iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57339

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Image Forgery Detection using Adaptive Oversegementation and Key Point Matching

Mrs. Anujna M[1], Jatin Singh[2], Mohammed Zayed Pasha[3], Harsh[4]
[1]*Asst. Professor, Dept of Computer Science and Engineering, KSSEM, Bangalore*
[2, 3, 4]*Student, Computer Science and Engineering, KSSEM, Bangalore*

Abstract: ***The scope of this paper is to propose a image forgery detection application by combining adaptive oversegmentation and feature point matching, the suggested scheme presents a novel method for detecting copy-move forgery in images. Using superpixel-based analysis, it divides the image into erratic blocks, extracts feature points, and fine-tunes areas that could be fakes. The accuracy of the detected forged areas is then improved by morphological operations. Results from experiments indicate that this method performs better than current ones, especially under difficult circumstances.***

I. INTRODUCTION

Copy-move forgery stands as a prevalent form of image manipulation, involving the duplication and insertion of a section of an image into another part of the same image. This technique aims to disguise or replicate specific content within the image, potentially misleading viewers by creating the illusion of identical objects or scenes. Experts in digital forensics and image processing have actively devised methods to detect such alterations. They employ algorithms and techniques to unveil instances of copy-move forgery by scrutinizing inconsistencies in duplicated regions, identifying patterns, or examining discrepancies in pixel values indicating potential tampering. Several common approaches include block matching, which involves comparing image blocks to spot similarities, using keypoints to identify replicated regions, analyzing the frequency domain via Discrete Wavelet Transform (DWT), and employing machine learning and deep learning models trained on large datasets to recognize manipulation patterns.

Despite these efforts, detecting and preventing image tampering remains an ongoing challenge due to the continual advancements in editing tools and methods. Consequently, ongoing research in developing robust forgery detection methods remains crucial to uphold the credibility and integrity of digital images. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich et al. [1] A proposed forgery detection method involved dividing the image into overlapping blocks, matching quantized DCT coefficients to find tampered areas. Keypoint-based methods, using image keypoints for matching, were also suggested to detect duplications robustly.

II. TERMINOLOGIES

A. Machine Learning

Machine learning, a subset within artificial intelligence, involves crafting algorithms that empower machines to learn from data to enhance their performance. It draws upon principles from computer science, mathematics, and statistics, aiming to discern and comprehend patterns in datasets. Its foundation rests on the concept of statistical learning and encompasses various tasks like natural language processing, predictive modeling, and image recognition.

The utility of machine learning techniques spans numerous domains, offering assistance in forecasting and extracting valuable insights from vast datasets. Their adaptability to assimilate extensive information and accommodate new data makes them invaluable across industries such as manufacturing, healthcare, finance, and entertainment. Machine learning's applications are diverse, aiding in deciphering complex data and facilitating informed decision-making processes, making it an indispensable asset in modern technological landscapes.

B. OPEN CV

OpenCV, an acronym denoting Open Source Computer Vision Library, stands out as an adaptable open-source tool crafted for the intricacies of computer vision and image processing. Its expansive functionality covers a wide spectrum of applications, ranging from image analysis and object recognition to machine learning tasks. Supporting multiple programming languages, including

©IJRASET: All Rights are Reserved

Python and C++, OpenCV emerges as a popular choice for real-time computer vision applications. The library's appeal lies not only in its diverse applications but also in its user-friendly attributes, facilitated by a modular design and comprehensive documentation. This accessibility caters to both newcomers and seasoned professionals in the field.

The widespread adoption of OpenCV has left an indelible mark on various domains, propelling advancements in robotics, augmented reality, and autonomous systems. Its role in pushing the boundaries of computer vision technologies is significant, reflecting its impact on reshaping how we interact with visual data. OpenCV serves as a linchpin in fostering innovation, providing the tools and framework necessary for researchers, developers, and engineers to explore and pioneer new frontiers in computer vision, thereby contributing to the evolution of technology in dynamic and transformative ways.

C. CNN (Convolutional Neural Network)

Convolutional Neural Networks (CNNs) represent a pivotal advancement in deep learning tailored for image processing and pattern recognition. Comprising layers that progressively learn hierarchical features using convolutional filters, CNNs excel at discerning intricate details such as edges and textures within images. The integration of max pooling further aids by reducing spatial dimensions, optimizing computational efficiency.

