International Journal of Computer
Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 13, Issue 2, Jul–Dec 2024; 65–72
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations
IASET

MOBILE NET-DRIVEN DEEP LEARNING APPROACH FOR ROBUST DETECTION OF IMAGE FORGERY

Jagabattula Saahitha, Borra. Sai Venkata Aravind Kumar, Bollineni Revanth, Gudipalli Sai Sri Sumanth & Dheeraj Sikhinam

Department of CSC, SRM Institute of Science and Technology, Ramapuram, Tamilnadu, India

ABSTRACT

The availability of advanced image altering tools such as Photoshop and GIMP has made it progressively harder to discern authentic and tampered photos, making the identification of image fraud an important topic of research. Conventional picture fraud detection techniques mostly rely on manually created features that are limited to identifying particular kinds of manipulation, including copy-move or splicing forgeries. However, because they have trouble identifying subtler or more intricate kinds of manipulation, these methods frequently have limited generalizability. The use of neural networks for autonomous feature extraction has significantly changed due to the quick progress in deep learning, which provides greater accuracy and variety in picture forgery detection tasks.

In this research, we propose a MobileNet-based deep learning system for image forgery detection. MobileNet is a good option for real-time applications where accuracy and speed are crucial because of its reputation for computational efficiency and smaller model sizes. The phases of the system architecture are data gathering, preprocessing, model implementation, assessment, and ultimate prediction. The pre-processed photographs in the study's dataset, which includes both authentic and manipulated photos, are resized to a consistent dimension and converted to grayscale. Next, our MobileNet model is trained to distinguish between actual and fraudulent images.

To make sure the model can consistently distinguish between real and manipulated images, its performance is assessed after training using important metrics like accuracy, classification reports, and confusion matrices. The outcomes show that MobileNet is superior to manual feature-based techniques in the detection of image forgeries, attaining a high degree of accuracy. This study adds to the continuing work in the area of computer image forensics by providing a practical yet effective method for spotting manipulated photos

KEYWORDS: *Image Forgery Detection, Deep Learning, MobileNet, Image Processing, Classification, Tampered Images, Real-Time Detection*

Article History

***Received:** 22 Sep 2024 | **Revised:** 28 Sep 2024 | **Accepted:** 05 Oct 2024*

INTRODUCTION

The alteration of visual content has become easy and commonplace with the rise of digital images and the accessibility of strong editing programs like Photoshop, GIMP, and CorelDraw. Although these tools allow for greater creative flexibility, they have also given rise to grave doubts about the veracity of photographs, particularly in fields such as social media, journalism, legal procedures, and medical imaging. It is getting harder and harder to tell the difference between real and manipulated photographs because of the capacity to manipulate images without leaving noticeable evidence[1]. Because of this, image fraud detection has become an important field of study in digital forensics with the goal of preserving the truthfulness of visual content.

Conventional methods of detecting image forgeries focus on manually created characteristics to find anomalies, like texture, uneven illumination, and pixel correlation. These techniques are usually intended to identify particular kinds of forgeries, like splicing or copy-move. But these methods' main drawback is that they aren't really generalizable. Every technique is frequently designed to identify a single kind of manipulation, making it useless against subtler or more intricate forgeries. Moreover, conventional detection approaches find it difficult to keep up with the advancements in picture alteration techniques.

Researchers have been using methods of deep learning, which have completely changed the area of computer vision, to get beyond these constraints. Convolutional neural networks (CNNs)[2], in particular, are deep learning models that have proven to be exceptionally good at automatically extracting complicated information from images, which makes them ideal for challenging applications like image forgery detection. MobileNet is a deep learning architecture that is particularly well-suited for real-time applications because of its computational efficiency and lightweight design. Because of its depth wise separable convolutions, MobileNet is the method of choice for applications that need to be accurate and quick while extracting high-level features from images in a tiny model size.

In this research, we describe a MobileNet-based deep learning-powered image forgery detection system. Our method focuses on classifying manipulated photographs in order to accurately separate authentic images from fakes[3]. Our approach goes through several phases, such as data preparation, training of models, and evaluation, using a dataset of real and fake photos. This results in a dependable and effective method for detecting image forgeries. The outcomes show that not only does our system perform better than conventional approaches[4], but it also offers an affordable solution for practical uses where the ability to identify manipulated photos is crucial to upholding the legitimacy and trustworthiness of digital content.

