Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/GC03.20260375
Published: February 2, 2026

ReLU-EfficientNet: A Robust Deep Learning Framework for Copy-Move Forgery Detection

Fasiha Fatma and Ali Javed
Department of Software Engineering,
University of Engineering and Technology Taxila, Punjab, Pakistan
fasihafatima628@gmail.com, ali.javed@uettaxila.edu.pk

Ahmad Alhabib
Department of Electrical Engineering,
Wayne State University, Detroit, MI, USA
FJ8971@Wayne.edu

Muteb Aljasem
School of Engineering,
University of Bowling Green State University, Bowling Green, OH, USA
Aljasem@bgsu.edu

Muidh Awadh Algahtani
Department of Industrial Engineering, Faculty of Engineering,
University of Tabuk, Tabuk 47512, Saudi Arabia
maalgahtani@ut.edu.sa

Abstract

Exponential growth of multimedia on cyberspace and availability of sophisticated image editing tools have raised the propagation of forged images, leading to a major threat to information integrity and authenticity. Among the conventional image forgery techniques, copy-move forgery (CMF), involving copying and pasting a region within the same image to conceal or duplicate an object, remains the most challenging to detect due to its context-preserving nature and presence of the same noise pattern on the forged regions. Further, CMF is more challenging to detect in the presence of different post-processing attacks. To counter these challenges, we propose a deep learning-based framework, ReLU-EfficientNet, designed for robust CMF detection under post-processing attacks. The proposed method enhances the EfficientNetB0 architecture with the introduction of ReLU activation to enhance discriminative feature extraction, accelerate convergence, and mitigate vanishing gradient problems. Further, we also introduce three dense layers to refine learned features, resulting in better separability, improved generalization, and robust classification performance. We evaluated the performance on two diverse benchmark datasets, MICC-F2000 and CASIA v2.0. The accuracy of 97% on MICC-F2000 and 96% on CASIA v2.0 illustrates the competency of the proposed method over several contemporary CMF detection methods. Furthermore, our method exhibits minimal overfitting and stable learning, thus providing strong generalization. These findings highlight the effectiveness and computational efficiency of our ReLU-EfficientNet method for CMF detection.

Keywords
Copy-move forgery detection, deep learning, EfficientNet, ReLU, image forensics.

1. Introduction

The easier availability of low-cost imaging devices and social media platforms has motivated users to generate an enormous amount of multimedia content, including images. Digital images are widely used in various domains, including communication, journalism, surveillance, and social media, to record events, deliver information, and serve as evidence in legal and security contexts. However, the access to different cutting-edge image editing tools has made image manipulation faster and more realistic. Such manipulations can distort facts, spread disinformation, and reduce public trust in digital media. Copy-move forgery (CMF) is one of the most frequently used techniques among others, being most difficult to detect. CMF involves copying and pasting a region within the same image to either conceal or duplicate objects, making the forgery appear visually seamless.

Conventional copy-move forgery detection (CMFD) methods relied on handcrafted feature extraction. Techniques such as Scale-Invariant Feature Transform (SIFT), Speeded-Up Robust Features (SURF), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are frequently employed to spot duplicated regions by analyzing texture and structure. These traditional approaches are effective in certain conditions, but often experience degraded performance under different transformations, like rotation, scaling, blurring, or compression. Point-based methods like SIFT and SURF perform well on clean images but show lower results under noise or post-processing attacks (Gani and Qadir 2021; Priyanka et al. 2020). The conventional approaches lack robustness under different geometric transformations and post-processing attacks due to the complexity and diversity of modern-day digital images.

Deep learning (DL) approaches have been effectively applied to combat various image forgeries. Convolutional Neural Networks (CNNs) learn hierarchical and discriminative features automatically from raw pixels, without requiring manual feature engineering approaches. Studies (Tahaoglu et al. 2021; Ryu et al. 2008) have shown that CNN-based models perform better than traditional techniques by learning fine-grained variations in texture, color, and geometry. However, deep networks still face challenges such as long training times, high computational cost, and overfitting on small or imbalanced datasets. EfficientNet (Niu et al. 2021) addresses many of these issues through compound scaling of depth, width, and resolution, achieving improved accuracy with fewer parameters. Recent studies (Jain and Kundra 2024; Reyad et al. 2023) revealed that employing advanced activation and optimization techniques can significantly enhance convergence speed and accuracy in detection and classification tasks.

Detecting copy-move forgery is more difficult due to the presence of similar noise patterns, color tonality, lightning, textures, etc., in copied and pasted regions. Moreover, forgers often used different transformations like rotation, rescaling, blending, etc., to further complicate detection. These challenges present a motivation to develop more effective CMFD methods robust to the above-mentioned challenges. The objectives of this research work include the development of a reliable CMFD approach robust to different post-processing attacks. To counter these, this research introduces an end-to-end DL-based framework for robust CMFD under post-processing transformations. Our method presents an improved version of the EfficientNet-B0 backbone with ReLU activation to improve feature extraction, convergence speed, and generalization. The major contributions of this research are as follows:

- We present an effective and robust DL method, ReLU-EfficientNet, to reliably detect copy-move image forgery under post-processing attacks.
- We introduce ReLU activation in the EfficientNet-B0 backbone to enhance feature extraction, expedite convergence, improve stability, and reduce vanishing gradient issues.
- We introduce three dense layers with dropout to combine and refine features for improved generalization and robust classification performance.
- Extensive experimentation on two diverse benchmarks, MICC-F2000 and CASIA v2.0, with an average accuracy of 97% and 96%, respectively, signifies the efficacy of our technique for CMFD.

