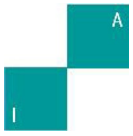
Inteligencia Artificial 27(73), 80-91
doi: 10.4114/intartif.vol27iss73pp80-91



INTELIGENCIA ARTIFICIAL

http://journal.iberamia.org/

CNN-based Approach for Robust Detection of Copy-Move Forgery in Images

S.Arivazhagan, R.Newlin Shebiah, M.Saranyaa, R. Shanmuga Priya

Centre for Image Processing and Pattern Recognition, Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu 626005, India
newlinshebiah@mepcoeng.ac.in

Abstract: The evolution of image manipulation techniques has presented a paradoxical scenario in contemporary visual culture. This phenomenon operates as a double-edged sword, offering both creative liberation and ethical dilemmas. Consequently, there is a need to develop automated mechanisms capable of discerning such forged data. The proposed methodology leverages transfer learning, utilising pre-trained deep learning models as a foundation and fine-tuning them specifically for the task of copy-move forgery detection. This approach uses the knowledge learned from large datasets, enhancing the network's ability to discern subtle patterns indicative of copy-move manipulations in images. Further, this research introduces a custom-designed CNN architecture tailored to the intricacies of copy-move forgery, optimising feature extraction and classification. Experimental evaluations conducted on diverse datasets, namely MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD demonstrate the effectiveness of the proposed method with a True Positive Rate (TPR) of 100%.

Keywords: Copy and Move Forgery, Convolutional Neural Network, Transfer Learning, Deep learning

1 Introduction

The rapid rise of social networking services in the digital age has led to an unprecedented surge in the creation and dissemination of media content, spanning across audio, images, and videos. The widespread availability of software tools on the internet has facilitated the manipulation and alteration of this media content, rendering what was once a complex task into a commonplace activity. Forgery is the act of fraudulently creating or materially altering a legal document with the intent to defraud. There are numerous types of image forgeries, including copy-move, splicing, morphing, and retouching. Copy-move image forgery occurs when a portion of an image is duplicated or cloned and then pasted in a different location within the same image. The creation of a forged image by splicing together two or more distinct images is another form of forgery. In this forgery, one object from one image is replaced with another object from another image. Copy-move forged documents are among those that are difficult to identify due to the similarities between duplicated and forged data.

The generation of fake faces images using Generative Adversarial Networks (GANs) stands out as a particularly alarming phenomenon. This technology allows the alteration of a face in an original image with one observed in another image or video, giving rise to deep fake images and videos. This issue has escalated rapidly on social networks, posing a significant threat. The proliferation of deep fake content, facilitated by tools like FotoForensics, JPEGsnoop, Ghiro, Forensically, Amped Authenticate, izitru, and others, has made image manipulation accessible even to individuals without technical expertise. In Figure 1, an example of a copy-move forgery image is presented. Figure 1a displays the original image, while Figure 1b exhibits the forged version.

ISSN: 1137-3601 (print), 1988-3064 (on-line)

Figure 1: Example of Copy-Move Forgery image (a) Original Image (b) Forged Image [1]

Copy-move forgery detection techniques have evolved over the years, employing various approaches to identify manipulated images. The standard method involves the use of local feature extractors like SIFT (Scale-Invariant Feature Transform), SURF (Speeded Up Robust Features), and ORB (Oriented FAST and rotated BRIEF). These techniques extract features from specific regions of the image, allowing for the detection of duplicated or altered elements. Additionally, orthogonal moment-based feature extraction has been utilized in conjunction with these methods. One of the primary distinctions in detection methods lies between block-based algorithms and feature keypoint-based algorithms. In the former, the image is divided into small blocks, and features are extracted from each block. In the latter, keypoints throughout the entire image are located, and their attributes are extracted. Both methods facilitate the construction of matched block pairs, enabling the identification of manipulated regions within the image. There are two fundamental approaches to detecting image manipulation: active and inert. Active methods involve replicating specified data, such as a digital watermark, into the image during or after the collection process. This integrated data is utilized to detect manipulation actively. In contrast, passive approaches, also known as "blind approaches," identify forgeries without the need for additional information.

CNNs (Convolutional Neural Networks) have emerged as highly effective tools for detecting copy-move image forgeries due to their ability to automatically learn and extract intricate information from images. Unlike traditional block-based and keypoint-based methods, CNNs do not rely on hand-crafted features that may be susceptible to changes in image quality, scale, or rotation. Instead, CNNs can autonomously learn pertinent image features across various levels of abstraction, ranging from basic edges to complex shapes and textures. This adaptability allows CNNs to excel at identifying intricate forms of image manipulation, making them a powerful and versatile tool in the field of digital forensics.

