STM JOURNALS

Journal of
Advances in Shell Programming

ISSN: 2395-6690
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoASP

https://journals.stmjournals.com/joasp

Research JoASP

Innovations in Forensic Imaging: Leveraging Deep Learning for Authenticity Verification

Vishwajeet Mhetre[1], Sudershan Dolli[2,*], Sharvani Mahajan[3], Vyankatesh Kalme[4]

Abstract

The advent of digital media has necessitated advancements in forensic imaging, especially for the detection and verification of image authenticity. In this context, digital image forensics plays a critical role in identifying manipulated or counterfeit images. This paper presents a new method that uses deep learning techniques to enhance image forgery detection. The approach utilizes a convolutional neural network (CNN) to automatically learn and recognize the intricate features present in both authentic and altered images. The network is meticulously trained on a diverse dataset encompassing a wide array of real and fake images. These images undergo various manipulation techniques, including splicing, copy-move, and retouching, ensuring comprehensive exposure to potential forgeries. By analyzing subtle pixel-level discrepancies and spatial relationships, the CNN is equipped to discern authentic images from those that have been tampered with. Our approach utilizes the Busternet deep learning architecture, renowned for its efficacy in image analysis, to develop a sophisticated copy-move forgery detection system. This architecture excels in recognizing minute differences in image regions, enabling precise localization and verification of altered segments. The experimental results demonstrate the model's superior performance in detecting forgeries, highlighting its potential as a powerful tool in digital forensic investigations. This work underscores the significant promise of deep learning applications in forensic imaging, paving the way for enhanced methods of image authenticity verification and contributing to the broader field of digital forensics.

Keywords: Busternet, convolutional neural networks (CNN), deep learning, image forgery detection (IFD)

INTRODUCTION

Image forgery, the act of altering or manipulating images to deceive viewers, has become increasingly prevalent in today's digital age. From social media platforms to legal evidence, the authenticity and integrity of digital images are critical. Detecting image forgeries plays a vital role in ensuring trustworthiness and reliability in various domains, including forensics, journalism, and entertainment. Traditional methods of image forgery detection often rely on manual inspection or basic digital analysis techniques. However, with the rapid advancements in deep learning and artificial intelligence, more sophisticated and accurate forgery detection systems have emerged. Deep learning models, particularly convolutional neural networks (CNNs), have shown remarkable capabilities in learning complex patterns and features from image data, making them well-suited for image forgery detection tasks. The essence of using deep learning for image forgery detection lies in its ability to automatically extract relevant features, identify inconsistencies, and discern subtle manipulations that may elude human perception or traditional algorithms. By training deep learning

***Author for Correspondence**
Sudershan Dolli
E-mail: sudershandolli@gmail.com

[1,3,4]Student, Department of Electronics & Telecommunication Engineering, Smt. Kashibai Navale College of Engineering (SKNCOE), Pune, Maharashtra, India
[2]Assistant Professor, Department of Electronics & Telecommunication Engineering, Smt. Kashibai Navale College of Engineering (SKNCOE), Pune, Maharashtra, India

Received Date: July 03, 2024
Accepted Date: July 25, 2024
Published Date: August 1, 2024

Citation: Vishwajeet Mhetre, Sudershan Dolli, Sharvani Mahajan, Vyankatesh Kalme. Innovations in Forensic Imaging: Leveraging Deep Learning for Authenticity Verification. Journal of Advances in Shell Programming. 2024; 11(2): 28–33p.

models on large datasets of authentic and manipulated images, these systems can learn to distinguish between genuine and forged content with high accuracy.

In consonance with image evolution, image faking, either by the photographer or through image manipulations, also has been followed alongside image/photography advancements traditionally. The gains made by the beneficiaries of fake photography can be in terms of both political and economic. The prolonged sustenance and continuing prevalence of forged and manipulated images can be credited to naïve and trusting public. Owing to vastly circulating counterfeited visuals on easily and globally accessible electronic media currently [1], there is no denial to the fact that physically or seeing is believing now. Over the past decade, the rapid advancement of smartphones, surveillance cameras, social media, and networking services has led to a tremendous increase in the volume of digital image data [2].