2. Literature Review

This section critically analyses the existing state-of-the-art (SOTA) CMFD methods. The research community has explored various point-based, block-based, DL-based, and hybrid approaches to counter the threats of CMF.
The point-based approach identifies keypoints in the image to get transformation invariance and resistance to post-processing attacks for CMF. Niu et al. (2021) proposed a moment invariant method based on SIFT keypoints, and achieved good accuracy and efficiency for CMFD. For accurate localization, this method employed clustering, filtering, and SSIM; however, this method struggles to achieve better results under geometric distortions. Hegazi et

al. (2021) introduced a DBSCAN-GORE method to successfully reduce false detections while improving operational efficiency. However, it has limited performance when dealing with complex textured regions. Lyu et al. (2021) presented a double matching approach using Delaunay triangle matching, DBSCAN, and RANSAC localization to boost precision and robustness under scaling and rotation transformations. This approach requires longer matching time when it comes to large image datasets. Jiang et al. (2024) presented a dynamic keypoint-detection approach for CMFD. This method is unable to perform well on noisy and compressed images.

Existing works have also employed block-based methods for CMFD by splitting an image directly into smaller parts and comparing the extracted characteristics. (Mahdi and Ali 2024) extracted features from overlapping blocks using a multiple-stage Local Binary Pattern (LBP) and angular second moments, along with standard variance with SVM for classification. This approach shows degraded performance under geometric transformations and other post-processing attacks. Amiri et al. (2024) employed DWT and DCT with the Equilibrium Optimization Algorithm (EOA) to detect the CMF, but were unable to achieve better performance under compression and complex post-processing attacks. Priyanka et al. (2020) have used a DCT-SVD approach to enhance the detection robustness. The method used DCT features with SVD reduction and applied SVM and K-means algorithms to perform both classification and localization tasks. The method demonstrated reasonably better performance under noise, scaling, and compression, but it was unable to perform well under geometric transformations. The block-based methods experience problems when working with repeated block deviations and boundary irregularities that occur in light-textured or complex image regions.

Deep learning techniques have improved the performance of CMFD over the traditional approaches due to their ability to compute salient feature maps and better classification. Chang (2023) created a DL approach based on combining the ResNet18 with a vision transformer to achieve both the detection and localization of forged regions. Jaiswal and Srivastava (2022) developed a CNN model to improve the CMFD under scaling and geometric transformations; however, with poor generalization ability to tackle new forgeries. Kumaret et al. (2024) used the DenseNet model to detect the copy-move and splicing forgeries, but with higher computational complexity. Khalil et al. (2023) developed a CNN-based system for reasonable forgery detection performance while maintaining a lower computational cost. However, it is important to mention that it achieved lower performance than deeper DL models. Abbas et al. (2021) provided a comparative analysis to assess the performance of SVGGNet and MobileNetV2 models for CMFD. This study revealed that MobileNetV2 showed better accuracy and false positive reduction under noise, rotation, and blurring attacks. Zabiya et al. (2024) used a standard CNN model, whereas (Oraby et al. 2024) used an ensemble deep neural network with XGBoost to identify CMF regions. These approaches are unable to spot forged segments of small regions and have limited generalizability. Nazir et al. (2022) proposed an enhanced Mask RCNN model. The system used DenseNet-41 to achieve better accuracy while making the model more resistant to post-processing attacks. The model shows better feature extraction with a low computational cost. Moreover, DL methods in general are computationally more expensive than traditional methods.

The development of hybrid techniques that combine block-based and keypoint-based techniques has resulted in enhanced detection performance in challenging image manipulation scenarios. The hybrid model suggested by (Singh and Kumar 2024) developed the emperor penguin optimization technique and obtained better performance under a variety of forgeries, including the CMF. However, the model's adaptability and timeline for convergence are still limited for datasets of considerable size. Kaur et al. (2024) proposed a hybrid model to detect CMF using a CNN and wavelet-transformed picture coefficients, but showed lower performance on images with post-processing attacks of different severity levels. Tinnathi and Sudhavani (2021) presented a dynamic gradient swarm optimization method for CMF detection, but it was unable to perform well under extreme geometric variations. Yu et al. (2025) presented an efficient ConvNeXt-UperNet framework for CMFD. Dell'Olmo et al. (2025) employed a hybrid CMFD method using traditional clustering of forged region predictions with deep learning. This method was unable to cope well with unseen tampering variations. By combining BRISK and SURF descriptors with DBSCAN clustering, (Bilal et al. 2020) successfully minimized false positives and improved robustness towards noise and compression attacks. However, a significant drop in performance was reported when handling low-contrast images. Diwan and Roy (2024) proposed a dual-stage pipeline combining CNN-learned localized descriptors with traditional keypoint detection for CMFD, but with added computation cost.

The current CMFD techniques show several limitations. Methods with handcrafted features are ineffective with noisy data, compression, and post-processing. The performance of keypoint-based and block-based techniques is limited under geometric transformations. The hybrid and DL methods achieve better results than all other traditional methods,

but with increased computational cost. Lightweight CNNs are proposed to reduce the computational cost of DL techniques, but these approaches suffer from limited generalization ability.

3. Methodology

This section provides a detailed explanation of our deep learning framework, ReLU-EfficientNet for CMF detection. To effectively extract complex features from forgery images, we used the EfficientNetB0 network combined with the ReLU activation function to enhance feature extraction. Additionally, we introduced three dense layers to combine and refine features for improved generalization and robust classification performance. The workflow of the proposed method is illustrated in Figure 1.

3.1 Preprocessing

The images are of different sizes; therefore, data preprocessing is essential before model training to ensure that the image dimensions are consistent and uniform across the entire dataset. Thus, the images were resized to 128 × 128 × 3. Then, the pixel intensity values are rescaled to a predefined range of 0 to 1 to enhance the data presentation and quality, which can improve model training and detection performance.

