WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing Image Forgery Detection Using Machine Learning and Deep Learning

Nareddy Shivareddy[1], Dr. V. Uma Rani[2]

[1]Post Graduate Student, M. Tech (SE) Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad,
Email: shivabusiness0205@gmail.com)
[2](Head of The Department, Professor, Department of Information Technology, Jawaharlal Nehru Technological University Hyderabad,
Email: umarani@jntuh.ac.in)

ABSTRACT

In the digital era, image manipulation poses a significant challenge to the credibility of visual content, particularly in sensitive fields such as law enforcement, journalism, and forensic investigations. This study focuses on enhancing the detection of forged images using advanced Machine Learning (ML) and Deep Learning (DL) techniques. Image forgery, which involves altering an image to mislead viewers, typically occurs through two primary methods: copy-move and splicing. The copy-move technique involves duplicating a portion of an image and pasting it elsewhere within the same image to conceal or replicate content. In contrast, splicing entails merging elements from different images to fabricate a new, deceptive composition. Accurately identifying such manipulations is critical, as images often serve as decisive evidence in legal and investigative contexts. To address this, the proposed work integrates both ML and DL models to improve the accuracy and reliability of forgery detection systems. The experimental results demonstrate the approach's effectiveness in distinguishing authentic images from tampered ones, thereby contributing to the advancement of digital image forensics.

Keywords — Image Forgery Detection, Copy-Move Forgery, Image Splicing, Convolutional Neural Network (CNN), Deep Learning Algorithms, SqueezeNet, MobileNetV2, Passive Image Forensics, Digital Image Manipulation, Zernike Moments (ZM), Block Discrete Cosine Transform (BDCT), Image Integrity Verification, Forgery Classification, Feature Extraction Techniques, Forged Region Localization, CASIA Dataset, Machine Learning in Forensics, Artificial Intelligence in Image Forensics, Computer Vision for Forgery Detection

INTRODUCTION

In the current digital era, images serve as a potent means of communication and sharing information. Nevertheless, the swift progress in image editing tools has made it simpler to change visual content, leading to significant worries regarding the authenticity and reliability of digital images. Image forgery, defined as the alteration of an image to deceive or misguide, presents a considerable risk in multiple domains, such as digital forensics, journalism, legal inquiries, and national security.

Detecting such alterations has thus become an essential area of study. Among the most prevalent forms of image forgery are copy-move manipulation, in which a portion of the image is replicated and relocated within the same image to hide or distort content, and image splicing, where sections from various images are merged to form a singular, misleading representation. Recognizing these forgeries is difficult because of the advanced nature of contemporary editing software. The objective of this project is to enhance image forgery detection by combining traditional machine learning methods with the robust features of deep learning. By utilizing sophisticated algorithms and techniques for feature extraction, this research aims to increase the accuracy, resilience, and dependability of forgery detection systems.

LITERATURE REVIEW

[1] With the increasing sophistication of rendering software, synthetic images now exhibit a level of realism that often challenges the authenticity of photographic evidence. Lyu et al. [1] addressed this issue by proposing a statistical method based on wavelet transformations to distinguish photorealistic images from real ones. Their model analyzed first-order and higher-order wavelet coefficients, revealing structural patterns that reliably differentiate between the two types of images.

[2] According to Bebis et al. [2], image manipulation has become widespread due to the accessibility of powerful editing tools. Their survey outlined two primary forms of forgery: copy-move, where image regions are duplicated internally, and splicing, where external content is integrated into the

original image. The authors discussed the vulnerabilities introduced by such tampering and reviewed common detection challenges, including handling transformations like scaling, blurring, and noise addition.

[3] Hussain [3] proposed a non-intrusive method for detecting copy-move forgeries using the dyadic wavelet transform (DyWT). The method focused on identifying structurally similar regions within the image, relying on statistical measures extracted after segmentation. This technique eliminated the need for embedded metadata and demonstrated better performance than existing methods in terms of detection accuracy and robustness.

[4] Granty Regina et al. [4] reviewed passive image forgery detection approaches that operate without prior knowledge of the source or embedded data. These techniques rely on inconsistencies in visual and statistical properties—such as lighting direction, color anomalies, and compression artifacts—to detect tampered regions. The study emphasized the growing importance of such methods in forensic and legal contexts, where image evidence must be validated.

[5] Choudhary Shyam Prakash [5] introduced a unified system capable of identifying both copy-move and splicing forgeries. The approach used block-based DCT (BDCT) and adaptive thresholding to extract features, followed by classification through a support vector machine (SVM). Zernike Moments were employed to accurately localize forged regions in copy-move scenarios. Experimental evaluations on the CASIA v1.0 and v2.0 datasets showed the method's high precision in multi-type forgery detection.