Digital images often provide more information and are more effective than text-based communication, making them powerful and reliable tools for conveying information across various digital platforms. Their use has transformed every sector, whether public or private. It is important to note that, in our rapidly advancing technological landscape, there are many tools and software—both paid and free—that can manipulate digital images, raising concerns about their authenticity and reliability [3]. The use of these tools and software makes it easier to forge and post-process the content of image without considerably lowering its quality or leaving any visible imprints. As a result, the manipulated digital images can be misused to communicate wrong information, fake news, or fulfil any malignant agenda. According to Elaskily et al. [4], forgery can be categorized into five types based on the techniques applied: (1) copy-move (cloning), (2) splicing, (3) retouching, 4) resampling, and (5) morphing.

LITERATURE SURVEY

It is common for literature surveys to involve collaboration among multiple researchers, experts, or authors who contribute their knowledge, expertise, and insights to compile a comprehensive review of the literature in a specific field or topic. The collaboration could involve anywhere from one researcher to a team of experts, depending on the depth and breadth of the survey and the resources available for conducting the research.

With regards to digital image forgery detection techniques, these can be categorized into two broad approaches: (1) active image forensic methods and (2) passive (blind) image forensic methods [5]. To counter the rapidly complicating forgery methods due to easily accessible technologically advanced tools, passive image forensic methods that basically rely on underlying statistical imbalances created because of forgery, have also undergone massive evolution. Presently, deep learning-based techniques are regarded as state-of-the-art for image processing due to their enhanced accuracy and automatic feature extraction capabilities. These techniques apply layer-based algorithms to process data, recognize and classify visual objects.

In a bid to emulate all other fields, the field of digital image forensics is being influenced by deep learning too. The approach of using deep learning techniques for digital image forgery detection by contemporary image processing researchers has received considerable attention in the recent past [6]. It is due to the reason that the use of conventional statistical digital image forgery detection methods poses limitation of manual application of feature extraction techniques for the desired output. Whereas, deep learning-based methods consist of hierarchical neural networks applied in stacked (deep) layers that function layer-wise in feature extraction to give the output. Some of the most relevant research work done in the field of digital image forgery detection using deep learning methods is covered analytically in the succeeding paragraphs.

Chen et al. [7] presented an approach of median filtering forensic technique built on CNN for digital image forgery detection. The CNN network architecture used in their scheme consisted of eight layers

by introducing a filter layer as the input layer. Through alternative convolution and pooling layers, numerous features were obtained to aid hierarchical learning process by the layers and then classify. This technique can be regarded as the first of its kind which used amalgamation of median filtering and CNN framework. The researchers were able to show significantly improved results for copy-move, cut-pasting forgeries and detecting median filtering from low resolution and Joint Photographic Experts Group (JPEG) compressed images as compared to other well-known image forensic tools that worked on hand-designed features.

Bayar and Stamm [8] proposed CNN architecture, namely constrained CNN, that was capable of learning image modification features adaptively followed by accurate identification of manipulation type that the image had suffered. The designed tool using constrained CNN was aimed to be potent digital image manipulation detection tool which could be used for general purpose. This state-of-the-art work contributed a CNN with more sophisticated and deeper architecture that contained a constrained convolutional layer. This network performed efficiently not only to detect manipulations on JPEG images but also discriminated between the variations in manipulation actions.

Rao and Ni [9] introduced a simplistic (10-layered) CNN-based deep learning approach which relied on automatic utilization of red-green-blue (RGB) color images as input to train a hierarchical depiction. The technique proved equally efficient for copy-move and splicing forgeries. The novelty of the method was automatic learning of features for two forgery types, that is, copy-move and splicing.

Yang et al. [10] presented an improved method for digital image forensics. The technique was based on the idea of taking care of both categories of smooth filtering, that is, linear and nonlinear, and was specially focused to detect the forged images which had been post-treated with filtering performed to reduce the border discontinuity. The presented CNN framework consisted of six layers before the classifier for the output. The approach showed robustness against degradation of images by JPEG compression. However, it was vulnerable against the cut-paste forgery not post-processed with smooth filtering.

