Vol.15, Issue No 2, 2025

Optimized CNN for Accurate Images Forensics and Tampering Detection

[1]VUYURI KOMALI SIVA MAHESWARI, [2]PENMETSA DIVYA NAGANJALI, [3]PULAMANTULA BHANU SRI PRAKASH, [4]PILLA SRIDHAR, [5]Mr. K.T.V. SUBBARAO

[1234]Student Department of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

[5]Assistant Professor, Department of CSE, DNR College of Engineering & Technology, Balusumudi, Bhimavaram, India.

Abstract

The issue of picture fraud has become more commonplace than ever before due to the widespread use of digital photographs in many applications. Our innovative Convolutional Neural Network (CNN)-based picture forgery detection system can identify a wide range of image modifications, such as splicing, retouching, and copy-move, and is presented in this study. To address the issue of picture fraud detection more effectively, our suggested approach combines deep learning techniques with Error Level Analysis (ELA). By testing the suggested approach on a collection of real-life photos, we were able to get a remarkable 93% detection accuracy. In a number of contexts, including digital image analysis, security, and forensics, our technique proved to be more effective than previously used methods for detecting picture forgeries. When it comes to the increasing issue of picture alteration and forgery in today's visual media environment, the suggested CNN-based image forgery detection system provides a strong and efficient answer. CNNs can learn feature hierarchies, which is a huge plus since it means they can identify patterns in images at various sizes and orientations. As a result, they excel in jobs like medical picture analysis, object identification, and face detection. To top it all off, CNNs are very versatile and can be fine-tuned by training them on massive datasets.

INTRODUCTION

Modern visual media producers are increasingly worried about picture forging, which is the manipulation of digital images for the purpose of misleading or deceiving consumers. There is an immediate and critical demand for efficient picture forgery detection systems due to the widespread use of digital photographs in industries including journalism, social media, and online commerce. Forensics uses these algorithms to find evidence of manipulation in crime scene photos, while security uses them to spot fake papers and photos. Additionally, online advertising and e-commerce may benefit from picture forgery detection systems by checking product photographs for signs of manipulation. Various deep learning techniques may be used to create this sort of model. Developments in areas such as natural language processing, picture and voice recognition, and more have resulted from deep learning's ability to train computers to see connections and patterns in data that people would miss. One effective method for detecting picture fraud that has arisen in recent years is the use of Convolutional Neural Networks, or CNNs. By examining intricate picture attributes, these deep learning algorithms can detect even the most minute indications of tampering. Even when dealing with noise or compression artifacts, forgery detection systems based on convolutional neural networks (CNNs) can reliably recognize copy-move, splicing, retouching, and other picture modifications. CNN's many neuronal layers allow it to analyze the image's complicated elements. [8] In their research, Ali et al. [2] referenced comparing different approaches. Accurate experimental results were shown. A visual representation of the result was provided to enhance comprehension.

LITERATUREREVIEW

Review of relevant literature for the current article A Graphical User Interface (GUI) for the identification of digitally manipulated photographs was designed by Ranjan et al. [1]. This approach is both efficient and practical, with an accuracy rate of 96.4%. Based on research into digitally altered documents, it offers

a way to tell the difference between the original and the digitally altered versions of a document. Machine Learning, Copy-Move, Slice, and Convolutional Neural Networks

Because of CNN's powerful self-learning capabilities, Amit Doegara et al.[3] used the algorithm to identify picture forgeries. Active and passive modalities were both used. Digital signatures or watermarks may be pre-inserted into photos using the active mode technique. It is not necessary to pre-embed any digital signature or watermark on the photographs when using the passive mode technique. To make picture fraud detection more reliable, Boubacar Diallo et al.[4] laid forth a method. Their approach for camera identification was based on convolutional neural networks. Since lossy compression, like JPEG, is believed to be the most popular way of intentionally or unintentionally hiding photo forgeries, they tested the technique on this alteration. Trained CNN is given a variety of compressed and uncompressed images with varying quality levels. B. Literature study about current online resources Forensically [10] has a number of useful capabilities, including the ability to identify clones and analyze error levels, and it is easy to use. Among its many uses are ELA, MetaData provision, clone detection, and more. To some extent, forensics is like using a magnifying glass. When seen by authorized users, it reveals information that is normally kept secret. The clone features' subfeatures aren't entirely clear. The website does not display the proportion of forgeries.

