Journal of Intelligent Systems and Internet of Things
Vol. 18, No. 02, PP. 99-110, 2026
DOI: https://doi.org/10.54216/JISIoT.180207

Exposing Image Tampering: A Deep Learning Approach to Copy-Move Forgery Detection for Secure Digital Image Forensics

Nadia Mahmood Ali[1], Sameer Abdulsttar Lafta[2], Amaal Ghazi Hamad Rafash[3,*]
[1]Middle Technical University, Institute of Medical Technology Al-Mansur; Baghdad, Iraq
[2]Middle Technical University, Technical Instructors Training Institute, Baghdad, Iraq
[3]Middle Technical University, Electrical Engineering Technical College, Baghdad, Iraq
Emails: nadiam@mtu.edu.iq; sameer.abdsattar@mtu.edu.iq; amaal.ghazi@mtu.edu.iq

Abstract

Nowadays, with the proliferation of mobile devices and the internet around the world that are available for everyone, and due to the low prices versus their high capabilities, images are considered one of the most common ways of transmitting information between users, advancement of image processing and editing tools, simplified the process of editing and changing photographs such as in magazines, newspapers, scientific journals, and on social media or on the Internet. As a result, the propagation of manipulated photographs that misrepresent the truth is prevalent, whether deliberate or inadvertent. We propose a method that uses deep learning based convolutional neural network in order to detect instances of the copy-move forgeries in images which can help to ensure data authenticity in digital forensic investigations. In this case, our method is intended to improve digital evidence integrity by detecting complicated changes quickly and precisely. This work can supports cybersecurity applications like anti-fraud systems, fake news detection, and social media forensics. The findings of the experiment demonstrate that the suggested approach is capable of detecting forgery against multiple copies and post-processing activities. The dataset's images used for both training and testing are MICC-F2000, composed of 2,000 images, 700 tamper and 1,300 originals. The findings indicate a testing accuracy of 98.00% and a training accuracy of 99.17%.

Received: March 18, 2025 Revised: June 06, 2025 Accepted: July 19, 2025

Keywords: Image forgery; Copy-move; Digital forensics; Deep learning; Convolutional neural network

1. Introduction

When compared to other media, digital images in general are easier for people to interpret. Pictorial information may be derived by the human visual system faster than any other sort of information may. Roughly, 75% of the information a visual system perceives is made up of this information [1]. While there are other varieties of digital picture fraud, copy-move is the most significant and oftenly used kind. It is challenging to identify and simple to use. The characteristics of the resulted image are found to match with that of the original image where the copied and pasted region comes from and the subsequent changes are made to the overall image. Thus, methods that employ well-known statistical measures to compare different areas of an image do not help to identify the copy-move type of tampering. Moreover, a variety of transformations may be applied to the manipulated image to increase its realism. These days, hundreds of digital photos are handled every day by several applications, including courtrooms, social media platforms, newspapers, and journals. The media is rich in such photos, it has become very easy to produce these pictures with the help of digital image processing

tools, and great editing skills, however, these works are almost impossible to erase completely. Sometimes it can be quite challenging to determine with the naked eye whether a digital image is fabricated or not. Verifying the legitimacy and dependability of the photos has become crucial since the goal of this manipulation is frequently to purposefully divert the recipient's attention [2]. In digital forensics, where precision and effectiveness are crucial, as well as in communication systems, the use of intelligent procedures is crucial. Similar to how we utilize CNNs to identify tampering in digital photos, intelligent techniques can greatly improve system performance and decision-making [3].

Images are typically seen as a more effective medium for human communication than words. Pictorial information can be extracted by the human visual system more quickly than any other kind of information. [3]. Although there are many other kinds of forgery images, copy-move forgery (CMF), often known as cloning, represents the most prevalent type since it is simple to use and difficult to detect. This kind of forger duplicates a portion of a picture and pastes it once more. The duplicated areas can have any size or form, and they can combine many kinds and be rotated, translated, and scaled. Compared to other types of forgeries, this one is harder to detect since standard techniques to find incompatibilities that compare several picture segments using statistical measures do not work for CMF detection. [4]. Especially, if the counterfeit image goes through further image enhancement procedures including image blurring, color quantization, and Gaussian noise injection. The degree of optimization achievable through the manipulation of the image makes it difficult to identify forged images [5].

The authenticity of digital images plays a crucial role in various fields such as journalism, law enforcement, scientific publishing, and social media. However, the widespread availability of advanced image editing tools has made it increasingly easy to manipulate photographs, often with the intent to mislead viewers or falsify digital evidence. One of the most common and deceptive forms of manipulation is copy-move forgery, where a portion of an image is duplicated and pasted elsewhere within the same image to hide or replicate objects.