The highlights of this paper can be summarized as follows:

- The paper uses transfer learning, capitalizing on pre-trained deep learning models such as Alexnet, VGG16 and MobilenetV2, and fine-tuning them specifically for copy-move forgery detection.
- Introducing a specialized CNN architecture tailored to the unique challenges posed by copy-move forgery, the paper optimizes the processes of feature extraction and classification. This custom-designed architecture enhances the accuracy and efficiency of detecting manipulated content in images.
- The proposed methodology undergoes rigorous evaluation on diverse datasets, including MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD. Through these experiments, the efficacy of the approach is demonstrated, showcasing its ability to effectively detect copy-move forgeries across varied contexts and datasets.

The paper is organized as follows: Section 1 provides an introduction, contextualizing the significance of automated copy-move forgery detection in contemporary visual culture. Section 2 reviews related works in the field of image manipulation detection. Section 3 delves into the methodology, detailing the transfer learning framework and the design principles behind the custom CNN architecture. Section 4 presents the experimental descriptions and evaluation discussion. Finally, Section 5 concludes the paper, summarizing the contributions, discussing implications in the domain of automated image manipulation detection.

2 Literature Survey

In the realm of digital imagery, the growing prevalence of image manipulation techniques has necessitated the development of robust forgery detection methods. This literature survey explores the evolution of forgery detection techniques, spanning from traditional methods relying on hand-crafted features to cutting-edge approaches driven by deep learning algorithms.

Mahdian and Saic [2] have employed blur moment invariants to achieve the automatic detection and localization of duplicated regions, demonstrating robust performance even in scenarios characterized by blur degradation, added noise, and arbitrary contrast variations. Ryu et al. [2] utilizes Zernike moments to discern duplicated regions within an image. By capitalizing on the algebraic invariance of Zernike moments, particularly their resistance to rotation, the proposed approach exhibits noteworthy efficacy in detecting forged regions, even in cases where the manipulated regions have undergone rotation. Amerini et al. [4] utilized Scale Invariant Feature Transform (SIFT), which is resistant to scaling, rotation, and illumination variations, making it well-suited for localizing image forgeries. Muhammad et al. [5] employed the discrete Dyadic undecimated Wavelet Transform, focusing on the approximation and detail sub-bands. These sub-bands were subdivided into overlapping blocks, each with a 50% overlap, from which coefficients were extracted as features. The researchers harnessed the similarity among coefficients within approximation blocks and the dissimilarity between coefficients in detail blocks, utilizing this information for proficient copy-move detection. Haseena et al [6] introduced the Deep Texture Variation Network, incorporating convolution and pyramid pooling techniques. It offers a robust solution for detecting facial forgery, even in the presence of common image distortions such as JPEG compression and blur.

Barad and Goswami [7] proposed a comparative analysis of various deep learning techniques used to detect manipulation. For forgery detection, both block-based and keypoint-based deep learning-based methods employ manually constructed features such as DCT, DWT, PCA, SIFT, and SURF. The researchers evaluated their methods using datasets such as CASIA v1.0, CASIA v2.0, and DVMM. Remarkably, their approaches achieved high accuracy rates, with 98.04%, 97.83%, and 96.38% accuracy on CASIA v1.0, CASIA v2.0, and DVMM datasets, respectively.

Pun et al [8] introduced an innovative approach for detecting copy-move forgery. Their method utilized adaptive over-segmentation to divide the host image into non-overlapping, asymmetrical blocks. SIFT feature elements from each block were extracted and stored as BlockFeatures (BF). By matching these feature points, suspected forgery areas were approximated. The method was tested on a dataset comprising 80 original images, 80 realistic copy-move forgeries, and 108 images of realistic cloning (GRIP dataset). Impressively, even in challenging conditions such as geometric transformations, JPEG compression, and downsampling, the method exhibited outstanding performance, achieving a detection accuracy of 97.22 percent in identifying copy-move forgeries.

Li and Zhou [9] introduced a keypoint-based copy-move forgery detection algorithm that employs hierarchical feature point matching and localization methods. Unlike traditional approaches, this method avoids clustering or segmentation techniques. Instead, it proposes an innovative iterative localization approach and hierarchical matching strategy to address challenges in keypoint matching. Various techniques, including discrete cosine transform (DCT), discrete wavelet transform (DWT), principal component analysis (PCA), and singular value decomposition (SVD), were utilized to design block features, enhancing their robustness against common distortions like geometric transformations. By leveraging the resilience of the SIFT algorithm and incorporating color information from each keypoint, this method achieves remarkably high detection accuracy.On a similar note, Abbas et al. [10] presented an efficient copy-move forgery detection and classification model for digital images. Their approach involves a lightweight yet robust deep learning model based on a dual-domain convolutional neural network. This model enables accurate detection and localization of manipulated regions within digital images.

