IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

Digital Image Forgery Detection Using Deep Learning

DR.A.Emmanuel Peo Mariadas[1], Eswar.K[2], Akash kumar.s[3], Ashwath.s[4]

Professor, Department of Computer Engineering, E.G.S. Pillay Engineering College, Nagapattinam, TamilNadu, India[1]

U.G. Student, Department of Computer Engineering, E.G.S. Pillay Engineering College, Nagapattinam, TamilNadu, India[2,3,4]

ABSTRACT: The importance of ensuring the authenticity and reliability of digital images has grown significantly, primarily due to the ease of modifying such images with the progress of digital image editing tools. Consequently, there is a growing emphasis on the development of techniques for detecting image manipulation. One particular area of focus in digital image authentication is copy-move forgery detection. This project presents a survey and a comparative study on copy-move forgery detection techniques in digital images, databases, and evaluation metrics. The study aims to provide insights into the effectiveness of different methods in detecting copy-move forgeries. The Project discusses prominent detection techniques, including block-based, keypoint-based, transform domain, hybrid methods, deep learning, and GAN approaches. The findings highlight the strengths, weaknesses, and key similarities and differences among the approaches. This study contributes to the understanding of the state-of-the-art in copy-move forgery detection and provides guidance for future research in this field.

KEYWORDS : Deep Learning, GAN, Digital image, Forgery detection

I. INTRODUCTION

A.Overview

Since the beginning of photography, people and organizations have been relentless in their efforts to modify photos in order to trick audiences. At first, this task required a great deal of experience and hours of work from technicians with professional training. But since the invention of digital photography, almost anyone can now alter images with ease and produce results that are almost as good as professional. Thus, social challenges have emerged as a result of this extensive accessibility, ranging from the veracity of images provided by the media to the editing of model photos to improve their look or body image.

A growing number of academics and professionals are interested in image forgery detection due to the wide range of image modification techniques accessible. Even if there are a lot of detection techniques available, it might be difficult to choose which ones are the most effective and realistic to use. A high detection rate algorithm might also show a significant false positive rate at the same time. Furthermore, although runtime plays a major role in an algorithm's effectiveness and usability, it is frequently discussed in academic contexts rather than in terms of real-world applications.

To streamline this complex task, algorithms will be categorized into five distinct types: JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling Detection, and Light & Color Anomaly Detection.

Specific research will then be conducted on each group, assessing the general efficiency of the described algorithm types. If a method is deemed reliable, an algorithm from that group will be implemented. These categories are chosen based on the entirely different detection methods they employ, promising diverse outcomes depending on the type of image forgery.

Algorithms for JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling Detection, and Light & Color Anomaly Detection will be divided into five categories in order to simplify this intricate process. After that, specific studies will be carried out on each group to evaluate the overall effectiveness of the mentioned

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

algorithm types. The implementation of an algorithm from that category will occur if a method is found to be dependable. These categories promise varied results dependent on the sort of picture fraud, and they were selected based on the distinctly different detection techniques that each one uses.

B. Image Processing

The editing and analysis of digital images by computer algorithms is referred to as image processing. It includes a broad range of methods designed to improve, evaluate, and decipher images for a variety of uses in different sectors. Image processing is essential for deriving useful information from visual input in a variety of applications, including satellite remote sensing and medical imaging. Image enhancement to increase quality, image segmentation to divide images into relevant parts, and image classification to classify objects within images are common tasks in image processing. Furthermore, computers can analyze and comprehend visual data thanks to image processing techniques like edge detection, feature extraction, and pattern recognition. This opens the door for developments in computer vision, autonomous cars, and machine learning.

C. Deep Learning

Deep learning, a subset of machine learning, represents a powerful and versatile approach to artificial intelligence that has revolutionized numerous fields, including computer vision, natural language processing, and speech recognition. At its core, deep learning involves training neural networks with multiple layers to automatically learn and extract complex patterns and features from large volumes of data. By leveraging hierarchical representations of data, deep learning models can achieve remarkable accuracy and generalization, surpassing traditional machine learning algorithms in many tasks. One of the key strengths of deep learning lies in its ability to learn directly from raw data, eliminating the need for manual feature engineering and enabling the development of end-to-end solutions for various applications. From image recognition and medical diagnosis to autonomous driving and language translation, deep learning continues to push the boundaries of artificial intelligence, driving innovation and transforming industries across the globe.

