	Memory consumption (MB)	Time consumption (second)
AES	2.72	0.70	0.2574
DES	0.15	0.70	4.5801
RSA	0.38	0.70	1.8697
DSA	0.10	0.70	7.2596

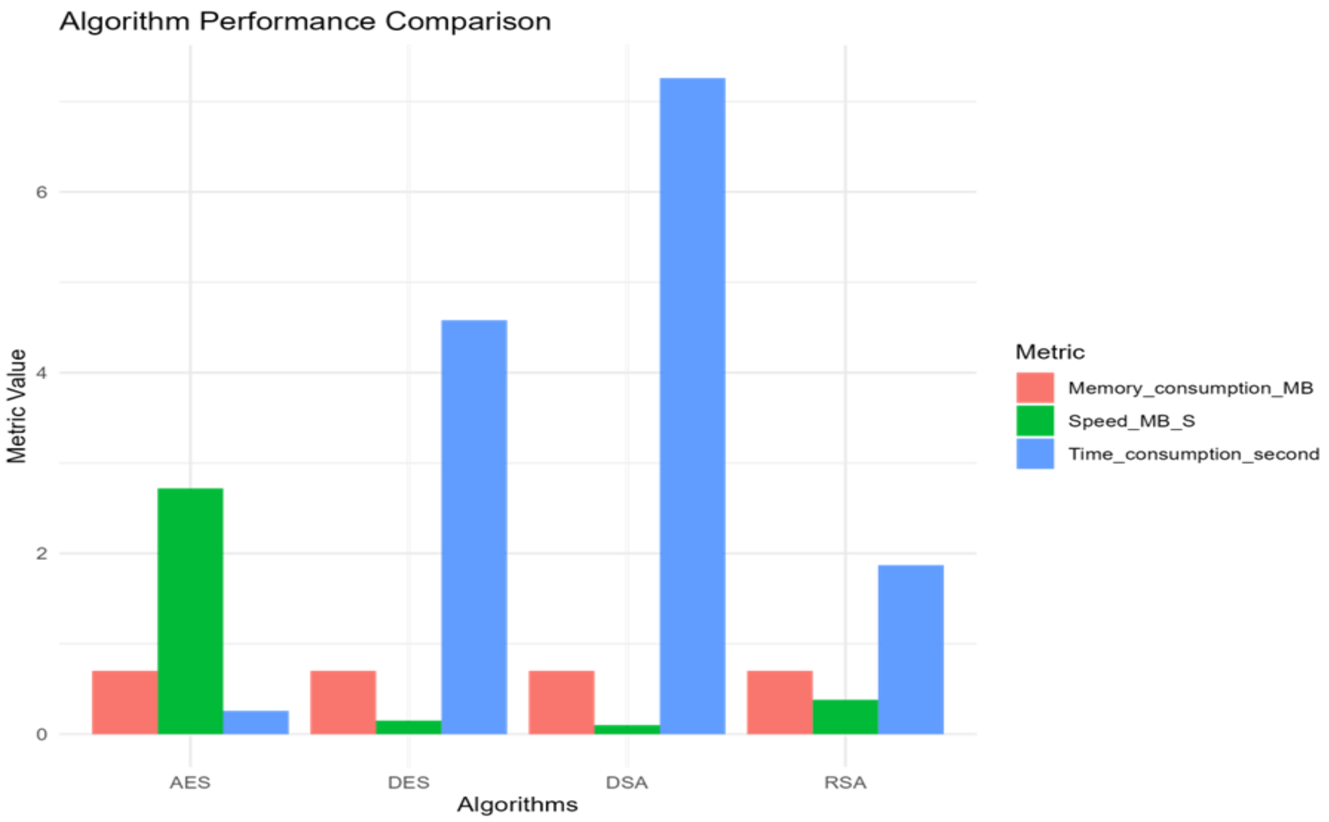


Figure 2: Performance of metrics based on file

The bar graph in Figure 2 above presents a comparative analysis of four encryption algorithms AES, DES, DSA, and RSA—across three key performance metrics-based file: memory consumption (MB), speed (MB/s), and time consumption (seconds) based on file processing. The results show that:

AES (Advanced Encryption Standard): AES demonstrates a balanced performance with a moderate speed of 2.72 MB per second, low memory consumption (0.70 MB), and swift time consumption of 0.2574 seconds. This makes AES a commendable choice for file-based encryption, offering an equilibrium between processing speed and efficient resource utilization.