The challenge with copy-move forgery lies in its subtlety. Since the duplicated regions originate from the same image, they typically share the same characteristics such as color, texture, and noise patterns, making manual detection or traditional automated methods unreliable — especially when tampered regions undergo additional transformations like rotation, scaling, or noise injection to mask the forgery further.

Although several detection techniques have been developed, many of these either require heavy computational resources or fail to maintain high accuracy when faced with real-world post-processing manipulations. Moreover, approaches that employ deep learning often prioritize complex model architectures, which, while powerful, may limit their usability in practical forensic scenarios where computational efficiency is equally critical.

This study addresses these challenges by proposing a solution that combines convolutional neural networks (CNN) with Error Level Analysis (ELA) preprocessing, aiming to enhance detection robustness while maintaining computational simplicity. The primary problem this research seeks to solve is the lack of accurate, efficient, and resilient methods for detecting copy-move forgery under common image manipulations, which is essential for ensuring the integrity and credibility of digital images in security-sensitive contexts.

Despite the increasing attention given to image forgery detection, particularly copy-move forgeries, many of the existing methods still fall short when facing real-world challenges. Current approaches often struggle to accurately identify tampered regions when the forged images undergo common post-processing operations such as rotation, scaling, brightness adjustments, or noise addition — manipulations that are frequently used to disguise forgery traces. Additionally, many models depend on deep and computationally intensive architectures or traditional feature-based matching techniques that limit their practicality in large-scale or time-sensitive forensic investigations.

While convolutional neural networks (CNNs) have significantly advanced image analysis tasks, their application to copy-move forgery detection still faces gaps, particularly in integrating effective preprocessing techniques that could enhance performance without increasing complexity. One such underutilized technique is Error Level Analysis (ELA), which can reveal inconsistencies in image compression — a valuable clue for forgery detection. However, ELA remains largely disconnected from many modern deep learning models, leaving room for innovation in combining these tools for a more effective solution. Given these limitations, there remains a clear need for a detection framework that is not only accurate and resilient against post-processing manipulations but also computationally efficient and accessible for practical forensic use. To address these challenges, this paper introduces a focused and efficient deep learning-based approach for copy-move forgery detection, with the following key contributions:

1 Development of a CNN-based framework integrated with Error Level Analysis (ELA): We introduce a method that combines CNN's feature extraction power with ELA's capability to highlight compression anomalies, improving detection accuracy while reducing model complexity.

2 Design of a lightweight CNN architecture: Our model employs four convolutional layers, one max-pooling layer, and a fully connected layer, optimized to achieve high performance (98% detection accuracy) with lower computational overhead compared to deeper models.

3 Robustness against real-world forgery scenarios: The proposed method demonstrates strong resilience against various post-processing operations, including rotation, scaling, noise injection, and brightness modification — conditions under which many conventional approaches often fail.

4 Comprehensive experimental validation: We conduct rigorous testing on benchmark datasets (MICC-F2000 and CoMoFoD), confirming the model's effectiveness and superiority over several existing methods.

5 Contribution to digital forensics and cybersecurity: This work supports forensic investigations and cybersecurity efforts by providing a practical and reliable tool for verifying the authenticity of digital images and preventing the spread of manipulated visual content.

2. Related Works

Recently, many schemes have been proposed for detecting copy-move forgery. According to Kuznetsov [6] proposed a method which applies VGG-16 convolutional neural network for the detection of the forgeries to digital images. The network design uses an image patch as an input in order to get the classification outcomes. Their fine-tuned model had a classification accuracy of 97.80% while the model trained at zero stage had accuracy of 96. 4%. Also, Mallick, Devjani, *etal*. [7] proposed a technique with the use of the Convolutional Neural Networks (CNN) for detecting the picture fraud such as copy and move. The proposed method takes advantage of the CNN technique to obtain features from two databases of varying complexity of CASIA v2. 0 and NC 2016. Hence, experimental results suggest that the performance of the classification declines with increasing complexity of the data. Another study by Thakur, Rahul, and Rajesh [8] proposed and developed a method of detection splicing and CMFD image forgery the design focuses upon the detection of the traces that are left by various post-processing operations for splicing and copying, such as blurring, PEG compression, adjusting contrast, and adding noise. The proposed approach achieves an accuracy of 95.97% on CoMoFoD and 94.26% on BOSSBase.