One of the fundamental aspects of image processing is the digital representation of images using pixels, which are individual picture elements that form the building blocks of digital images. Each pixel contains numerical values representing the intensity or color of the corresponding point in the image. Image processing algorithms operate on these pixel values to perform various operations, such as enhancing contrast, adjusting brightness, or applying filters to remove noise. Additionally, advanced image processing techniques leverage mathematical and statistical methods to extract features or patterns from images, enabling tasks such as object recognition, image classification, and image restoration. With the rapid advancements in computer hardware and software technologies, image processing has become increasingly sophisticated, enabling the development of powerful applications and solutions that leverage visual information for a wide range of purposes, from enhancing digital photos to analyzing complex medical images and satellite imagery.

II. RELATED WORK

W Shan, D Zou, P Wang, Image splicing forensic technologies reveal manipulations that add or remove objects from images. However, the performance of existing splicing forensic methods is fatally degraded when detecting noisy images, as they often ignore the influence of image noise. In this paper, we propose a new forgery detection network called the robust image forgery detection network (RIFD-Net) based on convolutional neural networks (CNNs). With the help of multi-classifiers and a denoising network, RIFD-Net can effectively filter out multiple types of image noise before forgery detection. To determine the extent of tampering, we follow the Siamese network to calculate the similarity between two image patches, without prior knowledge of forensic traces. Results

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

from extensive experiments on benchmark datasets indicate that our method outperforms existing image splicing forensic methods, achieving a substantial improvement of over 20% in the mean average precision (mAP) for forgery detection. Furthermore, RIFD-Net accurately locates splice areas, even in the presence of noise..

J Rao, S Teerakanok, Image tampering detection is becoming more and more important in image forensics, especially in today's society where advanced image editing tools are becoming more and more popular. At the same time, with the rapid growth of digital image technology and multimedia data, it is very important to ensure the authenticity and integrity of visual information. Therefore, to address this issue, we propose a novel image tampering detection method using a deep convolutional network (ResNet) combined with a Transformer decoding layer. While traditional algorithms only solve a single tamper detection problem, our method can detect multiple tampering means. We use ResNet as the backbone of feature extraction to obtain rich and hierarchical features from input images. We then employ Transformer's decoding layer to process these features, enabling the model to capture long-distance dependencies and complex patterns, which we believe can further improve the accuracy of image tampering detection. In the experiments, we conduct experiments on three datasets (CASIA, NIST, and IMD2020) to verify the performance of the model. According to the experimental results, our model performed well on the CASIA and IMD2020 datasets, and also achieved good results in the NIST dataset. Furthermore, we also test two main types of image tampering: Copy-move and Splicing. Our model performs very well in detecting the Splicing type of image tampering. The experimental results show that this study fully demonstrates the potential and effectiveness of deep convolutional networks (such as ResNet) and Transformer decoding layers in image tampering detection, and also verifies the high performance and excellent generalization ability of the model.

C Yan, S Li, H Li, In recent years, various convolutional neural network (CNN) based frameworks have been presented to detect forged regions in images. However, most of the existing models can not obtain satisfactory performance due to tampered areas with various sizes, especially for objects with large-scale. In order to obtain an accurate object-level forgery localization result, we propose a novel hybrid transformer architecture, which exhibits both advantages of spatial dependencies and contextual information from different scales, namely, TransU2-Net. Specifically, long-range semantic dependencies are captured by the last block of encoder to locate large-scale tampered areas more completely. Meanwhile, non-semantic features are filtered out by enhancing low-level features under the guidance of high-level semantic information in the skip connections to achieve more refined spatial recovery. Therefore, our hybrid model can locate spliced forgeries with various sizes without requiring large data set pre-training. Experimental results on the Casia2.0 and Columbia datasets show that our framework achieves better performance over state-of-the-art methods. On the Casia 2.0 dataset, F-measure improve by 8.4% compared to the previous method.

Ayush Roy; Sk Mohiuddin , The process of modifying digital images has been made significantly easier by the availability of several image editing software. However, in a variety of contexts, including journalism, judicial processes, and historical documentation, among others, the authenticity of images is of utmost importance. In particular, copy-move forgery is a distinct type of image manipulation, where a portion of an image is copied and pasted into another area of the same image, creating a fictitious or altered version of the original. In this research, we present a lightweight MultiResUnet architecture with the Similarity-based Positional Attention Module (SPAM) attention module for copy-move forgery detection (CMFD). By using a similarity measure across the patches of the features, this attention module identifies the patches, where a forged region is present. The lightweight network also aids in resource-efficient training and transforms the model into one that can be used in real time. We have employed four commonly used but extremely difficult CMFD datasets, namely CoMoFoD, COVERAGE, CASIA v2 and MICCF600, to assess the effectiveness of our model. The proposed model significantly lowers false positives, thereby improving the pixel-level accuracy and dependability of CMFD tools.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

