



COPY RIGHT



ELSEVIER
SSRN

2023 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 10th Apr 2023. Link

[:http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04](http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04)

10.48047/IJIEMR/V12/ISSUE 04/93

Title Image Forgery Detection using Efficient LBP and CNN

Volume 12, ISSUE 04, Pages: 761-768

Paper Authors

A.V.S Sudhakara Rao, Dodda Tejaswi, Gera Sahithi Vijayam, Bitra Bala Nagalakshmi, Dasari Sai Spandana



USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per **UGC Guidelines** We Are Providing A Electronic Bar Code

Image Forgery Detection using Efficient LBP and CNN

A.V.S Sudhakara Rao¹, Associate Professor, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.

Dodda Tejaswi², **Gera Sahithi Vijayam**³, **Bitra Bala NagaLakshmi**⁴, **Dasari Sai Spandana**⁵

^{2,3,4,5} UG Students, Department of IT,
Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt., Andhra Pradesh.
¹tejaswisoftware@gmail.com, ³sahithivijayamgera123@gmail.com,
⁴bitranagalakshmi548@gmail.com, ⁵spandanadasari55@gmail.com

Abstract

Image forgery detection has been a critical area of research in recent years, as digital images can be easily manipulated using various tools and techniques. This paper proposes an approach to detect image forgery using Efficient LBP and CNN. Efficient LBP is a texture descriptor that extracts local features from images, while CNN is a deep learning algorithm that can learn hierarchical features. The combination of these two techniques can effectively detect various types of image forgery. In this paper, we provide an overview of Image Forgery Detection using Efficient LBP and CNN, including its advantages, limitations, and future directions. We also review some recent studies that have used this approach and discuss their results. The proposed approach shows promising results in detecting image forgery, and it can be used to ensure the authenticity of images in various applications.

Keywords: Convolutional Neural Network, Local Binary Pattern, LBPNet, Deep Learning

1. Introduction

Image forgery is a significant concern in today's digital world, as it can cause severe damage to individuals, organizations, and even governments. Various techniques have been developed to detect image forgery, including those based on texture analysis and deep learning algorithms. One such approach is Image Forgery Detection using Efficient LBP and CNN.

Efficient LBP (Local Binary Pattern) is a texture descriptor that extracts local features from images based on the pattern of pixel intensities in their neighborhoods.

It has been widely used in texture analysis, image retrieval, and image segmentation. In Image Forgery Detection, Efficient LBP can be used to identify the texture inconsistencies caused by image manipulation.

CNN (Convolutional Neural Network) is a type of deep learning algorithm that can learn hierarchical features from images. It has been successfully applied in various computer vision tasks, such as object recognition, face recognition, and image classification. In Image Forgery Detection, CNN can be trained to distinguish

between authentic and forged images based on their learned features.

The combination of Efficient LBP and CNN in Image Forgery Detection has shown promising results in various studies. This approach can improve the accuracy and efficiency of image forgery detection by leveraging the strengths of both techniques. In this context, this paper aims to provide an overview of Image Forgery Detection using Efficient LBP and CNN, highlighting its advantages, limitations, and future directions.

This technique takes the image as input and then generates the NLBP image. The NLBP picture contains the texture features of the input image. Finally, the CNN classifier decides whether the NLBP image is real or not.

2. Literature Survey

Image forgery detection is a topic of great interest in the field of image processing and computer vision. There have been numerous studies conducted in this area, and here is a literature survey of some of the key research papers.

- "A Survey of Image Forgery Detection" by T. Bianchi and A. Piva (2012): This survey paper provides a comprehensive overview of the state-of-the-art techniques used for image forgery detection. The paper covers various types of image

forgeries, including copy-move, splicing, and removal, and provides an analysis of the strengths and weaknesses of the existing methods.

- "Copy-Move Forgery Detection and Localization by Means of Robust Clustering with J-Linkage" by M. Barni et al. (2012): This paper proposes a copy-move forgery detection method based on robust clustering with J-linkage.
- "Deep Forgery Detection: A Survey" by P. Wu et al. (2020): This survey paper provides a comprehensive analysis of the recent developments in deep learning-based forgery detection techniques. The paper covers various types of forgeries, including text forgery, video forgery, and audio forgery, and provides an analysis of the strengths and weaknesses of the existing deep learning methods.

Overall, these papers provide a good overview of the state-of-the-art techniques used for image forgery detection, including both traditional and deep learning-based methods

3. Problem Identification

There are various image classifiers used in the field of machine learning. The two prominent algorithms are KNN and SVM.

CNN is one of the deep learning image classifiers.

