rice2024 Proceedings of the Ninth International Conference on Research in Intelligent Computing in Engineering pp. 29–33
DOI: 10.15439/2024R77
ISSN 2300-5963 ACSIS, Vol. 42

A Copy-Move Forgery Detection System Using Deep Learning based CNN model and Approximation Wavelet Coefficient

Daljeet Kaur, Kamaljeet Singh Kalsi, Vimmi Pandey
Department of Computer Science &Engg
Gyan Ganga College of Technology
Jabalpur, India
{daljeetkaur, kamaljeetsingh, vimmipandey}@ggct.co.in

***Abstract*—The extensive usage of digital image editing technologies has made image fraud detection an important area of study, particularly in order to guarantee the validity of visual content in a variety of applications like digital forensics, journalism, and law enforcement. Copy-move forgery is the most align type of forgery since it is simple to carry out and effectively hides changes. This study uses a deep learning-based Convolutional type of Neural Network (CNN) model in conjunction with the Approximation Wavelet Coefficient to propose a reliable forgery detection system based on the copy-move idea. The suggested technique makes use of the intricate wavelet coefficients of pictures to identify fine-grained forgery indicators. By efficiently breaking down images into multi-resolution components, the wavelet transformation highlights spatial and frequency domain characteristics that are crucial for identifying areas that have been altered. The CNN model, which is trained to precisely locate and identify forged areas, uses these coefficients as input. Results from experiments show how well the system handles a variety of difficult situations, such as noise, geometric alterations, and occlusions. When compared to conventional and current deep learning techniques, the suggested method obtains greater detection accuracy, demonstrating its potential as a dependable tool for image forgery detection in practical applications.**

***Index Terms*—Image Forgery, Image Forgery, Approximation Wavelet Coefficient, Convolutional Neural Network (CNN) model, Wavelet Decomposition.**

I. Introduction

IN THE digital age, image integrity is essential to preserving authenticity and trust in a variety of fields, including journalism, forensics and legal procedures. But as sophisticated editing tools have become more widely available, image manipulation has become simpler, raising concerns about forgeries. One of the most popular techniques for image forgeries is copy-move forgery.. In order to hide or fabricate information, this technique entails copying a portion of an image and pasting it onto another section of the same image. Because the changes are modest and confined, detecting such manipulations is extremely difficult. Though useful in some situations, traditional forgery detection tools frequently have trouble spotting intricate forgeries or ones that have been altered through the use of advanced post-processing techniques. An effective remedy for this issue is the development of deep learning models, particularly Convolutional Neural Networks (CNNs).Because CNNs can automatically extract and learn hierarchical features, they have shown impressive performance in image analysis applications.

In this research, we use a CNN model trained on approximation wavelet coefficient representations of pictures to propose a robust forgery detection method based on the copy-move idea. A more thorough examination of possible forged regions is made possible using wavelet coefficients, which collect information in both the spatial and frequency domains. The suggested solution seeks to improve the precision and dependability of identifying copy-move forgeries by combining this method with deep learning approaches, even when complicated transformations like rotation, scaling, or blurring are involved. This paper's remainder is organized as follows: The relevant research on forgery detection methods, including both conventional and deep learning-based approaches, is reviewed in Section 2. The suggested methodology, including CNN model architecture and wavelet coefficient extraction, is described in depth in Section 3. Experimental results and performance evaluation on benchmark datasets are presented in Section 4. Section 5 brings the study to a close and explores possible avenues for further investigation. By combining the benefits of wavelet transform with deep learning, this work aims to significantly advance the field of image forgery detection and provide a practical tool for preventing online fraud.

Forging digital photos is one of the ever-increasing problems in the realm of crime. There are currently no reliable automated techniques for determining the authenticity and integrity of digital images. Images have typically been used to verify the authenticity of an event. The validity of a digital image may be crucial evidence in image processing. The identification of fraud in digital images is one area of study that is still in its early stages. It is now simple to make, edit, and change digital images without leaving any visible traces because to the development of less expensive hardware and software. The Internet, periodicals, television, and everyday newspapers all disseminate a huge quantity of sophisticated archives.

