Image forgery detection using Convolutional Neural Networks

[1] Praveenkumar Babu, [2]Sivanagireddy A,[3]Narsireddy M and [4]Yogapriya Jaganathan
[1,2,3]Dept.of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Chennai, India.
[4]Dept.of Computer Science and Engineering, Kongunadu College of Engineering and Technology, Thottiyam, India.
[1]mbp.praveen@gmail.com, [2]annapureddynagireddy0@gmail.com, [3]19121058@student.hindustanuniv.ac.in,
[4]yogapriya.j@gmail.com

Article Info
A. Haldorai et al. (eds.), *2nd International Conference on Materials Science and Sustainable Manufacturing Technology,* Advances in Computational Intelligence in Materials Science.
Doi: https://doi.org/10.53759/acims/978-9914-9946-9-8_23

Abstract -Digital forensics vital aspect of picture identity theft has drawn a lot of notice recently. In order to establish the primitive character of images, earlier studies looked at residual pattern noise, wavelet-transformed data and facts, image pixel resolution histograms, and additional characteristics of images. In an attempt to attain high-level picture illustration with the advancement of neural network-based innovations, convolutional neural networks have recently been utilized for recognizing image counterfeiting. This model suggests constructing a convolutional neural network with a structure that is distinct from previous studies in which we attempt to interpret the features derived from each layer of convolution to recognize a variety of picture manipulation using automated feature recognition. Three convolutional layers, one fully interconnected layer, and a SoftMax classifier constitute the suggested system. Our study utilizes our own data collection as the training data, which includes genuine pictures, spliced images, and further enhanced replicates with retouched and re-compressed images. Experimental findings make it abundantly obvious that the proposed network is optimal and versatile.

Keywords – Digital Forensics, Convolutional Neural Networks, Softmax, Spliced Images, Retouched, Re-Compressed Images**.**

I. INTRODUCTION

Counterfeiting with sensors is a crucial prerequisite in digital forensic investigations, which aim to tell the difference between genuine pictures and ones that have been altered [1]. Due to the profusion of image modification tools and the ease of sharing digital images, the problem of identifying phony photos has become more crucial. In recent years, segmentation, object detection, and picture classification have all been computer vision jobs where convolutional neural network networks (CNNs) have achieved notable outcomes. In this study, we propose a CNN model with "softMax" segmentation for the goal of identifying fake pictures.

Techniques for identifying altered images have become increasingly vital as image-transforming tools and the volume of manipulated photos on the web increase yearly [2]. Today, manipulating pictures is easy. Thankfully, a bunch of studies has been conducted on photo manipulation detection methods, and today many of them use convolutional neural networks (CNN). Techniques that have been suggested for this purpose have been outlined in numerous works. Convolutional neural networks must be modified to learn features for detecting tampering because they are typically built for detecting and categorizing characteristics of an image's contents [3]. Convolutional Layer is standardized to fit a constraint after each training step, enabling the layer to detect faces that are helpful for identifying picture modification.There are different types of techniques that image forgers may be using. Some manipulation detection algorithms aim to recognize a particular type of manipulation approach, whereas other methods are more all-encompassing.

So far, there are alternative manipulations that shift fragments of pictures to different portions, that are extremely distinct from these. It would therefore be intriguing to use the suggested layer including any copy move operations and research.There are a variety of techniques that image forgers should be using. Although some manipulation detection systems focused on a particular type of manipulation technique, others are more general. This model studies four different types ofimagemanipulationretouching, recompression, splicing andauthentic [4]. But still, there are additional manipulations that move sections of pictures to different portions, that are extremely distinct from these. In the interest of understanding how the model responds to various copy-move manipulations, it would be fascinating to implement the recommended layer to specific copy-move operations.

II. LITERATURE SURVEY

Over the past ten years, deep learning techniques have become incredibly popular and have been used to solve a wide range of applications such as object detection [5], tracking [6], security surveillance [7], image forgery detection [8] and so on. This is because it has been demonstrated that they excel in classification difficulties in addition to regression and segmentation problems. Deep learning techniques have been researched in recent literature for image authentication as well, with the goal of improving accuracy over previously proposed, conventional methods. CNNs and other deep learning models are indeed able to autonomously determine descriptive features that capture the aspects of the input data that are ideally suited to the task at hand. M. Goljan et al., developed a revolutionary deep CNN architecture that utilizes a combination of convolutional, pooling, and fully connected layers is suggested for the identification of image forgeries [8]. The suggested method outperformed other cutting-edge techniques and demonstrated high accuracy on a variety of benchmark datasets. CNNs are used for watermarking scheme in digital pictures by S. Agarwal et al [9]. These findings suggest using convolutional, max-pooling, and fully connected layers in conjunction with CNN to identify fake pictures. The technique was evaluated on various benchmark datasets and outperformed other trying-to-cut techniques in terms of accuracy.

