CyberPeace editor@cyberpeace.net
THE CYBERPEACE JOURNAL
Supported by United Service Institution of India
Academic Partner Shah & Anchor Kutchhi Engineering College

Image Encryption and Decryption using Java Applet

Chinmay Nair
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
chinmayanand.16947@sakec.ac.in

Jalaj Mishra
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
jalaj.16946@sakec.ac.in

Samyak Jadhav
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
samyak.17244@sakec.ac.in

Soham Lad
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
soham.17251@sakec.ac.in

Pranali Pawar
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
pranali.pawar@sakec.ac.in

Meghali Kalayankar
Cyber Security
Shah and Anchor Kutchhi Engineering College
Mumbai, India
Meghali.kalyankar@sakec.ac.in

Abstract: ***In the current digital age, protecting the privacy and security of data,*** **especially visual content like images, has become paramount. To address this need, this paper presents a novel Image Encryption System implemented using Java Applet. The proposed system employs advanced cryptographic algorithms to encrypt images, ensuring robust protection against unauthorized access and data breaches. The encryption process begins by converting the image into a digital format, followed by partitioning it into blocks. Each block undergoes encryption using a mix of symmetric and asymmetric encryption methods, such as Rivest-Shamir-Adleman's (RSA) and Advanced Encryption Standard's (AES), respectively. Furthermore, a safe key management system is integrated to generate and manage encryption keys, further enhancing the system's security. To facilitate user interaction and ease of use, the encryption system is implemented as a Java Applet, providing a platform-independent solution accessible via web browsers. Users can securely upload their images through the applet interface, initiate the encryption process, and receive the encrypted output for safe storage or transmission. Furthermore, the system in corporate features for decryption, enabling authorized users to reverse the encryption.**

Keywords—Image Encryption, AES Algorithm, Web Browser, Java Applet, Robust protection

I. INTRODUCTION

The protection and integrity of data are of utmost importance. As almost all data today is shared via computer networks, there's been a significant rise in network attacks. To protect data from various attackers, it needs to be encrypted and securely stored before transmission. Encryption works by obscuring data, converting the original text into cipher text. Various algorithms are used in encryption to alter data into different formats. Cryptographic methods use a pair of keys, each with distinct characters, for both encrypting and decrypting data. The plain text is encoded into cipher text with a key, then decoded back to plain text to complete the decryption. However, it's crucial to find a balance between security and ease of use., as multi-factor authentication systems can be more cumbersome for users. Transmitting and storing data in a way that only authorized users may read is known as cryptography. The science of protecting data by encoding it into an unintelligible form is called cryptography. Sensitive data can be safely protected by using mathematical techniques for both encryption and decoding. Both the encryption and decryption processes require the key value. The difficulty of deriving the original text and determining the key value is what gives the algorithm its potency. The algorithm can be roughly categorized as symmetric or asymmetric based on the keys. An algorithm that employs the same keys for encryption and decryption is known as symmetric. The two subtypes of symmetric algorithms are stream and block encryptions. A stream cipher works on a single piece of data, while a block cipher works on a block of data byte of information. An asymmetric algorithm encrypts data using one key, and decrypts it using the other. To prevent the message from being decoded, the key needs to be kept a secret. Authentication (demonstrating one's identity), non-repudiation (ensuring the recipient knows the sender is not pretending), integrity (ensuring the data is

accurate, correct, and reliable), and privacy/confidentiality (ensuring the message is only read by the intended recipient) are the four main goals of cryptography.