Ortega et al. [11] introduced two deep learning-based models, a custom one and a transfer learning-based one, to assess the performance of Copy-Move Forgery Detection (CMFD). CMFD can be implemented using both hand-crafted and deep learning methods. Previous approaches mainly focused on block-based, keypoint-based, or hybrid techniques. The second method employs either original architectures or modified versions of pre-trained

architectures like VGG-16. Various techniques, including the Fourier transform, discrete cosine transform (DCT), and Tetrolet transform, are employed to extract features using block-based algorithms. The study revealed that freezing the model above the block4 pool layer in the VGG-16 pre-trained model led to inferior classifier performance. Customized designs with fewer convolutional layers faced challenges in generalization compared to models with more layers. The models were evaluated using datasets including CG-1050-V1, CG-1050-V2, MICC-F220, MICC-F2000, CMFD, CASIA V1, CASIA V2, and MICC-F2000. The accuracy rates achieved were 98%, 94%, 95%, and 97% for CASIA, CMFD, and MICC-F2000, respectively.

Kang and Cheng [12] presented a methodical strategy and designed a simulation experiment that can efficiently and rapidly identify duplicated regions. Producing the singular value matrix from the image blocks using the enhanced singular value decomposition method and identifying forgeries in the region by matching image blocks using the correlation coefficient are the two primary contributions of this study. The outcome of the experiment demonstrates the algorithm's anti-noise and detection capabilities. As digital media evolves, more digital forgery techniques will emerge, and these techniques will modify traces in increasingly subtle ways, increasing the need for security protection and detection. 100 Testing images of size 512x512 pixels from a Samsung MS 15 digital camera were altered using Adobe Photoshop CS for the experiment, which yielded a 97% accuracy rating.

Yue Wu et al. [13] presented a complete DNN solution for image copy-move detection issues. This novel technique is wholly trainable, in contrast to conventional systems that involve numerous phases of parameter modification and training. Due to this, the forgery mask reconstruction loss is jointly optimised for all modules, and it is shown that the model can be trained using only fabricated training data and still outperform conventional methods. The initial strategy adequately illustrates the promising future of employing DNNs for problems such as image fusion detection and the image copy-move forgery detection problem. The datasets used for evaluation are the synthesised 10K dataset and the CASIATIDEv2.0 dataset. The CASIATIDE v2.0 contains 7491 authentic and 5132 altered-colour images, and the accuracy for the synthesised 10K dataset is 80.35 percent, while the accuracy for the CASIATIDE v2.0 is 67.8 percent.

Copy-Move Forgery Detection was proposed by Ahmed et al. [14] and consists of five steps: image pre-processing, overlapping block separation, determining the statistical feature mean and standard deviation, feature sorting into a matrix, and giving the feature vector to the SVM classifier to determine whether the image is real or not. Multiple transform domain-based copy-move image forgery detection (CMFD) techniques exist. In a blocking strategy, lexicographic sorting and DCT coefficients are utilised. CMFD employs transform types DWT and DCT, the stationary transform being DCT. The wavelet transform and the tetrahedral transform Due to their high computational complexity, several of these techniques are not resistant to post-processing operations such as blurring, lossy compression, or a combination of these operations. Utilised is the MICC-F220 dataset, which contains 220 images (110 authentic and 110 forgeries). The system achieves an improved detection rate of 98.44%.

Researchers have made significant strides in Copy-Move Forgery Detection (CMFD) by combining local binary pattern (LBP) with wavelet transform [15] and singular value decomposition [16]. Additionally, the application of center symmetric local binary pattern (CSLBP) [17], a variant of LBP, has enhanced CMFD's resilience against noise during feature extraction. Keypoint-based methods have also gained prominence in CMFD research. These methods leverage the robustness of keypoint features, making them ideal for handling challenges like scaling, rotation, and occlusion. The adoption of scale invariant feature transform (SIFT) in forgery detection [18] has paved the way for various SIFT-based transformations, including binarized SIFT [19], opponent SIFT [20], and affine SIFT [21], contributing to the advancement of CMFD techniques.

The survey illustrates the evolution of forgery detection techniques, highlighting the strides made in combating sophisticated image manipulations, and emphasizes the critical role played by advanced algorithms and deep learning in ensuring the integrity of digital imagery.

3 Proposed Work

The research methodology employed in this study focuses on utilizing deep learning techniques to detect copy-move image forgery, with a specific emphasis on the development and evaluation of an accurate and effective Convolutional Neural Network (CNN) model. To ensure seamless data preprocessing without compromising any image components, the input images undergo resizing. This step facilitates the subsequent stages of feature extraction and classification by optimizing the data's compatibility with the CNN model. The feature extraction stage is fundamental to the methodology and is facilitated through a sequence of four convolution layers followed by a max-pooling layer. Subsequently, the features extracted are channeled into a fully connected layer, consolidating the pertinent information and forwarding it to the softmax layer. This intricate process enables the CNN model to discern nuanced patterns within the image, crucial for accurate identification of copy-move forgeries. The classification stage, activated after feature extraction, distinguishes between forged and original images based on the processed data.

