JSRT JOURNAL

PAGES: 36-41
01/07/25

JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY VOLUME-3 ISSUE-7 JULY

Automated Detection of Image Forgery with Deep Learning

Shreedevi S Patil[1], Rani Prakash[2]

[1]*Student, Department of Computer Science and Engineering (MCA), Visvesvaraya Technological University, CPGS Kalaburagi, Karnataka, India. shreedevimalipatil19@gmail.com*

[2]*Professor, Department of Computer Science and Engineering (MCA), Visvesvaraya Technological University, CPGS Kalaburagi, Karnataka, India. rani.dhanshetty@gmail.com*

ABSTRACT

The image forgery techniques are used to provide the particular image in the form of computerized pictures with no errors in capturing of digital image information which shows the original image. While compared to normal images the edited images are difficult to find out the forged images. The image should maintain the authenticity and integrity to secure the picture from unauthorized users. In this paper, we have compared the digital image forgery and JPEG is the most common format used by the photographic images and the digital camera devices. These operations are performed in an adobe photo-shop using with the content of image security to restore some digital image with an authenticity and integrity to detect the digital image forgery using active and passive techniques.

***Keywords*: Deep Learning, Forgery, Automated Detection.**

I.INTRODUCTION

In this modern age we all are aware about the importance of digital technology. Digital image plays a vital role in many applications. At present, the digital technology has the integrity of the image. Over the past years the digital images of the field have emerged to restore some images. In this digital watermarking is one of the solutions to image authentication problem. Here the digital watermarking means hiding information in some text or image [1]. This is one of the copyright techniques to prove the ownership of the image. Tampering images are used to detect the image forensic tools that are only capable of digital cameras that should not rely on watermarks.

In nature the digital image forgery does not differ any image to compare to any conventional image forgery. Normally the digital images are dealing with the digital forgery [2], by using of photographs. One Can use some software tools by that the digital images carry the powerful computer graphics, Adobe Photoshop in this which we edit software's, and coral paint shop.

Some of the three main causes which are categorized in the process of providing the fake images, that are re-sampling, image splicing, and copy-move detection. One of the important processes of image is image security and it is a way to secure your home and business against crime and avoid becoming another statistic.

II. LITERATURE SURVEY

Chen et al [3] proposed an image splicing detection method that leverages 2-D phase congruency and statistical moments of the characteristic function to identify inconsistencies in image structures. Their approach is grounded in the observation that spliced regions disrupt the natural phase congruency of images, making them detectable through statistical analysis. The method avoids reliance on prior knowledge of the spliced regions and is effective across various image formats. Experimental results demonstrated high detection accuracy, making it a valuable tool for passive image forensics. This work laid the foundation for using frequency-domain features in tampering detection tasks.

Shuiming Ye et al [4] proposed a method to detect digital image forgeries by analyzing inconsistencies in blocking artifacts, which are typically introduced during JPEG compression. Their technique focuses on identifying variations in block boundaries, which can occur when tampered regions are compressed separately or differently from the original image. By measuring these inconsistencies, the method effectively highlights manipulated areas without relying on prior knowledge of image content. This approach is especially useful in detecting copy-move and splicing forgeries. The study demonstrates that compression artifacts can serve as reliable forensic features for image authentication.

M.Stamm et al [5] Stamm and Liu proposed a forensic approach that utilizes statistical intrinsic fingerprints to detect image manipulations. Their method focuses on identifying inconsistencies introduced during tampering by exploiting the inherent statistical properties of natural images. This technique enables the detection of various image editing operations such as splicing and retouching. The study provides a robust framework for passive image authentication without requiring pre-embedded watermarks or signatures.

Zhang Ting et al [6] Zhang and Wang developed a method for detecting copy-move forgery based on Singular Value Decomposition (SVD). Their approach extracts features from image blocks and uses similarity measures to locate duplicated regions. The method shows improved detection performance even under post-processing operations like rotation or compression. This work demonstrates the effectiveness of matrix decomposition techniques in digital image forensic analysis.
H. Farid et al [7] Farid presented a comprehensive survey of digital image forgery detection techniques, focusing on passive detection methods. He classified the techniques into several categories such as tampering detection, splicing, and re-sampling. The paper highlights the challenges in forgery detection and discusses various statistical and geometric cues that can indicate manipulation. This work serves as a foundational reference for researchers entering the field of digital forensics.

