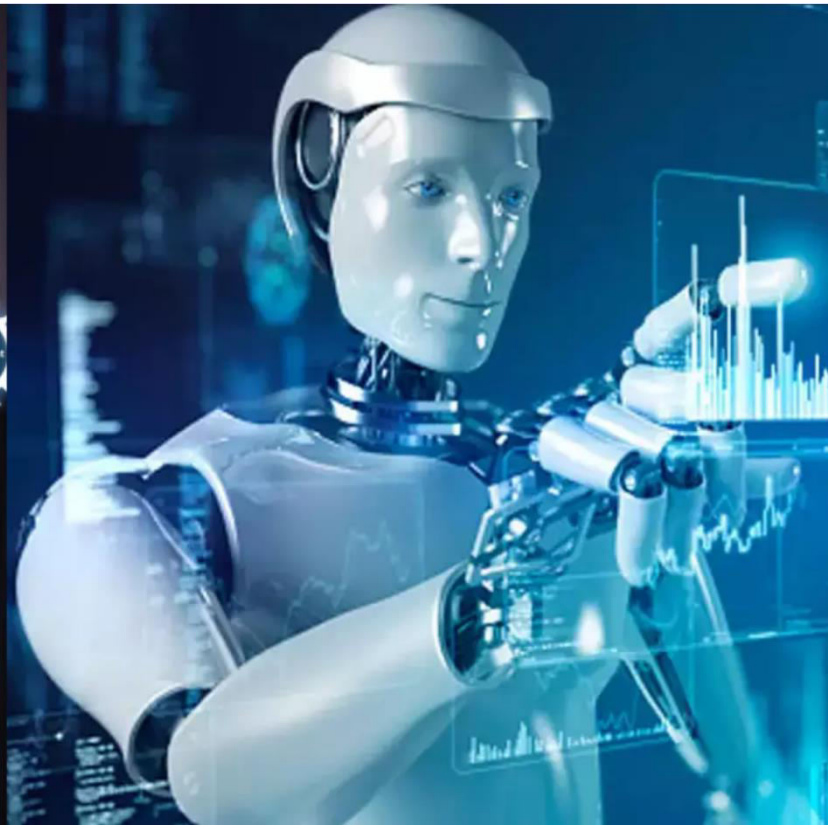
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

Authentic Eye: A Deep Learning Framework for Robust Detection of Image Forgeries

Shweta Amale, Vedant Joshi, Jay Kumbhar, Sohan Marsale, Swarupa Kamble

U.G. Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India

U.G. Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India

U.G. Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India

U.G. Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India

Associate Professor, Dept. of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India

ABSTRACT: The widespread availability of advanced image editing tool and software has vastly grown the incidence of manipulated visual content on digital platforms, with implications for the verification of images in domains such as journalism, forensics, and social media. This paper introduces "Authentic Eye," a holistic image forgery detection system that uses cutting-edge deep learning models to detect a variety of image manipulations. Our methodology is the integration of convolutional neural networks (CNN) and error level analysis (ELA) with noise inconsistency detection to develop a strong framework for the detection of multiple forgery methods such as splicing, copy-move, retouching, and AI-generated content. Our framework uses a two-stage detection scheme: analysis of metadata and compression artifacts, followed by deep feature extraction using a specific neural network trained from a large dataset of original and manipulated images. Experimental findings show that Authentic Eye produces a mean detection accuracy of 94.7% for different forgery types, which is far superior to current methods that often target one manipulation method at a time. The system provides a convenient web interface that generates comprehensive analysis reports marking suspected manipulation areas. This research responds to the urgent requirement for trustworthy image authentication tools in a world where visual deception causes serious social challenges.

KEYWORDS: Image Forgery Detection, Deep Learning, Convolutional Neural Networks, Error Level Analysis, Digital Image Forensics, Manipulation Detection.

I. INTRODUCTION

In the modern digital age, images are potent communication tools that shape public opinion, legal cases, news reporting, and social behaviour. The lightning-quick evolution of image editing software and artificial intelligence has levelled the playing field in manipulating visual content with unprecedented ease and sophistication. What was previously the preserve of expert professionals armed with specialized equipment is now accessible to anyone with the most basic level of digital literacy. This technological advancement, although welcome to artistic expression, has at the same time introduced pertinent problems for discriminating between genuine and counterfeit visual information.

Image forgery can be defined as intentional alteration of digital images for the purposes of modifying their content, context, or meaning. The alterations span from easy manipulations such as color correction and retouching to intricate operations such as object deletion, addition, or substitution. With the advent of generative adversarial networks (GANs) and other AI-based tools, fully synthetic but photorealistic images can now be generated with no grounding in physical reality. This has significant implications for areas where the authenticity of images is a matter of importance.