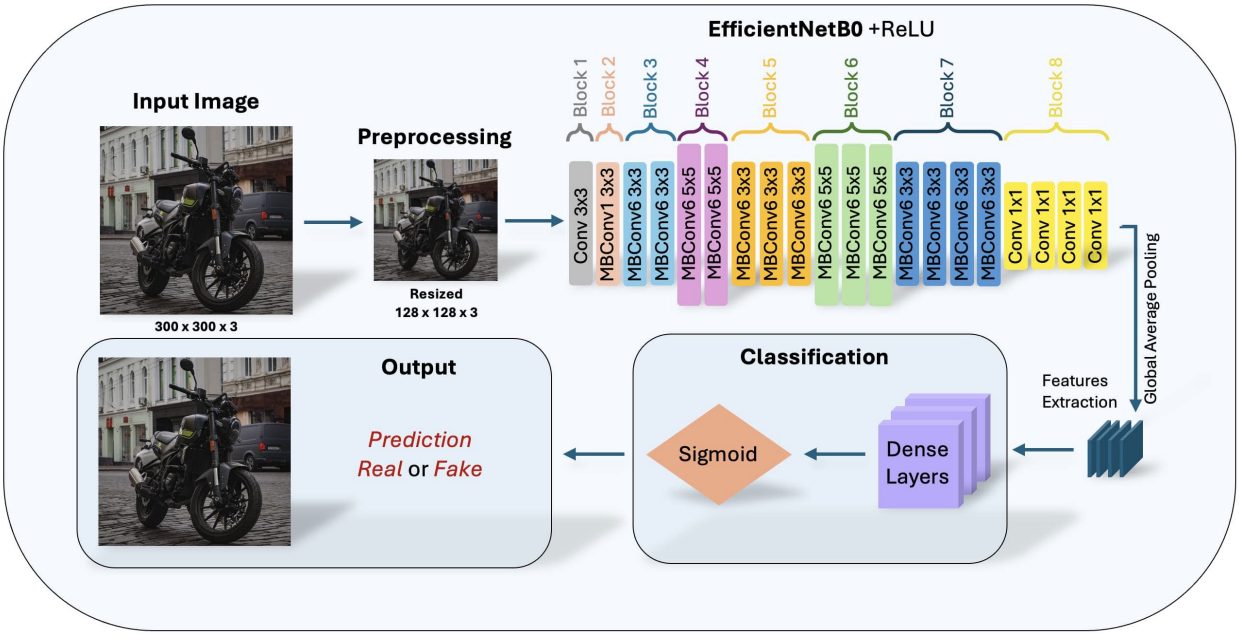

Figure 1. Workflow of the proposed method.

3.2 Feature Computation

The proposed method presents an improved version of EfficientNetB0 for CMFD. We selected the EfficientNetB0 model for architectural enhancements due to its dual benefits of better detection and generalization performance, and computational efficiency. EfficientNet is based on compound scaling, an approach to balancing network depth, width, and input resolution with the help of a simple and powerful scaling coefficient. This approach ensures that the network performs well with fewer parameters than traditional CNNs.

To enhance our method's capacity to learn significant features, a Squeeze-and-Excitation (SE) block is placed after each convolutional layer. By suppressing less useful channels in a feature map, the SE block facilitates the model to emphasize the most crucial ones. As demonstrated below, the squeeze process first uses Global Average Pooling (GAP) to downsample spatial data for each channel as:

$$z_c = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} X_c(i,j) \quad (1)$$

Here, *Xc*, *H,* and *W* represent the c^{th} channel of the feature map, its height, and width, respectively. The excitation step then uses two completely connected layers with Sigmoid as well as ReLU activations to determine the significance of each channel as:

$$s = \sigma\big(W_2 \cdot \delta(W_1 \cdot z)\big) \quad (2)$$

In Eq. (2), the sigmoid activation function is represented by σ and the weight matrices by W_1 and W_2. A weight ranging from 0 to 1 is provided for each channel by the output, s. Next, these adjusted weights are multiplied by the initial features to produce the modified feature maps as follows:

$$X_c' = s_c \cdot X_c \quad (3)$$

The network can enhance the quality of feature representations also adaptively highlight more relevant information by incorporating SE blocks into each convolutional layer. This helps the model in identifying minute details and small variations in images, leading to improved identification of copy-move forgeries.

After feature extraction, Global Average Pooling (GAP) is used to flatten the feature maps. It is followed by three additional dense layers introduced in our ReLU-EfficientNet to perform the classification. Our model consists of a dense layer of 512 neurons and 50% dropout, then a dense layer of 256 neurons and 50% dropout, and finally a third dense layer with 128 neurons followed by 50% dropout. The last stage is the binary prediction that involves one output layer with a single sigmoid neuron. The architectural details of our ReLU-EfficientNet are depicted in Table 1.

3.3 Activation Function

We introduce the ReLU activation in place of Swish in all Convolutional layers, due to its simplicity, faster convergence, and mitigating the vanishing gradient problem. The sparse activation property of ReLU enables fast learning with fewer computing resources. Furthermore, we added dropout layers between each dense layer to minimize the risk of overfitting. The combination of dropout and ReLU ensures the model remains lightweight while achieving better detection performance. ReLU is defined as:

$$f(x) = max(0, x) \quad (4)$$

3.4 Training Configuration and Optimization

We used the Adam optimizer to train our model due to its ability to adjust the learning rate during training (Reyad et al. 2023). The hyperparameters were set as: Learning rate=0.001, Batch size=32, and early stopping with patience of 5 epochs. We used the binary cross-entropy loss function in our model, as it penalizes incorrect predictions more heavily when the model exhibits higher confidence, thus improving the generalization. We computed the loss function as:

$$\mathcal{L}(y, y^{\wedge}) = -[\text{ylog}(y^{\wedge}) + (1 - y)\log(1 - y^{\wedge})] \quad (5)$$

Table 1. Architectural details of the proposed model

Blocks	**Layer Type**	**Kernel Size and Number of Layers**	**Stride Value**
1	Convolutional layer (EfficientNetB0)	3 × 3 conv	2
2	MBConv 1 Block (EfficientNetB0)	3 × 3 conv × 1	1
3	MBConv 6 Block (EfficientNetB0)	3 × 3 conv × 2	2
4	MBConv 6 Block (EfficientNetB0)	5 × 5 conv × 2	2
5	MBConv 6 Block (EfficientNetB0)	3 × 3 conv × 3	2
6	MBConv 6 Block (EfficientNetB0)	5 × 5 conv × 3	1
7	MBConv 6 Block (EfficientNetB0)	3 × 3 conv × 4	2
8	Convolutional layer (EfficientNetB0)	1 × 1 conv × 4	1
9	GlobalAveragePooling2D layer		
10	Dense layer	512 units	-
11	Dropout layer	50% dropout rate	-
12	Dense layer	256 units	-
13	Dropout layer	50% dropout rate	-
14	Dense layer	128 units	
15	Dropout layer	50% dropout rate	-
16	Output layer	Sigmoid activation	-

