IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

Image Forgery Detection Based on Fusion of Lightweight Deep Learning Methods

M. SOUNDARYA LAHARI[1], S. RAJENDER[2]

[1]M.Tech Student, Department of Computer Science and Engineering, Department of Computer Science and Engineering, Avanthi institute of engineering and technology, Guntapally, Abdullapurmet, Rangareddy District, 501512.

[2]Assistant Professor, Department of Computer Science and Engineering, Avanthi institute of engineering and technology, Guntapally, Abdullapurmet, Rangareddy District, 501512.

ABSTARCT:

In recent years, taking pictures has become really popular because we all have cameras. We use pictures in our everyday lives because they have a lot of information. Sometimes, we need to make pictures better to get more information from them. There are tools to make pictures better, but some people also use them to make fake pictures, which spreads false information. This makes the problem of fake pictures worse and happens a lot. People have made ways to find fake pictures over time. Recently, special computer programs called convolutional neural networks (CNNs) have become popular, and they are used to find fake pictures too. But most of these programs can only find one type of fake picture, like when you put two pictures together or copy part of a picture. So, we need a way to find all kinds of fake pictures quickly and accurately.
In our paper, we introduce a new computer program that can find fake pictures when the picture has been compressed twice. We teach our program by looking at the differences between the original picture and the one that has been compressed twice. Our program is not heavy, and it's faster than the best ones out there. We did some tests, and they show that our program is really good at finding fake pictures, with an accuracy of 92.23%.

INTRODUCTION :

In recent years, with the widespread availability of cameras and the increasing popularity of capturing images, the need for accurately detecting image forgeries has become a pressing concern. Images are an integral part of our daily lives, holding valuable information. However, the ease of image manipulation and forgery has raised issues of misinformation and trust. Traditional techniques for detecting image forgeries have been in use for some time, but they are often limited in their ability to address the diversity of forgery methods.

To tackle this challenge, our project focuses on the development of a robust and efficient image forgery detection system. We leverage the power of lightweight deep learning models to address this issue. These models have the advantage of being quick and effective, making them a promising choice for this task. Our approach aims to extend beyond the detection of specific types of forgeries, such as image splicing or copy-move, and instead, provides a comprehensive solution for identifying a wide range of image manipulations. By combining these lightweight deep learning models, our system offers a fusion-based approach to enhance detection accuracy, making it a valuable contribution to the field of image forgery detection. The results of our experiments are encouraging, indicating the potential for a reliable and efficient forgery detection system that can play a vital role in addressing the challenges posed by the prevalence of manipulated images.

Literature Review:

Various approaches have been proposed in the literature to deal with image forgery. The majority of traditional techniques are based on particular artifacts left by image forgery, whereas recently techniques based on CNNs and deep learning were introduced, which are mentioned below. First, we will mention the various traditional techniques and then move on to deep learning based techniques.
In [14], the authors' proposed error level analysis (ELA) for the detection of forgery in an image. In [15], based on the lighting conditions of objects, forgery in an image is detected. It tries to find the forgery based on the difference in the lighting direction of the forged part and the genuine part of an image. In [16], various traditional image forgery detection techniques

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

have been evaluated. In [17], Habibi et al., use the contourlet transform to retrieve the edge pixels for forgery detection. In [18], Dua et al., presented a JPEG compression-based method. The discrete DCT coefficients are assessed independently for each block of an image partitioned into non-overlapping blocks of size 8 × 8 pixels. The statistical features of AC components of block DCT coefficients alter when a JPEG compressed image tampers. The SVM is used to classify authentic and forged images using the retrieved feature vector. Ehret et al. in [19] introduced a technique that relies on SIFT, which provides sparse keypoints with scale, rotation, and illumination invariant descriptors for forgery detection. A method for fingerprint faking detection utilizing deep Boltzmann machines (DBM) for image analysis of high-level characteristics is proposed in [20]. Balsa et al. in [21] compared the DCT, Walsh–Hadamard transform (WHT), Haar wavelet transform (DWT), and discrete Fourier transform (DFT) for analog image transmission, changing compression and comparing quality. These can be used for image forgery detection by exploring the image from different domains. Thanh et al. proposed a hybrid approach for image splicing in [22], in which they try to retrieve the original images that were utilized to construct the spliced image if a given image is proven to be the spliced image. They present a hybrid image retrieval approach that uses Zernike moment and SIFT features

Bunk et al. established a method for detecting image forgeries based on resampling features and deep learning in [23]. Bondi et al. in [24] suggested a method for detecting image tampering by the clustering of camera-based CNN features. Myung-Joon in [2] introduced CAT-Net, to acquire forensic aspects of compression artifact on DCT and RGB domains simultaneously. Their primary network is HR-Net (high resolution). They used the technique proposed in [25], which tells us that how we can use the DCT coefficient to train a CNN, as directly giving DCT coefficients to CNN will not train it efficiently. Ashraful et al. in [26] proposed DOA-GAN, to detect and localize copy-move forgeries in an image, authors used a GAN with dual attention. The first-order attention in the generator is designed to collect copy-move location information, while the second-order attention for patch co-occurrence exploits more discriminative properties. The affinity matrix is utilized to extract both attention maps, which are then used to combine location-aware and co-occurrence features for the network's ultimate detection and localization branches.

