African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 3, Issue 1, January-March 2024, Page No: 187-192
Website: *https://aaasjournals.com/index.php/ajapas/index*
معامل التأثير العربي 2023: (1.55) **SJIFactor 2023: 5.689** **ISI 2022-2023: 0.557**

Encryption of Photos: Protecting Privacy and Securing Sensitive Images

Nadya Musbah Mohamed Almannouni *
Department of Electric and Electronic Engineering, College of Technical Sciences Sebha, Sebha, Libya

*Corresponding author: nadyaalmannouni@yahoo.com

Received: January 18, 2024	Accepted: February 28, 2024	Published: March 10, 2024

Abstract:
One popular and extremely secure encryption algorithm is called Advanced Encryption Standard (AES). In 2001, the Data Encryption Standard (DES) was replaced by the National Institute of Standards and Technology (NIST). AES allows key sizes of 128, 192, and 256 bits and runs on set block sizes. It offers strong security, effective performance, and flexibility through the use of a substitution-permutation network (SPN) architecture. Virtual private networks (VPNs), wireless communication, network security, and data protection are among the fields in which AES finds use. Because it is widely used and standardized, it is an essential instrument for guaranteeing secure communication and data secrecy across various industries.

Keywords: Advanced Encryption Standard, Data Encryption Standard, Standards and Technology, Virtual Private Networks.

Cite this article as: N. M. M. Almannouni, "Encryption of Photos: Protecting Privacy and Securing Sensitive Images," African Journal of Advanced Pure and Applied Sciences (AJAPAS), vol. 3, no. 1, pp. 187–192, January-March 2024

تشفير الصور: حماية الخصوصية وتأمين الصور الحساسة

ناديه مصباح محمد سهل المنوني *
قسم الهندسة الكهربائية والإلكترونية، كلية العلوم التقنية سبها، سبها، ليبيا

الملخص
إحدى خوارزميات التشفير الشائعة والآمنة للغاية تسمى معيار التشفير المتقدم .(AES) في عام 2001، تم استبدال معيار تشفير البيانات (DES)به من قبل المعهد الوطني للمعايير والتكنولوجيا .(NIST) يسمح AES بأحجام مفاتيح تبلغ 128 و192 و256 بت ويعمل على أحجام محددة للكتل. فهو يوفر أمانًا قويًا وأداءً فعالاً ومرونة من خلال استخدام بنية شبكة التبديل والتبديل .(SPN) تعد الشبكات الخاصة الافتراضية(VPNs) ، والاتصالات اللاسلكية، وأمن الشبكات، وحماية البيانات من بين المجالات التي تستخدم فيها .AES نظرًا لاستخدامها وتوحيدها على نطاق واسع، فهي أداة أساسية لضمان الاتصالات الآمنة وسرية البيانات عبر مجموعة من الصناعات.

الكلمات المفتاحية: معيار التشفير المتقدم، معيار تشفير البيانات، المعايير والتكنولوجيا، الشبكات الخاصة الافتراضية.