K. Patil et al., proposed a deep CNN architecture that incorporates convolutional and pooling layers to detect image forgeries. The technique was validated on various benchmark datasets and outperformed other trying-to-cut methods in terms of accuracy and precision [10].S. Mukherjee et al., developed a hybrid CNN-LSTM architecture that incorporates convolutional and long short-term memory (LSTM) layers to detect image forgery [11]. The technique was examined on numerous benchmark datasets and outperformed other cutting-edge techniques in terms of accuracy and F1 score.

Using multi-stage deep convolutional neural networks by J. Zhang et al., a multi-stage deep CNN architecture that incorporates convolutional, pooling, and fully connected layers to detect image forgeries [12]. This model is tested on various benchmark datasets, the suggested strategy outperformed other cutting-edge techniques in terms of accuracy and F1 score. The effectiveness of the suggested method is thoroughly examined in the study, in addition to the effects of various network architectures and training parameters.

S. Bappy et al., proposed a CNN-based technique for recognizing image forgeries is presented, which includes fully connected, convolutional, and pooling layers [13]. The methodology consisted of successful performance when tested on benchmark datasets.With the help of spatially constrained pooling layers, Diallo et al., developed a deep CNN architecture for identifying photoshopped pictures. The strategy was evaluated on various benchmark problems and outscored other cutting-edge techniques in terms of accuracy [14].

Chen et al. investigatedadaptive CNNarchitecture which combines convolutional and pooling layers to detect image forgeries [15]. Tested on benchmark datasets, the proposed approach outperformed other cutting-edge techniques in terms of accuracy.Convolutional neural networks have been employed to detect copy-move forgeries in digital images, thus according to Tyagi et al [16]. This study indicates combining convolutional and pooling layers in conjunction with CNN to recognize copy-move forgeries in digital photos. The strategy was evaluated on baseline methods and outperformed other cutting-edge strategies in terms of accuracy. L. Li et al., proposed a hybrid CNN architecture built on convolutional and fully connected layers is proposed for the detection of image forgeries. The strategy was evaluated on benchmark datasets and outperformed other material removal approaches in terms of accuracy [17].

III . METHODOLOGY

In this section, we provide a brief description of the CNN model. CNN stands for convolution neural network. Its objective is to take the relevant information from the picture. Convolution, pooling, and fully linked layers are the three basic layers used during deep learning. This convolutional layer, the max-pooling layer, the flattening layer, and the full connection layer are only a few of the various layers that the illustration shows are used to correct for CNN. An inquiry parameter serves the purpose of the convolutional layer's training procedure. There seem to be numerous variations, with the training algorithm being the most well-known. Its multiple non-linear functions are demonstrated in **Fig 3.** The output layer Max-pooling layer is where they are mostly quite often used: It aggregates the features which are extracted from the image, compresses the sizes, and extracts the most important aspects that are observable in the image, as demonstrated in **Fig 1**. The max-pooling features are transformed into a one-dimensional matrix via the flattening layer. A layer that is fully coupled links each neuron. Then the testing images are compared with testing images in Sof
tmax later on classification is done.