During the training phase, batches of labeled images are fed into the CNN model, allowing it to learn and refine its feature extraction capabilities. The training dataset is pivotal in enhancing the network's ability to identify copy-move tampering accurately. As the CNN layers progress through the images, deeper layers extract intricate features specialized in identifying copy-move forgeries, while the initial layers focus on extracting low-level information such as edges and corners. The efficacy of the CNN model is quantified through the calculation of the loss function, which measures the disparity between the predicted output and the real labels. Various optimization techniques, including the selection of appropriate loss functions, optimization algorithms, mini-batch size, maximum number of epochs, initial learning rate, and learning rate schedules, are meticulously explored and specified in the training options. These parameters are fine-tuned to ensure the CNN model's optimal performance in detecting copy-move forgeries.

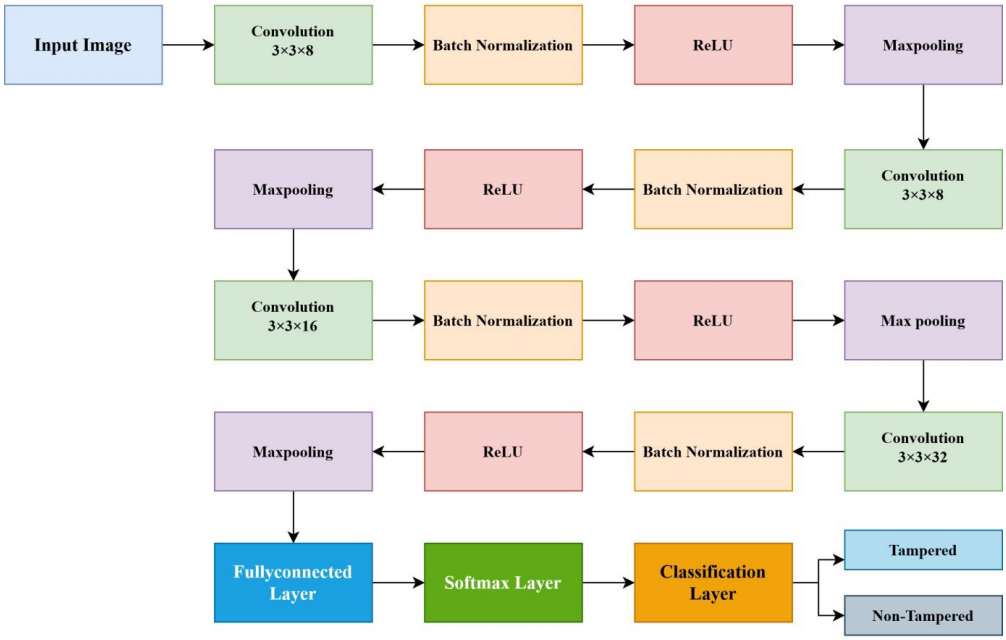


Figure 2. Architecture of the Proposed Network for Copy Move Forgery Detection

Upon completion of the training process, the CNN model is deployed to detect copy-move forgeries in new images. The accuracy of the trained classifier is rigorously evaluated by feeding it test features. Furthermore, the CNN model's performance is optimized for multiple metrics, including accuracy, precision, recall, and F1-score, through the strategic application of diverse loss functions and optimization approaches during the training phase. This comprehensive evaluation ensures the robustness and reliability of the proposed methodology in the realm of copy-move forgery detection.

The proposed architecture for copy move forgery detection is shown in Figure 2. The architecture has 4 sets convolutional layers, max-pooling layers, batch normalization layers and one fully connected layer, a softmax classifier that assesses whether the image has been altered are all included in the suggested CNN architecture. The convolutional layer then adjusts in order to extract its features when the input layer gets the input image of size 224 x 224 x 3 and produces a single scalar value representing the chance of the input image being a fake. To create its feature maps, the convolution layer employs a unique set of filters (size 3 x 3, stride 1, and padding). By employing a layer known as batch normalization, the output of the earlier levels is normalized.

