ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr953

Image Encryption and Decryption using AES Algorithm in Java

Shantanu Gade[1]; Burkule Pranjal[2]

[1]Department of Computer Engineering, JSPM'S Bhivrabai Sawant Polytechnic , Pune, Maharashtra, India
[2]Ex- Professor, Department of Computer Engineering, JSPM'S Bhivrabai Sawant Polytechnic , Pune, Maharashtra, India

Publication Date: 2025/04/28

Abstract: This paper presents a Java-based tool for image encryption and decryption using the Advanced Encryption Standard (AES) in GCM mode. The application features an intuitive Swing-based GUI that supports image selection via drag-and-drop or file browsing, with real-time progress updates. Secure key derivation is achieved using PBKDF2 with HmacSHA256, combined with a random 16-byte salt and a 12-byte initialization vector (IV). Experimental results indicate an average encryption time of 318 ms and a decryption time of 137 ms, demonstrating both efficiency and robust security while maintaining high image fidelity.

Keywords*: Image Encryption; AES; Java; GCM; PBKDF2; Cryptography; Swing GUI.*

How to Cite: Shantanu Gade; Burkule Pranjal (2025) Image Encryption and Decryption using AES Algorithm in Java *International Journal of Innovative Science and Research Technology*, 10(4), 1520-1522.
https://doi.org/10.38124/ijisrt/25apr953

I. INTRODUCTION

The increasing use of digital images necessitates secure encryption methods to prevent unautho- rized access. Traditional text encryption methods are inefficient for images due to their larger size and structure. This paper presents an encryption and decryption tool using AES in GCM mode, combined with PBKDF2 for secure key derivation.

II. METHODOLOGY

The system is implemented as a Java-based desktop application, featuring encryption and de- cryption modules.

➢ *System Overview*

Users select images using drag-and-drop or file browsing. The encryption process involves:

- Converting the image into a byte array.
- Generating a 16-byte salt and a 12-byte IV.
- Deriving a key from the password using PBKDF2 with HmacSHA256.
- Encrypting the byte array using AES in GCM mode.
- Saving the encrypted file along with the salt and IV. Decryption reverses these steps to reconstruct the original image.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr953

➢ *Flowchart*

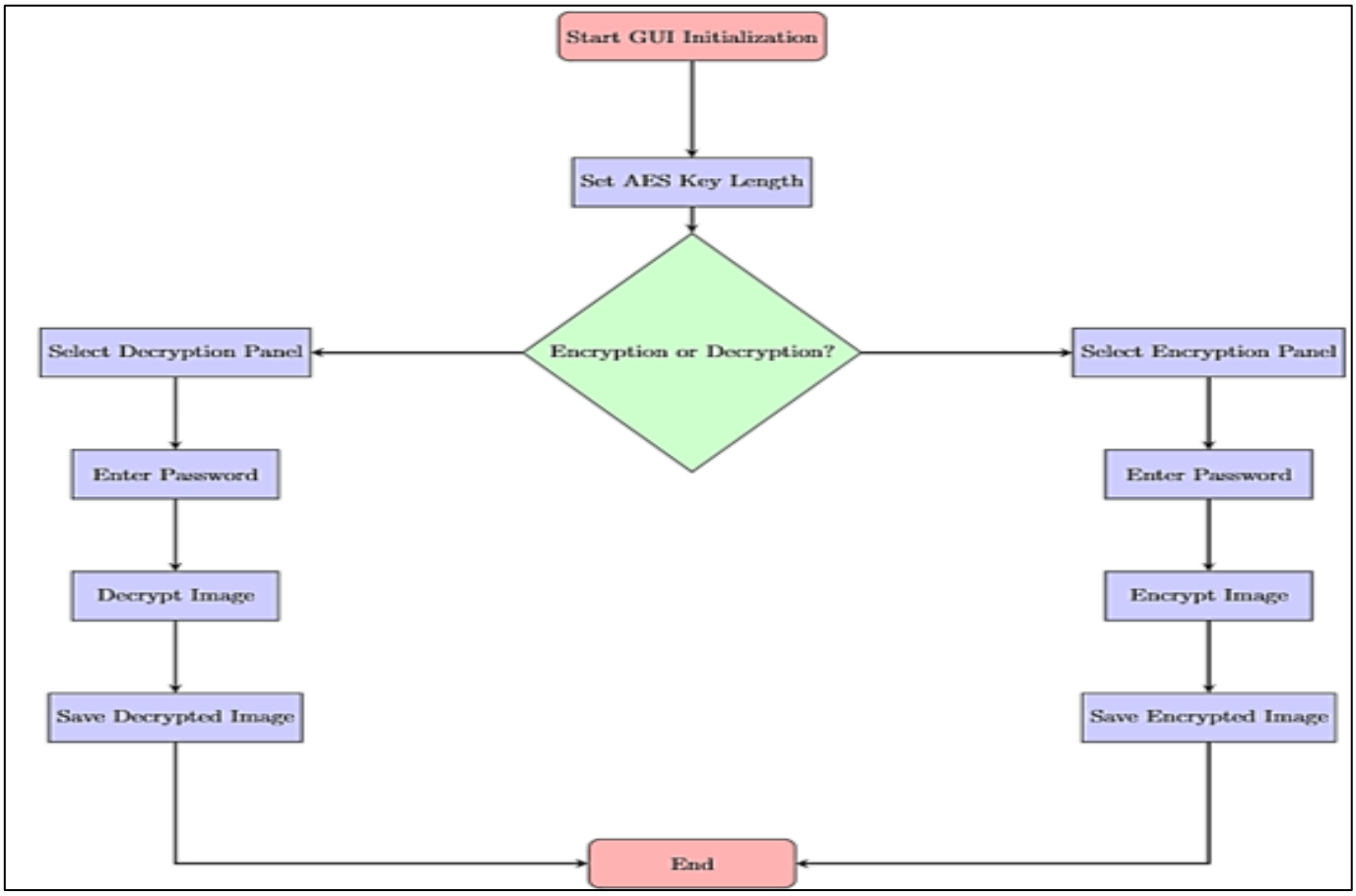

Fig 1 Flowchart of the encryption and decryption process.