A literature survey on image forgery detection using deep learning summarizes the latest advancements in detecting various types of image manipulations like copy-move, splicing, and retouching. It compares traditional methods with deep learning approaches like CNNs, generative adversarial networks (GANs), and recurrent neural networks (RNNs), highlighting deep learning's superior ability to handle complex forgeries. The survey covers feature extraction techniques such as local binary pattern (LBP), scale-invariant feature transform (SIFT), and histogram of oriented gradients (HOG), enhancing model performance. It also discusses common datasets, evaluation metrics, challenges like adversarial attacks, and suggests future directions like multimodal detection for improved accuracy and real-time systems for practical applications.

PRESENT METHODOLOGY

Image forgery and object detection using deep learning is centered on the implementation of the Busternet architecture and CNNs for image forgery detection (IFD). We started by preprocessing data to ensure image quality and consistency. The Busternet framework, designed specifically for IFD, integrated CNNs to capture intricate image features. Training involved large datasets augmented with synthetic data for enhanced model generalization. Through extensive experimentation, we fine-tuned the hyperparameters to optimize model performance. Evaluation across various datasets confirmed the scalability and effectiveness of our approach in real-world scenarios as shown in Figure 1.

EXPECTED RESULTS AND DISCUSSION

Image forgery and object detection using deep learning project, utilizing the Busternet architecture and CNN, includes improved accuracy and efficiency in detecting various types of image forgeries. This approach is designed to tackle issues like tampered areas, splicing, and copy-move forgeries. The

discussion will focus on the effectiveness of Busternet in enhancing IFD capabilities compared to traditional methods, highlighting its strengths in handling complex forgery techniques and providing insights into further advancements in deep learning-based IFD systems.

The login page of the image forgery and object detection serves as the entry point for authorized users as shown in Figure 2. It usually features fields for entering credentials like a username and password, as well as options for password recovery or account creation. The design is user-friendly, with clear instructions and error messages for incorrect entries. Enhanced security measures, such as CAPTCHA or two-factor authentication, may also be included.