4. Datasets

We used two diverse and large-scale datasets, MICC-F2000 (Amerini et al. 2011) and CASIA v2.0 (Dong et al. 2013), to test the effectiveness of our method. Both datasets consist of authentic and tampered images. MICC-F2000 comprises

2000 images, including 1300 authentic and 700 tampered samples, while CASIA v2.0 contains 12323 images, with 7200 authentic and 5123 tampered samples. The MICC-F2000 dataset includes the tampering of CMF with both plain forgery and post-processed attacks, such as blurring, rotation, compression, etc. On the other hand, CASIA v2.0 includes both the splicing and CMF, again, both plain forgery and post-processed attacks, such as blurring, noise, contrast adjustment, etc. Figures 2 and 3 provide a few snapshots of original and tampered images of the MICC-F2000 and CASIA v2.0 datasets.

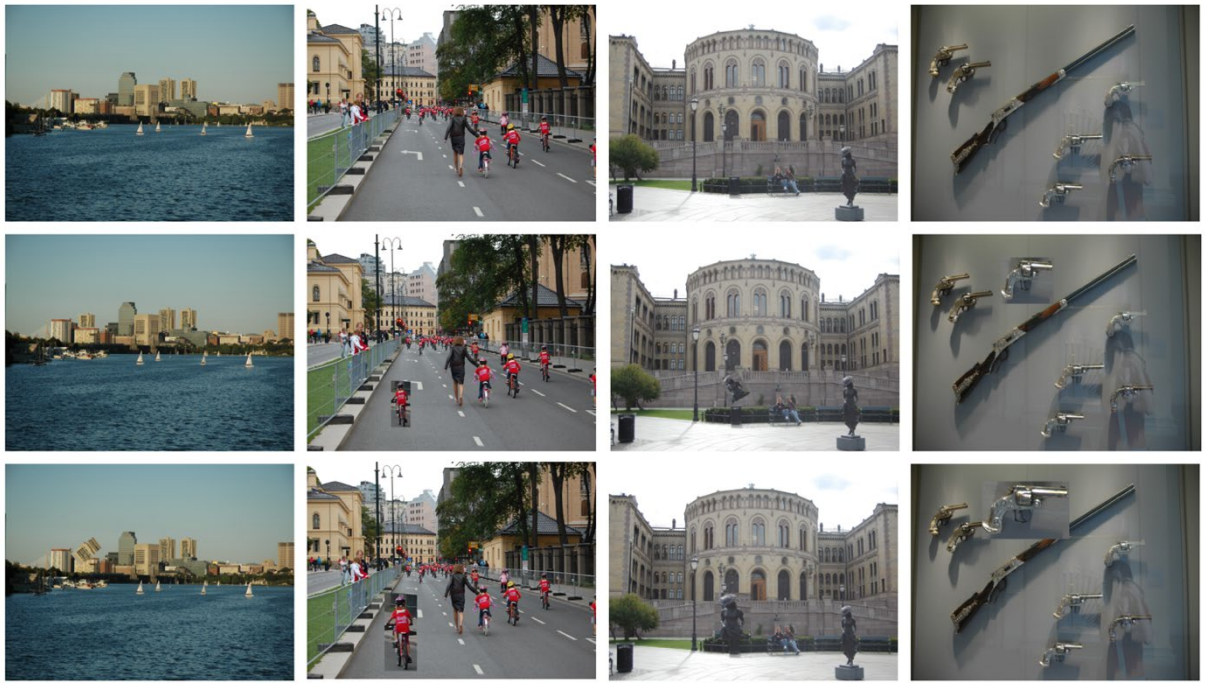

Figure 2. MICC-F2000 dataset: (Row 1- original images, rows 2 & 3-tampered/forged images).

Figure 3. CASIA v2.0 dataset: (Row 1- original images, rows 2 & 3-tampered/forged images).

5. Results and Discussion

This section provides the details of evaluation metrics, different experiments, and a discussion on the results of experiments conducted for performance evaluation.

5.1 Evaluation Metrics

To comprehensively evaluate the proposed model's performance, accuracy, precision, recall, and F1 score were used. Accuracy determines our method's ability to correctly classify images as authentic or forged, and is computed as:

$$\text{Accurancy} = \frac{\text{TP+TN}}{\text{TP+FP+TN+FN}} \quad (6)$$

where *TP*, *TN*, *FP*, and *FN* represent the numbers of true positives, true negatives, false positives, and false negatives, respectively.

Precision measures the proportion of correctly identified tampered images out of the entire images predicted as tampered and is calculated as:

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (7)$$

Recall measures the ability of the model to correctly detect all tampered images within the dataset, and is computed as:

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (8)$$

The F1 score is the harmonic mean of precision and recall, and gives a clear view of the model's overall performance. We calculated the F1 score as follows:

$$\text{F1 score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision+Recall}} \quad (9)$$

The confusion matrix is also used to provide an intuitive and visual representation of our method's performance.

5.2 Evaluation on MICC-F2000 and CASIA v2.0 dataset

We designed an experiment to evaluate the proposed ReLU-EfficientNet method using two diverse publicly available datasets, MICC-F2000 and CASIA v2.0. The datasets contain authentic as well as plain and post-processing attacks-based tampered images. We used 80% samples for model training and the remaining 20% unseen samples to test our model for both datasets. The results in terms of precision, recall, F1 score, and accuracy are shown in Table 2. We attained excellent detection accuracy of 97% on MICC-F2000 and 96% on CASAI v2.0, which demonstrates the efficacy of our method for reliable CMFD even in the presence of post-processing attacks.