Furthermore, Abidin, Arfa Binti, et al. [9] provide an in-depth analysis and thorough literature evaluation of cutting-edge deep learning techniques for identifying false copy-move images. In addition, Rao, Yuan, and Jiangqun [10] used convolutional neural network (CNN) to build a new hierarchical structures from the RGB color images by themselves in order to explain a new method for image fraud detection using deep learning techniques. Meanwhile, Kim, Dong-Hyun, and Hae-Yeoun Lee. [11] proposed A neural network has been effectively prepared to utilize the mistake-level examination with 4000 fake and 4000 genuine image neural systems that could perceive the picture as forgery or genuine at a most extreme achievement rate of 83%. A new method by Shifting focus to a deep learning model, Zhu, Ye, and colleagues [12] proposed an end-to-end neural network called the adaptive attention and residual refinement network (AR Net). The adaptive attention technique discusses the idea of zone and channel attention characteristics for the improvement of the gathering of contextual input and representation of information. In addition, the spatial pyramid pooling technique of Arrows is used to combine scaled correlation maps, which will give the rough mask. Besides, deep matching is employed for computing the auto-correlation within the feature maps. Lastly, a rough mask is improved by residual refinements module to ensure that object boundaries are not distorted. Preliminary results show that AR-Net outperforms state of the art approaches and accomplishes the goal of accurately detecting tampered regions the experiments have been executed on the Asia, Coverage, and Co-Mo FoD datasets.

Another study by AlShariah, M., Khader, & Saudagar [13] suggested models for Instagram images to help detect manipulated images and identify attacks on them. The system was developed with deep learning algorithms, which are CNN, AlexNet, and AlexNet. The results show that, with 97% of the other approaches, the proposal (Alex Net) detects fake pictures with greater efficacy. In addition, While Mahmood et al. [14] presented an extensive survey on different approach of forgery, forged data sets, and approaches for forgery detection. At image level, the authors looked at block-based and key-point based algorithms and at the pixel level, the deep learning algorithms. Findings have shown that block based approaches have high time and computational space complexity and still give poor results with geometric functions. Moreover, Li, J., Zhang, H., & Wang, L. [15] proposed SPA-Net, a deep learning-based model for copy-move forgery

detection that integrates a span-partial structure and an attention mechanism. The model enhances detection accuracy by focusing on forged regions while minimizing the influence of irrelevant background areas. However, while effective; SPA-Net's attention-based complexity may introduce computational overhead, which can limit its suitability for real-time forensic applications or resource-constrained environments. This emphasizes the need for simpler architectures that can maintain high accuracy without excessive computational demands.

3. Proposed Methodology

3.1 Detection of Copy-Move Forgeries

The detection of copy-move forgeries (CMFD) can be done in many different ways. However, the majority of the previously used techniques take a lot of time and are not resistant to post-processing assaults or transformations that are more complicated. The technique of deep learning has piqued the interest of researchers throughout the field, which has yielded promising findings in its application. As a result, forensic researchers aim to use deep learning techniques to identify forgeries in images.

The architecture of the system has been illustrated in Fig. 1. It is divided into two main sections: constructing a CNN model and preprocessing.

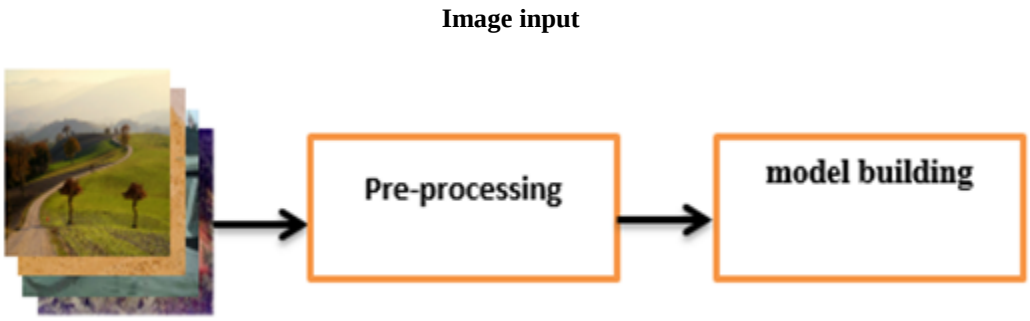

Figure 1. The proposed method

3.2 (Pre-process)

The four techniques that have been described in this section can be broken down into the following; Error-Level Analysis (ELA), Image Differences, Normalizations and Enhancement. This region is illustrated in the figure 2 below.