An integral aspect of CNN architecture involves fully connected layers that interpret the acquired features, facilitating accurate classification. Noteworthy is the utilization of shared weights, endowing CNNs with translation invariance and robust performance across different spatial locations. Inspired by the receptive fields of the visual cortex, CNNs mirror the biological mechanisms underlying visual perception.

This architectural mimicry contributes to their exceptional efficacy in diverse image-centric tasks, including image recognition, object detection, and facial recognition. The adaptability of CNNs has propelled advancements in computer vision and artificial intelligence, fostering breakthroughs in understanding and interpreting visual data. As a result, CNNs stand as indispensable tools in the contemporary landscape of machine learning, driving innovations that hinge on intricate visual understanding and analysis.

III. LITERATURE SURVEY

A. Analysis of Digital Image Forgery Detection using Adaptive Over Segmentation Based on Feature Point Extraction and Matching.

This paper reviews the evolution of image fraud detection methods, encompassing principle component analysis, quick copy-move detection, and the Fourier-Mellin Transform. While prior research explored forensic analysis using SURF and SIFT, computational efficiency remains a hurdle. To tackle this, a new approach is introduced here, combining feature point matching with adaptive over-segmentation. This innovative technique divides the host image into irregular chunks, optimizing processing efficiency. After segmentation, extracted feature points are matched, pinpointing labeled points indicative of potential forgery areas. Additionally, to refine precision, the proposed forgery region extraction method employs morphological processes and superpixel substitution.

This introduction of a pioneering detection approach stands as a unique contribution to image forgery detection. Contextualized within this literature survey, this method aims to surmount computational challenges while improving accuracy in identifying and isolating forged regions within digital images.

B. Image Forgery Detection using Adaptive Over-Segmentation and Feature Point Matching

Through a combination of key point-based techniques and adaptive over-segmentation, the examined literature presents a novel copy-move forgery detection strategy. By dynamically dividing the host image into irregular blocks, the Adaptive Over-Segmentation technique makes forgery detection easier by using point matching to identify feature points that are retrieved from each block. By substituting super pixels for feature points, combining related blocks into regions, and utilizing morphological processes, a second Forgery Region Extraction algorithm improves upon the initial one. The suggested technique outperforms current methods in a variety of circumstances, according to experimental results. The precision and resilience of copy-move forgery detection in digital picture forensics have greatly improved thanks to this thorough method.

C. A Study of Copy-Move Forgery Detection Scheme Based on Segmentation

Block-based method: This method makes use of features that are taken out of the individual digital image blocks. F used a thorough search to propose a direct method for CMFD. Therefore, processing this approach takes a long time.

On the CMF, changes like scaling, rotation, translation, and so forth are made. offered a technique based on the image's color characteristics.

Presented a fourier transform-based approach. If an image is altered by noise, blur, or any other means, neither of their works will be able to identify a fake.Rotated CMF regions cannot be detected by a Same Affine Transform Selection forgery if any modifications such as rotation, scaling, etc. are done on the copy-move regions. (SATS)-based method. suggested a technique for forgery detection that makes use of the texture of the image and the discrete wavelet transform (DWT) and cosine transform, respectively. However, what they do not detect

D. Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching

The presented research introduces an innovative method for detecting digital forgery in images, specifically addressing copy-move operations. The devised scheme employs adaptive over-segmentation and feature-point matching, enhancing the precision of forgery detection. To further refine the identification of forgery regions, a proposed Forgery Region Extraction algorithm replaces labeled feature points with small superpixels as feature blocks. Subsequently, neighboring feature blocks exhibiting similar local color features are merged, generating cohesive merged regions for more accurate detection. Looking ahead, a potential avenue for future research involves extending this forgery detection scheme to other forms of manipulation, such as splicing, and exploring its applicability in diverse media types, including video and audio. This expansion could significantly contribute to advancing digital forensics capabilities, providing a comprehensive approach to detect and combat various forms of digital manipulation across different mediums.

IV. CONCLUSION

In conclusion, this literature survey paper has presented a promising approach for image forgery detection by combining point key matching and adaptive oversegmentation. The proposed technique has demonstrated improved accuracy in identifying forgery regions in images. Further research can optimize its performance and explore real-world applications to enhance the authenticity and integrity of digital images.