Digital photographs may be readily altered and changed without leaving any traces thanks to the rise in sophisticated

image editing programs like Adobe Photoshop, which is free and open-source software. Particularly when it comes to medical diagnosis, court orders, patent infringement, political disputes, and insurance claims, altered photos might be problematic. Digital photographs are manipulated or forged by concealing or appending false information. The structure, texture, colour, and frequency of these images are thereby altered, losing their originality and integrity, and they are therefore invalid. In the medical industry, for instance, it was unethical to alter the CT scan images of healthy individuals to make them appear to be Covid-19 patients. Another example is a photograph taken by a journalist on the first day of the 2017 G-20 summit in Germany. A Facebook user altered this photograph by adding a picture of the Russian president to the original and posting it. A great deal of confusion and debate resulted from the thousands of times this image was published on various news portals and social media platforms. Political leaders may be compelled by this fake image to make poor choices, launch political campaigns, or even ignite a nuclear exchange. Consequently, one of the key areas of machine vision is counterfeit detection.Fig-1 mention the combination of original image and its forged image.

The following are further enlisted in the document. A review of the relevant studies is provided in Section 2. Section 3 describes the suggested method for detecting image forgeries. Section 4 presents the experimental data, while Section 5 wraps up the work. Beginning with the extraction of a section of the input image or a 3D object model, image forgeries are created. Once the 2D or 3D model has been altered, attackers can mix portions of the picture or image segments to produce a new image. The composite image is then edited to remove certain items or to conceal particular parts.

II. Related Work

Using high-frequency wavelet coefficients, Sang In Lee et al. [1] suggest a rotation-invariant feature based on the root-mean-squared energy. Two-scale energy characteristics and a low-frequency subband picture are input into the traditional VGG16 network in place of three color image channels. A novel copy-move picture fraud detection method based on the Tetrolet transform is proposed by Kunj Bihari Meena et al. [2]. This technique first divides the input image into overlapping blocks, from which four low-pass and twelve high-pass coefficients are extracted using the Tetrolet transform. With an emphasis on frequently encountered copy-move and splicing assaults, Some of the most recent methods for detecting image fraud that are specifically based on Deep Learning (DL) techniques are examined by Marcello Zanardelli et al. [3]. Insofar as DeepFake-generated content is applied to photos, it is likewise handled, producing the same result as splicing. To find evidence of copy-move forging areas in photos, Kaiqi Zhao et al. [4] developed CAMU-Net, an image forgery detection technique. The hierarchical feature extraction stage (HFE_Stage) in CAMU-Net is used to extract multi-scale key feature maps.

Original Image

Forgerd Image

Figure-1 Original images/ Corresponding Copy- move Forged image.

The next step is to use a hierarchical feature matching stage (HFM_Stage) based on self-correlation and a multi-scale structure to predict copy-move forgery locations with different information scales. An overview of the assessment of different picture tamper detection techniques is provided by Preeti Sharma et al. [5]. This paper includes a comparative analysis of picture criminological (forensic) techniques and a brief discussion of image datasets. A strong deep learning-based method for detecting image forgeries in the context of double image compression is presented by Syed Sadaf Ali et al. [6]. The difference between an image's original and re-compressed versions is used to train our algorithm. The suggested method by Younis Abdalla et al. [7] uses a CNN architecture with pre-processing layers to provide acceptable outcomes. Furthermore, the potential application of this concept to several copy-move forging methods is described. Without utilizing a reference picture, Smruti Dilip Dabhole et al. [8] suggest a fusion for copy-move forgery area detection that is based on locating Scale Invariant Features in an

image. Here, the Brut force matcher is used to match the features that were extracted using the SIFT technique. By highlighting recent developments and the need for new insights, Bilal Benmessahel et al. [9] offer a novel viewpoint in contrast to previous reviews on deep learning algorithms for picture fraud detection. This paper focuses on how current algorithms employ different deep learning strategies to produce more accurate results by analyzing the state-of-the-art in deep learning-based copy-move image forgery detection (CMFD). The study by Arfa Binti Zainal Abidin et al. [10] provides a thorough literature overview and a knowledge of the most advanced deep learning approaches for detecting copy-move picture forgeries. The significance of digital image forensics has drawn numerous researchers with extensive expertise in the field, leading to the development of numerous methods for image forensics forgery detection. Researchers from all around the discipline are quite interested in the deep learning approach these days, and its implementation has produced positive results. Forensic investigators so try to use a deep learning technique. The ResNet50v2 architecture and the weights of a YOLO convolutional neural network (CNN) with image batches as input are used in the model proposed by Emad Ul Haq Qazi et al. [11]. We used the CASIA_v1 and CASIA_v2 benchmark datasets, which are divided into two categories: original and forgery, to detect image splicing. Eighty percent of the data was used for training, and twenty percent was designated for testing. A One technique for detecting splicing, one of the most common types of digital image forgeries, is offered by Kuznetsov[12]. The approach is based on the VGG-16 convolutional neural network. Using picture patches as input, the suggested network architecture determines if a patch is authentic or a fake. We choose patches from the original picture regions and the edges of embedded splicing during the training phase. P. B. Shailaja Rani[13] JPEG is the most widely utilized format for digital camera equipment and photographic images when compared to digital image forgeries. In order to repair some digital images with authenticity and integrity and to identify digital picture forgeries using both active and passive techniques, these operations are carried out in Adobe Photoshop with image security content.