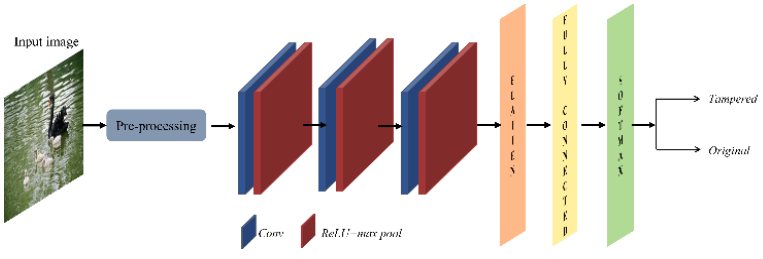


Fig 1. Proposed CNN Architecture

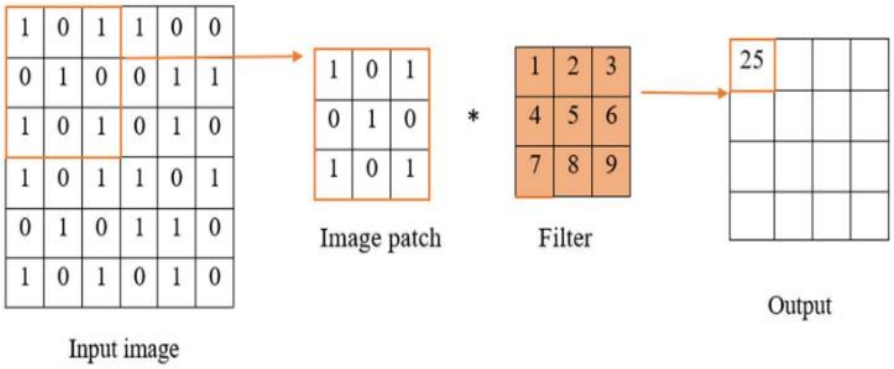


Fig 2. Matrix form of Image

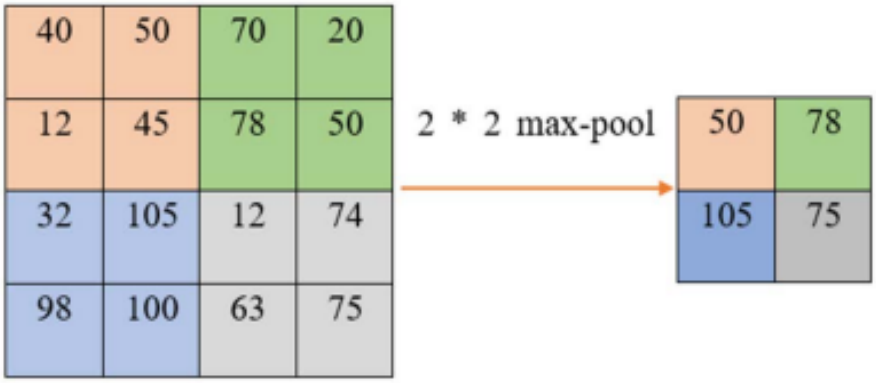


Fig 3. Maxpooling

Numerous levels of the Forgery detection approach were laid out in this work. The suggested approach is dependent on the CNN model, as demonstrated in **Fig 10**. The CNN technique employs the whole image, meanwhile, the conventional approach uses a block-based algorithm. The three stages of the approach that will be discussed are feature extraction, pre-processing, and classification.Matrix form of image is shown in **Fig 2** and Max pooling is shown in **Fig 3**.

Table 1. Architecture details of CNN

Input	Kernels	Filter size	Stride	Outputs	Param
300*300	32	3*3	1	298*298	896
298*298	Max pool	ReLU		149*149	0
149*149	64	3*3	1	147*147	18496
147*147	Max pool	ReLU		73*73	0
-	-	Dropout 0.1	-	-	-
73*73	128	3*3	1	71*71	73856
71*71	Max pool	ReLU		35*35	0
-	-	Dropout 0.1	-	-	-
Flatten	-	-	-	-	156800
Dense 1	-	-	-	-	23520150
Dense 2	-	-	-	-	604

Without cropping any image features in the pre-processing data stage, the input image is resized to proceed to the next stage. Three convolution layers are present in the feature extraction stage, which is followed by a max-pooling layer. A full connection layer connects all features to the dense layer at the conclusion of this phase. The categorization SoftMax stage is then activated to divide the data into two categories (forged or original).The use of convolution layers for feature

mining, where each convolution layer provides feature maps using a separate filter set (i.e., ReLU). The next max-pooling layer uses the image features produced by the first convolution layer in order to generate resized pooled feature maps, which are the inputs for the subsequent convolution layer. Fully Connected has included the final feature maps in addition to the final max-pooling in vector format. The dense layer divides the features that were taken from the fully connected layer into two categories: original and modified. The suggested model can be trained effectively for several epochs.Architecture details of CNN is shown in **Table 1.**