III. METHODOLOGY

A. Existing Methods

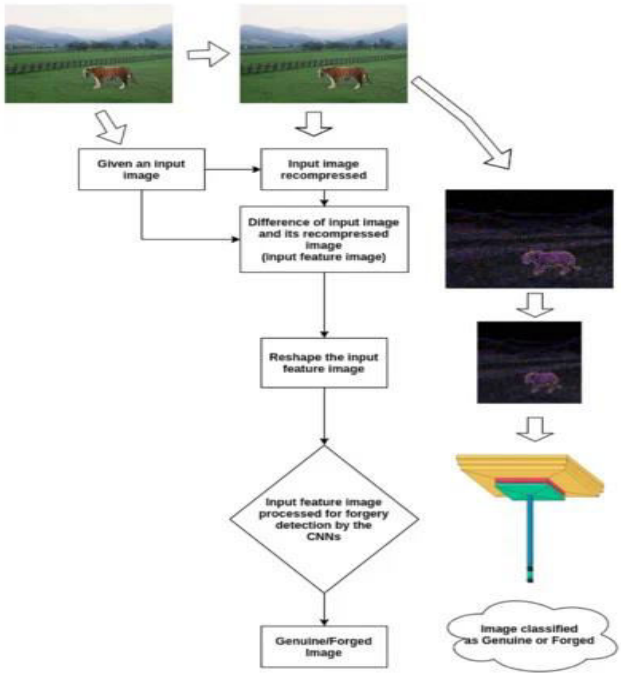
A novel incremental learning framework for face forgery detection, where we design an adapter-based incremental learning scheme combined with a confidence-based ensemble prediction mechanism. When confronted with new forgery methods, we incorporate small trainable adapter modules, which are retrained along with their corresponding classification layers, yielding a series of task-specific modules. Then we incorporate a confidence-based ensemble prediction mechanism to aggregate all predictions. Through comprehensive evaluations on multiple benchmark datasets (FF++, DFD, and Celeb-DF), our method successfully mitigates the catastrophic forgetting problem in a cost-effective manner and attains state-of-the-art performance in cross-dataset scenario.

B. Proposed System

The proposed approach acknowledges the inherent challenges in detecting image forgeries, particularly when parts of an image are copied from one source to another. Despite subtle changes that may occur during this process, which are often imperceptible to the human eye, Convolutional Neural Networks (CNNs) excel in identifying such alterations when analyzing manipulated images. By scrutinizing the differences between the original image and its compressed version, the forgery component becomes more apparent. Leveraging this distinction, a Deep Neural Network (DNN)-based model can be trained to effectively detect image forgery. Through this method, the model learns to discern patterns indicative of manipulation, enabling it to accurately identify instances of image tampering with a high degree of reliability and efficiency.

An essential aspect of the proposed approach lies in analyzing the disparity between the original image and its compressed version, as it accentuates the forgery component within the manipulated image. As images undergo compression, certain artifacts and distortions emerge, particularly in regions where manipulation has occurred. These discrepancies serve as indicators of potential tampering, providing valuable cues for the development of detection mechanisms. Leveraging this insight, a Deep Neural Network (DNN)-based model can be trained to effectively identify instances of image forgery by discerning subtle alterations in pixel values, textures, and structural elements. By capitalizing on the inherent differences between original and manipulated images, the proposed approach offers a robust framework for detecting and combating image forgery in various contexts, including digital forensics, content authentication, and multimedia security.

C. Proposed Architecture



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

IV. RESULT & DISCUSSION

The importance of ensuring the authenticity and reliability of digital images has become increasingly paramount, driven by the widespread availability and accessibility of digital image editing tools, which facilitate image manipulation with unprecedented ease. As a result, there has been a surge in research efforts focused on developing techniques for detecting image manipulation, with a particular emphasis on copy-move forgery detection. This paper presents a comprehensive survey and a comparative study of copy-move forgery detection techniques in digital images, examining various databases and evaluation metrics to provide insights into the effectiveness of different methods in detecting copy-move forgeries.

The survey encompasses an extensive review of prominent detection techniques, including block-based, keypoint-based, transform domain, hybrid methods, deep learning, and Generative Adversarial Network (GAN) approaches. Each technique is evaluated based on its ability to accurately detect instances of copy-move forgery, taking into account factors such as computational complexity, robustness to various types of manipulations, and computational efficiency. Through a comparative analysis, the strengths, weaknesses, and key similarities and differences among the approaches are elucidated, providing valuable insights into their respective performance and applicability in real-world scenarios.