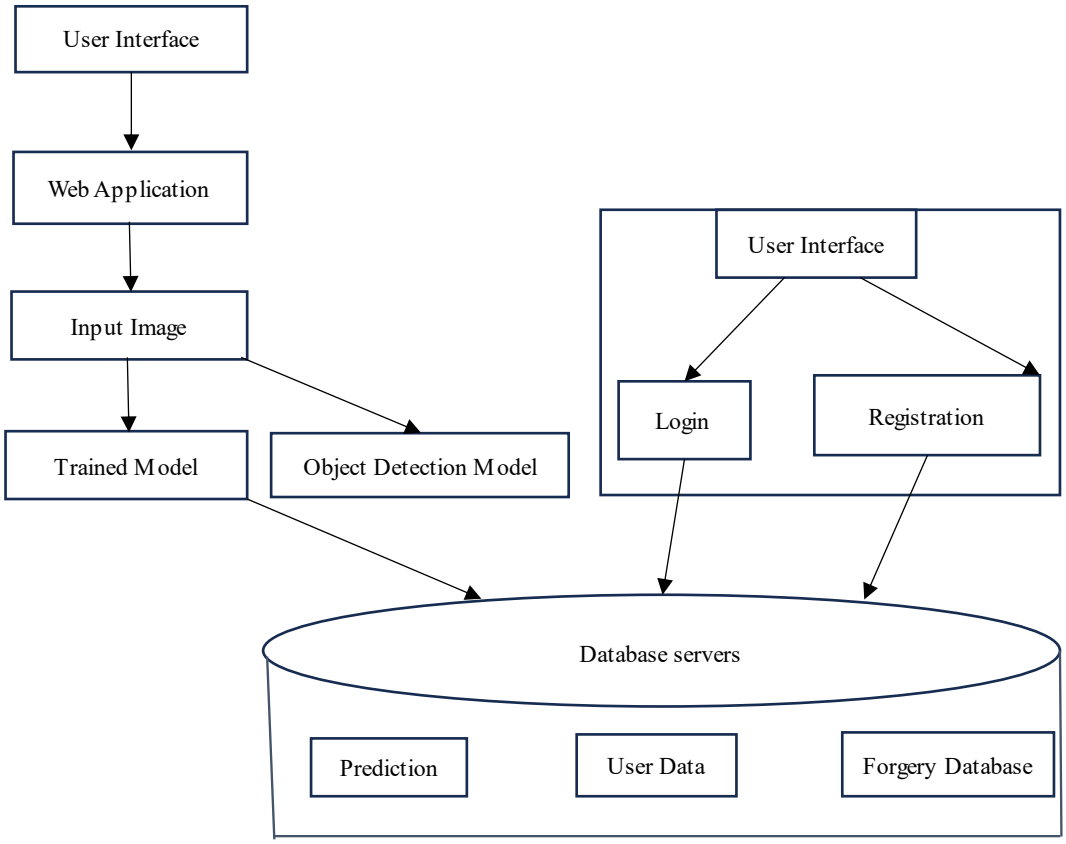

Figure 1. Object detection model.

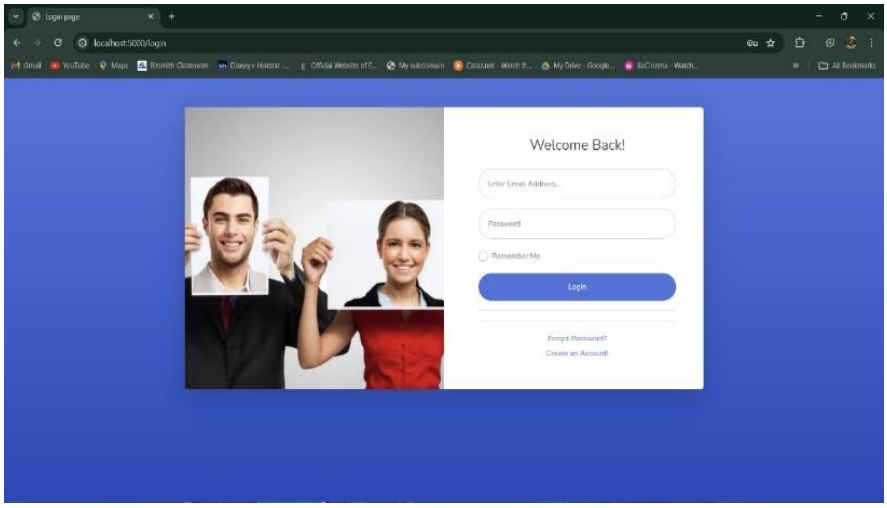

Figure 2. Login page.

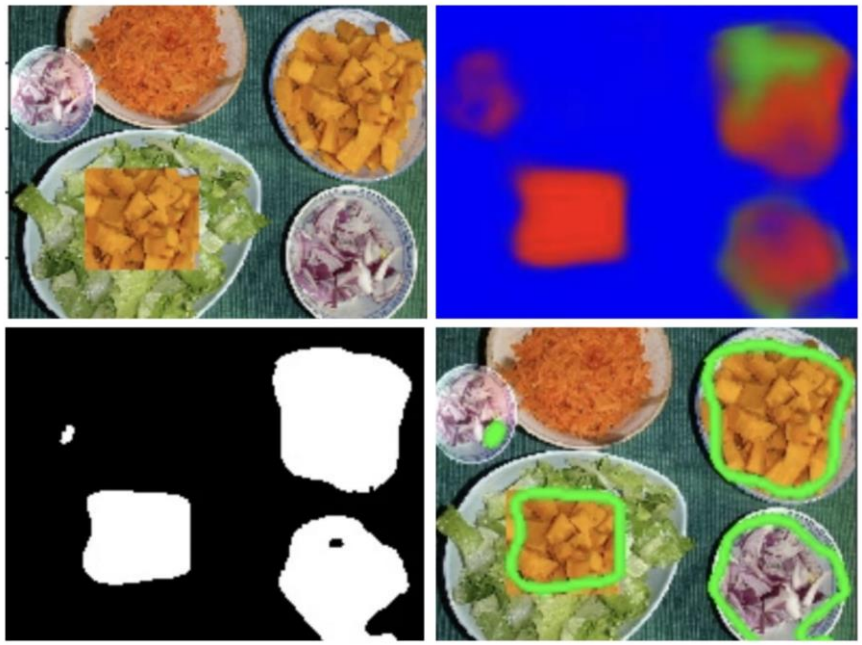

Figure 3. Forgery detection.