An option for a function that may identify forgeries is available in FotoForensics [11]. It shows the degree of mistake on the image, which indicates whether it was altered in Photoshop or not. Color will be seen in picture analysis if the image has been edited or manipulated. You will see a standard white hue on the image if it has not been altered. Not an easy UI to use. Very few features; the one that does exist is for forgery, however it does not display the proportion of fraud. There are a lot of tools and options for analysis in Amped Authenticate [12]. It is useful for determining if the photos have been altered or not. If you want to know if a photograph has been edited or is completely genuine, Amped Authenticate has you covered with its comprehensive tests, operations, and reports. We may scan and build object targets using Vuforia Object Scanner, which is a popular freemium platform.

METHODOLOGY

Architecture of the System Figure 1 below shows how the front end of the website requires the user to submit a picture. It is the CNN model's job to assess the picture. In order to build the model, the dataset will be trained and tested. It must pass through these steps in order to be transformed into a model. In the first step, known as pre-processing, we eliminate null values and clean up any noisy data in the collection. The picture moves on to the feature extraction step after the PreProcessing stage. During feature extraction, just the necessary features are retained while the unnecessary ones are eliminated. Instead of just applying an algorithm to the raw data, it produces superior results. To acquire the final result, the CNN algorithm is employed after feature extraction. The user gets shown the final outcome after all the operations have finished.

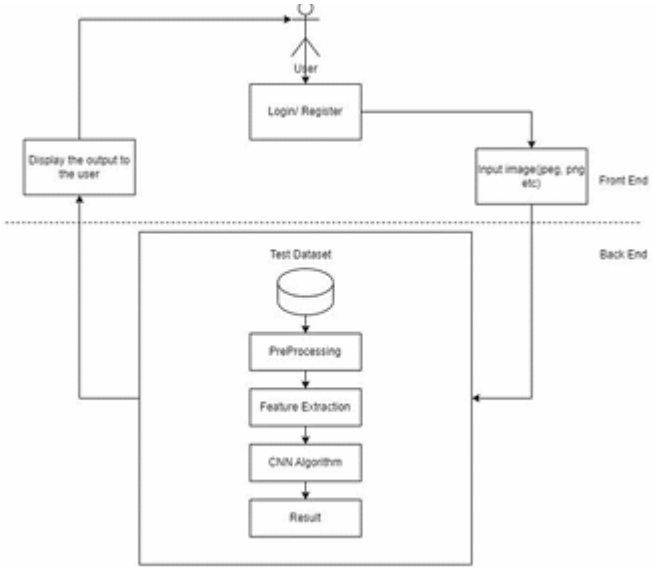

Fig. 1. System Architecture

B. Images with modified dataset details. About 7,000 photos have been validated, while roughly 3,000 have been altered. Therefore, in order to fulfill this condition, the model is trained using a mixture of two datasets: CASIA 2.0 [13] and MICC F200 [14]. Image forgeries may be classified into several categories, including copy-move, slicing, removal, and retouching forgeries. The model has to be trained with data that includes altered pictures of the kinds described above in order to identify these frauds. This

led to the creation of a unique dataset that includes some altered photographs. Two directories make up the dataset: authenticated images and How CNN Works Image forgery detection makes use of the convolutional neural network (CNN) technique to determine if a picture is real or fake using information taken from the original, preprocessed pictures. The system learns its features using convolution, pooling, and activation functions on a big dataset that includes both real and fake pictures. In order to extract useful characteristics, such edges and forms, from the input picture, the convolution layer uses a collection of learnable filters. In order to aid in feature extraction, the pooling layer decreases the feature maps' spatial dimensions. The activation function improves the network's capacity to learn intricate patterns and features by applying a nonlinear adjustment to the output of the convolution and pooling layers. Following feature extraction, the network's output is processed by a fully connected layer. This layer assigns probabilities to the learnt features. To classify the output as either legitimate or fabricated, we apply the softmax activation function to transform the data into a probability distribution. We then choose the class with the greatest probability as our final conclusion. The convolutional neural network (CNN) method learns to minimize the loss function and enhance classification accuracy by optimizing the network parameters during training. An optimization approach, such stochastic gradient descent (SGD), is used to update the parameters, and the error is propagated from the output layer to the input layer using the backpropagation process. Several forms of picture manipulation are detectable by the CNN algorithm. These include copy-move, splicing, removal, and retouching forgeries. The system can detect picture forgeries by examining the characteristics taken from the preprocessed pictures and finding the discrepancies and artifacts that go along with them. Image forgery detection performance using convolutional neural networks (CNNs) is sensitive to training dataset quality and variety, network design complexity, and optimization technique. IV.