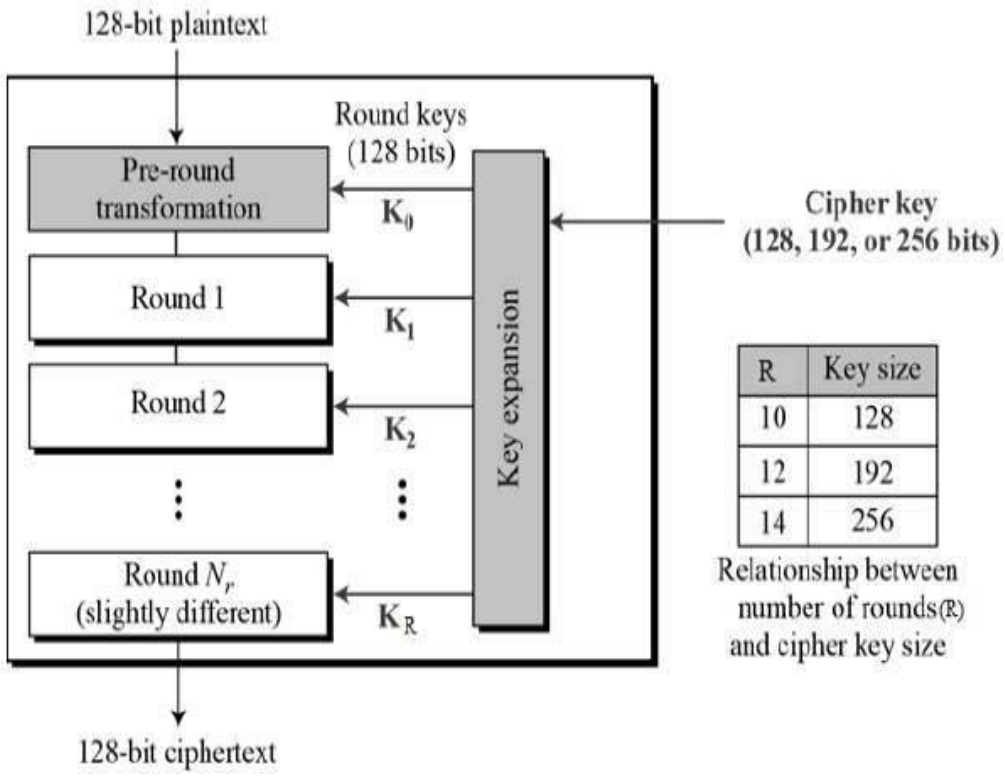
Introduction

The Advanced Encryption Standard (AES) is a widely recognized and extensively used encryption algorithm [1]. The same key is utilized for both the encryption and decryption processes because the encryption algorithm is symmetric [2]. Data security, network security, and communication protocols are just a few of the areas where AES has established itself as the de facto standard for protecting sensitive data [3].

The salient characteristics, background, and robustness of AES is discussed in this article as its main contribution along with its significance for guaranteeing data secrecy and secure communication. While the remaining section in the article organized as follows: Section 2 discussing the Overview of Advanced Encryption Standard. The Key Strengths of AES are placed in Section 3. Section 4 presents the main Applications of AES. The Importance of Encrypting Photos are positioned in Section 5. While the Encryption Techniques and Benefits of AES are tabulated in Section 6. The obtained Results and discussion of the utilized technique are taken place in Section 7. Eventually, the article closes with the summary Conclusion along with list of recent References.

Overview of Advanced Encryption Standard:

Several articles studied the importance of the AES techniques in securing the data. The AES was selected by the National Institute of Standards and Technology (NIST) in 2001 as a replacement for the aging Data Encryption Standard (DES) [4]. It was designed to provide a higher level of security and efficiency compared to its predecessor [5]. AES operates on fixed block sizes of 128 bits and supports key sizes of 128, 192, and 256 bits [6]. It employs a substitution-permutation network (SPN) structure, which consists of several rounds of transformations, including byte substitution, row shifting, column mixing, and key mixing [7].



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 1: Advanced Encryption Standard structure [8], [9].

AES is an iterative encryption, not a Feistel encryption. It is based on an "alternative permutation network". It consists of a chained series of operations, some of which involve replacing inputs with specific outputs (replacement) and others of shuffling bits (permutation).

Key Strengths of AES:

An effective symmetric encryption technique with many applications is the Advanced Encryption Standard (AES). Its principal strengths are as follows in Table 1.

Table 1: Key Strengths of AES [9].

Key Strengths of AES	Features	Ref
Robust Security	• AES is highly secure and resistant to various cryptographic attacks. • Its strength lies in the complexity of its internal operations, making it computationally infeasible to break the encryption by exhaustive key search or other known attacks.	[10]
Standardization and Adoption	• AES has gained worldwide recognition and acceptance as a standard encryption algorithm. • It is widely implemented in software libraries, operating systems, and hardware devices, ensuring interoperability and compatibility across different platforms.	[11]
Efficient Performance	• AES is designed to provide efficient and fast encryption and decryption processes. • It has been optimized for both software and hardware implementations, enabling high-speed encryption without compromising security.	[12]
Flexibility	• AES supports multiple key sizes, allowing users to choose the appropriate level of security based on their requirements. • It provides a balance between security and performance, making it suitable for a wide range of applications.	[6]

Applications of AES:
In many different situations where private and secure data transmission or storage is necessary, the AES is extensively utilized. Some typical uses for AES are listed below as demonstrated in Figure 2 [13].

