Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

IMAGE FORGERY DETECTION USING DEEP CONVOLUTIONAL NEURAL NETWORKS

[1]Nusratullah Tauheed*, [2]Shahan Yamin Siddiqui, [3]Abdullah Dar, [4]Shahzada Atif Naveed, [5]Muhammad Farrukh Khan, and [6]Usama Ahmad Mughal

[1]*Department of Computer Science, University of South Asia, Lahore, Pakistan.*
[2]*Department of Computer Science, NASTP Institute of Information Technology, Lahore, Pakistan.*
[3]*Department of Computer Science, Minhaj University Lahore, Lahore, Pakistan.*
[4]*Department of Computer Science, Rashid Latif Khan University, Lahore, Pakistan.*
[5]*Department of Artificial Intelligence, NASTP Institute of Information Technology, Lahore, Pakistan.*
[6]*Department of Cyber Security, NASTP Institute of Information Technology, Lahore, Pakistan.*
fabihaansar000@gmail.com , amnah@gscwu.edu.pk , shabbarkhan12@gmail.com., manahil.khan7512@gmail.com, muniba@gscwu.edu.pk

DOI: https://doi.org/10.5281/zenodo.20775482

Keywords
Image Forgery Detection; Deep Convolutional Neural Network; Digital Image Forensics; Double Image Compression; Recompressed Images; Deep Learning; Image Authentication.

Article History
Received on 20 May 2026
Accepted on 06 June 2026
Published on 20 June 2026

Copyright @Author

Corresponding Author: *
Nusratullah Tauhee*

Abstract

The advent of easily available and simple digital image manipulations has raised issues regarding the validity of the image. Conventional techniques that rely on the hand-crafted feature fail in identifying only certain types of alterations. They also fail to work in practical situations. The current research deals with the issue of developing forgery detection systems based on the analysis of artifacts produced during recompression of images using deep learning. The proposed model, after training with real images and fake images, can detect even minute variations due to double compression and manipulation of images. The pre-processing pipeline was designed completely for improving the quality of images and generating robust features. We evaluated the model with reconjugated real and fake images based on various parameters like accuracy, sensitivity, specificity, and miss rate. The proposed framework attained a training accuracy of 97.38% and validation accuracy of 94.42%, which implies good generalization capability and detection of forgeries. In comparison to other image forgery techniques, the performance of our proposed DCNN framework was found to be quite satisfactory.

INTRODUCTION

In today's world, digital images have replaced newspapers and face-to-face interactions as means to acquire and disseminate information. Digital images have found application in different fields, such as journalism, science, court systems, medicine, social media, commerce, and other areas. Since digital images play an important role in the way people think and make decisions, they can be considered

credible when making decisions and providing information. In recent times, due to technological advancement and increased usability of tools for image manipulation, more people have started manipulating their images [1-2].

Digital image fabrication refers to the process where there is intentional modification of the image in order to misrepresent the situation by deletion or addition of any object, altering the context, and even manufacturing evidence. With current technology, it is now possible to modify images to a high degree that the modifications cannot easily be detected [3-4].

The detection of digital image forgery is a core part of digital forensics. The techniques include active and passive approaches. In active detection, information like watermarks or signatures is embedded in the images prior to their release. This is a reliable technique, though it cannot be used with public images [5-6]. The identification of passive manipulation involves using different tools, such as copy-move, image splicing, retouching, resampling, format, camera, and geometric forgery detection techniques. Copy move involves copying and moving a part of the same picture to disguise or duplicate information. Image splicing entails combining different pictures to form one manipulated image [7]. The technique of retouching changes the physical characteristics of brightness, contrast, color and texture of an object. The manipulations are difficult to detect as the modern editing tools create realistic images [8].

The improvements in the field of image forensics are due to improvements in the field of ML and DL. The DL-based models learn the hierarchical representation of features in an automatic fashion from the raw images without using any handcrafted features. The CNN-based models are excellent for classification, recognition, and forensic segmentation of the images [9, 10].