This study adds to the expanding corpus of research in digital image forensics by providing a sophisticated, yet approachable method for detecting manipulated photos through the use of cutting-edge deep learning techniques.

LITRATURE SURVAY

[1] Manjunatha, S., & Patil, M. M. (2021, February)The research project aims to investigate current approaches for deep learning-based passive picture tampering detection in detail. The primary topic of this survey is the use of deep learning algorithms for tampering detection. Existing tampering detection algorithms have validated their accuracies in tampering detection using several images tampering datasets, including MICC, CASIA, UCID, and so on. The analysis reveals that not every technique—such as splicing, compression, rotation, resampling, copy-move, etc.—obtains acceptable accuracy for every type of assault. According to the study, in order to effectively identify tampering, it is crucial to create a deep learning-based feature extraction system that can more effectively learn the link between pixels. Unlike a previous study, this work discusses important advancements in deep learning-based passive picture forensic analysis tools. The benefits, drawbacks, dataset utilized, and type of assault taken into consideration are examined in relation to current approaches. The study also identifies unresolved problems and upcoming obstacles, and it offers a potential future solution for developing an effective deep learning tampering detection mechanism[5]. The results of the experiment indicate good performance in terms of TPR, FPR, and F1-Score.

[2] Sharma, P., Kumar, M., & Sharma, H. (2023). The digital image serves as vital proof in a variety of industries, including insurance claims, medical imaging, intelligence systems, criminal investigations, forensic inquiry, and journalism. Social media and the internet are reliable sources of information when it comes to images. However, photos can be maliciously manipulated or used for personal gain by using readily available software or editing programs like Photoshop, Corel Paint Shop, PhotoScape, PhotoPlus, GIMP, Pixelmator, etc. It is becoming more challenging to discern between actual and photo-realistic images when using active, passive, and other cutting-edge deep learning techniques like GAN methods. Nowadays, the main goal of digital picture tamper detection is to ascertain the consistency and legitimacy of digital images. Common tactics and solutions, like uniform data sets, standards, evaluation criteria, and generalized methodologies, are employed to address the main research concerns.The assessment of several picture tamper detection techniques is summarized in this publication. This paper includes a comparative examination of picture criminological (forensic) approaches and a brief discussion of image datasets. Additionally, the limitations of recently emerging deep learning approaches have been discussed. The goal of this research is to thoroughly examine image fraud detection techniques utilizing both traditional and cutting-edge deep learning methodologies.

[3] Castillo Camacho, I., & Wang, K. (2021).Seeing no longer equates to believing. The capacity to alter an image is now at our fingers thanks to many approaches. The organizations that develop and market these technologies have focused on reducing the need for specialist knowledge as the challenge of utilizing these strategies lowers. Moreover, modern image forgeries are so lifelike that it is challenging for the unaided eye to distinguish between authentic and fraudulent media. This may lead to a variety of issues, such as skewed public perception and the use of fabricated evidence in court. These factors make it crucial for us to have instruments at our disposal that can aid in truth-finding. This study provides an extensive assessment of the literature on picture forensics techniques, emphasizing deep learning-based approaches in particular. We address a wide range of picture forensics issues in this paper, such as identifying cameras, classifying computer graphics images, identifying purposeful image falsifications, detecting routine image alterations, and identifying Deepfake images as they emerge. This review has shown that, despite the fact that picture forgeries are getting easier to make, there are a number of ways to identify each type of one. Additionally provided are a survey of anti-forensic strategies and an evaluation of several image databases. Lastly, we make some recommendations for future research paths that the scientific community may take into account to address the spread of doctored photographs more successfully.

[4] Roobini,M.S (May 2004). The widespread availability of image alteration tools in the digital age has resulted in an unsettling rise in the production of false images that have the potential to mislead and fool people. These fakes are the result of a wide range of changes, including copy-move operations, face modifications, and image splicing. This research article explores the field of deep learning, an advanced method known for its capacity to discern intricate patterns in data, in an effort to tackle this mounting challenge. Improving the fundamental workings of current methods like CNN, GAN, Transfer Learning, and Surface Feature Utilization is the main goal. This work establishes the foundation for the creation of more accurate and effective methods to deal with the problems presented by fake photos by offering insights into the potential and constraints of deep learning techniques. Comparing the proposed adjustments to the existing approaches, the experimental results showed a 6% average improvement in accuracy and a 5% rise in F1-score.