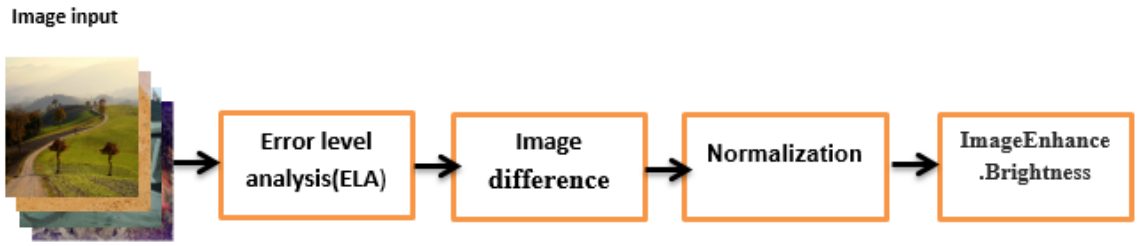

Figure 2. Steps of pre-processing

(Error_Level_Analysis (ELA)). Is a method for improving the CNN model's training efficacy by recognizing regions of an image with varying compression rates.

Image Difference. The differences between each of the pixels that makes up the original images or picture and the compacted picture in relation to pixels.

Normalizing images. Before use picture data for developing image classification modeling, it will be prepared. Normalizing the pixel intensities or values are good prerequisite steps to be performed on images inclusive of the range transformation where the intensities are scaled to a range of 0 and 1. As it is well understood that pixel values are inherently scaled between 0 and 255, normalization is already the primary strategy. This makes the implementation process quite easygoing and not very complex. It helps to speed up the learning rate of 'CNN' and makes it to soon approach the minimum of loss values in the validation data.

Image Enhance. When the brightness is greater than 1, the image will become brighter. When the brightness is less than 1, the image will become dark and then must be enhanced. Controlling an image's brightness, the factor of enhancement (0.0) produces a black image, and the factor of 1.0 produces the original image.

3.3 Model building

CNN model

A convolutional neural network (ConvNet or CNN) is a deep learning network design that is learned from input data. CNN has numerous layers that are convolutional and pooling. There is then one, or more layers that are totally joined after this stage as indicated below. CNN is helpful in obtaining features in the picture classification. In the case of Neural, network features can be defined as the traits or qualities of the data under consideration. Feature extraction represents one of the essential tasks in automated systems based on the use of machine learning procedures. The purpose of this action is to gain the favorable and valuable features and attributes. For the data. The suggested CNN consists of feature learning, four convolutional layers, one max-pooling layer, then a fully connected layer and Softmax for classification. Fig. 3 illustrates the architecture of the (C, N, N) convolutional neural network.

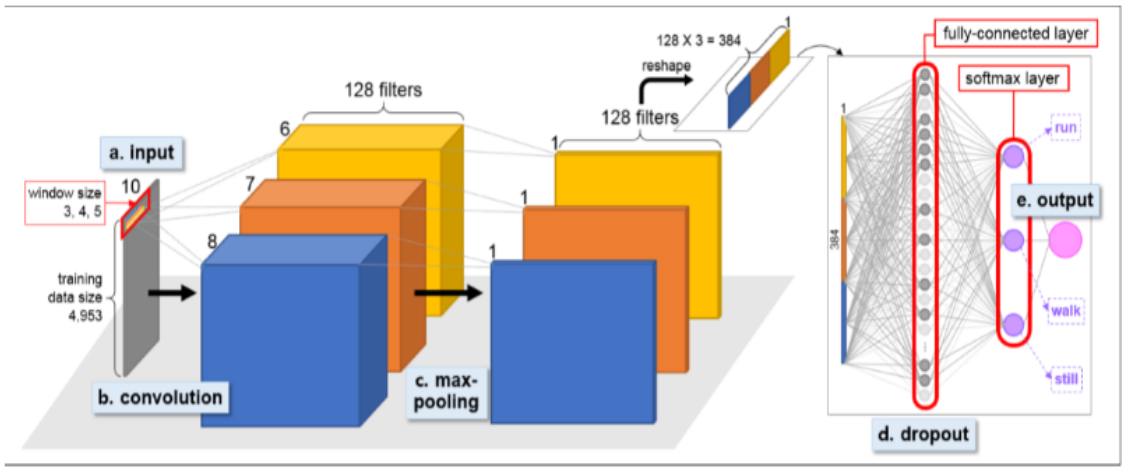

Figure 3. CNN Architecture

The convolution layer: The layer of convolution is responsible for the extraction of features from images. The resized 128x128x3 image serves as the first convolution layer's input. The first and second convolution layers, and 2 others two convolutions layers on the other hand, use 32 kernel filters using a 5x5 size matrix and strides of 1 or 2 pixels to move over every pixel in the image and calculate their dot product. The filter and convolution operations are displayed in Fig. 4.