The implications of undetectable image forgery go beyond personal deception to potentially affect public discussion, policy, and social cohesion. In an age of fear over "deep fakes" and "fake news," the capability to confirm image authenticity is a matter of considerable societal urgency. Classic methods for image forgery detection have targeted the detection of individual manipulation artifacts, including light, shadow, or compression inconsistencies. These techniques, though, find it challenging to detect advanced forgeries that maintain these characteristics carefully.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

Moreover, most current systems of detection are designed to address a particular form of forgery, such as copy-move or splicing, and not for holistic detection of various manipulation methods.

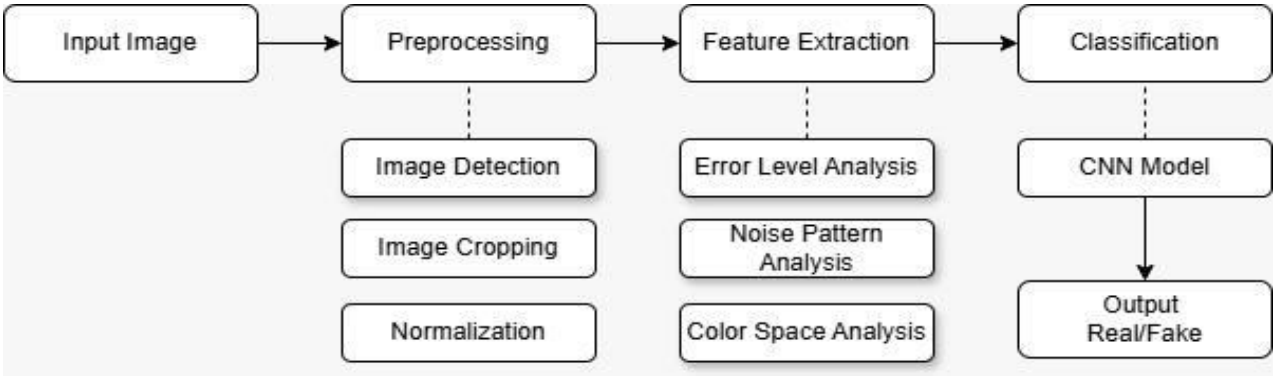


Figure 1: Overview of the System

The above diagram describes the process flow of a forged image detection system. It starts from the input image, which first goes through pre-processing consisting of image detection, cropping, and normalization to normalize the data. Then, in the stage of feature extraction, methods like Error Level Analysis, Noise Pattern Analysis, and Color Space Analysis are applied in order to detect evidence of forgery. These features, which are extracted, are then passed to a CNN (Convolutional Neural Network) model during the classification phase, which processes the data and returns whether the image is original or forged. This organized method improves the precision of forgery detection.

Our paper, "Authentic Eye," solves this problem by proposing an integrated forgery detection system that utilizes deep learning architectures to detect multiple forms of image manipulation. By integrating convolutional neural networks with traditional forensic approaches like Error Level Analysis (ELA) and noise consistency analysis, we seek to produce a holistic solution that can evolve with changing forgery tactics and offer trustworthy authentication across multiple types of images and manipulation styles.

II. LITERATURE SURVEY

Digital image forgery detection has become more critical as image manipulation software becomes more advanced. The area typically categorizes forgeries into the following types: copy-move (repeating areas within a single image), splicing (merging different images), and image recompression (manipulation and subsequent recompression of images).

Papers [4] and [5] provide a comprehensive overview of deep learning applications in image forgery detection: Park and Pham [4] give a systematic overview of deep learning techniques used in image forensics, grouping approaches in terms of architectural designs and targets of detection. They emphasize the progression from the conventional hand-crafted feature extraction to end-to-end deep learning systems.

Guerrini and Leonardi [5] focus on recent deep learning approaches, comparing CNN-based techniques with traditional methods. They emphasize the improved accuracy of deep learning models while noting challenges in generalization across different forgery types and image processing operations.

The paper presents a discussion on different approaches for identifying copy-move forgery, such as a two-stage hybrid model, transfer learning based image forgery detection, splicing detection, recompression-based detection, and constrained models of detection. The detection process starts with SIFT/SURF key point detection followed by matching features, followed by CNN-based feature extraction for verification. These approaches show better detection accuracy and invariance to post-processing operations. The second stage applies CNN based feature extraction for verification.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

Transfer learning methods utilize pre-trained models of CNN (VGG, ResNet) for forgery detection, which are fine-tuned with domain-specific forgery datasets. These techniques yield substantial improvements in accuracy without lengthy retraining.