DES (Data Encryption Standard): In contrast, DES exhibits slower speed at 0.15 MB per second, similar memory consumption (0.70 MB), but a significantly higher time consumption of 4.5801 seconds. While DES may appeal to scenarios prioritizing resource conservation, its extended processing time makes it less suitable for applications requiring rapid file encryption.

RSA (Rivest–Shamir–Adleman): RSA strikes a balance with a moderate speed of 0.38 MB per second, consistent memory consumption (0.70 MB), and a time consumption of 1.8697 seconds. Positioned as a practical choice for file-based encryption, RSA offers a compromise between speed and resource efficiency, making it versatile for a range of applications.

DSA (Digital Signature Algorithm): DSA exhibits the slowest speed at 0.10 MB per second and the highest time consumption of 7.2596 seconds, despite consistent memory consumption (0.70 MB). These results suggest that DSA may not be the most efficient option for file-based encryption, particularly in scenarios where quicker processing is crucial.

In conclusion, the findings from Table 1 emphasize the significance of considering the trade-off between speed, memory consumption, and time consumption when selecting an encryption algorithm for file-based applications. While AES emerges as a well-rounded choice, DES, RSA, and DSA cater to specific use cases, depending on the priority given to speed and resource efficiency in file encryption scenarios.

B. IMAGE

Table 3 below displays the results obtained for the following encryption algorithms (AES, DES, RSA, and DSA) with a specific emphasis on image-based evaluations.

Table 3: Image Results

Algorithms	Speed (MB/S)	Memory consumption (MB)	Time consumption (second)
AES	3.42	0.02	0.0060
DES	0.09	0.02	0.0010
RSA	0.29	0.02	0.0050
DSA	0.01	0.02	1.746

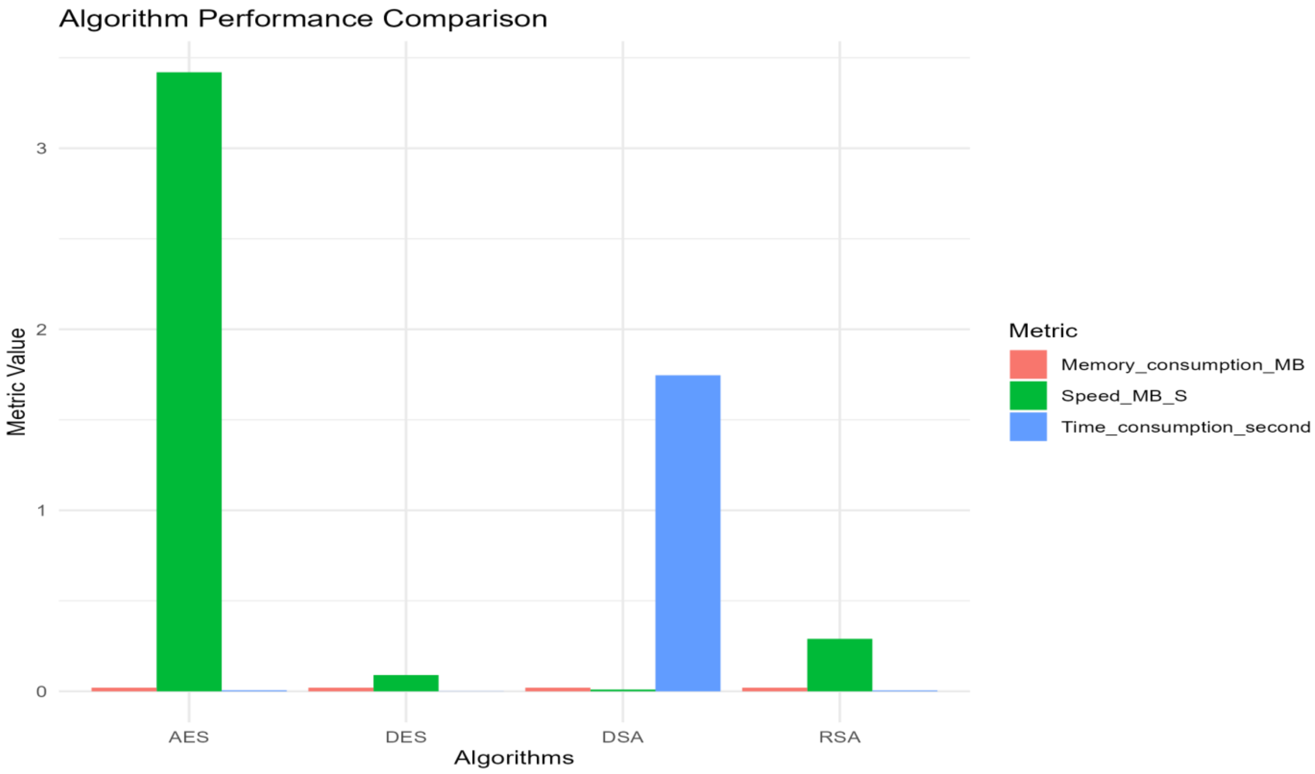


Figure 3: Performance of metrics based on image

The bar graph in Fig 3 above depicts the performance of four encryption algorithms—AES, DES, DSA, and RSA—based on image, evaluated across three key metrics: memory consumption (MB), speed (MB/s), and time consumption (seconds).