EXISTING SYSTEM

The Current methods in image forgery detection employ a variety of feature extraction and classification techniques aimed at identifying inconsistencies caused by tampering operations such as splicing and copy-move forgery.

One established approach involves analyzing the geometric and frequency characteristics of an image using the Block Discrete Cosine Transform (BDCT). This technique extracts statistical features by computing the differences between adjacent image blocks, which can be treated as a one-dimensional signal. To model the inter-block relationships across specific directions, Markov random fields are applied, capturing contextual dependencies that indicate potential tampering.

In addition, techniques based on the Gray-Level Co-occurrence Matrix (GLCM) have been employed to generate edge descriptors that reflect textural inconsistencies. These descriptors are calculated by evaluating the spatial relationship between pixel intensities over predefined orientations. The resulting edge maps are then used as discriminative features for forgery detection.

Another prominent method incorporates the Hilbert-Huang Transform (HHT) in combination with wavelet-based analysis. This hybrid approach enables the decomposition of image signals into intrinsic mode functions, enhancing the sensitivity to local modifications introduced during splicing. The moment-based statistical features derived from this transformation further strengthen the ability to detect subtle anomalies.

For the classification task, Support Vector Machines (SVMs) are commonly used due to their robustness in handling high-dimensional and non-linear feature spaces. SVM-based classifiers have demonstrated promising results in distinguishing tampered images from authentic ones, with some systems achieving classification accuracies as high as 85.86% on standard splicing datasets.

However, most traditional systems are designed to address either copy-move or splicing forgery, but not both within a unified framework. This limitation highlights the need for more generalized and adaptive models. In response to this challenge, machine learning techniques—especially those involving SVMs—have been adopted to improve detection accuracy and generalizability. Yet, even with these advances, the development of a single, reliable method that effectively handles multiple forms of image forgery remains an open research problem.

PROPOSED SYSTEM

The proposed system introduces an integrated approach that combines Zernike Moments (ZM) and Block Discrete Cosine Transform (BDCT) to enhance the detection of image forgeries, specifically focusing on both copy-move and splicing manipulations. Initially, the system evaluates whether the input image has been tampered with by analyzing structural and frequency-based features. Once tampering is suspected, a Convolutional Neural Network (CNN) is employed to further classify the type of forgery present—either splicing or copy-move. In cases where copy-move forgery is detected, the system performs additional analysis to precisely locate the manipulated regions. By merging traditional feature extraction techniques with deep learning-based classification, this method offers improved detection accuracy and localization capabilities, making it suitable for practical applications in digital image forensics.

ARCHITECTURE

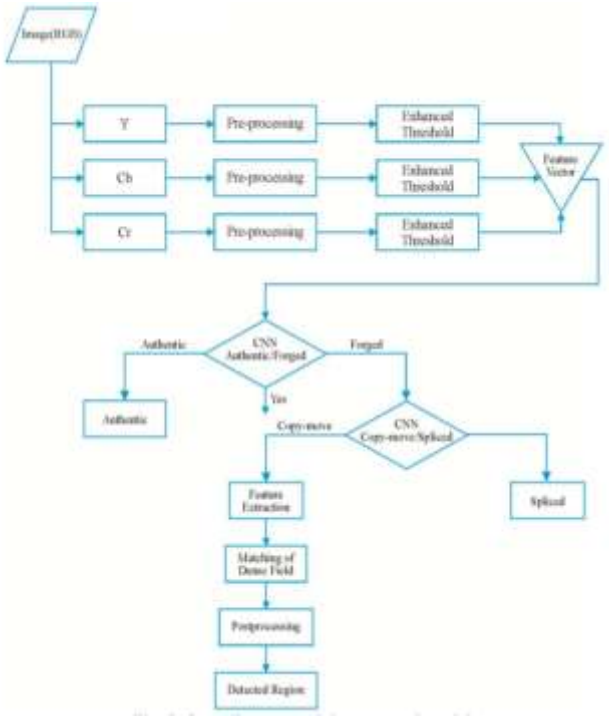

Figure No 1: Architecture

IMPLEMENTATION

In The proposed system is developed through a structured set of implementation modules to effectively detect image forgeries. The complete process includes data acquisition, preprocessing, model training, evaluation, and prediction.