Splicing

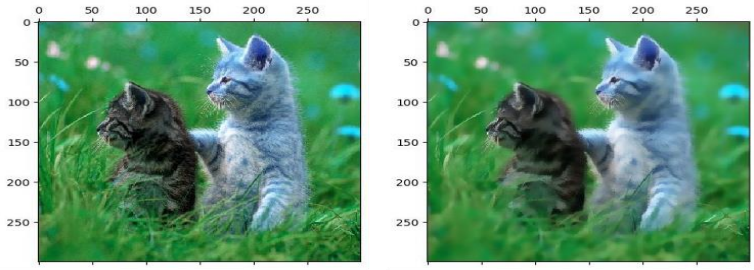
Image splicing is an image editing method that involves cloning a segment with one image and splicing it onto another. Postprocessing approaches like local/global blurriness, compressing, and resizing are recurrently used after image splicing.An illustration of spliced image is shown in **Fig 4.**

Original image Spliced image

Fig 4. Splicing

Retouching:

Photo retouching is the procedure for eliminating unwanted imperfections and optimizing the quality of photo details. This usually involves color and tone correction, the elimination of imperfections and bags under the eyes, and improvements to brightness, contrast, and saturation. An illustration of retouched image is shown in **Fig 5.**

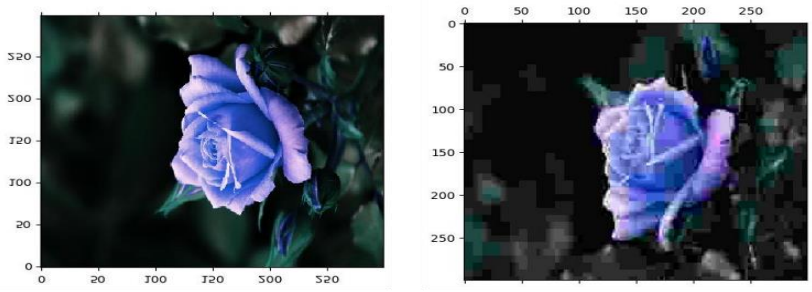


Original image Retouched image

Fig 5. Retouching

Image compression:

Image compression and decompression are significant because new technologies facilitate users to transfer elevated photographs while trying to generate the least amount of internet traffic. Image compression was handled by uncomplicated codecs in the early days of the Internet. Artificial neural network can now attempt to address the compression-decompression challenge in a more appropriate fashion as a result of the growth of machine learning. An illustration of image compression is shown in **Fig 6.**



Original image Compressed image

Fig 6. Image Compression

IV. RESULTS AND DISCUSSION

The performance of forgery image classification models can be evaluated using various metrics such as accuracy. The performance of these models can also vary depending on the dataset used for training and testing, as well as the type of forgery being detected (e.g., copy-paste, splicing, etc.).Some recent research in this area includes the use of deep learning architectures such as convolutional neural networks (CNNs) The performance of these models can also vary depending on the dataset used for training and testing, as well as the type of forgery being detected (e.g., copy-paste, splicing, etc.). Overall, while progress has been made in forgery image classification, it remains a challenging problem with many open research questions and opportunities for further investigation we constructed a convolutional neural networkfor detecting image forgery. The network has Six layers consisting of the image input layer, three convolutional layers, one fully connected layer, and a SoftMax classifier.We used our own data set that consists of spliced,authentic, retouched, and recompressed images.The proposed model is learned by different features which are more important in forgery image detection. Our model has shown **98.70%** accuracy which differentiates other models in accuracy and classifying forged images as shown in **Fig 7**.

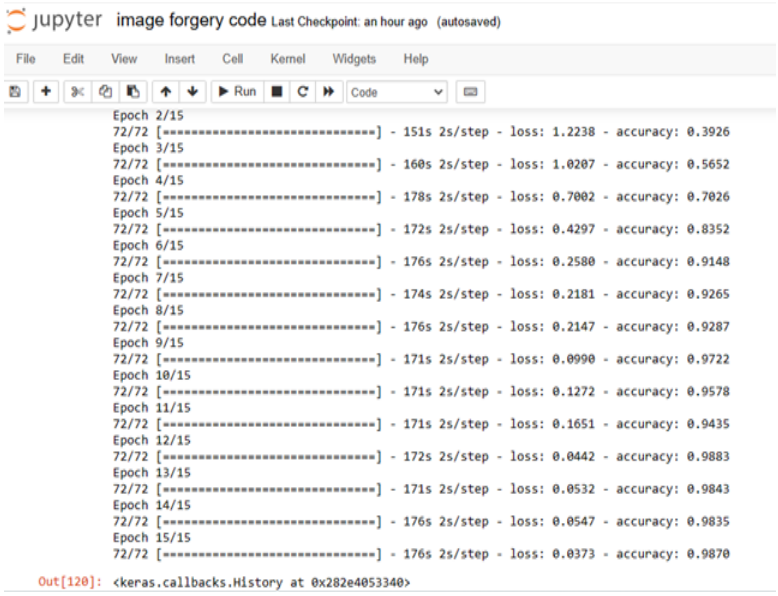


Fig 7. Screenshot of Accuracy achieved using proposed CNN Architecture.