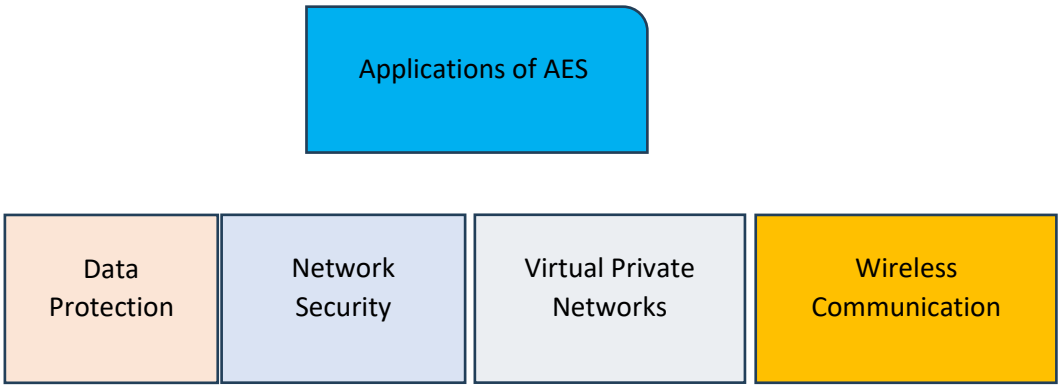


Figure 2: Applications of AES.

- Data Protection: AES is extensively used for securing sensitive data at rest, such as encrypting files and folders on storage devices or encrypting databases. It ensures that even if the data is compromised, it remains unintelligible without the decryption key.
- Network Security: AES plays a vital role in securing network communications. It is utilized in protocols like Secure Socket Layer (SSL) and Transport Layer Security (TLS) to establish secure connections between clients and servers, protecting data transmission from eavesdropping and tampering.
- Wireless Communication: AES is employed in wireless communication protocols like Wi-Fi Protected Access (WPA2) to safeguard wireless networks against unauthorized access and data interception.
- Virtual Private Networks (VPNs): AES is a fundamental component of VPN technology, ensuring the confidentiality and integrity of data transmitted over public networks.

In today's digital world, where photos play a significant role in personal and professional communication, the need for ensuring the privacy and security of sensitive images has become critical [8]. Encryption of photos provides a robust solution to protect the confidentiality of visual data, preventing unauthorized access and safeguarding personal information. In this article, we will explore the importance of encrypting photos, various encryption techniques, and the benefits of employing encryption for securing sensitive images.

The Importance of Encrypting image

1. Privacy Protection: Photos often contain personal, sensitive, or confidential information. Encrypting photos ensures that even if they are intercepted or accessed by unauthorized individuals, the content remains encrypted and unintelligible without the decryption key.

2. Data Breach Mitigation: Data breaches and hacking incidents have become common, and photos are not exempt from such threats. Encryption adds an extra layer of security, making it significantly more challenging for attackers to gain access to the visual content.

3. Prevent Unauthorized Sharing: Encrypting photos can help prevent unauthorized sharing or distribution of sensitive images. If an encrypted photo is shared without the necessary decryption key, the recipient will not be able to view the image.

Encryption Techniques and Benefits

The Encryption Techniques and Benefits are tabulated in Table 2.

Table 2: Encryption Techniques and Benefits.