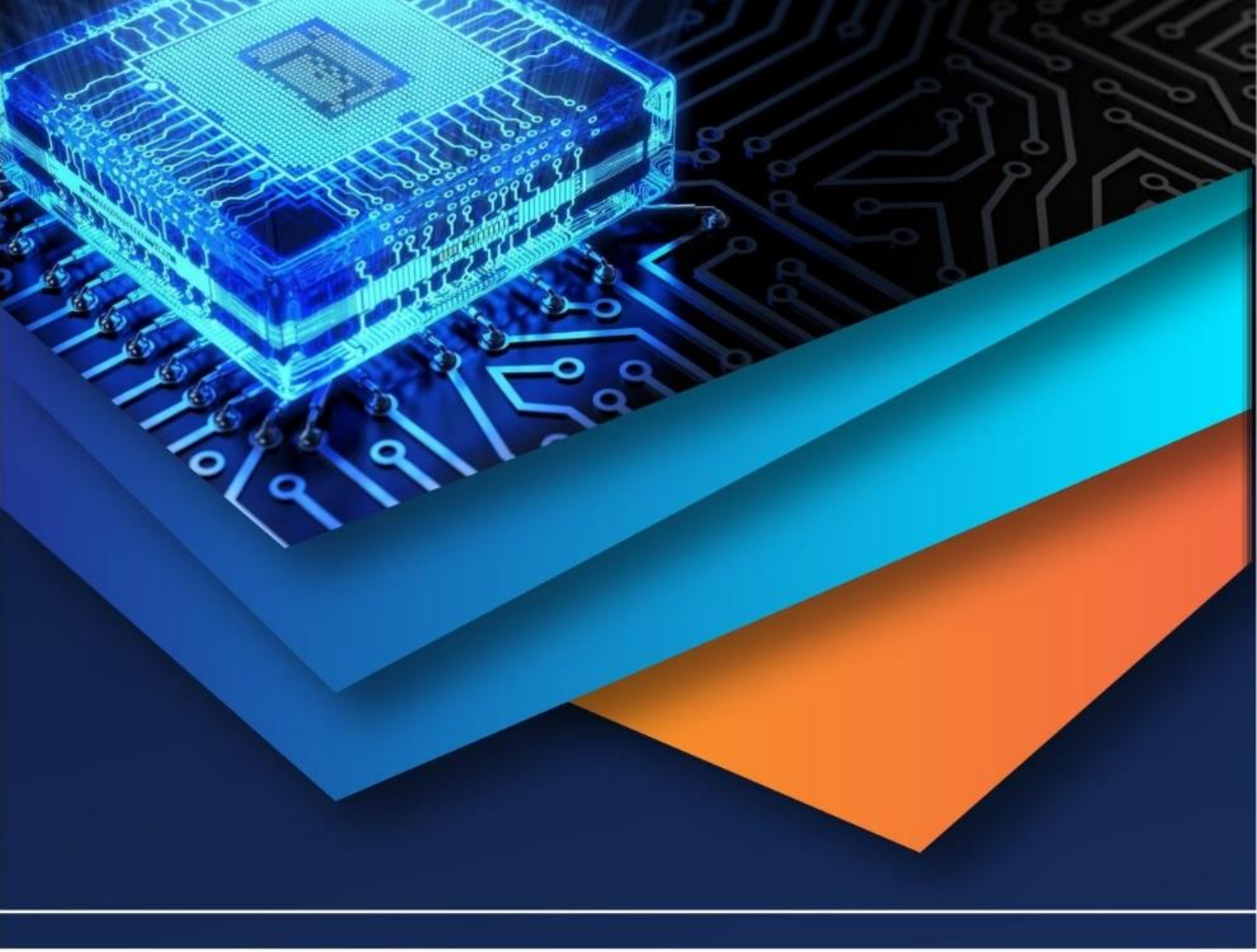
V. ACKNOWLEDGEMENTS

We are thankful to Mrs.Anujna.M, Assistant Professor for being our Project Guide, under whose able guidance this project work Phase-1 has been carried out successfully.

REFERENCES

[1] Analysis of Digital Image Forgery Detection using Adaptive Over Segmentation Based on Feature Point Extraction and Matching Ch. SUDARSHAN, U. SATHISH KUMAR
[2] Image Forgery Detection using Adaptive Over-Segmentation and Feature Point Matching RAVI BABU KANCHARLA, NAGI HYMAVATHI
[3] A Study of Copy-Move Forgery Detection Scheme Based on Segmentation Mohammed Ikhlayel , Mochamad Hariadi and Ketut Eddy Pumama
[4] Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching Chi-Man Pun, Senior Member, IEEE, Xiao-Chen Yuan, Member, IEEE, and Xiu-Li Bi

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)