[5]Yang, P(2020)One of the most popular methods for blindly confirming the authenticity and integrity of digital images is image source forensics. Many academics have used data-driven methods to this job in recent years, motivated by the exceptional results these techniques have produced on machine vision problems. We outline the most significant data-driven techniques that address the issue of image source analysis in this survey. In an effort to bring structure to this

enormous discipline, we have broken it down into five smaller topics: source camera identification, source social network identification, computational graphics (CG) image forensic, recaptured image forensic, and GAN-generated picture detection. In addition, the works on counter- and anti-forensics are included. We have outlined the benefits and drawbacks of each of these tasks' current proposed techniques in this exciting and diverse field of study.

METHODLOGY

Data Collection

The dataset included in this study is made up of both authentic and altered photos, including several kinds of forgeries such removal, splicing, and copy-move. To guarantee diversity, these photos were collected from both specially constructed databases and publicly accessible sources. Each photograph's authenticity was confirmed, and standard image alteration programs like Photoshop by Adobe and GIMP were used to produce the forgeries in order to mimic realistic tampering[6]. A variety of resolutions for both colour and grayscale photographs are included in the dataset.

Data Preprocessing

In order to guarantee consistency in the input data and raise the model's accuracy, preprocessing is essential. The dataset was pre-processed using the subsequent procedures.

Resizing: The photographs were all downsized to a specific dimension (e.g., 224x224 pixels) in order to comply with the MobileNet architecture's requirement for input size. These guarantees input shape consistency and expedites the learning process of the model.

Grayscale Conversion: The photos were transformed to grayscale, even though MobileNet can handle RGB inputs, in order to reduce input complexity and concentrate on feature extraction without the additional variation of colour information[7].

Normalization: The pixels were scaled to fall from 0 to 1 by dividing by 255. This stage expedites the convergence of the model by ensuring that the data entered parameters are on an identical scale.

Data Augmentation: rotate, enlargement, and flip were some of the data augmentation strategies used to increase the model's generalizability and avoid overfitting. As a result, the dataset is more diverse and the model is more resilient to changes in image orientation and transformation.

Splitting the Dataset

The dataset was divided into test and training sets in order to train and assess the model. Generally, training took up 70% of the data, with the remaining 30% going toward testing. This division guarantees that a model has an adequate amount of unseen data for assessment and an adequate amount of knowledge for understanding the patterns in both genuine and fake images[8]. Furthermore, during training, a tiny percentage (usually 10%) of the sample set was reserved for validation in order to track the model's success and avoid overfitting.

Model Implementation

The MobileNet architecture was chosen as the primary basis for image forgery detection due to its efficiency and lightweight design. Real-time applications can benefit from MobileNet's depthwise separable convolutions, which drastically lower computing costs without sacrificing accuracy[9].

MobileNet: In comparison to conventional convolutional layers, the number of parameters in the MobileNet architecture is significantly reduced because to the use of depthwise and point-by-point convolutions. Because of this, the network can operate quickly and efficiently, which makes it perfect for applications like detecting image forgeries.

Transfer Learning: Transfer learning was used since it saves a lot of data when building a deep learning model from scratch. Our forgeries dataset was used to refine a MobileNet model that was originally trained on the ImageNet set of images. Transfer learning makes use of the pre-trained model's information to enhance performance and shorten training time[10].

Layers Added: A few more fully linked layers have been included on top of the model that had been trained in order to modify the MobileNet architecture for the goal of binary classification (actual vs. forged)[11]. The last layer produced a probability between 0 and 1 representing the possibility that the image was manipulated or authentic using a sigmoid activation function.

Training the Model

The binary cross-entropy function for loss, which works well for binary classification problems, was used to train the MobileNet model. Because of its computing efficiency and adjustable learning rate, the Adam optimizer was used. The learning rate was meticulously adjusted to guarantee convergence without overfitting during training[12], and the model's weights were updated repeatedly based on the loss function.

Key Parameters during Training

- **Epochs**: 50–100 epochs of training were given to the model, according to the validation results.
- **Batch Size**: A single batch of 32 was selected in order to balance model accuracy and training time.
- **Early Stopping:** Early stopping was used to prevent overfitting; training was stopped if the validation loss did not improve after a certain number of epochs.

Evaluating the Model

When the model was trained, its success on the examination dataset was evaluated using many key indicators.

