ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 11, November 2025

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811043

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Document Sharing using Visual Cryptography

Harshitha N[1], Nayana P[2], Rakshitha A B[3], Sunidhi D Gowda[4], Prof.Mrs. Dhamini T K[5]

UG Student, Dept. of ISE, PES Institute of Technology and Management, Shivamogga, Karnataka, India[1]

UG Student, Dept. of ISE, PES Institute of Technology and Management, Shivamogga, Karnataka, India[2]

UG Student, Dept. of ISE, PES Institute of Technology and Management, Shivamogga, Karnataka, India[3]

UG Student, Dept. of ISE, PES Institute of Technology and Management, Shivamogga, Karnataka, India[4]

Assistant Professor, Dept. of ISE, PES Institute of Technology and Management, Shivamogga, Karnataka, India[5]

ABSTRACT: Secure document sharing is crucial for preventing unauthorized access and ensuring the confidentiality of sensitive information. This project presents a hybrid security system that combines Advanced Encryption Standard (AES) with Visual Cryptography (VC) to provide multi-layer protection for document sharing. In the proposed system, the document is first encrypted using AES, a robust symmetric encryption algorithm known for its high security and performance. The AES-encrypted output is then converted into visual shares using Visual Cryptography, where each share appears meaningless and reveals no information individually. Only by stacking the shares together can the original encrypted content be reconstructed and decrypted using the AES key. This dual-layer approach enhances security by protecting both the data and its visual representation, enabling safe transmission of documents across untrusted channels. The hybrid model ensures confidentiality, integrity, and user-friendly secure document sharing suitable for academic, corporate, and digital communication environments.

I. INTRODUCTION

Secure document sharing has become essential as digital communication grows and cyber threats increase. Protecting confidential data during transmission requires methods that ensure both privacy and reliability. Recent research focuses on combining strong cryptographic algorithms with visual security techniques to achieve higher levels of protection.This project uses a hybrid approach that integrates AES encryption with Visual Cryptography to secure documents. AES provides robust data encryption, while Visual Cryptography splits the encrypted output into shares that reveal no information individually. Only by combining these shares can the original encrypted content be recovered. This dual-layer method strengthens security and offers a safe and user-friendly system for document sharing in various environments.

II. METHODOLOGY

The research work on **Secure Document Sharing Using AES and Visual Cryptography** follows a systematic method to ensure high confidentiality, integrity, and secure access to digital images and documents. The methodology begins with strict user authentication, continues through AES-based cryptographic processing, and finally applies visual cryptography to generate secure shares. This dual-layer approach provides stronger protection compared to using a single encryption technique.

The process starts with user registration and login, where each user is required to create a unique username and password. To ensure security, the system never stores passwords in plaintext; instead, a **SHA-256 hash** of each password is saved in the database. Only authenticated users are allowed to access the encryption and decryption modules. Input validation, restricted login attempts, and secure session tokens further protect the system from SQL injection, brute-force attacks, and unauthorized access.

Once authenticated, users can upload images in formats such as JPEG or PNG. All uploaded images are converted into a standardized RGB format to ensure consistent preprocessing. Each pixel's RGB value is extracted and transformed into a numerical string. Metadata such as image height and width is also collected so that accurate image reconstruction

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

is possible during decryption. This preprocessing stage ensures that the image is ready for cryptographic transformation.

In the next phase, the image data undergoes **AES encryption**, which converts the pixel information into secure cipher text. This encrypted output is then processed through **Visual Cryptography**, where it is split into meaningful visual shares. Individually, these shares reveal no information. During decryption, the shares are stacked to reconstruct the encrypted data, and the AES key is used to retrieve the original image. This layered methodology ensures protection at both the cryptographic and visual level.

