International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

Advanced Image Encryption and Decryption using Open CV

N. Aravindhan[1], V. Mallika[2]

[1]*Assistant Professor, Department of Master of Computer Applications, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

[2]*MCA, Department of Master of Computer Applications, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India.*

***Abstract*-- The rapid growth of digital communication and online data sharing has increased the importance of protecting digital images from unauthorized access and cyber threats. Images are widely used in healthcare, banking, military communication, cloud storage, and social media platforms, making image security a critical concern in modern systems. This project focuses on advanced image encryption and decryption using OpenCV and Python to provide secure image transmission and storage. The proposed system converts original images into encrypted formats using pixel manipulation, XOR operations, and key-based transformation techniques. The encryption process makes the image unreadable to unauthorized users, thereby ensuring confidentiality and data protection. During the decryption phase, the encrypted image is restored to its original form using the correct secret key. OpenCV is used for efficient image processing, pixel extraction, and image reconstruction operations. The system is designed to achieve strong security with faster processing speed and accurate image recovery. Experimental analysis shows that the proposed method effectively protects image data while maintaining image quality after decryption. The developed solution can be applied in secure communication systems, medical image protection, military applications, cloud security, and confidential digital data management environments.**

***Keywords* -- Image Encryption, Image Decryption, OpenCV, Python Programming, Digital Image Security, Pixel Manipulation, Cryptographic Techniques, Secure Data Transmission, Image Processing, Confidential Data Protection, XOR Encryption, Pixel Shuffling, Cybersecurity, Secret Key Authentication, Secure Image Storage**

I. Introduction

Digital images have become an important part of modern communication systems and are widely used in healthcare, banking, military services, cloud computing, education, and social media platforms. As the use of image sharing through the internet continues to grow rapidly, protecting confidential image information from unauthorized access has become a major concern. Cyberattacks, hacking, illegal copying, and data theft may lead to serious privacy and security problems. Traditional data security methods are not fully suitable for image files because digital images contain large amounts of pixel information and high redundancy.

Therefore, advanced image encryption techniques are required to provide secure image transmission and storage. Image encryption converts the original image into an unreadable encrypted format using mathematical operations and secret keys, while image decryption restores the encrypted image back to its original form. This paper presents an advanced image encryption and decryption system using OpenCV and Python. The proposed approach applies pixel transformation, XOR operations, and image scrambling methods to improve image security and confidentiality. The system provides efficient encryption performance, secure image protection, and reliable image recovery with minimal quality loss after decryption.

II. Litrerature Review

Several researchers have proposed different techniques for protecting digital images using cryptography and image processing methods. Early image encryption approaches mainly used substitution and transposition techniques, which offered limited security against modern cyber threats. Later, encryption standards such as DES and AES were introduced to improve data confidentiality and protection. Researchers also developed methods based on chaotic systems, pixel shuffling, and key-based transformations to enhance encryption strength and reduce unauthorized access. In recent years, OpenCV-based image encryption techniques have become popular because OpenCV provides efficient image processing operations, faster computation speed, and flexible implementation support. Advanced methods combining cryptography with image processing have

III. Problem Statement

The increasing use of digital images in communication systems, cloud storage, medical applications, and social media platforms creates several security challenges.

- Inefficiency of traditional image security methods
- High computational complexity in existing encryption systems
- Reduction in image quality after decryption

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

This research focuses on developing an advanced image encryption and decryption model that provides strong security, faster processing speed, and accurate image recovery using OpenCV-based image processing techniques.

IV. Proposed System

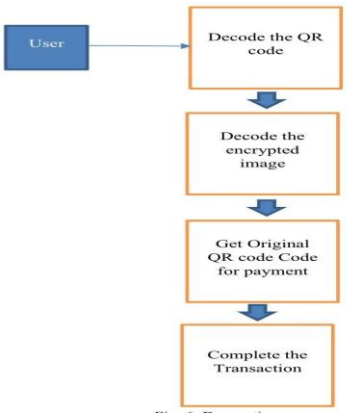
A. System Overview

The proposed system consists of multiple stages:

1. Image Upload
2. Image Preprocessing
3. Secret Key Generation
4. Image Encryption
5. Encrypted Image Storage
6. Image Decryption

The system processes digital images efficiently and provides secure image protection with accurate image B.