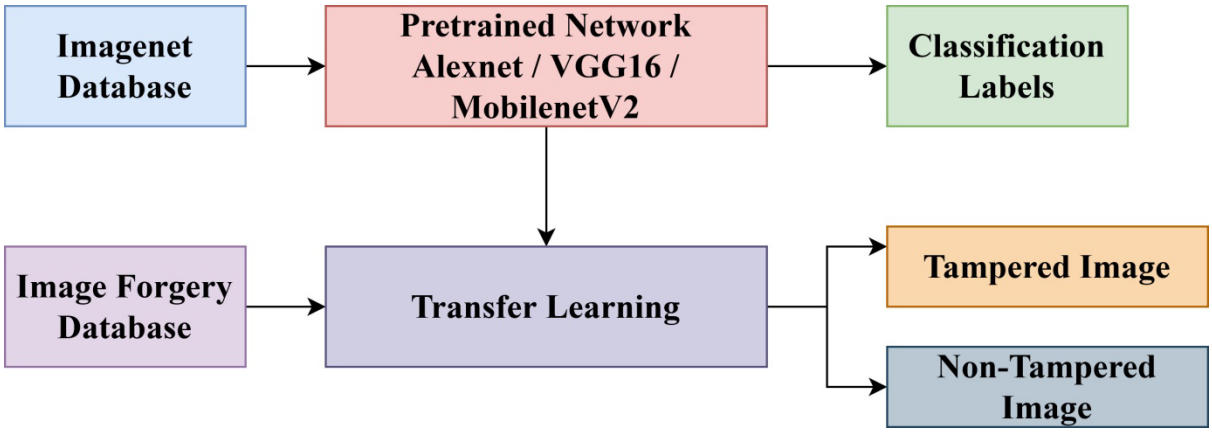


Figure 3. Transfer Learning for Copy Move Forgery Detection

Figure 3 shows the illustration for transfer learning for Copy Move Forgery Detection.

VGG-16 Architecture [22]: VGG-16, a renowned image classification model, was originally developed for the ImageNet Challenge utilizing a subset of 1000 classes. Its distinguishing features include a MaxPooling layer preceding a stack of 13 convolutional layers, with 3 x 3 and 1 x 1 filters employing a stride of 1 pixel, and 3 fully connected (FC) layers. VGG-16's activation function, network depth, number of filters in convolutional layers, and the arrangement of convolutional layers before pooling distinguish it from custom-designed architectures. The pre-trained VGG-16 model was chosen for this study due to its sequential architecture, facilitating a direct comparison between the custom model and the transfer learning model of the same type. Recent research has demonstrated the utility of VGG-16 in tasks such as detecting forged images and colorization from online sources. Despite having more parameters and longer inference durations than alternative architectures like Inception or ResNet, VGG-16 can be pruned for real-time applications without compromising performance.

MobileNet V2 [23]: This study utilizes an upgraded version of the MobileNetV2 model, originally proposed by Sandler et al., for image categorization. The model is modified to suit the binary classification task of identifying two classes—Authentic and Forged. The base layers of the MobileNetV2 model are frozen to prevent their weights from changing during backpropagation. Additional layers, including global average pooling, a dense layer with two outputs corresponding to the classes, and a SoftMax function at the output, are added. The model employs a 3 x 3 kernel size and can process input images up to 224 x 224 x 3 dimensions. ReLU6 activation, batch normalization, and dropout functions are integrated into the design.

AlexNet [24]: In this method, images are divided into blocks, and feature vectors are extracted using AlexNet. Comparisons of these feature vectors identify similar blocks, which are then clustered to detect potential forgeries. The approach utilizes convolutional operations based on pooling and ReLU activation functions to extract deep features. Features are derived from the fully connected f7 layer, with the dataset's images pre-processed and resized to 227 x 227 to match the model's initial input layer. Convolutional layers apply a series of filters to extract features, generating feature maps indicating the presence of specific features in the input image. The output of convolutional layers undergoes processing in fully connected layers, involving matrix multiplications and nonlinear transformations, culminating in a softmax function to produce a probability distribution across

classes. The predicted class, determined by the highest probability, is compared with the ground truth label to assess prediction accuracy.

4 Results and discussion

This section consists of comprehensive assessment of the proposed approach in different dataset. And the results are also compared with the other existing methods.

The Commonly used and well-known datasets like MICC-F2000 [25], MICC-F600 [25], MICC-F220 [25] and CoMoFoD [1] are used to evaluate Copy move image forgery detection algorithms. The information regarding the datasets are shown in Table 1 and some of the sample images are shown in Figure 4. MICC-F220 comprises a total of 220 images, evenly distributed between 110 tampered images and 110 original images. The dimensions of these images range from 722 × 480 to 800 × 600 pixels, with the manipulated region accounting for 1.2% of the entire image area. MICC-F2000 encompasses 2000 images, divided into 700 tampered images and 1300 original images. These images are of high resolution, measuring 2048 × 1536 pixels. In this dataset, the manipulated region constitutes 1.12% of the total image area. MICC-F600 comprises 600 images, with 152 images featuring tampered regions and 448 images representing the original state. The dimensions of these images vary, ranging from 800 × 532 to 3888 × 2592 pixels. Notably, the size of the manipulated region differs across images within this dataset.