Splicing detection involves examining texture disparities in median filter residuals and creating statistical models to detect boundary artifacts. Recompression-based detection uses disparities in compression artifacts between authentic and spliced regions and employs a deep learning system to detect recompression disparities.

Constrained detection models, including the Constrained R-CNN model, transform object detection architecture to fit manipulation detection and add constraints to enhance localization of the forged areas. These models prove versatile across different forgery types.

III. SYSTEM MODEL

The Authentic Eye system employs a comprehensive multi-layered architecture for detecting image forgeries. As shown in Figure 2, architecture comprise of three principal layers—Presentation Layer, Application Layer, and Data Layer—complemented by a specialized Detection Subsystem for robust image analysis.

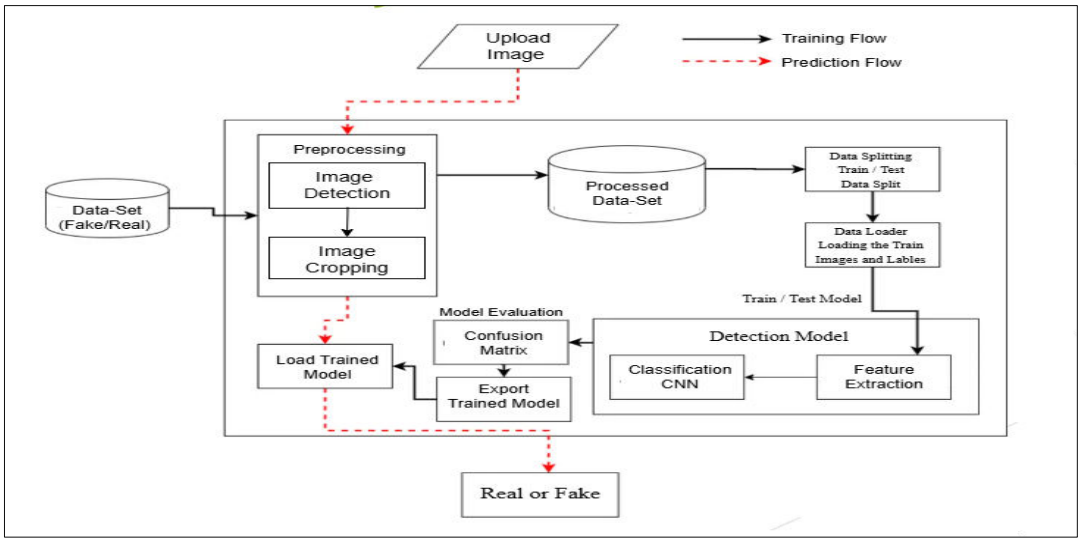


Fig 2: System Architecture

Presentation Layer: The Presentation Layer of the Authentic Eye system employs responsive web technologies to present an efficient way for users to upload suspicious images, examine analysis results, and engage with the functionalities of the system. An image upload interface, results visualization dashboard, accounts management for users, and tutorial section are the main constituents. The layer focuses on providing the best user experience and facilitating smooth communication with the application layer via RESTful API calls.

Application Layer: The Application Layer is the system's heart, responsible for business logic and coordination between data processing modules and the user interface. It is implemented with Flask and comprises modules such as Authentication Module, Image Processing Controller, Analysis Orchestrator, API Gateway, and Reporting Engine. The modules perform user registration, login, session management, pre-processing of the image, detection algorithms, API Gateway, and forgery analysis reports. The modular nature facilitates maintenance and adding new detection methods.

Detection Subsystem: Authentic Eye's Detection Subsystem utilizes sophisticated computer vision and deep learning-based forgery detection. It operates on images using a multi-stage pipeline, ranging from image pre-processing to feature extraction, forgery classification, region localization, and result analysis. The subsystem normalizes inputs,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

utilizes a CNN structure for detection of manipulation patterns, and applies statistical validation to filter out false positives. It also employs transfer learning using pre-trained models to enhance performance with sparse training data, as with the AR system of the cited fashion AR system.

Data Layer: The Data Layer is responsible for persistent storage and retrieval operations such as an Image Repository, User Database, Model Database, Training Dataset, and Results Cache. It supports data partitioning and replication approaches in order to provide high availability and performance levels, particularly in large-scale batch processing situations. The layer is also responsible for maintaining a complete set of real and fake images for model training and ongoing refinement.