AES (Advanced Encryption Standard): With a commendable speed of 3.42 MB per second, minimal memory consumption (0.02 MB), and efficient time utilization (0.0060 seconds), AES emerges as a robust choice for image encryption. Its balanced performance makes it suitable for applications where both speed and resource efficiency are critical.

DES (Data Encryption Standard): While DES exhibits a lower speed at 0.09 MB per second, it compensates with remarkably low memory consumption (0.02 MB) and swift processing time (0.0010 seconds). Though not the fastest, DES proves valuable when conserving resources is a top priority in image encryption tasks.

RSA (Rivest–Shamir–Adleman): Striking a balance between speed (0.29 MB/s) and memory consumption (0.02 MB), RSA offers a moderate yet efficient encryption solution, with a time consumption of 0.0050 seconds. This positions RSA as a practical choice for image-based encryption tasks, appealing to scenarios where a compromise between speed and efficiency is necessary.

DSA (Digital Signature Algorithm): DSA demonstrates a significantly lower speed at 0.01 MB per second, coupled with moderate memory consumption (0.02 MB). However, its extended time consumption of 1.746 seconds suggests that DSA may not be the most time-efficient option for image encryption, particularly in situations requiring quicker processing.

In conclusion, the results underscore the need for a nuanced consideration of speed, memory consumption, and time consumption when selecting an encryption algorithm for image-based applications. AES emerges as a versatile choice, while DES, RSA, and DSA cater to specific use cases depending on the priority given to speed and resource efficiency.

C. Video

Table 4 below showcases the outcomes derived from the evaluation of encryption algorithms (AES, DES, RSA, and DSA) specifically in the context of video data.

Table 4: Video Results

Algorithms	Speed (MB/S)	Memory consumption (MB)	Time consumption (second)
AES	33.76	60.79	1.8007
DES	32.36	60.79	1.6007
RSA	34.22	60.79	1.7766
DSA	24.03	60.79	2.5297