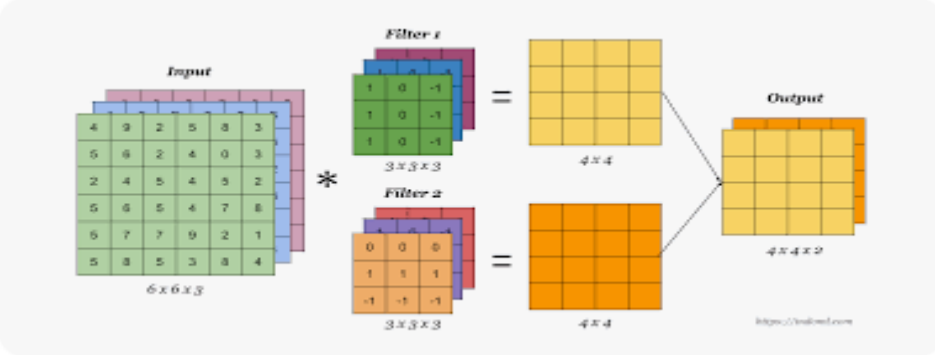

Figure 4. Conventional operation and Conventional Function.

(Activation Function AF): In the (neural network), the activation function eliminates unnecessary pixels, like a negative value. The Rectified Linear Unit (ReLU) is an activation function that is nonlinear and defined as the positive part of its argument. (Fig6) shows the ReLU.

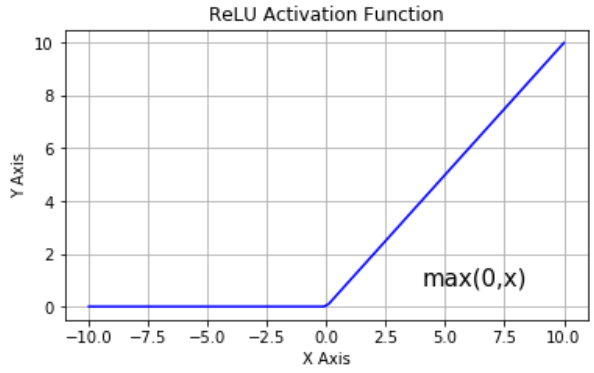

Figure 5. Rectified Linear Unit (ReLU)

The Max Pooling layer: Reducing the number of pixels in the output of preceding convolutional layer is the goal of the pooling layer that follows. The second step for the spatial dimensions is used to perform the max-pooling layer employing (2 x 2) dimension kernels. The scale has been reduced to one fourth of the original size. Further in an attempt to reduce the risk of overfitting, a dropout of 0. 25 is applied to the layer. In figure 6 below shows how Max pooling is done on the 4x4 photos.

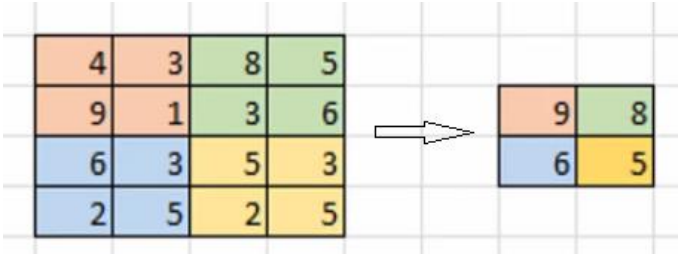

Figure 6. Max-Pooling operations

This leads to achieving a new flattened layer that contains only one column of feature results. The flat column perceptron was created to go through a fully connected layer comprising of 256 neurons in order to classify and predict images. Therefore, with an aim of reducing overfitting, a dropout rate of 0. 5 will be implemented after the carry out a completely linked layer. The best way to understand the holistic conceptualization of the layers is by viewing Figure 8, which presents the connectivity of all the layers.

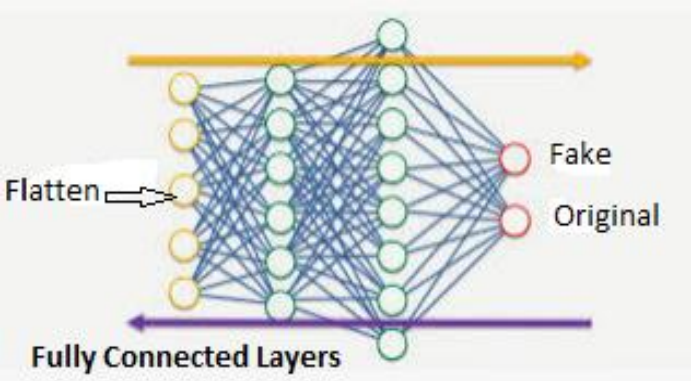

Figure 7. fully connected layer

Soft Max function: In models of neural networks that predict the multinomial distribution of probabilities, softmax function is utilised for an activation function in its output layers. The probability value ranges from zero to one.