Figure 4: Sample Images from MICC-F2000 database

The two data divisions, original and Forged, were split into 80% and 20% partitions, respectively, for testing purposes.

TABLE 1. Details of the Dataset used

Dataset	Total	Tampered	Original
MICC-F220	220	110	110
MICC-F600	600	160	440
MICC-F2000	2000	700	1300
CoMoFoD	9427	4709	4718

Performance Measures: Table 2 displays the confusion matrices of the proposed approaches. In Table 2, the fake images are marked with a negative sign while the original ones are marked with a positive sign.

TABLE 2 Confusion Matrices of the Proposed Architecture

Dataset	Classes	+	-
MICC-F220	+	21	1
	-		22
MICC-F600	+	71	17

	-		32
MICC-F2000	+	244	16
	-		140
CoMoFoD	+	936	8
	-	7	935

The numbers TP and FP stand for the proportions of falsely discovered tampered images and authentically detected altered images, respectively. The number of altered images that were mistakenly used as original images is represented by the FN. The number of authentically identified original images is represented as TN. Their decision was supported by the fact that Forged images were (correctly) projected to be forged with a higher success rate and Real images were (falsely) predicted to be Forged with a lower success rate. The True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate(FNR) for MICC-F220 is 100%, 95.65%, 4.34% and 0%. The True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate(FNR) for MICC-F600 is 100%, 65.30%, 34.69% and 0%. The True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate(FNR) for MICC-F2000 is 100%, 89.74%, 10.25% and 0%. The True Positive Rate (TPR), True Negative Rate (TNR), False Positive Rate (FPR), False Negative Rate(FNR) for CoMoFoD is 99.25%, 99.15%, 0.74% and 0.84%. The comparison of recall, precision and F1-score for dataset MICC-F220, MICC-F600, MICC-F220 and CoMoFoD are shown in the Table 3.

TABLE 3 Performance measure of the Proposed Architecture for Copy Move Forgery Recognition

Dataset	Precision	Recall	FI-score
MICC-F220	0.9562	0.9776	0.0454
MICC-F600	0.6530	0.7900	0.1931
MICC-F2000	0.8974	0.9459	0.0615
CoMoFoD	0.9915	0.9919	0.0084

In our study, we employed the VGG-16 neural network architecture to tackle the challenging task of copy-move image forgery detection. Unlike its predecessors like AlexNet, VGG-16 utilizes relatively small receptive fields, employing 3x3 convolutions with a stride of 1. This design choice enhances the network's ability to capture intricate features within the images. Additionally, VGG-16 differs from previous architectures by transitioning from small to large convolution kernels and omitting several fully connected layers. This modification increases the model's complexity and parameter count, allowing it to learn more intricate patterns from the input data. Table 4 presents the performance measures of the VGG16 model for copy-move forgery recognition. However, despite these enhancements, our results indicate that VGG-16 exhibits varying levels of accuracy across different datasets. On the MICC-F220 dataset, the accuracy stands at 50%, while it improves to 61.67% on MICC-F600, further increasing to 66.25% on MICC-F2000, and achieving the highest accuracy of 70.23% on the CoMoFoD dataset.

TABLE 4 Performance measure of the VGG16 for Copy Move Forgery Recognition

Approach	Dataset used	Accuracy (%)
VGG 16	MICC-F220	50
	MICC-F600	61.67
	MICC-F2000	66.25
	CoMoFoD	70.23

MobileNetV2 utilizes inverted residual blocks with bottlenecking features, leading to a significant reduction in the number of parameters. This reduction, coupled with a decrease in bottleneck channel size, results in improved speed and efficiency compared to its predecessor.

Table 5 presents the accuracy results of the MobileNetV2 approach on different datasets, namely MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD. The accuracy percentages indicate the model's

effectiveness in recognizing patterns within the datasets. For instance, on the CoMoFoD dataset, MobileNetV2 achieves the highest accuracy of 78.56%, showcasing its strong performance in image recognition tasks with varying complexities and sizes.

TABLE 5 Performance measure of the MobileNetV2 for Copy Move Forgery Recognition

Approach	Dataset used	Accuracy (%)
MobileNETV2	MICC-F220	47.73
	MICC-F600	74.17
	MICC-F2000	69.75
	CoMoFoD	78.56

The provided text discusses the performance of AlexNet, a groundbreaking deep learning architecture that significantly influenced the field of machine learning. AlexNet is known for its 5 convolutional layers and 3 fully connected layers, a design that surpassed previous models like LeNet due to its increased number of filters per layer, stacked convolutional layers, and connections with activation functions. Table 6 presents the accuracy results of the AlexNet approach on different datasets, including MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD. The accuracy percentages indicate the effectiveness of AlexNet in recognizing patterns within these datasets. For instance, on the MICC-F600 dataset, AlexNet achieves an accuracy of 67.50%.