System Architecture



The architecture includes:

- Frontend: HTML and CSS interface for image upload and display
- Backend: Python-based processing using Flask
- Database: Stores encrypted image information and secret keys
- Encryption Module: Performs image encryption operations
- Decryption Module: Restores encrypted images into original form
- OpenCV Module: Handles image processing and pixel manipulation

C. Encryption feature

1) Image processing Features

- *Pixel value transformation*
- *RGB channel separation*
- *Image resizing*
- *Pixel normalization*

2) Security Features

- *XOR-based encryption*
- *Pixel shuffling techniques*
- *Secret key generation*
- *Secure image reconstruction*

3) Protection Features

- Confidential image storage
- Unauthorized access prevention
- Secure image transmission
- Accurate image recovery

V. Methodology

A. Image Preprocessing

Image preprocessing is important to improve encryption efficiency and image quality.The following steps are applied:

- Image resizing
- Noise removal
- RGB channel separation
- Pixel normalization

B. Encryption Techniques

1) XOR Encryption

A simple and efficient method used to secure image pixel values using secret keys.

2) Pixel Shuffling

A technique used to rearrange image pixels randomly for improving security strength.

3) Key-Based Encryption

Used to provide secure encryption and accurate image decryption using secret keys.

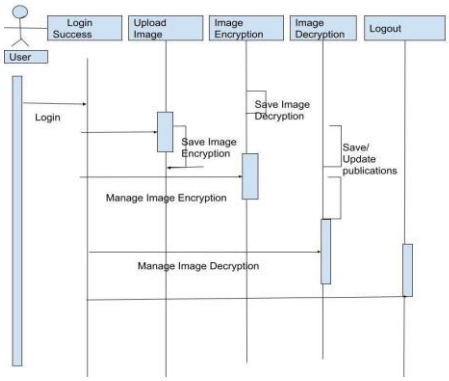
C. OpenCV Processing

OpenCV techniques are used for image processing and analysis:

- Pixel value extraction
- Image transformation
- Image encryption processing
- Image reconstruction and decryption

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 05, May 2026)

VI. System Flow



The System Follows These Steps:

1. User uploads the image
2. Image preprocessing is performed
3. Secret key is generated
4. Image encryption is applied
5. Encrypted image is stored securely
6. User enters the decryption key
7. Image decryption is performed

VII. Hardware And Software Requirements

A. Hardware Requirements

- *Processor: Intel® Core™ i9-14900K @ 3.20 GHz*
- *RAM: 16 GB*
- *Storage: 1 TB*

B. Software Requirements

- Frontend: HTML, CSS
- Backend: Python
- Framework: Flask
- Library: OpenCV

VIII. Experimental Results

The proposed system was tested using different digital image formats to evaluate encryption and decryption performance.

Performance Metrics

- *Encryption Speed*
- *Decryption Accuracy*
- *Image Recovery Quality*
- *Security Efficiency*

Results

- XOR-based encryption provided strong image security
- Pixel shuffling improved confidentiality and protection
- OpenCV enabled faster image processing performance
- Accurate image recovery was achieved after decryption

The system demonstrated:

- Secure image encryption and decryption
- Minimal image quality loss
- Fast processing speed
- Reliable image reconstruction

IX. Advantages Of The Proposed System

- Strong protection for confidential images
- Faster encryption and decryption process
- Efficient implementation using OpenCV
- Accurate image recovery after decryption
- Reduced risk of unauthorized image access

X. Applications

- Medical image protection systems
- Military and defense communication
- Secure cloud image storage
- Banking and financial security systems
- Digital forensic applications

XI. Future Works

Future enhancements include:

- Integration of AES and RSA encryption algorithms
- Real-time video encryption systems
- Artificial intelligence-based image security
- Blockchain-supported secure image storage
- Biometric authentication for image decryption
- Cloud-based encrypted image management systems

XII. Conclusion

This paper presented an advanced and secure approach for image encryption and decryption using OpenCV and Python. The proposed system effectively protects confidential digital images by applying pixel transformation, XOR operations, and image scrambling techniques. The encryption process converts the original image into an unreadable encrypted format, while the decryption process accurately restores the original image using the correct secret key.

The integration of OpenCV improves image processing efficiency and enables faster encryption and decryption operations. Experimental analysis shows that the proposed method provides strong image security, reliable image recovery, minimal quality loss, and efficient processing performance. The system successfully prevents unauthorized access and ensures safe image transmission and storage.

Furthermore, the proposed model is scalable and suitable for real-world applications such as medical image protection, military communication, banking systems, cloud storage security, and secure digital image sharing. The ability of the system to provide accurate image reconstruction and strong confidentiality makes it an effective solution for modern image security challenges. Overall, the proposed approach offers a reliable and efficient framework for protecting digital images in various secure communication environments.

REFERENCES

[1] Rafael C. Gonzalez and Richard E. Woods, Digital Image Processing, Pearson Education, 2018.

[2] William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 2017.

[3] S. Sridhar, Digital Image Processing, Oxford University Press, 2016.

[4] OpenCV Development Team, OpenCV Documentation, 2024.

[5] Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2015.