The (RMSProp) optimizer: one of the adaptive rate learning techniques is used in training.

Just fiew layers of convolution are required since the conversion procedure outputs into an ELA picture might highlight significant elements for determining whether an image is genuine or has been manipulated.

4. Implementation

4.1 Dataset

The MICC (Media Integration and Communication Center), (MICCF220, MICC-F8 Multi, MICC F600) and CoMoFoD (Copy-Move Forgery Detection) data sets were used to evaluate the proposed algorithm. Table1 shows MICC data-set [16]

Table 1: Lists details of the M I C C-F 220, M I C C-F 2 000, M I C C-F600, and M I C C-F6 datasets

Datasets	Distribution
M I C C – F 220.	This collection includes 220 images, 110 of which are tampering and 110 of which are the originals
M I C C-F 2000	This collection includes 2000 images; 700 of which are tampering and 1300 of which are the originals
M I C C- F 8 multi	Eight manipulated photos with realistic multi-copies
M I C C –F 600	This collection includes f 440 original images, 160 of which are tampering and 160 of which represent ground truth images

Fig 8 illustrates some examples of tampered images of the MICC.

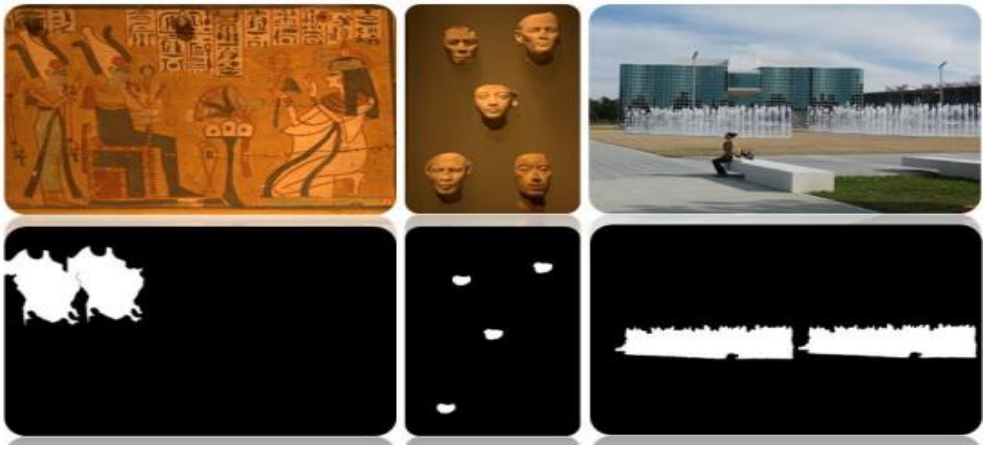

Figure 8. Some examples of tampered images of MICC. Images in the top row are forged and at the bottom are masks to show the place of tampering

These fake images are generated by randomly copying and pasting parts of a genuine photo. Fake photographs have undergone a variety of transformations, including rotation, translation, scaling, and combinations of these. These datasets are made up of variously sized, segmented photos. Between the pictures formats JPEG and PNG.

(Co M o F o D) is the dataset of Copy-Move forgery detection comprised of 200 forged images illustrating different forgery types. Each falsified photo has a mask on it indicating the manipulation location along with the genuine photo. Some examples of the altered images of (C o M o F o) [16] are depicted in Figure 9.

Figure 9. Examples of the altered images of CoMoFoD. The top photos are tempered, while the bottom photos are masks to show the place of tampering

The photographs collected are further divided according to the number of distortions used and whether these distortions are rotations and/or translations, scaling, or a combination of all. In addition, many post-processing strategies (e.g. Brightness change, image blur, noise adding) are applied. This dataset consists of images that have 512 × 512 sizes, divided between JPEG and PNG image formats. [16]

5. Experiment and Analysis

The Python programming language was used for implementing the suggested method. The dataset MICC-F2000 was used for analysis and testing. That composed of 2000 images; 700 tamper and 1300 originals

The data-set has been divided to 80% for training and 20% for testing

The suggested method's performance is measured by applying several performance measures such as the F-score, precision, accuracy, sensitivity, and recall. An overall estimate of the model's correctness can be obtained by the accuracy. In the case of actors, positivity means the evaluation of how well the predictions are made. Sensitivity defines the capacity of predicting actual value of picture. In addition, F-score is measure of how accurate the value of an image's actual category is. Recall is also known as sensitivity and it quantifies the likelihood that a certain image will be correctly classified bearing in mind that it has the right class value In contrast, precision quantifies the likelihood that a given image will be correctly classified for its actual value.