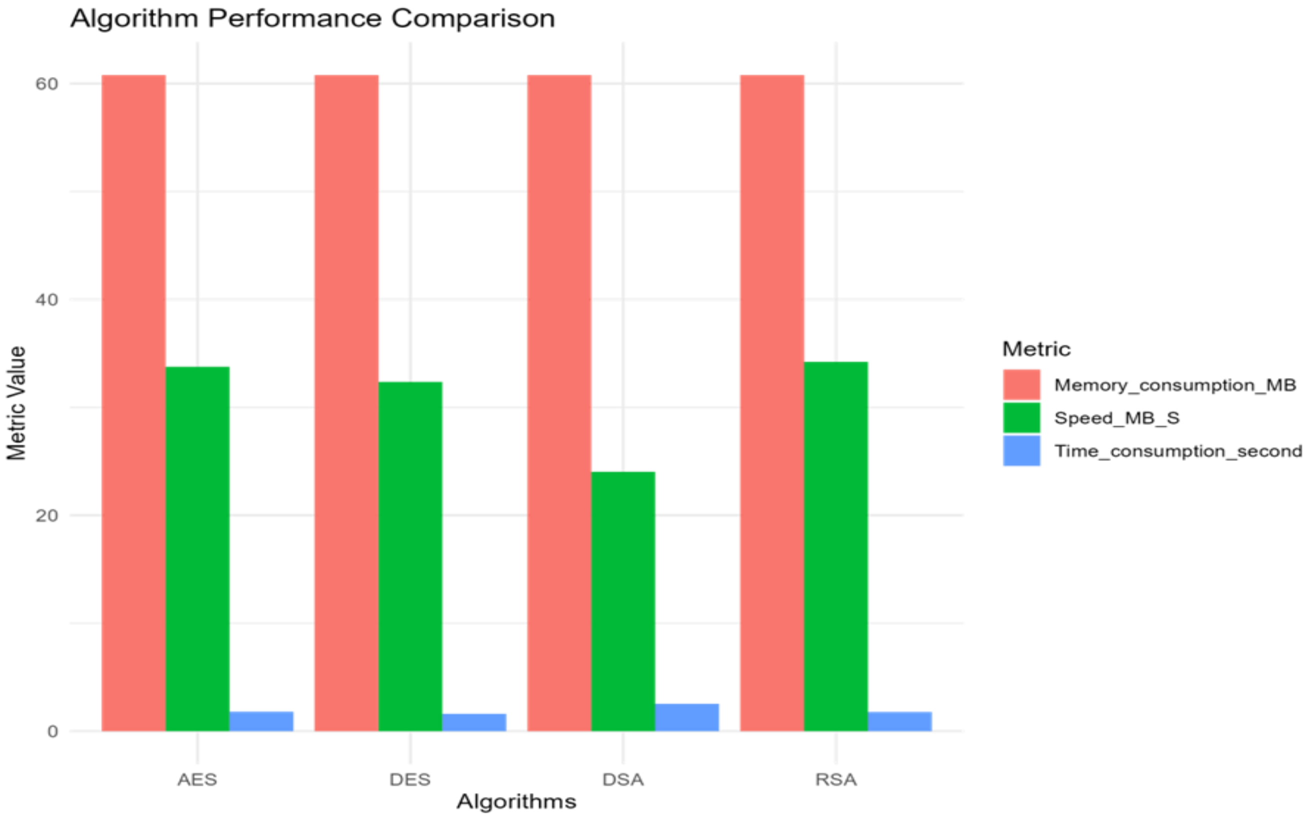


Figure 4: Performance of metrics based on video

The bar graph in Fig 4 above depicts the performance of four encryption algorithms—AES, DES, DSA, and RSA—evaluated across three key metrics-based video: memory consumption (MB), speed (MB/s), and time consumption (seconds).

AES (Advanced Encryption Standard): Noteworthy for its high speed of 33.76 MB per second, AES emerges as a robust contender for video encryption. However, this efficiency is accompanied by relatively higher memory consumption (60.79 MB) and a time consumption of 1.8007 seconds. While offering swift encryption, AES tends to be resource-intensive, making it suitable for scenarios where speed takes precedence over resource conservation.

DES (Data Encryption Standard): Following closely behind AES, DES exhibits competitive performance in video encryption. With a speed of 32.36 MB per second, similar memory consumption (60.79 MB), and a slightly quicker time consumption of 1.6007 seconds, DES strikes a balance between speed and resource utilization. It presents itself as a viable option for those seeking efficient video encryption without compromising too much on resource efficiency.

RSA (Rivest–Shamir–Adleman): RSA demonstrates commendable speed at 34.22 MB per second, comparable memory consumption (60.79 MB), and a time consumption of 1.7766 seconds. These results position RSA as an effective choice for video encryption, offering a balanced compromise between speed and resource efficiency. It presents itself as a versatile option suitable for a range of video encryption applications.

DSA (Digital Signature Algorithm): DSA lags behind in terms of speed, with 24.03 MB per second, and exhibits the highest time consumption of 2.5297 seconds. While maintaining consistent memory consumption (60.79 MB), DSA might be less suitable for video encryption scenarios that prioritize swift processing. Its extended time consumption suggests it may not be the most time-efficient option among the algorithms considered.

In conclusion, the results from Table 3 highlight the need for a nuanced decision-making process when selecting an encryption algorithm for video-based applications. AES, DES, and RSA each offer distinct advantages, catering to varying priorities in speed and resource efficiency. However, DSA may be less favorable in situations where rapid processing is a critical requirement.

COMPARATIVE ANALYSIS

A comparative analysis will be conducted to benchmark the performance of the encryption algorithm against other commonly used encryption methods. This helps in understanding its relative strengths and weaknesses.

Table 4: Comparison between AES, DES, RSA and DSA

CRITERIA	**AES**	**DES**	**RSA**	**DSA**
Type	Symmetric	Symmetric	Asymmetric	Asymmetric
Key length	128, 192, 256 bits	56 bits (key size)	Variable (commonly 2048)	Variable (commonly 2048)
Encryption speed	Fast	Moderate	Slower for large files	Slower for large files
Decryption speed	Fast	Moderate	Slower for large files	Slower for large files
Key distribution	Key exchange required	Key exchange required	Public key distribution	Public key distribution
Security strength	Highly secure	Weak (now considered insecure)	Secure	Secure
Common usage	Data encryption	Legacy systems, limited use	Public key cryptography	Digital signatures
Algorithm type	Block cipher	Block cipher	Asymmetric encryption	Digital signature algorithm

This table provides a brief overview of the characteristics and typical usage scenarios for each encryption algorithm. Keep in mind that the suitability of an algorithm depends on the specific requirements of the application.