Techniques and Benefits	Classifications	Remarks
Encryption Techniques	Symmetric Encryption	• Symmetric encryption uses a single key to both encrypt and decrypt the photo. • Popular symmetric encryption algorithms include (AES) and 3DES.
	Asymmetric Encryption	• It is known as public-key encryption, uses a pair of keys: a public key for encryption and a private key for decryption. • The public key is shared with others, while the private key remains securely with the owner.
	Hybrid Encryption	• Combines both symmetric and asymmetric encryption techniques. • The symmetric encryption algorithm is used to encrypt the photo.
Benefits of Encrypting	Data Confidentiality	• Encryption ensures that only authorized individuals with the decryption key can access and view the encrypted photos, maintaining the confidentiality of sensitive visual data.
	Data Integrity	Encryption can also provide data integrity, as any unauthorized modifications or tampering attempts on the encrypted photo.
	Compliance with Privacy Regulations	Encrypting photos helps individuals and organizations comply with privacy regulations.

Results and discussion

When utilizing AES to encrypt a picture as in Figure 3, the image data is split into fixed-size blocks and handled as binary data. AES encryption using a unique key is then applied to each block. Substitution, permutation, and XOR operations are used repeatedly during the encryption process to give the data a random, illegible appearance.

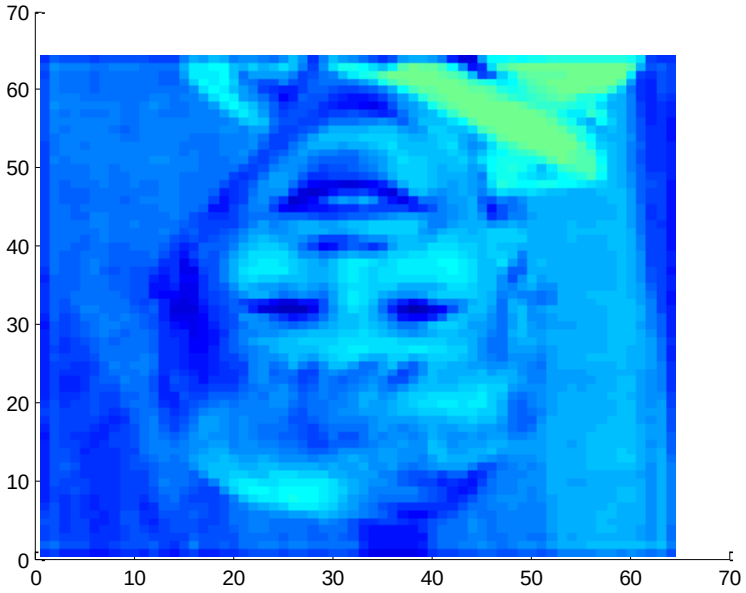


Figure 3: Sample of Encrypted Image.

The picture data as in Table 3 is converted into ciphertext the encrypted version of the image after encryption. It is not possible to read or perceive the ciphertext as an image directly. To undo the encryption and recover the original image, you'll need the matching decryption key and the AES decryption method.

Table 3: Encrypted data of the image.

	X	Y
Min	1	1
Max	64	64
Mean	32.5	32.5
Median	32.5	32.5
Mode	1	1
Std	44.55	44.55
Range	63	63

The operation of original, Encrypted, and decrypted is shown in Figure 4 along with their coding is tabulated in Table 4.

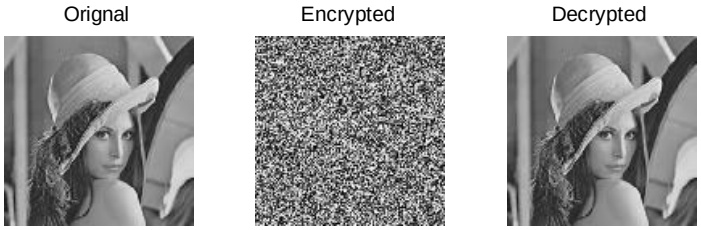


Figure 4 Original image and encrypted and decrypted image.