II. LITERATURE REVIEW

In the current digital era, when visual content is king, a primary mode of communication, ensuring the confidentiality and integrity of images has become paramount. From personal photographs to sensitive corporate data, the need to safeguard visual information from unauthorized access and tampering is ever-present. In response to this imperative, the integration of strong encryption methods, such the Advanced Encryption Standard (AES) algorithm, emerges as a critical solution for securing image data. Maintaining the Integrity of the Specifications Chinese textile and apparel industry annual report: social responsibility, China National Textile and Apparel Council (CNTAC), 2007, Corporate social responsibility (CSR) plays a crucial role in modern business practices. In 'Corporate Social Responsibility: Achieving Success through Altruism,' Falck and Heblich (2007) discuss how altruism can drive business success. Godfrey and Hatch's 2007 study in the Journal of Business Ethics explores CSR as a key component of 21st-century business strategy. The International Academy of Science, Technology, and Engineering's 2009 publication further examines the importance of CSR in modern industry. Carroll's 1999 paper in *Business and Society* traces the evolution of CSR concepts. Additionally, Leitão and Silva's work highlights the intersection of CSR and social marketing, particularly within academic institutions Roles in Promoting Public Policies? November 7, 2007, posted as MPRA Document 2954. At the heart of this endeavor lies the AES algorithm, renowned for its strength, efficiency, and widespread adoption in various security applications. Originally established as a federal measure that the US government uses to protect sensitive data, AES has since gained global recognition as a cornerstone of modern encryption practices. Its ability to withstand cryptographic attacks and maintain computational efficiency makes it an ideal candidate for protecting image data from unauthorized access or manipulation.

III. METHODOLOGY

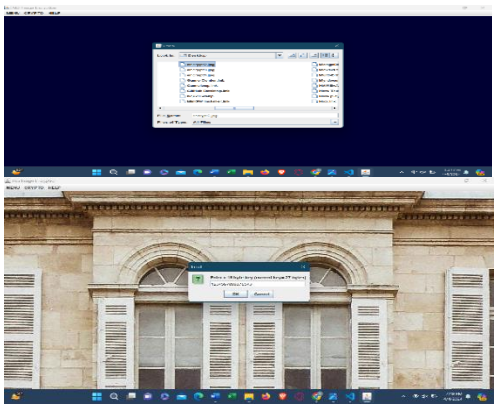
The objective of the project is to enhance the security of digital images by implementing robust encryption and decryption techniques using the Advanced Encryption Standard (AES) algorithm. The focus is on preventing unauthorized access and maintaining confidentiality throughout both transmission and storage processes. The project is designed to safeguard confidentiality of sensitive visual information contained in digital images. By encrypting images using AES, the project ensures that only authorized users with the decryption key can access and view the original content, thereby safeguarding against unauthorized access and data breachesAbbreviations and Acronyms. The main goal of the project is to enhance the security of digital images by applying Advanced Encryption for strong encryption and decryption processes. This system secures images by encrypting them, thereby blocking unauthorized access and ensuring that only users with proper authorization can view the content correct decryption key can view the content. Another purpose is to preserve the confidentiality of sensitive visual information contained in digital images. Encryption ensures that even if the images are intercepted during transmission or stored on insecure servers, the content remains protected and inaccessible to unauthorized parties. The project aims to protect the integrity of digital images by ensuring that they remain unaltered and tamper-proof during transmission and storage. Decryption using the correct key verifies the authenticity of the images, preventing unauthorized modifications or tampering. Equations