Yue et al. in [27] proposed BusterNet for copy-move image forgery detection. It has a two-branch architecture with a fusion module in the middle. Both branches use visual artifacts to locate potential manipulation locations and visual similarities to locate copymove regions. Yue et al. in [28] employed a CNN to extract block-like characteristics from an image, compute self-correlations between various blocks, locate matching points using a point-wise feature extractor, and reconstruct a forgery mask using a deconvolutional network. Yue et al. in [3] designed ManTra-Net that is s a fully convolutional network that can handle any size image and a variety of forgery types, including copy-move, enhancement, splicing, removal, and even unknown forgery forms. Liu et al. in [29] proposed PSCC-Net, which analyses the image in a two-path methodology: a top-down route that retrieves global and local features and a bottom-up route that senses if the image is tampered and predicts its masks at four levels, each mask being constrained on the preceding one.

In [30] Yang et al., proposed a technique based on two concatenated CNNs: the coarse CNN and the refined CNN, which extracts the differences between the image itself and splicing regions from patch descriptors of different scales. They enhanced their work in [1] and proposed a patch-based coarse-to-refined network (C2RNet). The coarse network is based on VVG16, and the refined network is based on VVG19. In [31] Xiuli et al., proposed a ringed residual U-Net to detect the splicing type image forgery in the images. Younis et al. in [32] utilized the reliability fusion map for the detection of the forgery. By utilizing the CNNs, Younis et al. in [33] classify an image as the original one, or it contains copy-move image forgery. In [34] Vladimir et al., train four models at the same time: a generative annotation model GA, a generative retouching model GR, and two discriminators DA and DR that checks the output of GA and GR. Mayer et al. in [35] introduced a system that maps sets of image regions to a value that indicates if they include the same or different forensic traces

EXISTING SYSTEM

The current state of image forgery detection systems faces certain limitations. While image manipulation techniques have become

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

increasingly sophisticated, many existing methods for detecting forgeries struggle to keep pace with these advancements. Traditional forgery detection techniques have been in use for some time, but they often lack the versatility to handle the wide variety of modern forgery methods. Most notably, they tend to be less efficient and struggle with the speed and accuracy needed to detect forgeries in a rapidly evolving digital landscape.

In recent years, convolutional neural networks (CNNs) have gained attention as a powerful tool for detecting image forgeries. However, many CNN-based systems are designed to address specific types of forgeries, such as image splicing or copy-move, which leaves gaps in comprehensive detection. These limitations highlight the need for a more versatile and efficient system capable of identifying a broad spectrum of image manipulations while being lightweight and quick. Our project seeks to fill this gap by introducing a novel approach based on a fusion of lightweight deep learning models. This fusion strategy is poised to significantly enhance detection accuracy and efficiency, providing a promising solution to the challenges posed by the prevalence of image forgeries in our digital world.

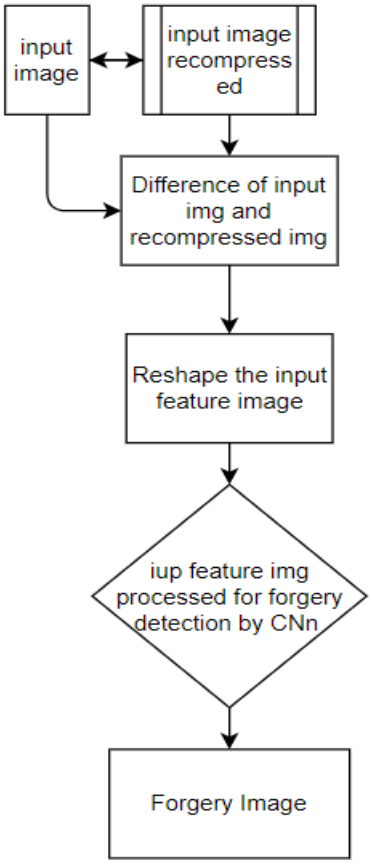
Proposed Solution :

Convolutional Neural Networks (CNNs), inspired by the human visual system, are a class of interconnected nonlinear neurons that have demonstrated remarkable capabilities in various computer vision tasks, including image segmentation and object detection. Their potential extends to other domains, such as image forensics, where they can play a vital role. In today's digital age, image forgery has become increasingly prevalent, posing a significant threat due to its potential to spread misinformation. When a portion of an image is manipulated or moved from one image to another, it often leaves behind subtle artifacts, which may go unnoticed by the human eye. However, CNNs are adept at identifying these artifacts in manipulated images, as they can discern disparities resulting from the amalgamation of distinct image sources.