- **Accuracy:** The proportion of properly categorized photographs to all of the test set's images.
- **Confusion Matrix:** To give a thorough explanation of true positives, false positives, true negatives, and false negatives, a confusion matrix was created. This aids in evaluating how well the model distinguishes between authentic and fake photos.
- **Precision, Recall, and F1-Score:**In order to gain insight into the model's capacity to reduce false positives and false negatives, these metrics were calculated from the confusion matrix.
- **ROC Curve and AUC:** The discriminative power of the model was assessed using the area under the curve (AUC) and the receiver operating characteristic (ROC) curve. Better performance is indicated by a higher AUC.

Final Prediction

The model's performance was assessed before the system was put into use for real-time prediction. Feeding individual test photos into the training MobileNet model and identifying them as genuine or fake is the last prediction step[13]. A probability score is provided with the findings to indicate the level of confidence in the categorization. Imagining the confusion matrix, classification report, and accuracy score are all included in this step.

RESULT AND DISCUSSION

Model Performance and Accuracy

After building the MobileNet algorithms on the dataset, the system demonstrated an excellent level of accuracy in classifying photographs as authentic or fraudulent. The robustness of the Mobile Net design in identifying minute details in the images was demonstrated by the regular evaluation of the model's accuracy utilizing samples for training and testing. The system demonstrated a 90% average success rate on the entire set of tests, suggesting that its trainee was excellent in learning to distinguish between real and altered photographs.

Confusion Matrix and Classification Report

We produced a confusion matrix and classification report in order to assess the system's classification performance in more detail. The confusion matrix provides information on how successfully the model differentiates between authentic and fake images by showing the number of true positives, false positives, true negatives, and false negatives. The classification report gives specific metrics for each class (actual and fake photos) including recall, precision, and F1-score. The model's effectiveness in accurately detecting both real and altered photos is suggested by the system's high recall rates and precision, together with a low number of false positives and false negatives.

- **Precision:** The model produced quite few erroneous positive predictions, as evidenced by the accuracy values for the two categories being above 90%.
- **Recall:** A significant fraction of the true occurrences in both classes were effectively detected by the model, as evidenced by recall values that were likewise above 90%.
- **F1-Score:** The model's good balance among precision and recall was demonstrated by the comparably high F1-scores

Comparative Analysis with Traditional Methods

The suggested MobileNet-based solution fared better than conventional image forgery detection systems, which mostly depend on manually created features and particular tampering detection methods, in a number of important areas. Conventional techniques are frequently restricted to identifying particular kinds of forgeries, like splicing or copy-move. On the other hand, higher ability to be generalized and the detection of a greater variety of image modifications were made possible by the deep learning-based technique, especially when utilizing MobileNet, since it eliminated the need for manual feature engineering. Furthermore, in comparison to conventional techniques, the deep learning model's detection capabilities are greatly improved by its automatic learning of intricate patterns in the photos.

Impact of Pre processing and Dataset

The preprocessing phase, which involved resizing and grayscale conversion of the photos, was critical to the system's overall efficiency. The approach made sure the model concentrated on identifying the essential features rather than meaningless changes in image dimensions or colour by standardizing the image input. The success of the model was also aided by the high Caliber and variety of the dataset. The addition of other kinds of tampered images (such as cutting, copy-move, and removal) improved the model's ability to generalize and function well in situations where forgeries are common and difficult to identify.

Challenges and Limitations

Even though the system has a high accuracy rate, there were several difficulties in its creation and assessment. The detection of incredibly delicate forgeries, where the alterations were almost invisible to the human eye as well as the model, was one of the main limits. These scenarios posed difficulties, and although the model functioned flawlessly, these edge cases might require extra training data or modifications to the model's design. Furthermore, the system's dependence on grayscale images might make it less sensitive to hue-based manipulations in some situations, indicating the possible advantage of adding color channels in later versions.

Discussion on Real-World Applicability

The study's findings show that the suggested approach can be successfully implemented in a range of real-world settings when image authenticity is crucial, including news media, digital forensics, and the verification of legal evidence. Real-time image forgery detection is made possible by the MobileNet architecture, which makes it appropriate for incorporation into high-speed processing systems like automated material verification platforms or surveillance systems. However, to keep up with the increasing complexity of picture tampering techniques, regular modifications to the model and dataset will be required.