Table 4 correlation coefficient of original image and encrypted image.

original image		encrypted image	
1.000	0.9744	1.000	-0.0040
0.9744	1.0000	-0.0040	1.0000

Conclusion

Encrypting photos is a crucial practice to protect privacy, secure sensitive images, and mitigate the risks of unauthorized access and data breaches. The Advanced Encryption Standard (AES) has become the encryption algorithm of choice for ensuring data confidentiality and secure communication. Its robust security, standardization, and efficient performance have made it a cornerstone of modern cryptographic systems. AES continues to evolve and adapt to emerging security challenges, remaining a critical tool in protecting sensitive information in an increasingly interconnected world. For future work, by employing encryption techniques such as symmetric encryption, asymmetric encryption, or hybrid encryption, individuals and organizations can ensure the confidentiality and integrity of visual data. Implementing photo encryption not only safeguards personal information but also helps comply with privacy regulations. As the digital landscape continues to evolve, encryption remains a vital tool for preserving privacy and maintaining the security of sensitive visual content.

References

[1] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Advanced approach for encryption using advanced encryption standard with chaotic map," Int. J. Electr. Comput. Eng., vol. 13, no. 2, p. 1708, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1708-1723.

[2] C. L. Chowdhary, P. V. Patel, and K. J. Kathrotia, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," pp. 1–18, 2020, doi: 10.3390/s20185162.

[3] S. A. Ajagbe, O. D. Adeniji, A. A. Olayiwola, and S. F. Abiona, "Advanced Encryption Standard (AES)-Based Text Encryption for Near Field Communication (NFC) Using Huffman Compression," SN Comput. Sci., vol. 5, no. 1, p. 156, 2024, doi: 10.1007/s42979-023-02486-6.

[4] Z. Li et al., "Novel quantum circuit implementation of Advanced Encryption Standard with low costs," Sci. China Physics, Mech. Astron., vol. 65, no. 9, p. 290311, Sep. 2022, doi: 10.1007/s11433-022-1921-y.

[5] L. Teng, H. Li, S. Yin, and Y. Sun, "A Modified Advanced Encryption Standard for Data Security," Int. J. Netw. Secur., vol. 22, no. 1, pp. 112–117, 2020, doi: 10.6633/IJNS.202001.

[6] C. Tezcan, "Optimization of Advanced Encryption Standard on Graphics Processing Units," IEEE Access, vol. 9, pp. 67315–67326, 2021, doi: 10.1109/ACCESS.2021.3077551.

[7] P. Jindal, A. Kaushik, and K. Kumar, "Design and Implementation of Advanced Encryption Standard Algorithm on 7th Series Field Programmable Gate Array," 2020 7th Int. Conf. Smart Struct. Syst. ICSSS 2020, pp. 18–20, 2020, doi: 10.1109/ICSSS49621.2020.9202114.

[8] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit," IEEE Trans. Quantum Eng., vol. 1, pp. 1–12, 2020, doi: 10.1109/TQE.2020.2965697.

[9] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "A Polymorphic Advanced Encryption Standard – A Novel Approach," IEEE Access, vol. 9, pp. 20191–20207, 2021, doi: 10.1109/ACCESS.2021.3051556.

[10] Z. Yang, Z. Sun, T. Z. Yue, P. Devanbu, and D. Lo, "Robustness , Security , Privacy , Explainability , Efficiency , and Usability of Large Language Models for Code," 2023, doi: 10.1145/xxxxx.

[11] M. A. N. Agi and A. Kumar, "International Journal of Production Economics Blockchain technology in the supply chain : An integrated theoretical perspective of organizational adoption," Int. J. Prod. Econ., vol. 247, no. June 2021, p. 108458, 2022, doi: 10.1016/j.ijpe.2022.108458.

[12] A. Ibrahim, F. Anayi, and M. Packianather, "Detection of three-phase induction motor faults using deep network-based transfer learning techniques," in 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering, MI-STA 2022 - Proceeding, 2022, pp. 133–138. doi: 10.1109/MI-STA54861.2022.9837619.

[13] M. Abomhara, O. Zakaria, O. O. Khalifa, A. . Zaidan, and B. . Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard," Int. J. Comput. Electr. Eng., vol. 2, no. 2, pp. 223–229, 2010, doi: 10.7763/IJCEE.2010.V2.141.