R. E. J. Granty et al [8] This paper surveys passive image tampering detection methods, categorizing them based on their ability to detect splicing, cloning, and resampling forgeries. The authors provide a comparative analysis of different techniques and their application scenarios. They emphasize the importance of passive approaches that do not require prior information or watermarks. Their review highlights the growing need for efficient and scalable tamper detection systems.

J. Fridrich et al [9] Fridrich and colleagues introduced one of the earliest techniques for detecting copy-move forgery in digital images. Their method divides the image into overlapping blocks and identifies duplicated areas using feature matching. It laid the groundwork for many subsequent advancements in block-based forgery detection. The simplicity and effectiveness of their technique make it a cornerstone in the field of image forensics.

H. Huang et al [10] Huang et al. proposed a method for detecting copy-move forgery using the Scale-Invariant Feature Transform (SIFT) algorithm. Their technique is capable of detecting duplicated regions even after geometric transformations like rotation, scaling, or noise addition. SIFT features are robust and provide better performance in complex tampering scenarios. The study contributes significantly to enhancing the robustness of passive forgery detection techniques.

III. EXISTING SYSTEM

Digital picture forgery detection is One field where the application of deep learning techniques is growing and more. The effectiveness of this technique in tackling the key task of identifying picture forgeries was shown using an existing system that used the MobileNetV2 architecture. Developed with mobile and embedded vision applications in mind, MobileNetV2 is a cutting-edge neural network architecture.

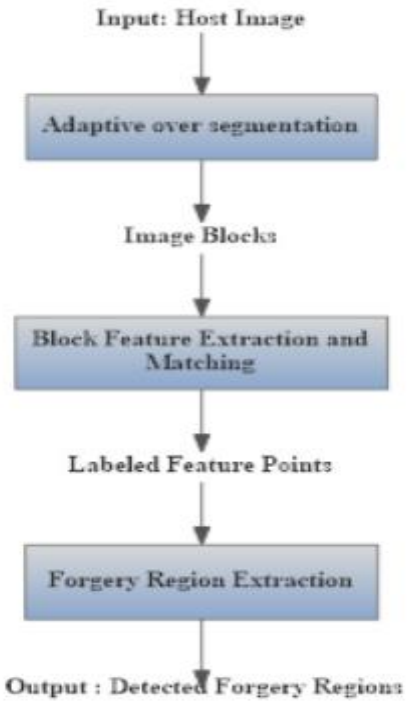
PROPOSED SYSTEM

In the proposed system for digital image forgery detection techniques, the focus lies on advancing the state-of-the-art through integration of deep learning models, particularly convolutional neural networks (CNNs), which excel in learning intricate features and patterns within images. The system aims to leverage CNNs for their capability to automatically extract discriminative features that distinguish between authentic and forged regions in images. Transfer learning techniques will be explored to enhance model performance by utilizing pre-trained networks and adapting them to detect specific types of image manipulations such as copy-move, splicing, and image inpainting. Additionally, the proposed system will incorporate robustness validation through adversarial training to ensure resilience against sophisticated forgery techniques aimed at evading detection.