CONCLUSION

The MobileNet-based picture forgery detection system's efficacy is confirmed by the findings and discussion in this part. The system shows to be a considerable improvement over conventional methods, providing a scalable and dependable solution for identifying manipulated photos, with excellent accuracy, precision, recall, and F1-scores. The difficulties found lay the groundwork for upcoming advancements, opening the door for ever more reliable image forgery detection algorithms.

REFERENCE

1. *Le-Tien, T., Phan-Xuan, H., Nguyen-Chinh, T., & Do-Tieu, T. (2019). Image forgery detection: A low computational-cost and effective data-driven model. International Journal of Machine Learning and Computing, 9(2), 1.*
2. *Zhang, Y., Goh, J., Win, L. L., & Thing, V. (2016). Image region forgery detection: A deep learning approach. In Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016 (pp. 1-11). IOS Press.*
3. *Zanardelli, M., Guerrini, F., Leonardi, R., & Adami, N. (2023). Image forgery detection: a survey of recent deep-learning approaches. Multimedia Tools and Applications, 82(12), 17521-17566.*
4. *Jaiswal, A. K., & Srivastava, R. (2022). Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model. Neural Processing Letters, 54(1), 75-100.*
5. *Aria, M., Hashemzadeh, M., & Farajzadeh, N. (2022). QDL-CMFD: A Quality-independent and deep Learning-based Copy-Move image forgery detection method. Neurocomputing, 511, 213-236.*
6. *Zhao, L., Chen, C., & Huang, J. (2021). Deep learning-based forgery attack on document images. IEEE Transactions on Image Processing, 30, 7964-7979.*

7. *Ali, S. S., Ganapathi, I. I., Vu, N. S., Ali, S. D., Saxena, N., & Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. Electronics, 11(3), 403.*

8. *Rao, Y., & Ni, J. (2016, December). 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) (pp. 1-6). IEEE.*

9. *Abidin, A. B. Z., Majid, H. B. A., Samah, A. B. A., & Hashim, H. B. (2019, December). Copy-move image forgery detection using deep learning methods: a review. In 2019 6th international conference on research and innovation in information systems (ICRIIS) (pp. 1-6). IEEE.*

10. *Cozzolino, D., Poggi, G., & Verdoliva, L. (2022). Data-Driven Digital Integrity Verification. In Multimedia Forensics (pp. 281-311). Singapore: Springer Singapore.*

11. *Manjunatha, S., & Patil, M. M. (2021, February). Deep learning-based technique for image tamper detection. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1278-1285). IEEE.*

12. *Sharma, P., Kumar, M., & Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimedia Tools and Applications, 82(12), 18117-18150.*

13. *Gaurav, A., Gupta, B. B., & Bansal, S. (2024). Forgery Detection Based on Deep Learning for Smart Systems. Digital Forensics and Cyber Crime Investigation: Recent Advances and Future Directions, 196.*

14. *Castillo Camacho, I., & Wang, K. (2021). A comprehensive review of deep-learning-based methods for image forensics. Journal of imaging, 7(4), 69.*

15. *Roobini, M. S., Marappan, S., Roy, S., Muneera, M. N., & Jayanthi, S. (2024, May). Augmenting Deep Learning Models for Robust Detection and Localization of Image Forgeries. In 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-8). IEEE.*

16. *Yang, P., Baracchi, D., Ni, R., Zhao, Y., Argenti, F., & Piva, A. (2020). A survey of deep learning-based source image forensics. Journal of Imaging, 6(3), 9.*

17. *Sun, K., Liu, H., Yao, T., Sun, X., Chen, S., Ding, S., & Ji, R. (2022, October). An information theoretic approach for attention-driven face forgery detection. In European Conference on Computer Vision (pp. 111-127). Cham: Springer Nature Switzerland.*

18. *Dang, L. M., Min, K., Lee, S., Han, D., & Moon, H. (2020). Tampered and computer-generated face images identification based on deep learning. Applied Sciences, 10(2), 505.*

19. *Zhang, W., Zhao, C., & Li, Y. (2020). A novel counterfeit feature extraction technique for exposing face-swap images based on deep learning and error level analysis. Entropy, 22(2), 249.*

20. *Arivazhagan, S., Russel, N. S., & Saranyaa, M. (2024). CNN-based approach for robust detection of copy-move forgery in images. Inteligencia Artificial, 27(73), 80-91.*