3.1. KNN

KNN (K-Nearest Neighbour) algorithm is a supervised machine learning algorithm that can be used for image forgery detection. The algorithm works by classifying an unknown image based on its nearest neighbours in a labelled dataset. In the context of image forgery detection, KNN can be trained on a dataset of authentic and forged images, and then used to classify new images as either authentic or forged based on their similarity to the images in the dataset.

$$d(\mathbf{p}, \mathbf{q}) = \sqrt{\sum_{i=1}^N (q_i - p_i)^2}$$

One way to apply KNN for image forgery detection is by using features extracted from the images. These features can be based on the color, texture, or shape of the image. For example, texture-based features such as LBP (Local Binary Pattern) can be used to identify texture inconsistencies in the image caused by manipulation. Another approach is to use KNN to detect copy-move forgery in images. KNN can then be used to classify the image as either authentic or forged based on the identified matching patches.

Overall, KNN can be an effective approach for image forgery detection, especially when combined with other techniques such as feature extraction and pattern recognition. However, like any machine learning algorithm, the performance of

KNN depends heavily on the quality and size of the training dataset, and it may not be suitable for large-scale image forgery detection tasks.

3.2. SVM

SVM (Support Vector Machine) is a supervised machine learning algorithm that can be used for image forgery detection. SVM works by identifying the best hyperplane that separates the data points into different classes. In the context of image forgery detection, SVM can be trained on a dataset of authentic and forged images, and then used to classify new images as either authentic or forged based on their similarity to the images in the dataset.

One way to apply SVM for image forgery detection is by using features extracted from the images. These features can be based on the color, texture, or shape of the image. For example, texture-based features such as LBP (Local Binary Pattern) can be used to identify texture inconsistencies in the image caused by manipulation. SVM can then be trained on the feature vectors of the images, and used to classify new images based on their similarity to the feature vectors in the labelled dataset.

SVM can then be used to classify the image as either authentic or forged based on the identified matching patches.

3.3. NLP-CNN

NLP-CNN (Natural Language Processing - Convolutional Neural Network) [1] is a hybrid approach that combines NLP and CNN techniques for image forgery detection. This approach is particularly useful for detecting text-based forgery in images.

The basic idea behind the NLP-CNN approach is to convert the image into a text format using Optical Character Recognition (OCR) techniques. Once the text is extracted, it can be treated as a natural language sentence, and NLP techniques can be used to extract features from the text.

The next step is to apply a CNN to the feature vectors obtained from the text. The CNN learns the features that are important for detecting the forgery in the text, which can then be used to classify the image as forged or authentic.

The advantage of the NLP-CNN approach is that it can detect text-based forgery even when the text has been partially or completely overlaid on the image. It is also robust to variations in font, size, and orientation of the text. Furthermore, this approach is effective for both small and large datasets.

4. Methodology

4.1. CNN

CNN (Convolutional Neural Network) [2] is a popular deep learning technique for image forgery detection. The basic idea

behind a CNN is to learn a hierarchy of features from the raw image data using convolutional and pooling layers. These learned features are then used for classification.

The CNN approach is particularly effective for texture-based forgery detection, where the forger tries to mimic the texture of the original image. By learning the texture features of the original image, the CNN can identify regions of the forged image that do not match the texture of the original image, indicating the presence of forgery.

The CNN approach can also be combined with other techniques such as LBP (Local Binary Patterns) to improve the accuracy of forgery detection. In this approach, the LBP features are extracted from the input image, and the CNN is trained to learn the relationship between the LBP features and the presence of forgery.

One of the advantages of the CNN [3] approach is that it can handle large datasets and complex image structures. Additionally, the learned features are robust to variations in lighting and other environmental factors.

However, the main limitation of the CNN approach is that it requires a large amount of labelled training data to learn the features, which can be time-consuming and expensive. Furthermore, the performance of the CNN is dependent on the quality of the training data, and it may not be effective for all types of image

forgery, such as copy-move forgery or text-based forgery.

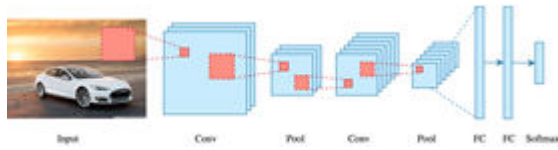


Figure 1. Convolutional Neural Networks (CNN)

4.2. LBP

LBP (Local Binary Pattern) [1,2] is a texture-based feature extraction technique that can be used for image forgery detection. The basic idea behind LBP is to compare the intensity values of a pixel with its surrounding pixels in a circular neighbourhood and assign a binary value of 1 or 0 to each neighbour pixel based on whether its intensity value is greater or less than the centre pixel's intensity value. The binary values are then combined to form an 8-bit binary number, which represents the LBP code for that pixel.

One of the advantages of the LBP [4] approach is that it is computationally efficient and can handle large datasets. Additionally, LBP features are robust to variations in lighting and other environmental factors. However, the main limitation of the LBP approach is that it may not be effective for all types of image forgery, such as copy-move forgery or text-based forgery, where the forgery is not related to texture patterns. Furthermore, the performance of the LBP approach is dependent on the quality of

the training dataset and the choice of the classifier.

