ISSN: 3107-6513

Design and Implementing of An AI-Based Image Authenticity Detection System

Nikhil R Babu[#1], Dr. B. Suresh[*2]
[*1]B.Sc. Internet of Things, Final Year, Department of Internet of Things and AIML, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India.
[*2]Assistant Professor, Department of Internet of Things and AIML, Nehru Arts And Science College, Coimbatore, Tamil Nadu, India.

Abstract:

The rapid growth of digital communication and multimedia data exchange, ensuring secure image transmission has become an important challenge. Traditional image encryption methods mainly focus on protecting confidentiality but do not verify whether the transmitted image has been tampered with during communication. Additionally, conventional static password-based authentication systems are vulnerable to security threats such as password theft, replay attacks, and keylogging.

To address these issues, an AI-based secure image transmission system with advanced authentication mechanisms is proposed. The system uses differentiated virtual passwords, secret functions, and codebook-based authentication to strengthen user security and prevent unauthorized access. Instead of static passwords, a dynamic virtual password is generated for each login session using a user-specific secret function and a periodically updated codebook. This dynamic authentication approach prevents attackers from reusing intercepted login credentials.

For secure communication, images are encrypted before transmission to protect confidentiality. At the receiver side, an Artificial Intelligence-based attack detection module analyzes the received image before decryption. The AI model detects possible attacks such as noise injection, blurring, cropping, and tampering. Decryption is performed only when the image is verified as safe, ensuring integrity and reliability in secure image transmission.

Keywords: *Image Encryption, Artificial Intelligence, Virtual Password, Secure Transmission, Attack Detection, Authentication System.*

INTRODUCTION

With the rapid growth of digital communication and multimedia data exchange, ensuring the secure transmission of images has become a critical challenge. Conventional image encryption techniques mainly focus on maintaining confidentiality but do not verify whether the transmitted image has been tampered with or attacked during communication. In addition, traditional static password-based authentication systems are vulnerable to several security threats such as password theft, replay attacks, and keylogging, which may lead to unauthorized access and data compromise.

To overcome these limitations, an AI-based secure image transmission system with advanced authentication mechanisms is proposed. The system integrates differentiated virtual passwords, secret little functions, and codebook-based authentication to strengthen user verification and prevent unauthorized access. Instead of relying on static passwords, the system generates a dynamic virtual password for each login session using a user-specific secret function and a periodically updated codebook, ensuring that intercepted credentials cannot be reused by attackers.

SYSTEM ANALYSIS

- Requirement analysis is the process of identifying and documenting the needs and expectations of users from a system. It helps developers understand what functions the system should perform and the conditions under which it should operate. Proper requirement analysis ensures that the system is designed according to user needs and

operates efficiently in real-world environments.

- In this project, requirement analysis focuses on identifying the functional and non-functional requirements needed to design and develop an Automatic Wet and Dry Waste
- Segregation System. The main objective of the system is to automatically detect and separate wet and dry waste using sensors, microcontrollers, and mechanical components. This helps reduce manual work and improves waste management efficiency.
- The system should be able to detect the type of waste material placed in the bin using appropriate sensors such as moisture sensors and proximity sensors. Based on the sensor data, the microcontroller processes the information and activates the mechanism to direct the waste into the correct container. This automated process ensures accurate waste segregation and helps maintain cleanliness in the environment.