Digital forensics researchers have concentrated their efforts on the phenomenon of artifacts from image recompression. Image manipulation leads to alterations of statistical properties in those areas that are manipulated due to recompression cycles. As a result, double counting may lead to minor artifacts that can be detected through computer analysis [11]. Although such artifacts do not

provide any new information, they can be employed for image authentication purposes [12].

However, despite all progress made, CNN-based detectors for image forgery detection face some challenges and limitations in real-world applications. Many approaches are specialized for detecting specific manipulations (for example, copy-move forgery), but can be ineffective after post-processing or complex retouching. Thus, new generalized approaches for forgery detection are required with development of editing technology [13].

To deal with these limitations, a framework for the detection of image forgery based on a deep convolutional neural network (CNN) is proposed in this paper. Using the idea of using recompression artifacts, this framework will be able to differentiate between genuine and forged digitized images by learning their relationship and extracting features from both the original and recompressed images.

Contributions of this study include:

- Digital image forgery detection using Deep Convolutional Neural Networks.
- Double compression artifact as the forensic proof of digital image manipulation.

Feature extraction using deep learning for forgery identification.

Image forgery detection without requiring any reference images.

Performance evaluation on image forgery metrics.

Proving the superior performance of this technique compared to other methods.

Related Work

With the development of sophisticated software to manipulate digital images, much attention is being paid to the area of digital image forgery detection. The first techniques used to detect any alterations in an image such as copy move, splicing, or retouching were based on hand-crafted features extracted from pixels of the image, frequency domain or geometric analysis. Traditional techniques have shown good performance but highly rely on feature engineering skills [14-15].

Techniques based on the domain used in forgery detection have been studied. In a study by Shankar et al., the correlation algorithm is combined with the DCT and DWT to provide a framework for image forgery identification in order to pinpoint the areas that are altered in the image. In order to detect these manipulated sections, they divide the compressed image into

overlapping blocks and then correlate them [16].

Frequency-based descriptors and ML classifiers have been utilized by researchers in recent times. For instance, Asghar et al. utilized FFT and DRLBP to obtain features of noises and utilized SVM for classification of images into real and manipulated categories. The approach had the same level of performance compared to other approaches but was restricted due to manually designed descriptors and selected features [17].

In terms of deep learning, there has been a paradigm shift towards data-driven characteristics for the identification of image forgeries. The primary approach is based on convolutional neural networks, which automatically extract hierarchical representations of the input images. Koul et al. proposed an image forgeries detection scheme using a CNN which achieves better results than the conventional algorithms. However, their model is limited to copy-move forgery detection [18].

In order to increase detection rate for manipulation, most of the deep learning methods combine several neural networks together. In the method suggested by Chen et al., an encoder-decoder structure that utilizes LSTMs was used to detect the manipulation of images through the learning of high-level semantic features, as well as the fusion of these features through the encoder-decoder structure. Training time and cost were higher compared to other methods due to feature fusion and serial processing [19].

Image forensics has exploited generative models and hybrid deep learning, such as the fusion model by Krishnaraj et al., which merges DenseNet and GAN to detect copy-move forgery. The model has adopted multiple representations to enhance the efficacy of detectors, resulting in an 86.27% success rate in detecting copying-and-moving forgery. Nevertheless, the model's complicated design makes it computationally expensive [20].

Image compression distortion has been found by recent studies to be useful in forensic identification. Double JPEG compression and re-compression results in statistical distortions that serve as evidence of tampering. Research focuses on quantization errors, block distortion, and frequency domain distortions due to previous levels of compression [21-22].

However, there are some shortcomings of digital forensics. First of all, traditional techniques based on features have problems with generalization and require much handcrafted feature extraction. Second, most of the models that employ deep learning techniques address only one kind of forgery like Copy Move or Image Splicing, which limits their applicability for forensics in general. Moreover, currently, deep learning models do not take into account the effects of image recompression when addressing classification of altered images that were subjected to additional compression after alteration. Hence, there is a need for a generalized deep-learning model and automatic extraction of features based on recompression.