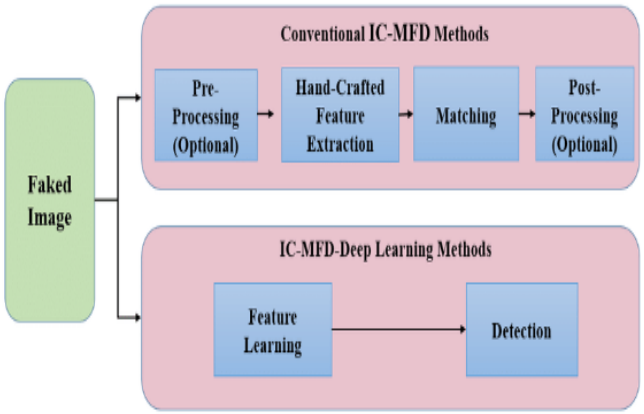
IV. METHODOLOGY

This section describes the proposed image forgery detection using adaptive over-segmentation [10] in details. Fig. 1 shows the framework of the proposed method for image forgery detection. Firstly, the adaptive over-segmentation method is proposed to divide the input image into nonoverlapping and irregular regions. Then SIFT

[9,10] is applied into each block to extract feature points as block features which are matched with each other to locate the points which can approximately specify the suspected forgery regions. Finally the forgery regions are detected according to the matched feature points.