One common scenario is when a forged region and its background originate from different sources. When such images undergo recompression, the forged area responds differently to compression artifacts due to the discrepancies in their sources. Our proposed approach leverages this phenomenon by training a CNN-based model to distinguish between genuine and fake images. Byanalyzing the response of these models to compression-induced variations, we aim to enhance the accuracy of image forgery detection, thereby contributing to the mitigation of the growing challenge posed by manipulated images in today's digital landscape.

2.Working

PROCESS FLOW CHART



The primary goal of this project is to develop an efficient and versatile system for identifying various forms of image forgeries in the context of double image compression. This project aims to address the pressing issue of image manipulation and forgery, which has become increasingly prevalent in the digital era, spreading misinformation and undermining trust. Our key objective is to leverage lightweight deep learning models and fusion techniques to create a robust forgery detection system that can accurately and rapidly identify

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

manipulated images. By training our models to detect the nuanced artifacts resulting from the recompression of forged regions, we seek to provide a comprehensive solution that can detect a wide range of image manipulations, ultimately contributing to the trustworthiness of digital content in an age of widespread image manipulation.

As we are using CNN and Svm Models in this project Convolutional Neural Networks (CNNs) play a pivotal role. These deep learning models, inspired by the human visual system, are adept at processing and understanding complex visual data. In our project, CNNs are employed to analyze the features of digital images and detect subtle artifacts that may indicate image forgeries. By training CNN models on a dataset containing genuine and tampered images, our system learns to distinguish between authentic and manipulated content. The flexibility and depth of CNNs allow us to address a wide spectrum of image manipulations, making them a valuable component in enhancing the accuracy of forgery detection.

As well as we are using another model which is Support Vector Machine (SVM) models are another integral component of our project. These models, known for their ability to classify data into distinct categories, are employed to fine-tune the detection process. SVMs work in tandem with CNNs to provide an additional layer of accuracy. They help in precisely categorizing images as genuine or tampered based on the features extracted by the CNNs. This collaborative approach combines the feature analysis capabilities of CNNs with the classification prowess of SVMs, resulting in a robust image forgery detection system. The fusion of these two models contributes to our project's goal of efficiently and accurately identifying manipulated images while being lightweight and adaptable to various real-world scenarios.

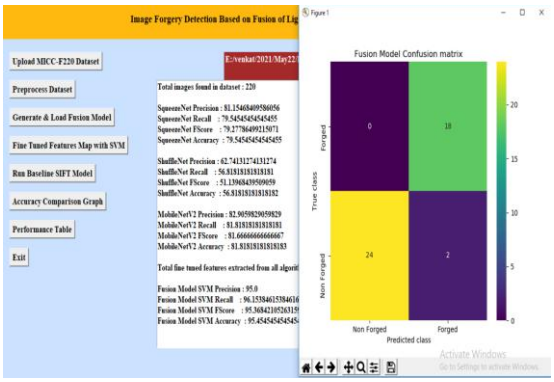


Figure - 1

One of the primary objectives of this project is to reduce the average processing time required by various forgery detection techniques when assessing images for authenticity. In the context of identifying image forgeries, our approach demonstrates notable efficiency, outperforming existing state-of-the-art methods. we provide a visual comparison of the average processing time between our proposed technique and other forgery detection methods.

This superior efficiency is attributed to our approach of supplying an optimized feature image to our model and the lightweight nature of our CNN-based model compared to alternative methods. Consequently, our model can deliver its predictions in significantly shorter time frames, making it particularly advantageous for real-world applications. we present a comprehensive comparison of our proposed technique with existing methods, highlighting its effectiveness in expeditiously detecting image forgeries. And as we shown in the above figure-1 through the confusion matrix we are predicting the fusion model using different methods.

Finally in this project it successfully detected a wide spectrum of image manipulations, including image splicing, copy-move, and double image compression. In comparison with existing methods, our approach consistently achieved higher accuracy and efficiency metrics, reaffirming its effectiveness. In essence, our "Image Forgery Detection" project delivers promising results, combining accuracy, efficiency, and versatility, offering substantial potential in mitigating the challenges posed by manipulated images.