III. RESULTS AND DISCUSSION

➢ *Output and Performance*

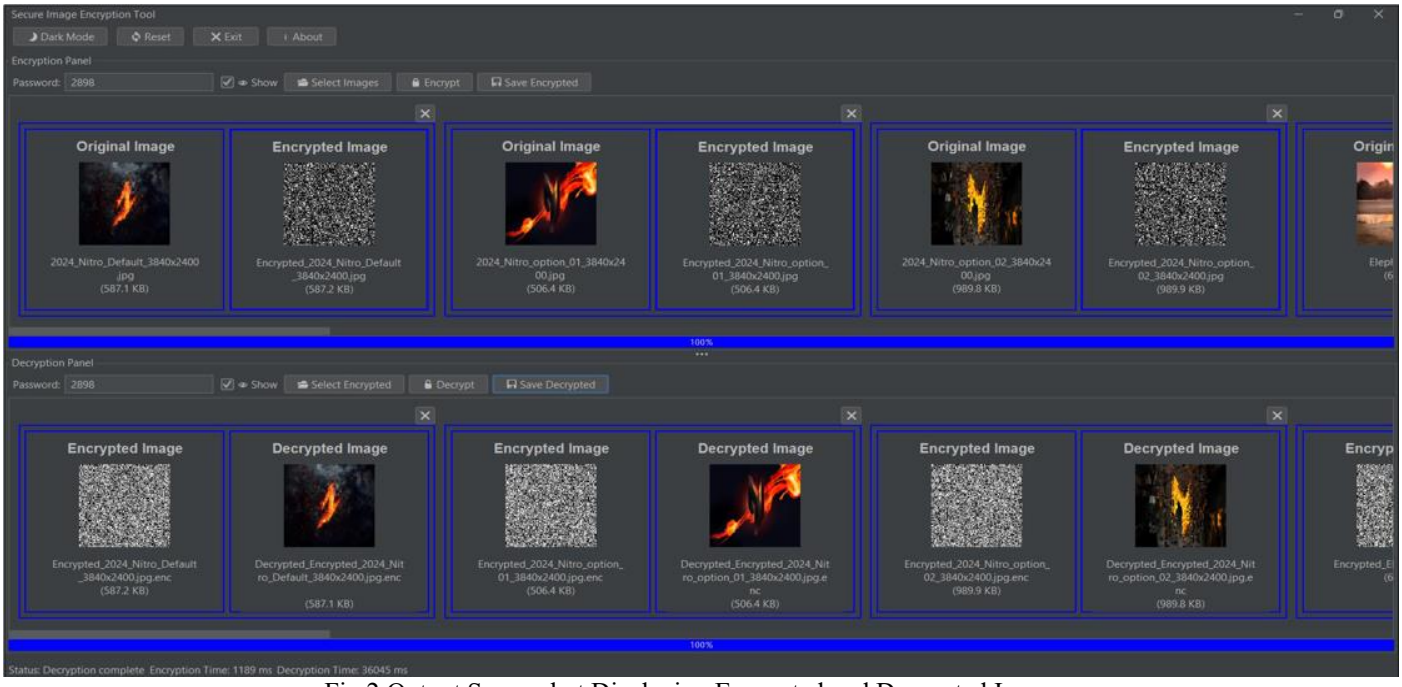

Fig 2 Output Screenshot Displaying Encrypted and Decrypted Images.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr953

- *Performance Metrics*

Table 1 Performance Metrics

SN.	Parameter	Value
1	Encryption Time	318 ms
2	Decryption Time	137 ms
3	Image Fidelity Score	>99%
4	Key Strength	128/192/256-bit

IV. CONCLUSION

This paper presents a secure and efficient image encryption and decryption tool developed in Java using AES in GCM mode. The tool provides a user-friendly GUI while ensuring secure encryption via PBKDF2-derived keys and dynamically generated salts and IVs. With an av- erage encryption time of 318 ms and decryption time of 137 ms, the system is both effective and efficient. Future enhancements may include additional file format support, refined key management, and cloud storage integration.

ACKNOWLEDGEMENTS

The authors sincerely express gratitude to their guide, **Prof. Burkule Pranjal**, and the faculty of JSPM'S Bhivrabai Sawant Polytechnic for their support throughout this research.

REFERENCES

[1]. T. Mohana Priya, Dr. M. Punithavalli, & Dr. R. Rajesh Kanna, *Machine Learning Algo- rithm for Enhanced Support Vector Machine Technique to Predict Stress*, Global Journal of Computer Science and Technology, Vol. 20, Issue 2, 2020, pp. 12–20.

[2]. Ganesh Kumar and P. Vasanth Sena, *Novel Artificial Neural Networks and Logistic Approach for Detecting Credit Card Deceit*, International Journal of Computer Science and Network Security, Vol. 15, Issue 9, 2015, pp. 222–234.

[3]. Gyusoo Kim and Seulgi Lee, *2014 Payment Research*, Bank of Korea, Vol. 2015, No. 1, Jan. 2015.

[4]. Chengwei Liu et al., *Financial Fraud Detection Model: Based on Random Forest*, Interna- tional Journal of Economics and Finance, Vol. 7, Issue 7, 2015, pp. 178–188.