The results of the differences between the F-score, precision and the recall of performance accuracy using evaluation data from both trained and untrained datasets are presented in Table 2.

Table 2: Shows the test of the F-score, Precision, and Recall of Performance Accuracy results in the case of testing data from both within and outside of training data

Performance outcomes for data-testing	**Accuracy**	**Precision**	**Recall**	**F-score**
Without training	94%	89%	100%	93.3%
Trained	98%	95%	100%	96.9%

The precision, recall, Acre, F score and sensitivity are computed from confusion matrix generated by classifier model. It is also used for computing classifier evaluation for True negative and True positive among other computations. It means that the CNN networking can also give false negative and false positive results. The confusion matrix has been depicted in the table below in form of a table 3.

Table 3: Confusion matrix for MMIC F2000

N=100	Actual Normal	Actual Fake
Predicted Normal	TP 50	FP 3
Predicted Fake	FN 0	TN 47

5.2 Performance Analysis

The results obtained from the proposed method have maximum training accuracy is 99.17% and 98% validation accuracy using (30 thirty) epochs. Fig10 illustrates an accuracy curve and loss curve.

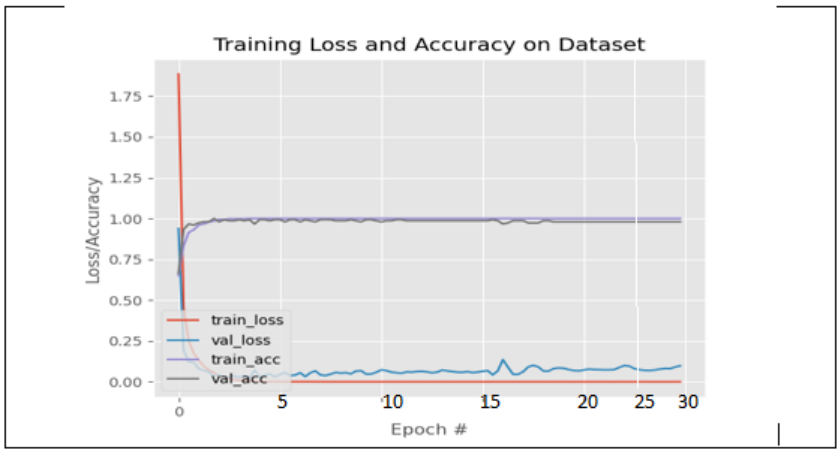

Figure 10. Different evaluation parameters of the model.

The figure above clearly demonstrates that epoch 5 has the best accuracy and precision of the five. Similar to the fourth period, the fifth period's completion results in the stabilization of validation losses. Thus, early stopping is a powerful approach to determining when to stop the training process in case of the decreasing of the validation accuracy or increasing of the validation loss. With the help of such translation of the picture using ELA, the process of training models becomes much faster, hence requiring fewer training epochs to provide a good convergence. In addition, by normalizing the RGB values of each pixel, the CNN model achieves a high convergence rate, leading to high classification accuracy. This proves that the picture is an ELA (Error Level Analysis) image, which is so useful when one wants to find out whether it is an original picture or else it has been manipulated. Comparing our findings to others, firstly comparing it to [7], our work shows more accuracey and sensitivity. This resulted from using CNN that employs two layers of convoluted, one Max-pooling layer is one fully connected layer and one softmax output layer. This lowers the training process's computing expenses, resulting in decreasing the required number of epochs and layers. Comparing our work to the CNNs used by [8] which used Laplacian filtering residual (LFR) and the median filter (SDMFR), since both are residuals filters that require a large number of layers, the training procedure has very high computing costs. Our model, training accuracy has been 99.17% and testing accuracy has been 98.0 while [8] achieved an accuracy of 95.97%.