ARCHITECTURE



V. RESULTS AND ANALYSIS

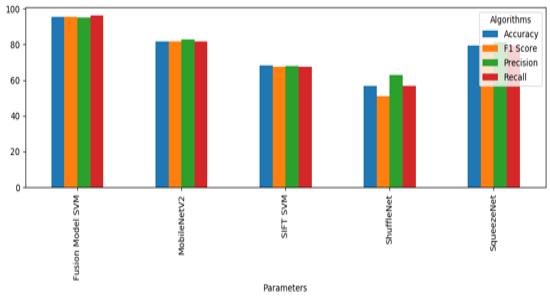


Fig1: Accuracy Comparison Graph

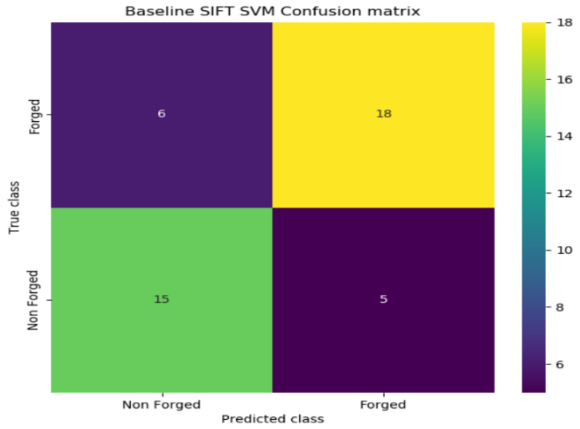


Fig2: Baseline SIFT SVM Confusion Matrix

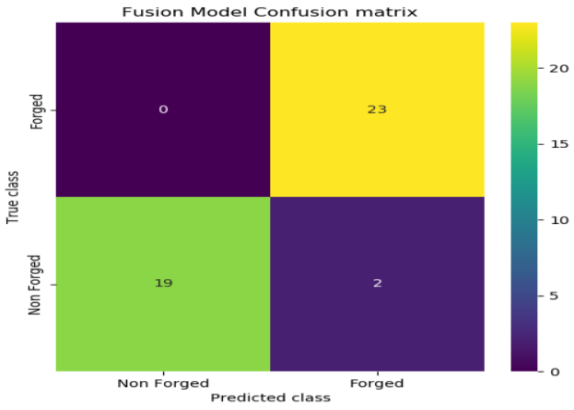


Fig3: Fusion Model Confusion Matrix

VI. SCREENSHOTS

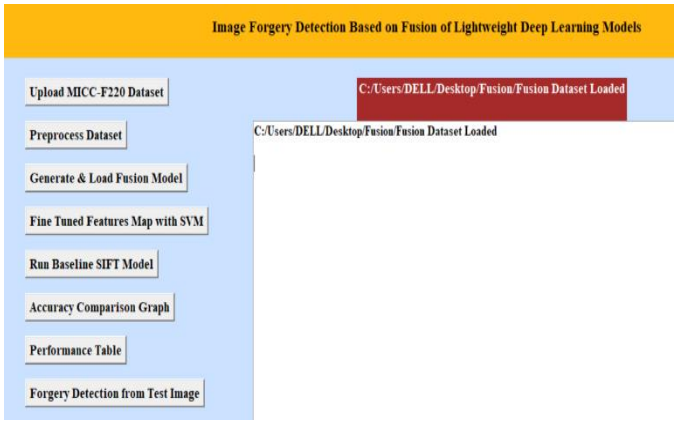


Fig4: Upload micc f220 dataset

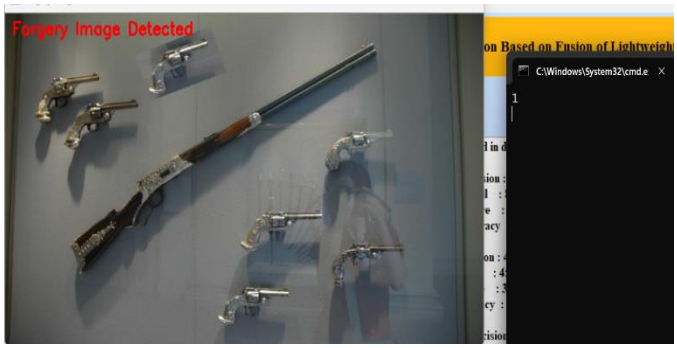


Fig5: Forgery Image

Fig6: Original Image

FUTURE SCOPE

The vast gaps in image manipulation detection techniques start with the continuously evolving methods of artificial intelligence and machine learning techniques to improve the quality of manipulated images and content. When it comes to identifying one unique reliable and accurate method for all possible images, many of the detection techniques fall short of data sets availability.

Even though all the highly specific methods are robust, one cannot deny the need for the presence of human intervention. This method is largely applicable across various image manipulation techniques.

VII. CONCLUSION

In this paper, the different methods of the digital image forgery detection techniques have been discussed. This technique is used to identify the fake image methods. JPEG is one of the devices that all the images are available in this format that provides with the help of Adobe Photoshop. The image should maintain the authenticity and

integrity to secure the picture from unauthorized users to detect the image and we detect the image with active and passive techniques, for example, splicing, re-sampling and copy-move, etc. this is the easiest way to detect the image forgery detection. The performance of different identification methods has been shown by the researchers. A further enhancement of this study is to show the proper tampering of images.

ACKNOWLEDGEMENT
Acknowledging image forgery detection involves recognizing the importance of techniques and technologies designed to identify and analyze altered or manipulated images. As digital images become more prevalent and editing tools more sophisticated, the need for reliable image forgery detection has grown significantly.

REFERENCES

1. A.C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling", IEEE Transactions on Signal Processing, 53 (2): 758-767, 2005.
2. A.C. Popescu and H. Farid, " Exposing Digital Forgeries in Color Filter Array Interpolated Images", IEEE Transactions on Signal Processing, 53 (10): 3948-3959, 2005
3. Chen, W., Shi, Y.Q., Su, W. "Image Splicing Detection uses 2-D Phase Congruency and. Statistical Moments of Characteristic Function," in society of photo-optical Instrumentation Engineers (SPIE) Conference Series, Feb 2007, Vol.6505.
4. Shuiming Ye; Qibin Sun; Ee-Chien Chang; "Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact," IEEE International Conference on Multimedia and Expo, 2007.
5. M. Stamm and K. Liu, Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints, Information Forensics and Security, IEEE, 2010, Vol. 5, No. 3, Pp.492-506.
6. Zhang Ting and Wang Rang-ding, Copy-Move Forgery Detection based on SVD in Digital Image, in Proc, 2nd International Conf, Image and Signal Processing (CISP), Tianjin, 2009, Pp. 1-5.
7. H. Farid, "A survey of image forgery detection," IEEE Signal Process. Mag., Vol. 26, no. 2, pp. 16–25, Mar. 2009.
8. R. E. J. Granty, T. S. Aditya, and S. Madhu, "Survey on passive methods of image tampering detection," in IEEE International Conference on Communication and Computational Intelligence (INCOCCI), 2010, pp. 431–6.
9. J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," Proceedings of the Digital Forensic Research Workshop, pp. 5-8, Aug. 2003.
10. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272- 6, Dec. 2008.