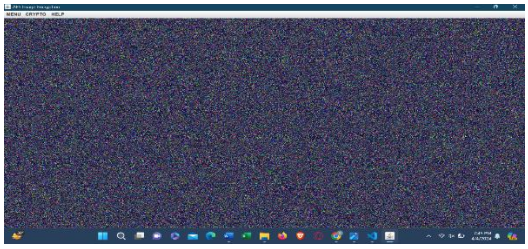
IV. USING THE TEMPLATE

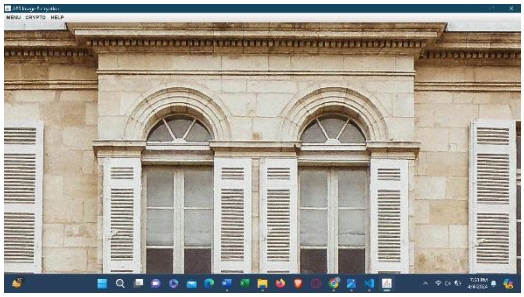
The project aim is the implementation of image encryption and decryption, using the Advanced Encryption Standard (AES) The approach to image encryption and decryption marks a significant step forward in data security, especially in protecting sensitive visual information transmitted across digital platforms. Through comprehensive research, development, and assessment, systems utilizing AES for image encryption and decryption have proven to be effective, efficient, and resilient in guarding digital images against unauthorized access and manipulation. Implementing AES offers numerous advantages, such as enhanced confidentiality, integrity, and authenticity of transmitted images. By employing AES encryption, individuals and organizations can trust that sensitive visual data is shielded from unauthorized viewers and potential threats, ensuring privacy and confidentiality. Furthermore, the future potential for AES-based image encryption and decryption is bright, with possibilities for innovation and integration with cutting-edge technologies like quantum-resistant cryptography, blockchain, and artificial intelligence. Ongoing research and development in this area will continue to push the boundaries of data security practicesand address evolving challenges in image communication and storage. Overall, Using the Advanced Encryption Standard (AES) method for image encryption and decryption. AES algorithm offers a reliable and efficient solution for securing digital images in various domains and applications. By prioritizing data security, confidentiality, and integrity, AES-based image encryption systems contribute to building trust and confidence in digital communication channels, fostering a safer and more resilient digital ecosystem.

V. RESULT

Overall, Utilizing the Advanced Encryption Standard (AES) technique for image encryption and decryption provides a dependable and effective means of securing digital images across different fields and applications. By focusing on data security, confidentiality, and integrity, AES-powered image encryption systems help establish trust and confidence in digital communication channels, promoting a more secure and robust digital environment.







VI. CONCLUSION

In conclusion, the implementation of Using the Advanced Encryption Standard (AES) method for image encryption and decryption represents a significant advancement in data security practices, particularly in safeguarding sensitive visual information transmitted over digital channels. Through careful research, development, and testing, image encryption and decryption systems utilizing AES have proven to be effective, efficient, and resilient in safeguarding digital images against unauthorized access and tampering.. The adoption of AES brings several key benefits, including enhanced confidentiality, integrity, and authenticity of transmitted images. By encrypting images using AES, both individuals and organizations can guarantee the privacy and confidentiality of critical visual data by keeping it shielded from prying eyes and potential dangers. Furthermore, the application of AES for image encryption and decryption in the future is promising, with opportunities for innovation and integration with emerging technologies such as quantum-resistant cryptography, blockchain, and artificial intelligence. Continued research and development efforts in this field will further advance data security practices and address evolving challenges in image communication and storage. Overall, employing the Advanced Encryption Standard (AES) technique for image encryption and decryption provides a trustworthy and effective approach to safeguarding digital images across various fields and applications. By emphasizing data security, confidentiality, and integrity, AES-driven image encryption systems play a crucial role in enhancing the security of digital communication channels.

REFERENCES

[1] A Novel Chaotic Key-Based Scheme for Image Encryption and Decryption, Jui-Cheng Yen and Jim-In Guo (2000). An Adapted AES-Based Image Encryption Algorithm.

[2] M. Zeghid, M. Machhout, L. Khiri, A. Baganne, and R. Tourki, 2007.

[3] “Secure Image Encryption Using Aes,” P. Radhadevi, P. Kalpana, 2012.

[4] "Image Encryption and Decryption Using Aes Algorithm," Roshni Padate and Aamna Patel, 2014.

[5] "Symmetric-Key Block Crypher for Image and Text Cryptography," Jose´ J. Amador, Robert W. Green, 2005.

[6] "Image Encryption for Secure Internet Multimedia Applications," by Philip P. Dang and Paul M. Chau, published in 2000. 7.

[7] "Image Encryption using Simplified Data Encryption Standard (S-DES)" by Sanjay Kumar and Sandeep Srivastava, 2014.

[8] Kumar Kundan Using the Advanced Encryption Standard, Rameshwar Saraf, Vishal Prakash Jagtap, and Amit Kumar Mishra decrypted text and images in 2014.

[9] Rahul Gupta and Soumiya Rasheed "AES Algorithm-Based Image Encryption Simulation," 2011.

[10] BG Subramanyan, VM Chhabria, and TG Sankar Babu, "AES Key Expansion-Based Image Encryption," 2011.