V. CONCLUSION

In this research, we conducted experiments with implementing a CNN to the challenge of categorizing photoshopped pictures. More specifically, a Neural network was utilized to extract characteristic features from an image database which would include splicing, recompression, retouched and authentic images. When it was over, it was utilized to train and try to assess a Softmax, with the latter achieving an efficiency level of 98.72% on our dataset. These results reinforce our prediction that the recognition accuracy decreases as the complexity of the samples. Thus, according to our research study, even when done by professionals, photograph manipulation may be identified with an accuracy of ever more than 98.72%. The implemented architecture, however, does not conveniently generalize to datasets with numerous underlying distributions, according to our conclusions. In summary, although there is definitely still a lot of work to be done in the field of photographic forgery detection, we anticipate artificial neural networks will eventually be able to recognize altered photographs regardless of how complicated they remain.

References

[1] M. C. Stamm, M. Wu and K. J. R. Liu, "Information forensics: An overview of the first decade", IEEE Access, vol. 1, pp. 167-200, 2013.
[2] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in IEEE Access, vol. 10, pp. 48622-48632, 2022.
[3] F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in IEEE Access, vol. 8, pp. 133488-133502, 2020.
[4] S.S. Ali et al., "Image Forgery Detection Using Deep Learning by Recompressing Images," Electronics 2022, 11, 403.
[5] P. Babu and E. Parthasarathy, "Optimized Object Detection Method for FPGA Implementation," 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2021, pp. 72-74.
[6] P. Babu and E. Parthasarathy, "FPGA implementation of multi-dimensional Kalman filter for object tracking and motion detection," Engineering Science and Technology, an International Journa, vol. 33, 2022.
[7] T. Daniya, J. T. Thirukrishna, B. S. Kumar and M. V. Kumar, "ICSA-ECNN based Image Forgery Detection in Face Images," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-4.
[8] M. Goljan et al, "Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images, "Forensic Science International, vol. 279, pp.8-21, 2017.

[9] S. Agarwal et al, “Improved approaches with calibrated neighboring joint density to steganalysis and seam-carved forgery detection in jpeg images,” ACM Transactions on Intelligent Systems and Technology, vol. 5(4), pp.1-30, 2015.
[10] K. Patil et al., "Effective "A novel forensic image analysis tool for discovering double JPEG compression clues,” Multimedia Tools And Applications, vol. 76(6),pp.7749-7783, 2017.
[11] S. Mukherjee and K. W. Bowyer, “Detecting facial retouching using supervised deep learning,” IEEE Transactions on Information Forensics and Security, vol. 11(9), pp.1903-1913, 2016.
[12] J. Zhang et al and R. Cipolla, “Segnet: A deep convolutional encoder-decoder architecture for scene segmentation,”IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.39(12), pp.2481-2495, 2017.
[13] S. Bappy and L. Verdoliva, “A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection,” IEEET Transactions on Information Forensics & Security, vol. 9(4), pp.554-567, 2014.
[14] T. Thamaraimanalan et al., "Machine Learning based Patient Mental Health Prediction using Spectral Clustering and RBFN Algorithms," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1840-1843, doi: 10.1109/ICACCS54159.2022.9785142..
[15] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 2017, pp. 2152-2156, doi: 10.1109/ICASSP.2017.7952537.
[16] K. Meena and V. Tyagi, "A copy-move image forgery detection technique based on Gaussian-Hermite moments", Multimedia Tools Appl., vol. 78, pp. 33505-33526, Dec. 2019.
[17] S. Walia, K. Kumar, M. Kumar and X. -Z. Gao, "Fusion of Handcrafted and Deep Features for Forgery Detection in Digital Images," in IEEE Access, vol. 9, pp. 99742-99755, 2021, doi: 10.1109/ACCESS.2021.3096240.