Table 2. Evaluation on MICC-F2000 and CASIA v2.0 datasets

Dataset	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)
MICC-F2000	94	97	95.5	97
CASIA v2.0	97	94	95.5	96

5.3 Confusion Matrix Analysis

We designed a confusion matrix analysis experiment to assess the classification performance of our ReLU-EfficientNet method on both datasets. This evaluation helps to visualize the model's prediction of correctly and incorrectly classified samples. Figure 4 shows the confusion matrix outcomes on both datasets.

For the MICC-F2000 dataset, we can observe that our method predicted an FP of 18 and an FN of 42 among the 2000 total images. These results indicate that the model achieved exceptionally high classification accuracy with 682 true positives and 1258 true negatives, and only 60 samples among 2000 were misclassified. These misclassifications are caused by manipulations involving highly similar texture patterns or low-contrast duplicated regions. Nevertheless, the ratio of FNs to total forged samples remained negligible, confirming our method's strong capacity to generalize even on smaller-region manipulations. This demonstrates that ReLU-EfficientNet can effectively capture fine-grained spatial correlations and local inconsistencies within the MICC-F2000 dataset.

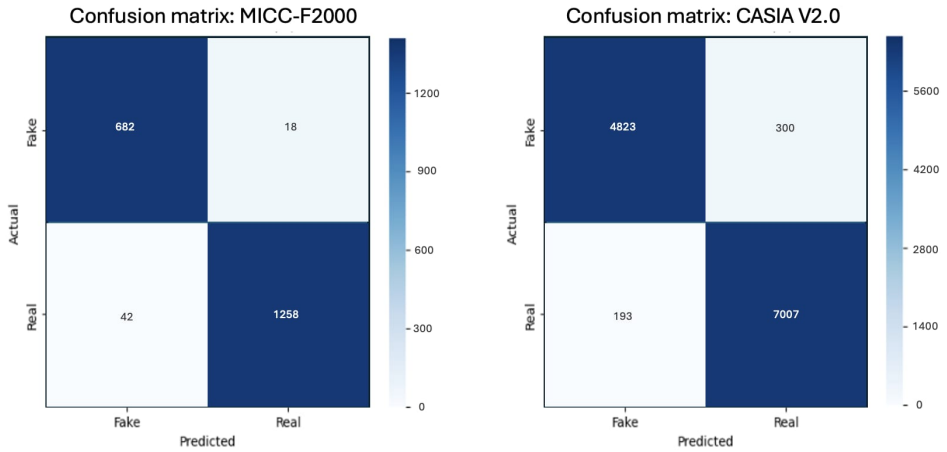

Figure 4. Confusion matrix of MICC-F2000 and CASIA-v2.

For the larger CASIA 2.0 dataset, our method predicted 300 FPs and 193 FNs among 12000+ images. These misclassifications (FNs) are attributed to some manipulated regions, particularly those with blended or overlapping tampered areas, with low contrast and massive noise. Similarly, the increase in FPs can be attributed to genuine images containing complex textures or lighting inconsistencies, which were mistakenly recognized as forged. Still, our method attained impressive results even under complex real-world conditions. This analysis demonstrates the robustness of our ReLU-EfficientNet method across datasets of varying complexity and CMF regions with a variety of post-processing attacks.

5.4 Comparative Analysis

A comprehensive comparative analysis was performed to assess the effectiveness of the proposed ReLU-EfficientNet method against several existing contemporary CMFD methods. The purpose of this evaluation was to determine the degree of improvement achieved by our method in terms of accuracy when applied to different datasets. The comparative study encompassed both classical handcrafted feature-based techniques and DL architectures, ensuring a balanced and fair assessment across model categories on two datasets.

Table 3. Performance comparison with SOTA approaches

Method	**Model Type**	**Dataset Used**	**Accuracy (%)**
(Vaishali and Neetu 2023)	ResNet-101	MICC-F2000	96.87
(Arivazhagan et al. 2024)	CNN-VGG16 Model	MICC-F2000	66.25
(Korsipati et al. 2025)	Optimized CNN heads	MICC-F2000	96.92
ReLU-EfficientNet (Proposed)	**End to end DL model**	**MICC-F2000**	**97.00**
(Joshi et al. 2022)	EfficientNetv2	CASIA v2.0	93.15
(Tankala et al. 2023)	ResNet-101	CASIA v2.0	77.00
(Dar et al. 2024)	GAN-CNN	CASIA v2.0	90.56%
ReLU-EfficientNet (Proposed)	**End to end DL model**	**CASIA v2.0**	**96.00**

As shown in Table 3, the CNN-based model (Arivazhagan et al. 2024) employed a VGG-16 backbone and achieved 66.25 % accuracy on MICC-F2000. This approach is sensitive to post-processing attacks, and lower results indicate a need for improvement. Vaishali and Neetu (2023) used the ResNet-101 DL model and achieved an improved accuracy of 96.87% over (Arivazhagan et al. 2024). Korsipati et al. (2025) used a lightweight CNN head improved by Focal Loss and SE-enhanced fused-MBConv layers using compound scaling and achieved 96.92% accuracy on the MICC-F2000 dataset, demonstrating the effectiveness of multi-level feature aggregation in improving CMFD. DL-based methods such as ResNet-101 (Tankala et al. 2023) and the CNN-based model (Dar et al. 2024) achieved 77% and 90.56% accuracy, respectively, on the CASIA v2.0 dataset, showing notable improvements in feature representation over handcrafted models. Similarly, the EfficientNet-v2 architecture (Joshi et al. 2022), evaluated on the CASIA v2.0 dataset, attained 93.15% accuracy, indicating moderate performance due to dataset complexity and class imbalance. In contrast, our ReLU-EfficientNet achieved 97% accuracy on MICC-F2000 and 96% on CASIA v2.0, outperforming all competing methods. This significant improvement demonstrates that integrating the ReLU activation function with the

EfficientNet compound scaling strategy enhances both discriminative learning and generalization across forgery under different post-processing attacks. The model's lightweight structure further ensures reduced computational overhead, making it highly suitable for real-time forensics applications.