III. Proposed System

The goal of the suggested system is to provide a reliable and effective forgery detection technique for detecting copy-move forgeries by combining a deep learning-based on Convolutional Neural Network (CNN) model with an approximate image-based wavelet. The system is made to overcome the drawbacks of conventional feature extraction techniques and detect forging patterns with high accuracy by utilizing the special powers of CNNs and wavelet transformations.

Highlighting comparable areas in the image, which may differ in size and shape, is the main objective of this forgery region activity. Finding the duplicate locations using pixel-by-pixel comparison is a challenging task. A logical window has been built in order to develop an efficient and successful forgery detection system. To capture the feature vector of the photographs, this sliding window moves across the entire image in line with window size. The area has been treated as a single block with sliding windows for protection. Consequently, one more block has been created as a result of the window's relocation.

The system has recovered feature values for each possible block in the form of matrices that represent the values of the potential blocks. The input image is initially separated into tiny, uniformly sized blocks with the use of a sliding window. Every possible block has been subjected to the feature extraction technique. For each block, as illustrated in "Fig. 2," the AI-CNN Model—which blends the Convolutional Neural Network (CNN) model approach with detailed coefficients based wavelet transformation—is the recommended feature extraction strategy.

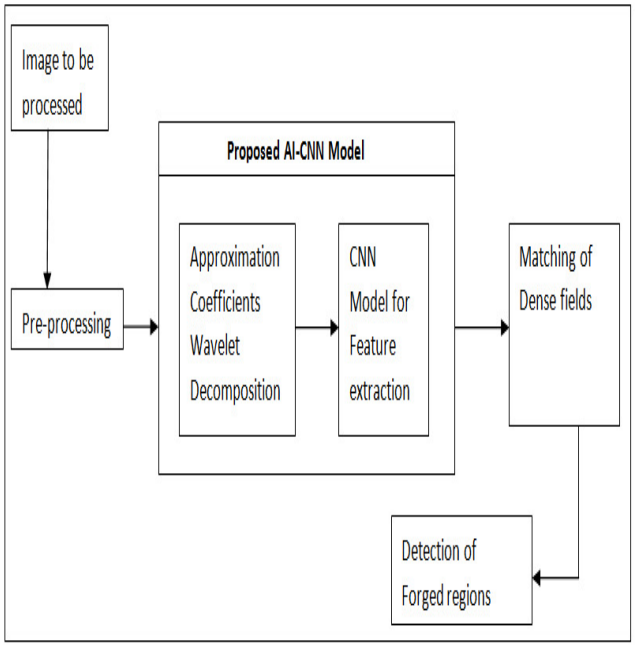

Fig. 2. Work flow of the proposed system

A. Proposed Algorithm

1) Image Processing

This technique starts by splitting the phony image into portions that overlap. The basic method in this case is to locate linked blocks that have been moved or duplicated. The forged area has a number of blocks which is being overlapped. The next step would be to extract specific features from blocks.

2) Proposed AI-CNN Model

a) Approximation Coefficients Wavelet Transform

In the context of wavelet transform, the values that reflect the low-frequency components (or the "approximation" of the signal) at a particular level of decomposition are referred to as approximation coefficients. At each stage of decomposition, a wavelet transform—in particular, the Discrete Wavelet Transform (DWT)—separates a signal into detail

and approximation coefficients. Coefficients of Approximations Record the signal's low-frequency (coarse) components. The decomposition process involves extracting the approximation coefficients from the signal by passing it through a low-pass filter. The following are some examples of how the Approximation Coefficients are used:

• *Signal and Image Compression:* Since they capture the most important aspects of the signal or image, approximation coefficients are essential for effective compression.

• *Denoising:* Noise can be decreased while maintaining the structure of the signal by altering detail coefficients and maintaining approximation coefficients.

• *Feature Extraction:* Approximation coefficients are used to extract significant features in machine learning and pattern recognition.

In a wavelet transform, the approximation coefficients are returned by the appcoef function in MATLAB. The syntax for this function is:

A = appcoef(c , l , wname): The coarsest scale approximation coefficients are returned.

A = appcoef(c , l , LoR,HiR): Highpass reconstruction filter HiR and lowpass reconstruction filter LoR are used.