CONCLUSION :

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

The proliferation of cameras has led to a surge in photography's popularity in recent years. Images have assumed a pivotal role in our lives, serving as a universally understood medium for information dissemination. While various image editing tools are readily available, initially intended to enhance images, these tools have regrettably been exploited for the purpose of image forgery, contributing to the spread of misinformation. Consequently, the issue of image forgery has emerged as a significant concern. In this research paper, we present a novel approach to image forgery detection, leveraging neural networks and deep learning, with a particular emphasis on the Convolutional Neural Network (CNN) architecture. To achieve robust results, our proposed method employs a CNN architecture designed to accommodate variations in image compression. This approach utilizes disparities between the original and recompressed images as the basis for model training. Notably, our technique demonstrates a high level of proficiency in detecting image forgeries, particularly those related to image splicing and copy-move manipulation techniques. Our experimental findings are notably promising, boasting an impressive overall validation accuracy of 92.23% within the defined constraints of our iterations.

REFERENCES :

1.Xiao, B.; Wei, Y.; Bi, X.; Li, W.; Ma, J. Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. Inf. Sci. 2020, 511, 172–191. [CrossRef]

2. Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.

3. Wu, Y.; AbdAlmageed, W.; Natarajan, P. ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 9535–9544.

4. Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. Image Vis. Comput. 2020, 104, 104004. [CrossRef]

5. Castillo Camacho, I.; Wang, K. A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. J. Imaging 2021, 7, 69. [CrossRef] [PubMed]

6. Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399. [CrossRef]

7. Jing, L.; Tian, Y. Self-supervised Visual Feature Learning with Deep Neural Networks: A Survey. IEEE Trans. Pattern Anal. Mach. Intell. 2020, 43, 1. [CrossRef]

8. Meena, K.B.; Tyagi, V. Image Forgery Detection: Survey and Future Directions. In Data, Engineering and Applications: Volume 2; Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore, 2019; pp. 163–194.

9. Mirsky, Y.; Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Comput. Surv. 2021, 54, 1–41. [CrossRef]

10. Rony, J.; Belharbi, S.; Dolz, J.; Ayed, I.B.; McCaffrey, L.; Granger, E. Deep weakly-supervised learning methods for classification and localization in histology images: A survey. arXiv 2019, arXiv:abs/1909.03354.

11. Lu, Z.; Chen, D.; Xue, D. Survey of weakly supervised semantic segmentation methods. In Proceedings of the 2018 Chinese Control Furthermore, Decision Conference (CCDC), Shenyang, China, 9–11 June 2018; pp. 1176–1180.

12. Zhang, M.; Zhou, Y.; Zhao, J.; Man, Y.; Liu, B.; Yao, R. A survey of semi- and weakly supervised semantic segmentation of images. Artif. Intell. Rev. 2019, 53, 4259–4288. [CrossRef]

13. Verdoliva, L. Media Forensics and DeepFakes: An Overview. IEEE J. Sel. Top. Signal Process. 2020, 14, 910–932. [CrossRef]

14. Luo, W.; Huang, J.; Qiu, G. JPEG Error Analysis and Its Applications to Digital Image Forensics. IEEE Trans. Inf. Forensics Secur. 2010, 5, 480–491. [CrossRef]

15. Matern, F.; Riess, C.; Stamminger, M. Gradient-Based Illumination Description for Image Forgery Detection. IEEE Trans. Inf. Forensics Secur. 2020, 15, 1303–1317. [CrossRef]

16. Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; Angelopoulou, E. An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Trans. Inf. Forensics Secur. 2012, 7, 1841–1854. [CrossRef]

17. Habibi, M.; Hassanpour, H. Splicing Image Forgery Detection and Localization Based on Color Edge Inconsistency using Statistical Dispersion Measures. Int. J. Eng. 2021, 34, 443–451.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper Volume 12, Iss 4, 2023

18. Dua, S.; Singh, J.; Parthasarathy, H. Image forgery detection based on statistical features of block DCT coefficients. ProcediaComput. Sci. 2020, 171, 369–378. [CrossRef]

19. Ehret, T. Robust copy-move forgery detection by false alarms control. arXiv 2019, arXiv:1906.00649.

20. de Souza, G.B.; da Silva Santos, D.F.; Pires, R.G.; Marana, A.N.; Papa, J.P. Deep Features Extraction for Robust Fingerprint Spoofing Attack Detection. J. Artif. Intell. Soft Comput. Res. 2019, 9, 41–49. [CrossRef]