5.5 Ablation study

To analyze the impact of different architectural design enhancements during the development of the proposed method, we conducted an ablation study to compare the performance of the baseline EfficientNet model with different configurations. More precisely, we compared the performance under three different settings: i) Baseline EfficientNet with Swish activation, ii) EfficientNet with ReLU activation, and iii) EfficientNet with ReLU and three additional dense layers with dropout. We performed this ablation study on both the MICC-F2000 and CASIA v2 datasets separately, and the results are shown in Table 4. The baseline EfficientNet method with Swish activation attained an accuracy of 77.99% on MICCC-F2000 and 78.25% on the CASIAv2. Next, we examined the performance of the enhanced model after replacing the Swish activation with ReLU. The objective of this experiment was to examine the effect of ReLU in terms of improving convergence and gradient flow over the swish activation in the EfficientNet model. The outcomes of this enhancement revealed an increase in accuracy from 77.99% to 83.12% on MICC-F2000 and from 78.25% to 82.56% on the CASIA v2 dataset. This experiment revealed the effectiveness of ReLU activation for improved feature sparsity, stability, and convergence over the Swish activation in the EfficientNet model. Finally, we investigated the effect of adding additional dense layers in our architecture for CMFD. For this purpose, we added three additional dense layers with dropout in our proposed ReLU-Efficient method and achieved significant performance improvement. Specifically, the accuracy further increased to 97% and 96% on the MICC-F2000 and CASIA v2 datasets, respectively. These findings demonstrate that integration of these additional dense layers in our method improves the feature learning capacity for improved generalization and robust CMFD performance of our model. Thus, the introduction of ReLU activation and additional dense layers with dropout in the baseline EfficientNet model presents a more potent solution to reliably spot copy-move forgeries.

Table 4. Ablation study.

Dataset	Architectural Enhancements	Accuracy (%)
MICC F2000	Baseline EfficientNet with Swish	77.99
	EfficientNet with ReLU	83.12
	ReLU-EfficientNet (ReLU+ 3 dense layers with dropout)	97.00
Casia V2	Baseline EfficientNet with Swish	78.25
	EfficientNet with ReLU	82.56
	ReLU-EfficientNet (ReLU+ 3 dense layers with dropout)	96.00

5.6 Discussion

The proposed ReLU-EfficientNet method demonstrated exceptional performance, achieving 97% accuracy on the MICC-F2000 dataset and 96% on the CASIA v2.0 dataset. These results highlight the model's strong capability in learning discriminative features that effectively distinguish between authentic and forged image regions. The integration of the ReLU activation significantly enhanced the stability of the network, enabling more efficient gradient flow and better learning of nonlinear relationships within image data. This improvement allowed the model to capture fine-grained forgery traits, such as duplicated textures, irregular boundaries, and subtle inconsistencies in pixel intensity patterns. Compared to existing DL architectures like VGG16, ResNet101, and EfficientNetv2, our ReLU-EfficientNet not only achieved higher classification accuracy but also computational efficiency. The reduced model size and shorter inference time make it particularly suitable for real-time forensic applications, where rapid and reliable analysis of digital evidence is critical. Furthermore, the compound scaling mechanism of EfficientNetB0, which jointly optimizes the model's depth, width, and resolution, contributed to a better balance between accuracy and efficiency. This design strategy allowed the model to utilize fewer trainable parameters while maintaining high representational capacity. As a result, the ReLU-EfficientNet achieved robust generalization across different datasets and forgery types, confirming its effectiveness and efficiency for CMFD.

6. Conclusion

This paper has presented a DL-based approach, ReLU-EfficientNet, for effective detection of CMF. Experimental evaluation on two diverse standard datasets with 97% accuracy demonstrates strong resilience against CMF on images under diverse post-processing attacks and forged regions with smaller size and complex patterns. The introduction of

ReLU activation in the EfficientNetB0 architecture ensures capturing complex spatial inconsistencies and subtle duplication artifacts without compromising computational performance. The optimized network design resulted in a compact and powerful model, capable of distinguishing forged regions from authentic content with high precision and minimal false detections. The proposed work can be extended to address more challenging forgery types, including GAN-generated and multi-modal image manipulations. Incorporating adversarial training and real-time learning mechanisms could further enhance the robustness and adaptability of forgery detectors under diverse manipulations.

References

Abbas M., Ansari M. , Asghar M. , Kanwal N. , Neill T. , Lee B. "Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks." 2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI), , pp. 125–30, 2021https://doi.org/10.1109/SAMI50585.2021.9378690.

Agarwal R., and Verma O. "Robust Copy-Move Forgery Detection Using Modified Superpixel Based FCM Clustering with Emperor Penguin Optimization and Block Feature Matching." Evolving Systems, vol. 13, pp. 1–15, 2022,https://doi.org/10.1007/s12530-021-09367-4.

Al-Azani S., and El Sayed A. "Using Word Embedding and Ensemble Learning for Highly Imbalanced Data Sentiment Analysis in Short Arabic Text." Procedia Computer Science, vol. 109, pp. 359–66, 2017,https://doi.org/10.1016/j.procs.2017.05.365.

Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security, 6(3), 1099–1110, 2011, https://doi.org/10.1109/TIFS.2011.2129512

Amiri E., Mosallanejad A. and Sheikhahmadi A., Copy-Move forgery detection using EOA, DWT and DCT. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, *30*(2), pp.222-227, 2024. https://doi.org/10.5505/pajes.2023.94395

Arivazhagan S, Russel NS, Saranyaa M. CNN-based approach for robust detection of copy-move forgery in images. Inteligencia Artificial. vol 27, no.73, pp. 80-91, 2024. https://journal.iberamia.org/index.php/intartif/article/view/1078

Bilal M., Habib A., Mehmood Z., Saba T., Rashid M. "Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering." Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 2975–92, 2020,https://doi.org/10.1007/s13369-019-04238-2.