CONCLUSION AND RECOMMENDATION

In conclusion, the findings presented in this chapter contribute significantly to the understanding of encryption algorithm performance for file security. The nuanced insights into each algorithm's strengths and weaknesses provide a basis for informed decision-making in selecting the most suitable encryption approach for specific use cases.

The experimental results emphasize the importance of considering both speed and resource utilization in choosing encryption algorithms. The analysis of security trade-offs guides practitioners in tailoring encryption configurations to meet specific security requirements while maintaining acceptable performance levels. As technology continues to evolve, the conclusions drawn from this research will serve as a valuable reference for designing secure and high-performance systems. The recommendations provided in this chapter offer practical guidance for system designers, security professionals, and researchers working towards achieving an optimal balance between file security and operational efficiency.

The recommendations are building upon the observed performance characteristics, the recommendation section offers practical guidance for selecting encryption algorithms based on specific file, image and video security requirements. It takes into account factors such as encryption speed, resource efficiency, and security trade-offs. The recommendations aim to assist practitioners and system designers in making informed decisions when implementing file security measures, considering both the strengths and weaknesses of different encryption approaches. It’s recommended that next researcher should use large datasets of files, images and videos. Also, energy consumption should also be analyze based on hardware configuration.

References

[1] Abidemi Adeniyi, E., Lucky Imoize, A., Bamidele Awotunde, J., Lee, C.-C., Falola, P., Gbenga Jimoh, R., & Adeola Ajagbe, S. (2023). Performance Analysis of Two Famous Cryptographic Algorithms on Mixed Data. *Journal of Computer Science*, *19*(6). https://doi.org/10.3844/jcssp.2023.694.706

[2] Alex, S. A., A, P., Patil, R. N., Kanavalli, A., & Karki, N. M. (2022). Implementation and Comparison of File Security Using AES, DES and RSA and Anomaly Detection in Videos Using Convolutional Auto Encoder. *Webology*, *19*(1), 664–675. https://doi.org/10.14704/WEB/V19I1/WEB19047

[3] Alothman, R. B., Saada, I. I., & Al-Brge, B. S. B. (2022). A Performance-Based Comparative Encryption and Decryption Technique for Image and Video for Mobile Computing. *Journal of Cases on Information Technology (JCIT)*, *24*(2), 1–18. https://doi.org/10.4018/JCIT.20220101.OA1

[4] Bruce, S. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Compan. moz-extension://eda3413d-5059-4a5d-afb9-bb40aa4e5c87/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fciberativismoeguerra.files.wordpress.com%2F2017%2F09%2Fbruce-schneier-data-and-goliath_-2015.pdf

[5] Das, D., Roy, S., Gupta, K., & Sahoo, B. (2022). Performance Evaluation of Symmetric Encryption Algorithms Using MCDM Methods. *Proceedings - 2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security, ISSSC 2022*. https://doi.org/10.1109/ISSSC56467.2022.10051594

[6] Jb, A., & Choudhary, R. (n.d.). *Image Encryption for Secure Data Transfer and Image based Cryptography*. Retrieved January 18, 2024, from www.ijert.org

[7] Kaur, M., Singh, S., & Kaur, M. (2021). Computational Image Encryption Techniques: A Comprehensive Review. *Mathematical Problems in Engineering*, *2021*. https://doi.org/10.1155/2021/5012496

[8] Keerthan, N. K. S., Marri, S. P., & Khanna, M. (2023). Analysis of Key Based Cryptographic Algorithms and its Applications. *3rd IEEE International Conference on Technology, Engineering, Management for Societal Impact Using Marketing, Entrepreneurship and Talent, TEMSMET 2023*. https://doi.org/10.1109/TEMSMET56707.2023.10150061

[9] Kulkarni, A., Kulkarni, S., Haridas, K., & More, A. (2013). Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study. In *International Journal of Computer Applications* (Vol. 65, Issue 1).

[10] Stallings, W., Columbus, B., New, I., San, Y., Hoboken, F., Cape, A., Dubai, T., Madrid, L., Munich, M., Montréal, P., Delhi, T., São, M. C., Sydney, P., Kong, H., Singapore, S., & Tokyo, T. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION*. www.pearsonglobaleditions.com

[11] Su, Z., Lian, S., Zhang, G., & Jiang, J. (2011). Chaos-based video encryption algorithms. *Studies in Computational Intelligence*, *354*, 205–226. https://doi.org/10.1007/978-3-642-20542-2_6/COVER