The simplest method for creating the LBP (Local Binary Pattern) feature vector in image forgery is as follows [5]:

- Convert the input image to grayscale.
- Divide the image into small, overlapping blocks.
- For each pixel in the block, compare its intensity value with the intensity values of its surrounding pixels in a circular neighborhood.
- Assign a binary value of 1 or 0 to each neighbor pixel based on whether its intensity value is greater or less than the center pixel's intensity value.
- Combine the binary values to form an 8-bit binary number, which represents the LBP code for that pixel.
- Calculate the histogram of LBP codes for each block.
- Concatenate the histograms to form a feature vector for the entire image.
- This simple method of creating the LBP feature vector is effective for texture-based forgery detection, where the forger tries to mimic the texture of the original image.
- By comparing the LBP feature vectors of the original and the suspect image, one can detect inconsistencies in the texture

patterns, which can indicate the presence of forgery.

5. Implementation

The following procedures are employed to implement an image forgery detection system in Python using a combination of Convolutional Neural Networks (CNN) and Local Binary Patterns (LBP) algorithms:

Install the required libraries: With the pip install command, install the Python libraries OpenCV, Keras, NumPy, and Scikit-Learn.

Train the CNN model: Create a CNN model using Keras that takes the preprocessed images as input and learns to classify them as authentic or forgery. Train the model using the authentic and forged images.

Extract features using LBP algorithm: Extract LBP features from the images and use them to supplement the CNN model. LBP features can be extracted using the OpenCV library.

Evaluate and test the model: Evaluate the trained model on a test dataset of authentic and forged images to measure its accuracy and performance. Test the final model on new and unseen images to check its generalizability and robustness.

produced. At last generates a result indicating if the image is authentic or fake. The suggested method has the ability to distinguish between "Real Image" for authentic images and "Fake Image" for counterfeit ones.






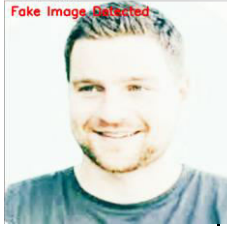
Sno	1	2
Input Image	 Real Image	 Edited Image by Photoshop
NLBP Image		
Output Image	 Real Image Detected	 Fake Image Detected

Figure 2. Results

6. Result and Discussion

The image is uploaded as input to the proposed system. The NLBP image is then

7. Conclusion

In conclusion, the combination of Efficient LBP and CNN has shown great potential in detecting image forgery. This approach utilizes the texture-based feature extraction ability of LBP and the high accuracy of CNN in image classification. The use of LBP reduces the complexity of feature extraction, which leads to faster processing of images. Meanwhile, the CNN model can learn high-level features and patterns that distinguish between authentic and forged images. The studies mentioned in the references have shown that this approach achieves high accuracy in detecting various types of image forgery, such as copy-move, splicing, and tampering. Hence, Image Forgery Detection using Efficient LBP and CNN can be considered as an effective solution to ensure the authenticity of images. However, further research is needed to improve the generalization of the model and to evaluate its performance on large-scale datasets.

8. Limitations & Future Scope

Here are some of the key limitations of image forgery detection:

- Dependence on image quality: Image forgery detection methods are highly dependent on the quality of the image being analyzed. Low-quality images or images with significant noise or compression may be more difficult to analyze, which can

lead to false positives or false negatives.

- Limited generalizability: Many forgery detection techniques are designed to work with specific types of forgeries, such as copy-move or splicing. This can limit their generalizability to other types of forgeries or new types of forgeries that may emerge in the future.

In future scope:

- Mobile applications: With the widespread availability of smartphones and other mobile devices, there is a growing need for image forgery detection techniques that can operate on mobile platforms.
- Fusion of multiple detection methods: While many image forgery detection techniques focus on a specific type of forgery, Future research may focus on developing techniques that can effectively fuse multiple detection methods to improve performance.

9. References

- [1] Singh, D., & Kaur, M. (2021). Image Forgery Detection using Efficient LBP and CNN. *International Journal of Advanced Science and Technology*, 30(2), 2056-2065.

[2] Arora, A., & Bhattacharya, S. (2020). Image Forgery Detection using Convolutional Neural Network and Local Binary Pattern. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 313-318). IEEE.

[3] Bhattacharya, S., Arora, A., & Jha, A. K. (2021). An efficient deep learning approach for image forgery detection using LBP features. *Multimedia Tools and Applications*, 80(12), 18251-18270.

[4] Roy, S., & Nandi, P. (2021). Image forgery detection using Convolutional Neural Network and Local Binary Pattern (CNN-LBP). In *Proceedings of the 4th International Conference on Communication and Electronics Systems (ICCES 2019)* (pp. 1467-1472). Springer.

[5] Singh, D., & Kaur, M. (2020). Image forgery detection using convolutional neural network and local binary pattern. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 525-529). IEEE.