1) Data Collection:

The dataset used consists of forged and authentic images gathered from publicly available sources. The data is split into training and testing subsets in a typical 70:30 ratio to ensure proper learning and unbiased evaluation. Class distribution is maintained across both subsets to preserve statistical balance during training and validation.

2) Data Preprocessing:

To ensure data quality, preprocessing steps are applied. These include handling missing values, removing outliers, resizing images, and normalizing pixel values. These steps enhance the model's performance by making the input more consistent and suitable for machine learning and deep learning algorithms.

3) Model Selection:

The detection framework leverages both classical machine learning and deep learning models. Support Vector Machines (SVM) are used for structured statistical analysis, while Convolutional Neural Networks (CNNs) are employed for deep feature learning and classification. A portion of the dataset is allocated for training, and the rest is used for evaluating model performance using metrics such as accuracy, precision, recall, and F1-score.

4) Prediction and Evaluation:

After training, the models are tested on unseen data to assess their accuracy in detecting forged regions. Evaluation is done using a confusion matrix, which provides insight into false positives and false negatives. CNN-based models like GoogleNet are utilized for prediction due to their ability to learn complex features from images and provide region-based localization of forgeries.

4.4 Algorithm

The core algorithm is based on a Convolutional Neural Network (CNN) architecture, which is optimized for image classification tasks. A multi-layer CNN is designed using TensorFlow to detect subtle differences between original and tampered regions. The architecture includes convolutional layers, ReLU activation functions, pooling layers, and fully connected layers that progressively extract and learn relevant features. The final layer outputs the probability of an image being forged.

Each neuron in the network computes a weighted sum of its inputs followed by a non-linear activation. Activation functions like ReLU and Sigmoid are employed to introduce non-linearity, enabling the network to learn complex patterns. The CNN is trained using backpropagation and gradient descent to

minimize classification error. This architecture ensures robustness in detecting both copy-move and splicing types of forgeries with improved precision and reliability.

RESULTS

- Training with Authenticated Images to identify the fake Images.

Figure No 2: AUTHENTICATED IMAGE

- Identifying the fake Images.

Figure No 3: Identifying Fake Images

CONCLUSION

This work introduces an effective approach for detecting image forgery, specifically targeting both copy-move and splicing techniques within a unified framework. The proposed system initiates by converting the input images to the YCbCr color space, followed by preprocessing steps involving block-based discrete cosine transform (BDCT) and image decorrelation to extract meaningful features. These features are then utilized to train a convolutional neural network (CNN) model using labeled authentic and tampered images. The CNN classifier demonstrates high reliability in identifying forgery types, achieving classification accuracies of 99.03% for copy-move detection and 99.11% for splicing detection. The results validate the effectiveness of the model in recognizing subtle image manipulations. Future enhancements will focus on testing the robustness of the model across more complex and diverse datasets to further improve generalization and detection accuracy. systems.

REFERENCES

1. S. Lyu and H. Farid, “How realistic is photorealistic?” IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.

2. H. Farid, “A survey of image forgery detection,” IEEE Signal Processing Magazine, vol. 2, no. 26, pp. 16–25, 2009.

3. Muhammad, Najah, Muhammad Hussain, Ghulam Muhammad, and George Bebis, "Copy-move forgery detection using dyadic wavelet transform.", In Proceedings of IEEE Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV2011), pp. 103-108, 2011.

4. J. Granty Regina Elwin, T. S. Aditya, and S. Madhu Shankar, “Survey on passive methods of image tampering detection,” in Proceedings of the International Conference on Communication and Computational Intelligence (INCOCCI ’10), pp. 431–436, December 2010.

5. Pun C-M, Bo L, Yuan X-C (2016) Multi-scale noise estimation for image splicing forgery detection. J Vis Commun Image Represent 38:195–206 6. 20. Hakimi F (2015) Image-splicing forgery detection based on improved lbp and k-nearest neighbors algorithm. Electron Inf Plan, 3 7. Shi Y, Chen C, Chen W (2007) A natural image model approach to splicing detection. In: Proceedings of the 9th workshop on Multimedia & security, pp 51–62. ACM

8. Wang W, Dong J, Tan T (2009) Effective image splicing detection based on image chroma. Image Processing (ICIP), 2009 16th IEEE International Conference on, pp 1257–1260. IEEE

9. Li X, Jing T, Li X (2010) Image splicing detection based on moment features and hilbert-huang transform. In: 2010 IEEE international conference on information theory and information security (ICITIS), pp 1127–1130. IEEE

10. Zhao X, Li J, Li S, Wang S (2011) Detecting digital image splicing in chroma spaces. Digital Watermarking 6526:12–22.