Chang S. Can Deep Network Balance Copy-Move Forgery Detection and Distinguishment? 2023, https://arxiv.org/abs/2305.10247.

Chen H., Chang C., Shi Z., Lyu Y. "Hybrid Features and Semantic Reinforcement Network for Image Forgery Detection." Multimedia Systems, vol. 28, no. 2, pp. 363–74, 2022, https://doi.org/10.1007/s00530-021-00801-w.

Dar N.A., Atsya R. and Kumar A., November. Deep Learning-Based Approach for Detecting Copy-Move Forgery in Digital Images. In 2024 27th International Symposium on Wireless Personal Multimedia Communications (WPMC) (pp. 1-5). 2024,IEEE. https://doi.org/10.1109/WPMC63271.2024.10863322

Dell'Olmo P., Kuznetsov, O., Frontoni, E., Arnesano, M., Napoli, C. and Randieri, C., Dataset dependency in CNN-based copy-move forgery detection: A multi-dataset comparative analysis. *Machine Learning and Knowledge Extraction*, *7*(2), p.54, 2025. https://doi.org/10.3390/make7020054

Diwan A. and Roy A.K.,. Cnn-keypoint based two-stage hybrid approach for copy-move forgery detection. *IEEE Access*, *12*, pp.43809-43826, 2024. https://doi.org/10.1109/ACCESS.2024.3380460

Dong, J., Wang, W., & Tan, T., CASIA Image Tampering Detection Evaluation Database (Ver. 2.0) [Dataset]. In: 2013 IEEE China Summit and International Conference on Signal and Information Processing. https://doi.org/10.1109/ChinaSIP.2013.6625374.

Gani G., and Qadir F. "Copy Move Forgery Detection Using DCT, PatchMatch and Cellular Automata." Multimedia Tools and Applications, vol. 80, no. 21, pp. 32219–43, 2021, https://doi.org/10.1007/s11042-021-11174-7.

Hegazi A., Taha A., Selim M. "An Improved Copy-Move Forgery Detection Based on Density-Based Clustering and Guaranteed Outlier Removal." Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 9 pp. 1055–63, , 2021,https://doi.org/10.1016/j.jksuci.2019.07.007.

Jain E., and Kundra D. "EfficientNet-Based Deepfake Detection: A Robust Approach for Real and Fake Media Classification." Global Conference on Communications and Information Technologies (GCCIT), 2024, pp. 1–6, 2024 . https://doi.org/10.1109/GCCIT63234.2024.10862025.

Jaiswal A., and Srivastava R. "Detection of Copy-Move Forgery in Digital Image Using Multi-Scale, Multi-Stage Deep Learning Model." Neural Processing Letters, vol. 54, no. 1, pp. 75–100, 2022, https://doi.org/10.1007/s11063-021-10620-9.

Jiang L., Lu Z.., Gao Y. and Wang Y., Image Copy-Move Forgery Detection and Localization Scheme: How to Avoid Missed Detection and False Alarm. *arXiv preprint arXiv:2406.03271*. 2024. https://doi.org/10.48550/arXiv.2406.03271

Joshi R., Gupta A., Kanvinde N. and Ghonge, P., October. Forged image detection using SOTA image classification deep learning methods for image forensics with error level analysis. In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE. 2022.

Khalil A., Ghakwash A., Eksayed H., Salama G., Ghalwash H. "Enhancing Digital Image Forgery Detection Using Transfer Learning." IEEE Access, vol. 11, pp. 91583–94, 2023, https://doi.org/10.1109/ACCESS.2023.3307357.

Korsipati, J.R., Yanamala, R.M.R., Pallakonda, A., Raj, R.D.A. and Prakasha, K.K., Multi-resolution transfer learning for tampered image classification using SE-enhanced fused-MBConv and optimized CNN heads. Scientific Reports, 15(1), p.32717, 2025. https://doi.org/10.1038/s41598-025-17799-0

Kaur D. , Kalsi K. , and Pandey V.," A Copy-Move Forgery Detection System Using Deep Learning based CNN model and Approximation Wavelet Coefficient", Proceedings of the 2024 Ninth International Conference on Research in Intelligent Computing in Engineering, Vol. 42, pages 29–33, 2024. http://dx.doi.org/10.15439/2024R77

Kumar A. , Kumar V. , Kumar B. "Hybrid Dense Net Based Segmentation Framework for Automated Forgery Detection: Analyzing Copy-Move and Image Splicing Techniques", *International Journal of Intelligent Systems and Applications in Engineering*, 12(4), pp. 3313, 2024. https://www.ijisae.org/index.php/IJISAE/article/view/6831

Lyu Q., Luo J., Liu K., Yin X., Liu J., Lu W. "Copy Move Forgery Detection Based on Double Matching." Journal of Visual Communication and Image Representation, vol. 76, 2021, p. 103057,https://doi.org/10.1016/j.jvcir.2021.103057.

Mahdi M. and Ali N. , Copy Move Image Forgery Detection using Multi-Level Local Binary Pattern Algorithm. *Journal of Engineering*, *30*(06), pp.141-157, 2024. https://doi.org/10.31026/j.eng.2024.06.09

Meena K., and Tyagi V. "A Copy-Move Image Forgery Detection Technique Based on Tetrolet Transform." Journal of Information Security and Applications, vol. 52, p. 102481, 2020, https://doi.org/10.1016/j.jisa.2020.102481.

Nazir T., Nawaz M., Masood M., Javed A. "Copy Move Forgery Detection and Segmentation Using Improved Mask Region-Based Convolution Network (RCNN)." Applied Soft Computing, vol. 131, p. 109778, 2022, https://doi.org/10.1016/j.asoc.2022.109778.

Niu P., Wang C., Chen W., Yang H., Wang X. "Fast and Effective Keypoint-Based Image Copy-Move Forgery Detection Using Complex-Valued Moment Invariants." Journal of Visual Communication and Image Representation, vol. 77, 2021, p. 103068, https://doi.org/10.1016/j.jvcir.2021.103068.