The findings of the study shed light on the state-of-the-art in copy-move forgery detection, offering researchers and practitioners a comprehensive understanding of the available techniques and their relative merits. By synthesizing existing knowledge and identifying gaps in current approaches, this study lays the groundwork for future research endeavors aimed at advancing the field of digital image authentication. Moreover, the insights gleaned from the comparative analysis serve as a guide for the development of more robust and effective copy-move forgery detection methods, ultimately contributing to the enhancement of image authentication techniques and bolstering the integrity of digital images in various domains.

V. CONCLUSION & FUTURE WORK

A. Conclusion

The significance of ensuring the authenticity and reliability of digital images has become increasingly paramount in light of the ease with which such images can be manipulated using advanced digital editing tools. As a result, there has been a growing emphasis on the development of techniques for detecting image manipulation, particularly in the realm of copy-move forgery detection. This paper has presented a comprehensive survey and comparative study on various copy-move forgery detection techniques in digital images, encompassing databases and evaluation metrics. By examining prominent detection methods such as block-based, keypoint-based, transform domain, hybrid methods, deep learning, and GAN approaches, this study aimed to provide insights into the effectiveness of different approaches in detecting copy-move forgeries. Through the analysis of strengths, weaknesses, and key similarities and differences among these techniques, this study has contributed to advancing the understanding of the state-of-the-art in copy-move forgery detection. Furthermore, by shedding light on areas for improvement and future research directions, this study serves as a valuable resource for guiding further advancements in digital image authentication and forensic analysis. Overall, the findings of this study underscore the importance of continued research and innovation in developing robust and reliable techniques for detecting image manipulation, thereby enhancing the integrity and trustworthiness of digital imagery in various applications and domains.

C. Future Work

Future research in copy-move forgery detection should aim to advance the state-of-the-art by exploring novel detection methods, improving evaluation methodologies, and addressing practical challenges in real-world deployment. By continuing to innovate and refine detection techniques, researchers can contribute to the development of more

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203144 |

robust and reliable solutions for ensuring the authenticity and reliability of digital images in various applications and domains.

REFERENCES

1. Suzhen Wang, Lincheng Li, Yu Ding, and Xin Yu, "One-shot talking face generation from single-speaker audio-visual correlation learning," in Proceedings of the AAAI Conference on Artificial Intelligence, 2022
2. Yuyang Qian, Guojun Yin, Lu Sheng, Zixuan Chen, and Jing Shao, "Thinking in frequency: Face forgery detection by mining frequency-aware clues," in Computer Vision–ECCV 2020
3. Shen Chen, Taiping Yao, Yang Chen, Shouhong Ding, Jilin Li, and Rongrong Ji, "Local relation learning for face forgery detection," in Proceedings of the AAAI conference on artificial intelligence, 2021
4. Hanqing Zhao, Wenbo Zhou, Dongdong Chen, Tianyi Wei, Weiming Zhang, and Nenghai Yu, "Multi-attentional deepfake detection," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2021
5. Yuchen Luo, Yong Zhang, Junchi Yan, and Wei Liu, "Generalizing face forgery detection with high-frequency features," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2021
6. Ke Sun, Taiping Yao, Shen Chen, Shouhong Ding, Jilin Li, and Rongrong Ji, "Dual contrastive learning for general face forgery detection," in Proceedings of the AAAI Conference on Artificial Intelligence, 2022
7. Pranjal Ranjan, Sarvesh Patil, and Faruk Kazi, "Improved generalizability of deep-fakes detection using transfer learning based cnn framework," in 2020 3rd international Conference on information and computer technologies (ICICT). IEEE, 2020,
8. Ke Sun, Hong Liu, Qixiang Ye, Yue Gao, Jianzhuang Liu, Ling Shao, and Rongrong Ji, "Domain general face forgery detection by learning to weight," in Proceedings of the AAAI conference on artificial intelligence, 2021
9. Hao Dang, Feng Liu, Joel Stehouwer, Xiaoming Liu, and Anil K Jain, "On the detection of digital face manipulation," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern recognition, 2020
10. Justus Thies, Michael Zollhöfer, and Matthias Nießner, "Deferred neural rendering: Image synthesis using neural textures," ACM Transactions on Graphics (TOG), vol. 38, no. 4, pp. 1–12, 2019.
11. Chengrui Wang and Weihong Deng, "Representative forgery mining for fake face detection," in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2021
12. Junyi Cao, Chao Ma, Taiping Yao, Shen Chen, Shouhong Ding, and Xiaokang Yang, "End-to-end reconstruction-classification learning for face forgery detection," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 202

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details