The image forgery and object detection project focuses on developing an advanced system for detecting various types of image forgeries. By leveraging deep learning techniques, especially the Busternet architecture and CNN, the system can accurately identify tampered regions, splicing, copy-move forgeries, and other forms of image manipulation. This project aims to enhance the capabilities of IFD systems by utilizing state-of-the-art deep learning models and algorithms as shown in Figure 3.

CONCLUSION

Image forgery detection using deep learning marks a significant advancement in countering the increasingly sophisticated digital image manipulations. Deep learning techniques offer substantial advantages, reshaping forgery detection with outcomes previously difficult using traditional methods. Our project underscores this evolution, showcasing a range of forgery detection techniques and highlighting deep learning's promise. Specifically, we focused on implementing the Busternet architecture to bridge gaps identified in existing literature. This approach exemplifies the project's commitment to pushing the boundaries of forgery detection using cutting-edge deep learning methodologies.

Acknowledgments

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals. We would like to extend my sincere thanks to all of them. We are highly indebted to Mr. S. P. Dolli for his guidance and constant supervision as well as for providing necessary information regarding the project and also for his support in completing the project. His constant guidance and willingness to share his vast knowledge made us understand this project and its manifestations in great depths and helped us to complete the assigned tasks on time. We would like to express our gratitude towards our parents and our classmates for their kind cooperation and encouragement which helped us in completion of this project. Our thanks and appreciations also go to our colleagues in developing the project and people who have willingly helped us out with their abilities.

REFERENCES

1. Teerakanok S, Uehara T. Copy-move forgery detection using GLCM-based rotation-invariant feature: a preliminary research. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, July 23–27, 2018. Vol. 2, pp. 365–369.

2. Phan-Xuan H, Le-Tien T, Nguyen-Chinh T, Do-Tieu T, Nguyen-Van Q, Nguyen-Thanh T. Preserving spatial information to enhance performance of image forgery classification. In: 2019 International Conference on Advanced Technologies for Communications (ATC), Hanoi, Vietnam, October 17–19, 2019. pp. 50–55.
3. Abd Warif NB, Wahab AW, Idris MY, Ramli R, Salleh R, Shamshirband S, Choo KK. Copy-move forgery detection: survey, challenges and future directions. J Netw Computer Appl. 2016; 75: 259–278.
4. Elaskily MA, Aslan HK, Elshakankiry OA, Faragallah OS, Abd El-Samie FE, Dessouky MM. Comparative study of copy-move forgery detection techniques. In: 2017 International Conference on Advanced Control Circuits Systems (ACCS) Systems & 2017 International Conference on New Paradigms in Electronics & Information Technology (PEIT), Alexandria, Egypt, November 5–8, 2017. pp. 193–203.
5. Ustubioglu B, Ulutas G, Ulutas M, Nabiyev VV. A new copy move forgery detection technique with automatic threshold determination. AEU – Int J Electron Commun. 2016; 70 (8): 1076–1087.
6. Abidin AB, Majid HB, Samah AB, Hashim HB. Copy-move image forgery detection using deep learning methods: a review. In: 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, December 2–3, 2019. pp. 1–6.
7. Chen J, Kang X, Liu Y, Wang ZJ. Median filtering forensics based on convolutional neural networks. IEEE Signal Process Lett. 2015; 22 (11): 1849–1853.
8. Bayar B, Stamm MC. Constrained convolutional neural networks: a new approach towards general purpose image manipulation detection. IEEE Trans Inform Forens Security. 2018; 13 (11): 2691–2706.
9. Rao Y, Ni J. A deep learning approach to detection of splicing and copy-move forgeries in images. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, December 4–7, 2016. pp. 1–6.
10. Yang B, Sun X, Cao E, Hu W, Chen X. Convolutional neural network for smooth filtering detection. IET Image Process. 2018; 12 (8): 1432–1438.