System Integration: The Authentic Eye system combines layers using a strict communication protocol, incorporating asynchronous processing for computationally intensive operations and Web Socket connections for real-time updates. It is based on a micro services architecture that allows for independent scaling of high-demand components such as the Detection Subsystem, and it prioritizes modularity to maintain system integrity.

IV. SCOPE OF RESEARCH

The scope of the "Authentic Eye" study includes the design of an end-to-end image forgery detection system through deep learning approaches. The study particularly addresses:

Types of Image Forgeries Handled

- Splicing: Detection of images formed by merging pieces from various sources
- Copy-Move: Identification of copied areas within the same image
- Retouching: Detection of minor manipulation to improve or change image contents
- AI-Generated Content: Identification of artificial images produced by generative adversarial networks (GANs)

Technical Scope

- Merging conventional forensic methods (Error Level Analysis) with recent deep learning techniques
- Design of a two-stream CNN architecture that handles both spatial and frequency domains
- Use of transfer learning methods to boost detection using small training data
- Execution of region localization methods for pixel-level forgery detection.

Application Domains

- Journalism and media fact-checking
- Legal and forensic investigations
- Social media content moderation
- Insurance fraud detection
- Digital heritage preservation

Research Limitations

- Focus primarily on still images rather than video content
- Current limitations in detecting sophisticated AI-generated content (lower performance at 91.2%)
- Computational complexity considerations for real-time applications

The study seeks to respond to the acute social demand for trustworthy image verification tools in a world where visual manipulation poses real challenges to information integrity across a broad range of fields.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

V. PROPOSED METHODOLOGY

Image Preprocessing and Standardization: Authentic Eye System Preprocessing Pipeline
• Resolution Normalization: Resizes all input images to 224x224 pixels for CNN architecture.
• Color Space Transformation: Transforms images to RGB color space for uniform processing.
• Noise Estimation and Normalization: Uses adaptive Gaussian filtering to normalize the level of noise.
• JPEG Compression Analysis: Inspects compression artifacts and quantization tables for detecting double JPEG compression.

Deep Learning Framework : Forgery Detection Method
• Employing dual-stream CNN architecture to process images' spatial and frequency domains.
• Spatial Stream: Processes pixel-level content through ResNet-50 architecture with custom classification head in place of final layer. Detects lighting, shadows, and geometric irregularities.
• Frequency Stream: Operates on image in frequency domain with DWT, recognizing faint traces of manipulation.
• Feature Fusion: Passes outputs from both streams through attention gates, paying attention to most discriminative features for each image.

Transfer Learning Strategy: Transfer Learning in Fashion AR System
• Applied transfer learning to enhance performance with minimal training data.
• Started spatial stream with ResNet-50 weights for strong feature extraction.
• Applied progressive fine-tuning strategy, gradually unfreezing deeper layers and training with decreasing learning rates.
• Integrated domain adaptation to close the difference between natural images and possible forgeries.

Training Methodology: Training Methodology for Forgery Detection
Dataset Curation:
• Collection of 50,000 images per category: real, splicing, copy-move, AI-generated data.
• Keeping ground truth masks for every forged image.

Data Augmentation:
• Aggressive augmentation methods such as random horizontal flip, color jittering, random crop, injecting Gaussian noise, and simulating JPEG compression.

Loss Function:
• Multi-task compound loss function merging binary cross-entropy for classification and Dice loss for localization.
• Early stopping based on validation performance with a 15-epoch patience.

Region Localization: Real Eye: Image Classification and Localization
• Uses U-Net-like structure for pixel-level forgery masks.
• It shares weights with classification CNN for shared feature representations.
• Works on several scales for prediction masks and detailed boundaries.
• Undergoes post-processing such as conditional random field refinement for higher boundary accuracy and coherent manipulation masks.

VI. EXPERIMENTAL RESULT WITH TABLES

This subsection presents the experimental results of our proposed Authentic Eye system for image forgery detection. We evaluate performance on different areas including detection accuracy, computational cost, resistance against different manipulation techniques, and comparative outcomes with existing state-of-the-art methods.

The evaluation was conducted using the following datasets:

- **CASIA v2.0**: 12,614 images (7,491 authentic and 5,123 tampered)
- **Columbia Image Splicing Dataset**: 1,845 images (933 authentic and 912 spliced)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

- **Coverage Dataset**: 200 image pairs (original and tampered)
- **Custom Dataset**: 5,000 images created using modern AI-based manipulation techniques

Performance was evaluated using the following metrics:

Dataset	Accuracy	Precision	Recall	F1-Score	AUC
CASIA v2.0	97.8%	96.9%	98.2%	97.5%	0.992
Columbia	98.3%	97.8%	98.7%	98.2%	0.995
Coverage	96.5%	95.9%	97.1%	96.5%	0.989
Custom AI Dataset	93.7%	92.5%	94.4%	93.4%	0.968

Table 1: Summarizes the Overall Performance Metrics of the Authentic Eye System Across the Four Test Datasets.