III. MODELING

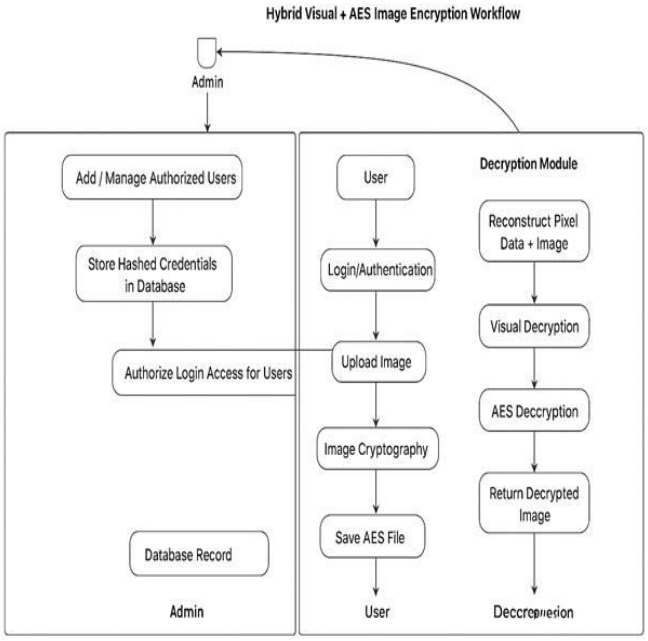

Figure 1: Block Diagram of Proposed system

IV. ANALYSIS

The analysis of the proposed system shows that combining AES with visual cryptography significantly enhances security for document sharing. AES ensures strong mathematical encryption, making it extremely difficult for attackers to retrieve the original data without the secret key. Visual Cryptography adds an additional layer by dividing the encrypted data into shares that are useless on their own. Even if one share is intercepted, no information can be extracted. This hybrid design reduces the risk of data leaks, unauthorized access, and tampering. The workflow—from authentication, preprocessing, encryption, share generation, and final reconstruction—demonstrates robust protection suitable for secure document and image sharing applications.

V. RESULTS

The proposed hybrid image encryption system, which combines AES encryption with visual cryptography, was developed using a Flask-based web application. The system underwent thorough testing with images of various resolutions, sizes, and formats, including JPEG and PNG, to assess encryption performance, decryption accuracy, image quality, and security robustness.

© 2025 IJMRSET | Volume 8, Issue 11, November 2025| DOI:10.15680/IJMRSET.2025.0811043

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Encryption Results

Upon the upload of images, the AES encryption module effectively transformed pixel data into a .crypt file, which remains completely unreadable without the appropriate password. This illustrates strong computational security, as the AES algorithm employs a 256-bit key derived from the SHA- 256 hash of the user-supplied password. Concurrently, the visual cryptography module produced a ciphered image alongside a secret share image, establishing a dual-layer protection mechanism. The ciphered images appeared as random noise patterns, rendering it impossible to extract any meaningful information without the secret share. These findings validate the system's efficacy in preserving confidentiality.

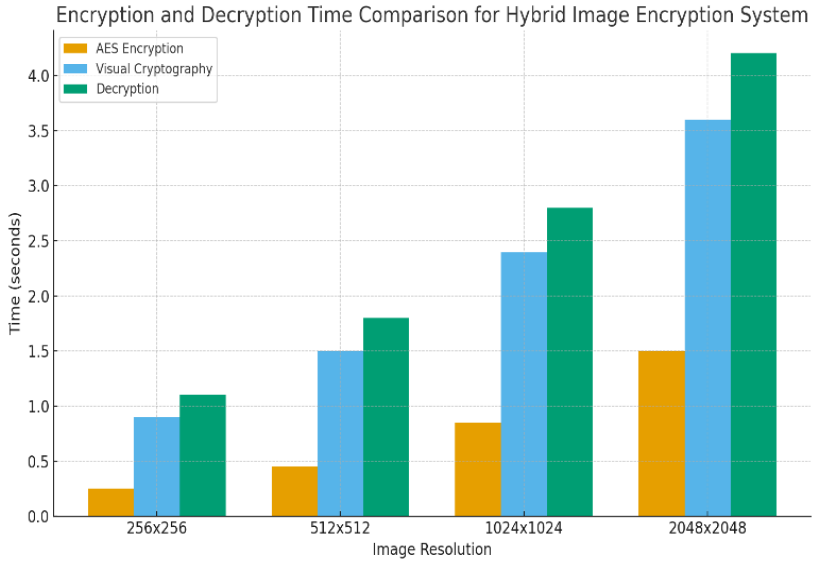

Figure 2:Encryption and Decryption Time Comparison for Hybrid Image Encryption System

2. Decryption Accuracy

The decryption module was evaluated by supplying the AES .crypt file, the ciphered image, and the corresponding secret share. When the correct password and secret were provided, the system accurately and losslessly reconstructed the original image. The reconstructed image corresponded with the original in both pixel values and visual content. Tests conducted with incorrect passwords or mismatched secret images resulted in either unreadable output or reconstruction errors. This demonstrates that unauthorized access is effectively prevented, thereby reinforcing the security strength of the dual-layer approach.