TABLE 6 Performance measure of the Alexnet for Copy Move Forgery Recognition

Approach	Dataset used	Accuracy
ALEX NET	MICC-F220	52.27
	MICC-F600	67.50
	MICC-F2000	62.50
	CoMoFoD	69.34

In the comparison of the proposed method with state-of-the-art methods for the MICC-F220 database (Table 7), MICC-F6000 database (Table 8), MICC-F2000 database (Table 9) several evaluation metrics, including True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate (TNR), were considered. The evaluation results for different methods are summarized below:

TABLE 7 Comparison of the Proposed Method with state of the art method for MICC-F220 Database

Authors	TRP	FPR	FNR	TNR
Amerini et al. [26]	100	8	0	92
Amerini et al. [25]	100	6	0	94
Mishra et al [27]	73.64	3.64	26.36	96.36
Kaur et al [28]	97.27	7.27	2.73	92.73
Elaskily et al [29]	100	0	0	100
Elaskily et al [30]	100	1.80	0	98.20
Proposed Method	100	4.34	0	95.65

TABLE 8 Comparison of the Proposed Method with state of the art method for MICC-F600 Database

Authors	TRP	FPR	FNR	TNR
Elaskily et al [29]	100	0	0	100
Amerini et al. [26]	93.42	11.61	6.58	88.39
Amerini et al. [25]	94.86	9.15	5.14	90.85

Elaskily et al [30]	98.40	6.35	1.60	93.65
Proposed Method	100	34.69	0	65.30

TABLE 9 Comparison of the Proposed Method with state of the art method for MICC-F2000 Database

Authors	TRP	FPR	FNR	TNR
Elaskily et al [29]	100	0	0	100
Amerini et al. [26]	69.20	12.50	30.80	87.50
Amerini et al. [25]	81.60	7.27	18.40	92.73
Elaskily et al [30]	94.50	11.35	5.5	88.65
Proposed Method	100	10.25	0	89.74

In the comparative evaluation across the MICC-F220, MICC-F6000, and MICC-F2000 databases, the proposed forgery detection method consistently achieves a perfect True Positive Rate (TPR), indicating its proficiency in correctly identifying manipulated regions. Notably, when scrutinizing the MICC-F220 database, the proposed method outperforms several state-of-the-art techniques, maintaining a TPR of 100% while exhibiting a relatively low False Positive Rate (FPR) of 4.34%. This suggests a commendable balance between accurate detection and minimizing false alarms. However, the evaluation on the MICC-F6000 database reveals a higher FPR of 34.69%, indicating a potential sensitivity to false positives in this specific dataset. Despite this, the method maintains a perfect TPR, showcasing its robustness in identifying actual forgeries. In the context of the MICC-F2000 database, the proposed method again excels with a flawless TPR and a relatively low FPR of 10.25%.

5 Conclusions

In conclusion, the proposed CNN-based approach stands as a potent solution for the detection of copy-move forgery in images. Leveraging transfer learning, the method harnesses the power of pre-trained deep learning models—Alexnet, VGG16, and MobilenetV2—fine-tuned explicitly for the task of forgery detection. This custom-designed framework optimizes feature extraction and classification processes, elevating the accuracy and efficiency of detecting manipulated content in images. The adaptability of the methodology is underscored by its successful application across diverse datasets, namely MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD.
The experimental evaluations conducted reveal compelling results, solidifying the effectiveness of the proposed approach. True Positive Rates (TPR) consistently reaches 100%, demonstrating the method's proficiency in correctly identifying tampered images. Notably, the False Positive Rates (FPR) remains impressively low, indicating a minimal incidence of false positives—authentic images erroneously identified as manipulated.

References

1. D. Tralic, I. Zupancic, S. Grgic, & M. Grgic (2013). CoMoFoD - New Database for Copy-Move Forgery Detection. In *Proc. 55th International Symposium ELMAR-2013* (pp. 49–54).
2. B. Mahdian, & S. Saic (2007). Detection of copy-move forgery using a method based on blur moment invariants. *Forensic Sci. Int., 171(2), 180–189.*
3. S.-J. Ryu, M.-J. Lee, & H.-K. Lee (2010). Detection of copy–rotate–move forgery using Zernike moments. In *Information Hiding* (pp. 51–65).
4. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, & G. Serra (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Trans. Inf. Forensics Secur., 6(3), 1099–1110.*
5. G. Muhammad, M. Hussain, & G. Bebis (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digit. Investig., 9(1), 49–57.*