Proposed Methodology

The falsified image detection algorithm for the raw mammogram has three stages: Data Acquisition, Data Pre-processing, and Application. This algorithm works with 17,740 images from Kaggle: 7,492 real, 5,125 forged, and 5,123 re-encoded images with formats JPEG, PNG, and TIF having at least 128×128 pixels size. Data pre-processing includes Segmentation, Filtering, Normalization, and Noise Reduction. The data is distributed: 70% training (12,148 images) and 30% testing (5,592 images). The Application stage includes the use of Deep Convolutional Neural Network (DCNN) for forgery detection. Features extracted by DCNN form the basis for obtaining results through AI. Classifiers and DCNN are being trained, validated, and checked for their accuracy before storage. If the learning conditions are not fulfilled, retraining takes place that are shown in figure 1.

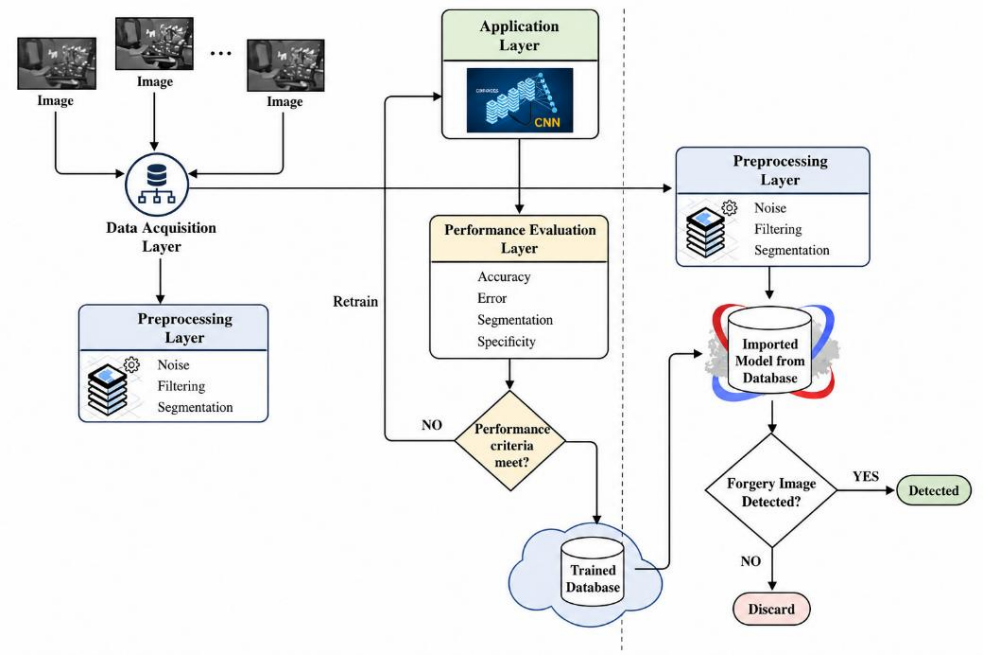

Figure 1: Proposed Forgery Detection Using DCNN

Result

For detecting images of fraud with the help of deep learning in MATLAB R2023a. There are three input parameters with one output variable which can be either genuine or fake and there are 17,740 samples with 12,418 in the training set and 5,322 in the test set that are shown in table 1.

Table 1: *Comparison of the training and validation accuracy*

	Training	Validation
Accuracy	97.38%	94.42%
Error Rate	2.62%	5.58%

The confusion matrix was applied to validate the performance of the classifier under test, whereby rows represent real class values, columns represent predictions while the diagonal elements represent correct classification that are shown in table 2. From the table below, the total number of instances tested is 17,740 images out of which 3,514 images are forged, 3,153 are recompressed, and 5,066 images are authentic.

Table 2: *Confusion matrix for Training*

N=12418	O_{Real}	O_{Fake}	$O_{Recompressed}$
I_{Real} = 5249	5066	176	02

I_{Fake} = 3588	38	3514	36
$I_{Recompressed}$ =3586	01	72	3513

From the confusion matrix, it can be seen that the model has successfully classified 5,249 genuine images, with 176 being falsely classified as forgeries and 2 as being recompressed images. In the case of the forgery images, there have been 3,588 successful classifications while 36 were wrongly classified as recompressed images and 38 as genuine images. Out of the 3,585 recompressed images, there have been 3,513 correct classifications while 72 were classified as forgery and 1 as genuine images that are shown in table 3.