SYSTEM FLOW DIAGRAM

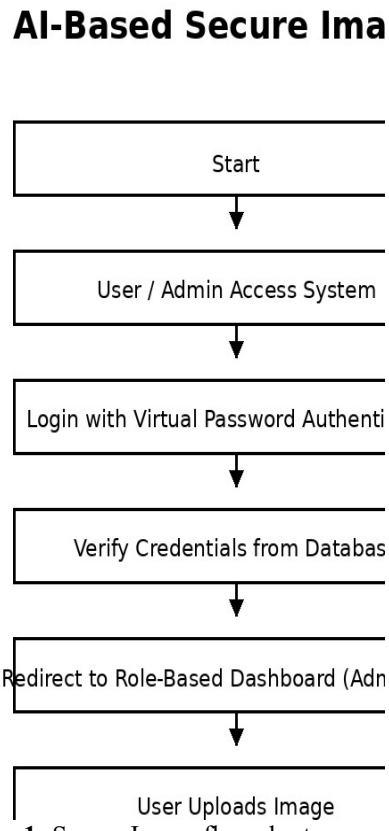

Figure 1: Secure Image flow chart

SYSTEM ARCHITECTURE

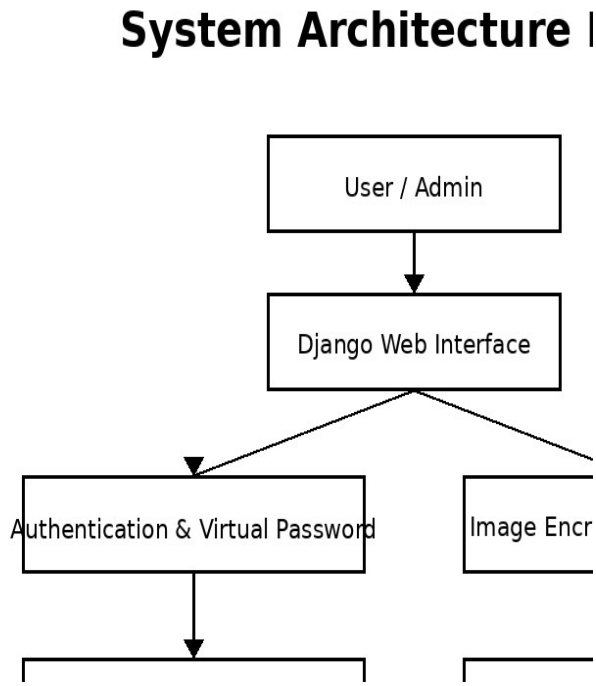

Figure 2: AI System Image Architecture Diagram

RESULT AND DISCUSSION

- The proposed AI based secure image transmission system with advanced authentication mechanisms was implemented and tested to evaluate its performance, security, and reliability. The system integrates encryption techniques, artificial intelligence based attack detection, and role-based access control to ensure secure image transmission. Several experiments were conducted to verify the effectiveness of the system in protecting image data and detecting potential attacks during the transmission and storage process.
- During testing, users were able to successfully upload images through the secure interface. The system performed pixel-level encryption using XOR-based encryption before storing the images on the server. The encrypted images were stored separately from the encryption keys, which improved the security of the stored data. When authorized users requested image retrieval, the system verified user identity and ownership before performing decryption. The results showed that the

encryption and decryption processes were performed efficiently without significant delay, ensuring smooth user experience while maintaining strong security.

- The AI-based attack detection module was evaluated by simulating different types of attacks such as image corruption, noise injection, and pixel manipulation. The system analyzed encrypted image patterns and statistical features to detect abnormalities. Experimental results showed that the system was able to correctly identify tampered images and block the decryption process when an attack was detected. This prevented compromised images from being accessed or displayed, thereby maintaining the integrity of the image data.
- The role-based access control mechanism also worked effectively by restricting system functions based on user roles. Normal users were allowed to upload and retrieve their own images, while administrators were provided with additional privileges such as monitoring logs and simulating attacks. The feedback module allowed users to report issues and suggestions, which contributed to improving system usability and reliability.
- Overall, the results demonstrate that the proposed system provides a secure and efficient environment for image transmission. The combination of encryption techniques, AI-based attack detection, and advanced authentication mechanisms significantly enhances the protection of sensitive image data. The system successfully maintains confidentiality, integrity, and controlled access, making it suitable for applications that require secure image communication such as medical imaging systems, secure data sharing platforms, and digital forensic environments.

CONCLUSION

The AI-Based Secure Image Transmission System successfully addresses the growing need for protecting sensitive image data in modern digital communication environments. By integrating image encryption with intelligent attack detection mechanisms, the system ensures not only confidentiality but also integrity and reliability of image data.

The use of virtual password-based authentication strengthens user security and minimizes the risk of password theft and replay attacks. Role-based access control enables secure separation of privileges between administrators and users, while encrypted image storage prevents unauthorized access to original data. The AI-based attack detection module effectively identifies tampering or corruption before decryption, thereby preventing compromised images from being accessed.

Additionally, the admin attack simulation panel allows controlled testing of system robustness, and the feedback module enhances user interaction and system improvement. The rich and responsive user interface improves usability and transparency. Overall, the proposed system provides a secure, intelligent, and user-friendly platform for image transmission and storage.

Although the proposed system achieves its intended objectives, several improvements can be made in the future to enhance its performance, scalability, and security. Advanced deep learning models such as Convolutional Neural Networks (CNNs) can be integrated for more accurate image tampering detection. The system can also be extended to support additional multimedia formats like video and audio encryption. Security can be further improved by implementing multi-factor authentication (MFA) and blockchain-based storage for tamper-proof audit logs. In addition, cloud-based deployment, real-time attack alerts, and performance optimization can help the system handle large-scale image datasets more efficiently.

REFERENCES

1. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 7th Edition, 2017.
2. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 2nd Edition, 2015.

ISSN: **3107-6513**

3. R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Pearson Education, 4th Edition, 2018.
4. A. K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall, 2014.
5. S. Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy," *Technical Report*, Chalmers University of Technology, 2000.
6. Chandramouli, R., and Memon, N., "Analysis of LSB Based Image Steganography Techniques," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 539–543, 2001.
7. Patcha, A., and Park, J., "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," *Computer Networks*, Elsevier, vol. 51, no. 12, pp. 3448–3470, 2007.
8. Goodfellow, I., Bengio, Y., and Courville, A., *Deep Learning*, MIT Press, 2016.
9. Django Software Foundation, "Django Documentation," https://docs.djangoproject.com/
10. Oracle Corporation, "MySQL 8.0 Reference Manual," https://dev.mysql.com/doc/
11. OpenCV Contributors, "Open Source Computer Vision Library," https://opencv.org/
12. Scikit-learn Developers, "Machine Learning in Python," https://scikit-learn.org/