6. S. H., S. S., D. S. D., & A. N. (2023). TVN: Detect Deepfakes Images using Texture Variation Network. *Inteligencia Artificial, 26(72), 1–14.*
7. V. Barad, & R. Goswami (2020). Image Forgery Detection using Deep Learning. In *6th International Conference on Advanced Computing & Communication Systems (ICACCS)* (pp. 1687–1691). IEEE.
8. C.-M. Pun, E. X.-C. Yuan, & X.-L. Bi (2015). Image Forgery Detection Using Adaptive Over-segmentation and Feature Point Matching. *IEEE Trans. Inf. Forensics Secur.*.
9. Y. Li, & J. Zhou (2015). Fast and Effective Image Copy-Move Forgery Detection via Hierarchical Feature Point Matching. *IEEE Trans. Inf. Forensics Secur.*.
10. M. N. Abbas, M. S. Ansari, N. Kanwal, M. N. Asghar, T. O'Neill, & B. Lee (2021). Lightweight Deep Learning Model for Detection of Copy-move Image Forgery with Post-processed Attacks. In *IEEE International Conference on Systems, Signals and Image Processing (IWSSIP)*.
11. Y. Rodriguez-Ortega, D. M. Ballesteros, & D. Renza (2021). Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. *Sensors*.
12. L. Kang, & X.-P. Cheng (2010). Copy-move Forgery Detection in Digital Image. In *3rd International Congress on Image and Signal Processing (CISP2010)* (pp. 860–864). IEEE.
13. Y. Wu, W. Abd-Almageed, & P. Natarajan (2018). Image Forgery Detection Using Multi-Stream Convolutional Neural Network. In *IEEE Winter Conference on Applications of Computer Vision (WACV)* (pp. 1037–1046). IEEE.
14. I. T. Ahmed, B. T. Hammad, & N. Jami (2021). Copy-move Forgery Detection using Dynamic Texture Features and Hybrid Descriptor. In *IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)* (pp. 1–6). IEEE.
15. T. Mahmood, A. Irtaza, Z. Mehmood, & M. T. Mahmood (2017). Copy–move Forgery Detection through Stationary Wavelets and Local Binary Pattern Variance for Forensic Analysis in Digital Images. *Forensic Sci. Int., 279, 8–21.*
16. Y. Wang, L. Tian, & C. Li (2017). LBP-SVD based Copy Move Forgery Detection Algorithm. In *IEEE International Symposium on Multimedia* (pp. 553–556).
17. D. M. Uliyan, H. A. Jalab, & A. W. A. Wahab (2015). Copy Move Image Forgery Detection using Hessian and Center Symmetric Local Binary Pattern. In *IEEE Conference on Open Systems* (pp. 7–11).
18. H. Huang, W. Guo, & Y. Zhang (2008). Detection of Copy-move Forgery in Digital Images using SIFT Algorithm. In *Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (pp. 272–276).
19. G. Muzaffer, & G. Ulutas (2017). A Fast and Effective Digital Image Copy Move Forgery Detection with Binarized SIFT. In *40th International Conference on Telecommunications and Signal Processing* (pp. 595–598).
20. G. Jin, & X. Wan (2017). An Improved Method for SIFT-based Copy-move Forgery Detection using Non-maximum Value Suppression and Optimized J-Linkage. *Signal Process. Image Commun., 57, 113–125.*
21. A. Shahroudnejad, & M. Rahmati (2016). Copy-move forgery detection in digital images using affine-SIFT. In *2nd International Conference of Signal Processing and Intelligent Systems*.
22. Karen Simonyan, & Andrew Zisserman (2014). Very Deep Convolutional Networks for Large-Scale Image Recognition. *arXiv preprint arXiv:1409.1556*.
23. A. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, & H. Adam (2017). MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. *arXiv preprint arXiv:1704.04861*.
24. Alex Krizhevsky, Ilya Sutskever, & Geoffrey E. Hinton (2017). ImageNet Classification with Deep Convolutional Neural Networks. *Communications of the ACM, 60(6), 84–90.*
25. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, & G. Serra (2011). A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security, 6(3),1099–1110.*
26. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, & G. Serra (2013). Copy-move forgery detection and localization by means of robust clustering with J-linkage. *Signal Processing: Image Communication, 28(6), 659–669.*
27. P. Mishra, N. Mishra, S. Sharma, & R. Patel (2013). Region duplication forgery detection technique based on SURF and HAC. *Sci World J*.

28. H. Kaur, J. Saxena, & S. Singh (2015). Simulative comparison of copy-move forgery detection methods for digital images. *Int J Electr Electr Comput Syst IJEECS, 4.*
29. M.A. Elaskily, & et al. (2020). A Novel Deep Learning Framework for Copy-Move Forgery Detection in Images. *Multimedia Tools and Applications, 79(27–28), 19167–92.*
30. M.A. Elaskily, H.A. Elnemr, M.M. Dessouky, & O.S. Faragallah (2018). Two Stages Object Recognition Based Copy-Move Forgery Detection Algorithm. *Multimedia Tools and Applications*.