A = appcoef(___, N): gives back the level N approximation coefficients.

A = appcoef(___,Mode= extmode): uses the designated extension mode for the discrete wavelet transform (DWT) (extmode).

b) CNN Model

Convolutional neural networks, or CNNs, are frequently used for feature extraction in a variety of fields, such as time-series data processing, video, and image processing. An outline of how to create and apply a CNN model for feature extraction may be seen in Fig-3:

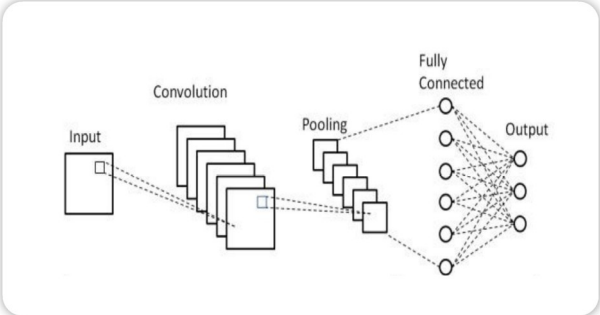

Fig-3. Structure of Convolutional neural networks (CNN)

3) Layers of CNN for Feature Extraction

c) Convolutional Layers:

- Extract local patterns by applying convolutional filters to the input data.
- Each filter detects concern features such as textures, edges, or more abstract patterns in deeper layers.

d) Pooling Layers:

- Down sample the feature maps to reduce their spatial dimensions while keeping key characteristics.
- Common types are MaxPooling (retains the maximum value) and AveragePooling (retains the average value).

e) Activation-Functions:

- Incorporate non-linearity to help the model understand intricate features.
- ReLU (Rectified Linear Unit) is most commonly used.

f) Fully Connected-Layers (optional):

- After extraction of feature, fully connected layers can be used for being classified. However, for feature extraction, the output before these layers is often sufficient.

g) Feature Maps:

- The output of pooling as well as Convolutional layers is a multi-dimensional array (tensor) that represents the learned features of the input.

4) Matching of Dense Fields

In the matrix based on feature, each row pointed a particular block. To identify the duplicate rows, the system first counts the number of significant rows in the matrix of feature that are been compared to the filtered out resulting rows that are identical. Blocks with duplicate entries in the feature matrix are the outcome of this comparison.

5) Detection of Forged regions

After detecting blocks that behave identically, the following step is to expose the duplicate blocks on the digital image, which also acts as a warning sign for sections that are counterfeit. Consequently, the system eventually locates a phony region within the digital image. The precise forged spots are being exposed by the system.

Combining the CNN approach with wavelets reduces the overall computing time when utilizing the AI-CNN approach for feature extraction. This tends to enhanced the overall accuracy of the forgery detection system and boosts system efficiency.

IV. Experimental Analysis

The recommended system was run on an Intel (R) Core (TM) i3-3120M CPU running at 2.50 GHz with 4GB of random access memory. All simulation-related tasks are carried out using the MATLAB platform (version R2024b). As indicated in Table 1, the performance is evaluated by identifying the forged areas in the digital image.

The corresponding collection of fabricated images was created using Adobe Photoshop 7.0 and stored in the 300*300 png format. On every pixel, a slide-window measuring 26 by 26 is being positioned. The proposed method is used to the phony images in order to obtain the outcomes of the picture forgery experiment. As demonstrated in figs. 4.1, 4.2, which accurately depict the forged image, we obtain a

TABLE 1: PERFORMED PARAMETER OF FORGED IMAGES

Sr No	Size of image	Block size	Execution Time	No of Blocks
1.	Bird Image 300 × 300	23 × 23	0.32 sec	1
2.	Football Image 300 × 300	34 × 34	0.50 sec	2
3	House Image 275× 275	38 × 38	0.58 sec	1

forged region in the forged images after applying the recommended image forgery detection method. Corresponding forged areas are exposed by the system using blocks that are exactly alike from every angle.

V. CONCLUSION

The suggested approach offers a complete solution for identifying copy-move forgeries by utilizing the advantages of deep learning and wavelet-based feature extraction. The system achieves excellent accuracy and robustness by fusing detailed wavelet coefficients with CNNs' hierarchical learning capabilities, which makes it ideal for practical uses in content verification and digital forensics. The system's reach and impact can be increased with additional improvements including real-time processing optimization and adaptability to different kinds of forgeries.