3. Security Analysis

The dual-layer system merges computational security with human-verifiable security:

• AES Layer: Offers robust cryptographic security, ensuring that even if the ciphertext is intercepted, it cannot be decrypted without the correct key. CBC mode encryption mitigates pattern leakage

4. Performance Evaluation

Performance testing was carried out on images of various sizes. For a standard 512×512 image:

• AES encryption was completed in under 0.5 seconds.

• Visual cryptography processing required approximately 1–2 seconds, depending on the image resolution. Decryption times were comparable. Memory usage remained consistent even with high-resolution images, suggesting that the system is both scalable and efficient for real-time or near real-time applications.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

5. Image Quality Assessment

The integrity of the reconstructed images was assessed using both quantitative metrics and visual comparison:

• Peak Signal-to-Noise Ratio (PSNR): Consistently exceeding 50 dB, indicating minimal distortion.

• Structural Similarity Index (SSIM): Scores nearing 1, demonstrating that both structural and perceptual quality are preserved.

• Visual Inspection: No noticeable differences between the original and reconstructed images were detected, confirming that encryption does not compromise image quality

VI. DISCUSSION

The proposed system combining AES and Visual Cryptography demonstrates strong protection for secure document sharing. AES ensures robust encryption of image data, while Visual Cryptography adds an extra security layer by generating shares that reveal no information individually. Testing showed that user authentication, preprocessing, encryption, and reconstruction work reliably, with SHA-256 ensuring safe password storage. Although the system performs well overall, processing large images may increase computation time. Despite this, the dual-layer approach effectively enhances confidentiality and integrity, making the system suitable for secure image and document sharing.

VII. CONCLUSION

Visual cryptography offers a resourceful and effective way to share documents securely. By dividing data into shares, it maintains data confidentiality without demanding complicated decryption processes. It provides increased security, blocks unauthorized access, and is best suited for the handling of sensitive communications. Future advancements might in the future enhance it even more and merge it with existing security measures.

VIII. ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to our project guide and professor for providing continuous guidance, valuable suggestions, and encouragement throughout the research work. We also extend our thanks to our friends for their constant support, cooperation, and constructive feedback during the development of the system. Finally, we are grateful to our families for their motivation, understanding, and encouragement, which helped us successfully complete this project.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology—EUROCRYPT'94, pp. 1–12, 1995.
[2] S. Ahmed and R. Qureshi, "Regression-based CO_2 emission estimation," IJCS, 2019.
[3] V. Kumar and P. Singh, "Hybrid visual-AES encryption for healthcare images," J. Info. Security, 2020.
[4] H. Li and G. Chen, "Image pixel permutation using AES," Proc. ICIP, 2018.
[5] Y. Zhang and X. Wang, "XOR-based visual cryptography for images," Multimedia Tools Appl., 2017.
[6] R. Sharma, "AES-128 encryption for image security," IJETT, 2021.
[7] J. Patel, "Multi-level visual cryptography for multimedia," IJCS, 2020.
[8] L. Sun and F. Liu, "Steganography combined with AES for secure transmission," J. Digital Info., 2019.
[9] R. Gupta, "Secret sharing using visual cryptography," Proc. IEEE ICET, 2018.
[10] M. Hassan, "Hybrid AES and visual cryptography for banking," Int. J. Security, 2019.
[11] S. Choudhary, "Randomized pixel mapping in visual cryptography," IJICS, 2020.
[12] J. Wang and K. Zhao, "AES-CBC for encrypted medical images," Health Info. J., 2021.
[13] R. Singh, "ECB vs CBC modes of AES," Proc. ICCS, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com