6. Conclusion

An interesting area of study within forensic science is the investigation of the efficacy of techniques for identifying fake photographs. Another important developmental issue in digital photo forensics is the presence of a specific type of photo manipulation, called copy-move forging. The majority of the algorithms used for copy-move forging detection take a lot of time to compute. This paper presents a successful method for the detection of copy-move frauds, utilizing deep learning strategies such as convolutional neural networks (CNN) in conjunction with error level analyses (ELA). CNN utilizes the following structures: four convolutional layers, one Max pool layer, one fully connected layer, and one softmax output layer. Within 30 epochs, this model can achieve a 99.17% training accuracy and a validation accuracy of 98%. Implementing ELA can enhance productivity and reduce computational costs of training. The reduction in the number of layers and epochs required compared to the previous method demonstrates this. Our model offers the following advantages: The ELA's picture characteristics approach enhances training effectiveness and accelerates CNN model convergence, significantly reducing the total number of training cycles required to obtain convergence. Experiments and analysis have shown that this algorithm can handle multiple copies, is easier to compute, works well with common post-processing operations, and can quickly and accurately find forged areas even after more complex changes like scaling or rotation have been made. Therefore, this research makes a substantial contribution to the field of digital photo forensics. For future works, it’s recommended to the proposed CNN-based approach shows robustness against common transformations like scaling and rotation, more complex post-processing techniques (e.g., geometric warping, in painting, adversarial noise) could challenge the model’s effectiveness. In addition, a promising future direction is extending the methodology to video forensics or multi-modal forgery detection, where both images and metadata (like timestamps or EXIF data) are analyzed together for better forgery detection.

Author Contributions

N.M.A.: Conceptualization, Methodology, Investigation, Writing—original draft.

S.A.L.: Project administration, Conceptualization.

A.G.H.R.: Investigation, Resources, Writing—review and editing..

All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Ethics Statement

The datasets utilized in this study, including MICC-F2000 and CoMoFoD, are publicly available and widely used for academic research in the field of image forgery detection. No personal, sensitive, or confidential data were involved in this research. Ethical approval was not required, as the study does not involve human participants, animals, or any form of personal data collection.

References

[1] M. Sivakumar, P. Roy, K. Harmsen, and S. Saha, "Satellite remote sensing and GIS applications in agricultural meteorology," in *Proc. Training Workshop Dehradun, India*, AGM-8, WMO/TD, 2004.

[2] M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2499–2512, 2016.

[3] M. V. K. Sivakumar, P. S. Roy, K. Harmsen, and S. K. Saha, "Satellite remote sensing and GIS applications in agricultural meteorology," in *Proc. Training Workshop Dehradun, India*, AGM-8, WMO/TD, vol. 1182, 2004.

[4] S. Walia and K. Kumar, "Digital image forgery detection: systematic scrutiny," *Aust. J. Forensic Sci.*, vol. 51, pp. 1–39, 2018.

[5] B. Shivakumar and S. S. Baboo, "Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors," *Int. J. Comput. Appl.*, vol. 27, no. 3, pp. 9–17, 2011.

[6] A. Kuznetsov, "Digital image forgery detection using deep learning approach," in *J. Phys.: Conf. Ser.*, vol. 1368, no. 3, p. 032028, Nov. 2019.

[7] D. Mallick et al., "Copy move and splicing image forgery detection using CNN," in *ITM Web Conf.*, vol. 44, 2022.

[8] R. Thakur and R. Rohilla, "Copy-move forgery detection using residuals and convolutional neural network framework: a novel approach," in *2019 2nd Int. Conf. Power Energy, Environ. Intell. Control (PEEIC)*, 2019.

[9] A. B. Z. Abidin et al., "Copy-move image forgery detection using deep learning methods: a review," in *2019 6th Int. Conf. Res. Innovation Inf. Syst. (ICRIIS)*, 2019.

[10] [Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE Int. Workshop Inf. Forensics Security (WIFS)*, 2016.

[11] D.-H. Kim and H.-Y. Lee, "Image manipulation detection using convolutional neural network," *Int. J. Appl. Eng. Res.*, vol. 12, no. 21, pp. 11640-11646, 2017.

[12] Y. Zhu et al., "AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6714-6723, 2020.

[13] N. M. AlShariah, A. Khader, and J. Saudagar, "Detecting fake images on social media using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 170-176, 2019.

[14] I. Amerini, L. Ballan, R. Caldelli, A. Bimbo, and G. Serra, "A sift-based forensic method for copy-move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[15] J. Li, H. Zhang, and L. Wang, "SPA-Net: A deep learning approach enhanced using a span-partial structure and attention mechanism for copy-move forgery detection," *Sensors*, vol. 23, no. 14, p. 6430, 2023, doi: 10.3390/s23146430.

[16] T. Mahmood et al., "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *J. Vis. Commun. Image Represent*, vol. 53, pp. 202-214, 2018.

[17] R. M. Yas and S. H. Hashem, "Intelligent approaches for enhancing networked routing protocol," *Iraqi J. Sci.*, vol. 62, no. 11, pp. 4121–4147, 2021, doi: 10.24996/ijs.2021.62.11.32.