Narasimhamurthy S., Mahadevachar V., Narasimhamurthy R. "A Copy-Move Image Forgery Detection Using Modified SURF Features and AKAZE Detector." International Journal of Intelligent Engineering & Systems 16, no. 4, 2023. https://doi.org/10.22266/ijies2023.0831.02

Oraby A., El-Sayed A. and Hamdan E.E., Deep Convolutional Networks For Copy-Move Image Forgery Detection. *Menoufia Journal of Electronic Engineering Research*, pp.37-48, 2025.https://doi.org/10.21608/MJEER.2025.344930.1101

Priyanka G., Singh, K."An Improved Block Based Copy-Move Forgery Detection Technique." Multimedia Tools and Applications, vol. 79, no. 19, , pp. 13011–35, 2020. https://doi.org/10.1007/s11042-019-08354-x.

Reyad M. , Sarhan A. , Arafa M. "A Modified Adam Algorithm for Deep Neural Network Optimization." Neural Computing and Applications, vol. 35, no. 23, 2023, pp. 17095–112, https://doi.org/10.1007/s00521-023-08568-z.

Ryu S., Lee H., Cho W., Kyu H. "Document Forgery Detection with SVM Classifier and Image Quality Measures." Advances in Multimedia Information Processing - PCM 2008, edited by Yueh-Min Ray Huang et al., Springer Berlin Heidelberg, pp. 486–95. 2008,

Singh S. and Kumar R. "Image Forgery Detection: Comprehensive Review of Digital Forensics Approaches." Journal of Computational Social Science, vol. 7, pp. 1–39, 2024,https://doi.org/10.1007/s42001-024-00265-8.

Tahaoglu G., Ulutas G., Ustubioglu B., Nabiyev V. "Improved Copy Move Forgery Detection Method via L*a*b* Color Space and Enhanced Localization Technique." Multimedia Tools and Applications, vol. 80, no. 15, 2021, pp. 23419–56, https://doi.org/10.1007/s11042-020-10241-9.

Tankala M. , and Rao, C. , Image counterfeiting detection and localization using deep learning algorithms. Revue d'Intelligence Artificielle, 37(1), p.191. 2023. https://doi.org/10.18280/ria.370124

Tinnathi S., and Sudhavani G."An Efficient Copy Move Forgery Detection Using Adaptive Watershed Segmentation with AGSO and Hybrid Feature Extraction." Journal of Visual Communication and Image Representation, vol. 74, 2021, p. 102966, https://doi.org/10.1016/j.jvcir.2020.102966.

Yu Z., Ni J., Zhang J., Deng H. and Lin Y., April. Reinforced Multi-teacher Knowledge Distillation for Efficient General Image Forgery Detection and Localization. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 39, No. 1, pp. 995-1003. 2025,https://doi.org/10.1609/aaai.v39i1.32085

Zabiya A., Madi F., and Abuzaraida M., *Detecting Copy-Move Forgery in Images Using Convolutional Neural Networks (CNNs).* "5th International Conference on Communication engineering and Computer Science (CIC-COCOS'24)", 24-25/04/2024, http://doi.org/10.24086/cocos2024/paper.1170

Zainal A., Kaur C., Saleh Al Ansari M., Borda R., Nageswaran A., El Aziz R. "Recognition of Copy Move Forgeries in Digital Images Using Hybrid Optimization and Convolutional Neural Network Algorithm." International Journal of Advanced Computer Science and Applications, vol. 13, p. 2022, 2022,https://doi.org/10.14569/IJACSA.2022.0131237.

Biographies

Fasiha Fatma earned her Bachelor of Science in Software Engineering in 2021 from the University of Engineering and Technology, Taxila. Her research interests are computer vision and machine learning.

Ali Javed (SM, 2016) received the B.Sc. degree with honors and 3rd position in Software Engineering from UET Taxila, Pakistan, in 2007. He received his MS and Ph.D. degrees in Computer Engineering from UET Taxila, Pakistan, in 2010 and 2016. He received the Chancellor's Gold Medal in the MS Computer Engineering degree. Dr. Javed is serving as an Associate Professor in the Software Engineering Department at UET Taxila, Pakistan. He served as a visiting academic in the James Watt School of Engineering, University of Glasgow, from May to August 2025. He has served as a Postdoctoral Scholar in the SMILES lab at Oakland University, MI, USA, in 2019, and as a visiting PhD scholar in the ISSF Lab at the University of Michigan, MI, USA in 2015. His areas of interest are Multimedia Forensics, Image Processing, Computer Vision, Video Content Analysis, Medical Image Processing, and Multimedia Signal Processing. He has published more than 150 papers in leading journals and conferences, including the IEEE Transactions. Dr. Javed is a recipient of various research grants from HEC Pakistan, National ICT R n D Fund, NESCOM, and UET Taxila, Pakistan. He has also served as an HOD in the Software Engineering Department at UET Taxila in 2014. Dr. Javed was selected as an Ambassador of the Asian Council of Science Editors from Pakistan in 2016. He is associated as a member with various professional bodies like IEEE, ACM, etc. He is also a professional member of the Pakistan Engineering Council.

Ahmad Alhabib earned his bachelor's degree in electrical engineering, with a concentration in power and energy, from Arizona State University in 2013. He completed a Master's in Electrical Engineering, with specialisation in Robotics, at Wayne State University in 2018. He is currently pursuing a Ph.D. in Electrical Engineering at Wayne State University. His research interests include solid-state electronics, smart sensors, robotics, and artificial intelligence applications.

Muteb Aljasem is an Assistant Professor at Bowling Green State University (BGSU), where he teaches courses in computer and electronic and robotics engineering. He earned his bachelor's degree from West Virginia University, a master's degree from the University of Michigan, and a Ph.D. from Wayne State University. His research interests centre on machine learning, computer vision, signal processing, and cybersecurity.

Muidh Awadh Algahtani is an Assistant Professor in the Department of Industrial Engineering, Faculty of Engineering, University of Tabuk, Tabuk. His research interests lie in the application of Machine Learning in different Industrial Applications.