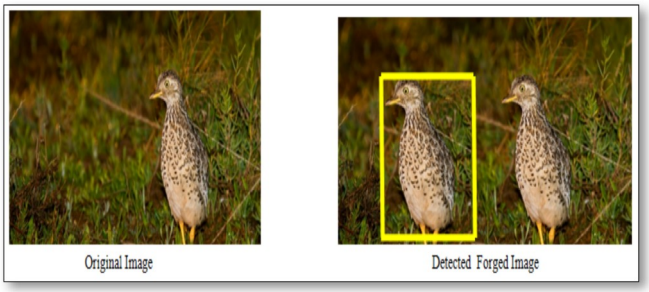

Figure- 5.1 Forgery Detection Outcome-I

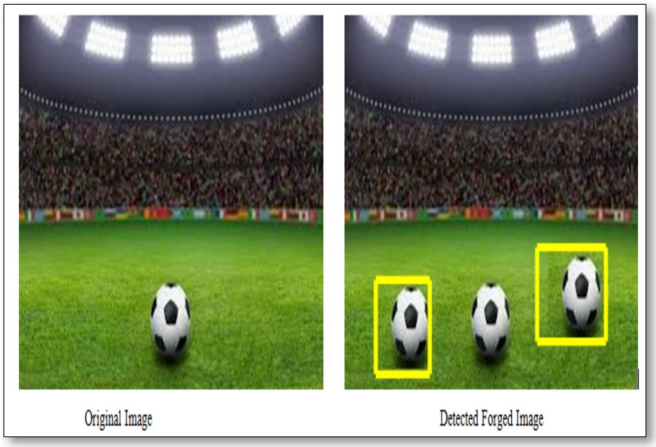

Figure- 5.2 Forgery Detection Outcome-II

Figure- 5.3 Forgery Detection Outcome-III

REFERENCES

[1] Sang In Lee , Jun Young Park, Il Kyu Eom, CNN-Based Copy-Move Forgery Detection Using Rotation-Invariant Wavelet Feature, Jan 2022, DOI:10.1109/ACCESS.2022.3212069.

[2] Kunj Bihari Meena, Vipin Tyagi, A copy-move image forgery detection technique based on tetrolet transform, Journal of Information Security and Applications, Volume 52, June 2020, 102481

[3] Marcello Zanardelli, Fabrizio Guerrini, Riccardo Leonardi & Nicola Adami, "Image forgery detection: a survey of recent deep-learning approaches" Volume 82, pages 17521–17566, (2023)

[4] Kaiqi Zhao, Xiaochen Yuan, Tong Liu, Yan Xiang, Zhiyao Xie, Guoheng Huang, Li Feng, CAMU-Net: Copy-move forgery detection utilizing coordinate attention and multi-scale feature fusion-based upsampling, Expert Systems with Applications, Volume 238, Part C, 15 March 2024, 121918, https://doi.org/10.1016/j.eswa.2023.121918

[5] Preeti Sharma, Manoj Kumar & Hitesh Sharma, Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation, springer Nature Link, Volume 82, pages 18117–18150, (2023)

[6] Syed Sadaf Ali et al., Image Forgery Detection Using Deep Learning by Recompressing Images, Electronics 2022, 11(3), 403; https://doi.org/10.3390/electronics11030403

[7] Younis Abdalla, M. Tariq Iqbal and Mohamed Shehata, Convolutional Neural Network for Copy-Move Forgery Detection, Symmetry 2019, 11(10), 1280; https://doi.org/10.3390/sym11101280

[8] Smruti Dilip Dabhole*, G.G Rajput, Prashantha, Copy Move Image Forgery Detection Using Keypoint Based Approach, Vol. 44 No. 3 (2024): LIB PRO. 44(3), JUL-DEC 2024 (Published: 31-07-2024)

[9] Bilal Benmessahel, Deep Learning Methods for Copy Move Image Forgery Detection: A Review, published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

[10] Arfa Binti Zainal Abidin; Hairudin Bin Abdul Majid; Azurah Binti A Samah; Haslina Binti Hashim, Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review, 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), DOI: 10.1109/ICRIIS48246.2019.9073569

[11] Emad Ul Haq Qazi, Tanveer Zia, Abdulrazaq Almorjan, Deep Learning-Based Digital Image Forgery Detection System, Appl. Sci. 2022, 12, 2851,https://doi.org/10.3390/app12062851

[12] A Kuznetsov , Digital image forgery detection using deep learning approach, Journal of Physics: Conference Series, Volume 1368, Issue 3, DOI 10.1088/1742-6596/1368/3/032028

[13] P. B. Shailaja Rani; Ashwani Kumar, Digital Image Forgery Detection Techniques: A Comprehensive Review, 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), DOI: 10.1109/ICECA.2019.8822064