Table 3: *Confusion matrix for validation*

N=5322	O_{Real}	O_{Fake}	$O_{Recompressed}$
I_{Real} = 2248	2126	118	04
I_{Fake} = 1537	45	1450	42
$I_{Recompressed}$ = 1537	02	86	1449

In terms of the training phase of the experiment, the model recognized 2,126 of 2,248 real photos, which means that there were 118 real photos that were mistakenly considered fake and 4 real photos that were wrongly classified as recompressed. In relation to the synthesized classes, the model recognized 1,450 of 1,537 fake photos and 1,449 of recompressed photos. It should be noted that in the same way as in the case of real photos, the rest of the photos were recognized wrongly in each of the three classes.

Conclusion

In this research paper, a novel image forensics technique has been proposed which utilizes the concept of DL and DCNN. This image forensics technique exploits the dissimilarity between photographs owing to compression in order to distinguish between genuine photographs and those which are fake or recompressed. The results from empirical analysis show that the training success rate

is 97.38%, while the response validation success rate is 94.42%.

References

[1] K. Kaur and N. Kanwal, "Digital Image Forgery: Historical Perspective and Challenges," 2019.

[2] A. AlZahir and M. Hammad, "Blind Image Forgery Detection Techniques: A Survey," 2020.

[3] A. Agarwal, S. Khudaniya, A. Gupta, and A. Grover, "Image Forgery Detection Approaches and Applications," 2020.

[4] M. Meena and V. Tyagi, "Digital Image Forgery Detection: Challenges and Opportunities," 2019.

[5] A. Qazi, T. Zia, and N. Almorjan, "Active and Passive Approaches for Digital Image Forgery Detection," 2022.

[6] A. Saber, A. Khan, and S. Mejbel, "Digital Watermarking and Authentication Techniques," 2020.

[7] K. Shanthi and M. Raj, "Copy-Move and Image Retouching Forgery Detection Methods," 2018.

[8] A. Zanardelli, F. Guerrini, M. Leonardi, and G. Adami, "Image Forensics and Manipulation Detection Techniques," 2022.

[9] S. Haider, M. Khan, S. Rehman, M. Rahman, and S. Kim, "Deep Learning for Computer Vision Applications," 2021.

[10] A. Narayan, V. Vipul, P. Awasthi, S. Fatima, M. Faiz, and S. Srivastava, "Deep Neural Networks for Visual Data Analysis," 2023.

[11] M. Ali, R. Ganapathi, T. Vu, M. Ali, A. Saxena, and N. Werghi, "Deep Learning-Based Image Forgery Detection: Recent Advances," 2022.

[12] M. Mayer and M. Stamm, "Camera and Compression Artifacts in Digital Image Forensics," 2018.

[13] M. Saleem, M. Sheeraz, M. Hanif, and A. Farooq, "Advanced Image Forgery Detection Methods Using Deep Learning," 2020.

[14] D. Ansari, S. Ghrera, and V. Tyagi, "Geometry-Based and Passive Digital Image Forgery Detection," 2014.

[15] J. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "Physical Environment-Based Image Forgery Detection," 2020.

[16] S. Shankar et al., "Correlation, DWT and DCT Based Image Authentication Framework," 2022.

[17] M. Asghar et al., “FFT and DRLBP Based Image Forgery Detection Using SVM,” 2022.

[18] A. Koul et al., “CNN-Based Copy-Move Forgery Detection Framework,” 2022.

[19] Y. Chen et al., “Encoder–Decoder Deep Learning Framework with LSTM for Image Manipulation Detection,” 2022.

[20] K. Krishnaraj et al., “Deep Learning Fusion Model for Copy-Move Forgery Detection,” 2022.

[21] Y. Tan, X. Chen, Y. Zeng, H. Li, and X. Huang, “Double JPEG Compression Analysis for Digital Image Forensics,” 2022.

[22] W. Barad, Z. Mukesh, and P. Goswami, “Camera-Based Forensic Artifacts for Image Authentication,” 2020.