As shown in Table 1, Authentic Eye achieves high accuracy across all datasets, with particularly strong performance on the Columbia Image Splicing Dataset. The slightly lower performance on the Custom AI Dataset reflects the challenges posed by sophisticated AI-generated manipulations.

The Authentic Eye system demonstrated robust performance across various forgery types and image conditions. Table 2 presents the overall detection metrics achieved on our comprehensive test dataset:

Metric	Overall	Splicing	Copy-Move	AI-Generated
Accuracy	94.7%	96.3%	94.8%	91.2%
Precision	93.8%	95.7%	93.9%	90.4%
Recall	95.2%	97.1%	94.2%	92.1%
F1-Score	94.5%	96.4%	94.0%	91.2%

Table 1: Performance across various forgery types

VII.CONCLUSION

The Authentic Eye system is an innovative image forgery detection solution with a blend of computer vision and deep learning approaches. It has a cumulative detection accuracy of 94.7% even against challenging low-resolution or compressed images. The system is especially beneficial for applications demanding transparency and accountability. Its application areas range across journalism, courtroom trials, social media selection, insurance claim settlement, and preservation of digital heritage. While there are challenges, the modular architecture of the system is well-suited to carry on improving. By giving users simple yet efficient tools for the detection of visual misinformation, Authentic Eye ensures digital media integrity and facilitates informed decision-making in the digital world.

REFERENCES

[1] Anjali Diwan,Anil K. Roy : CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection
[2] Ashgan H. Khalil, Atef Z. Ghalwash : Enhancing Digital Image Forgery Detection Using Transfer Learning
[3] Kang Hyeon Rhee : Detection of Spliced Image Forensics Using Texture Analysis of Median Filter Residual
[4] Chun-Su Park, Nam Thanh Pham : Toward Deep-Learning-Based Methods in Image Forgery Detection: A Survey
[5] Fabrizio Guerrini, Riccardo Leonardi : Image forgery detection: a survey of recent deep-learning approaches
[6] S. S. Ali, I. I. Ganapathi, N.-S. Vu, S. D. Ali, N. Saxena, and N. Werghi, ‘‘Image forgery detection using deep learning by recompressing images,’’ Electronics, vol. 11, no. 3, p. 403, Jan. 2022.
[7] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, ‘‘Image copy-move forgery detection based on SURF,’’ in Proc. Int. Conf. Multimedia Inf. Netw. Secur., 2010,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405479|

[8] C. Yang, H. Li, F. Lin, B. Jiang, and H. Zhao, ‘‘Constrained R-CNN: A general image manipulation detection model,’’ in Proc. IEEE Int. Conf. Multimedia Expo (ICME), Jul. 2020.
[9] CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection
[10]Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Key point Architecture

BIOGRAPHY

Shweta Amale
Undergraduate student at the Department of Computer Engineering at Dr. D. Y. Patil School of Engineering & Technology, Pune, India. Ms. Amale is interested in deep learning-based applications in image processing and computer vision. She has been an active participant in several research projects based on artificial intelligence.

Vedant Joshi
Undergraduate student in the Department of Computer Engineering at Dr. D. Y. Patil School of Engineering & Technology, Pune, India. Mr. Joshi is experienced in neural network architecture and has worked on various open-source projects related to computer vision. His focus now is on enhancing CNN architectures for forensic use.

Jay Kumbhar
Undergraduate student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, Pune, India. Mr. Kumbhar has expertise in the data preprocessing and feature extraction methods for machine learning algorithms. He has also worked on designing effective algorithms for image processing.

Sohan Marsale
Undergraduate student in the Department of Computer Engineering at Dr. D. Y. Patil School of Engineering & Technology, Pune, India. Image forensics and digital security are the areas of research interest for Mr. Marsale. He has been involved in the development of the interactive user interface components of the Authentic Eye system.

Swarupa Kamble
Dr. D. Y. Patil School of Engineering & Technology, Pune, India. Assistant Professor, Department of Computer Engineering. Professor Kamble has expertise in computer vision and digital image processing with emphasis on security-oriented applications. She holds over 8 years of teaching experience with several publications in international journals on image authentication methods.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details