RESULTS

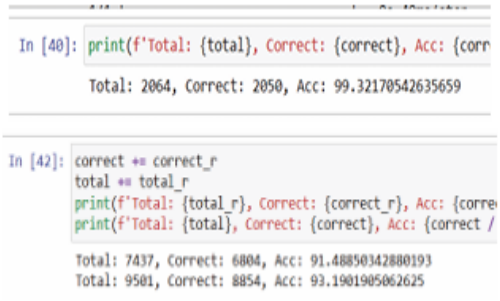

Fig. 2. Accuracy of the model

Achieving an accuracy of 99.3217% was possible after training the model with a little quantity of data, about 2000 photos, as illustrated in figure 2. Next, the model was trained and tested using 9500 photos, and it was estimated to reach an accuracy of 93%.

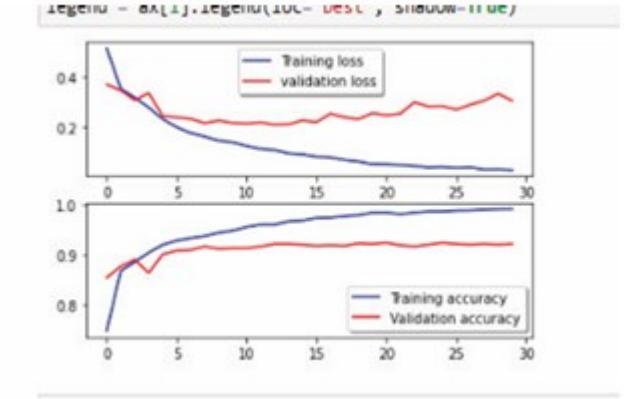

Figure 3: Accuracy and Loss The training validation accuracy and training validation loss of our model are shown in Figure 3. In order to train our model with a high detection accuracy, we had almost no loss, as shown in figure 3.

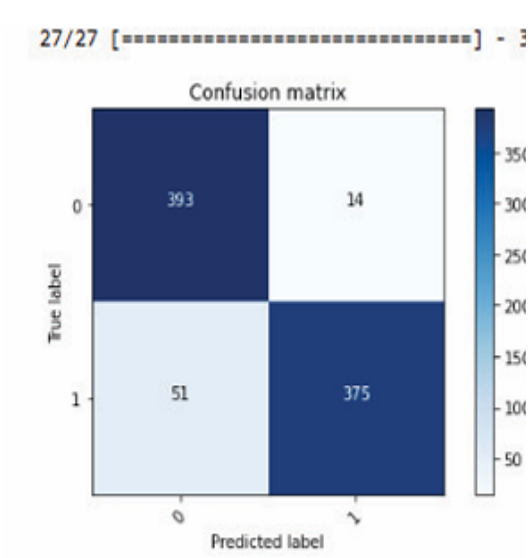

Figure 4. Matrix of Confusions Figure 4 displays the confusion matrix that was obtained during the model training process. Accurate result: 393 Reverse Positive: 14 Negative Misstatement: 51 Negative Validity: 375

Image 5. ELA One method for analyzing digital images for signs of tampering is Error Level Analysis (ELA). ELA is able to do its task by comparing the error levels across several picture sections. When an image is compressed and stored in a lossy format like JPEG, the amount of compression artifacts that remain is called the error level. Class A. User Interface Design

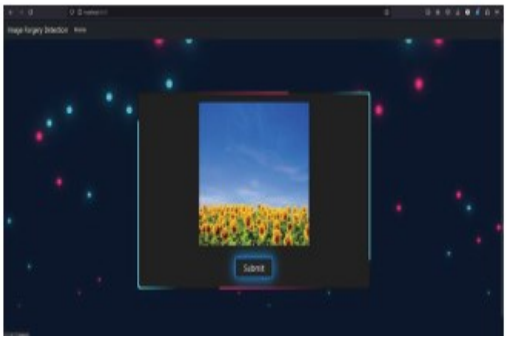

Fig. 6. Uploading Real Image

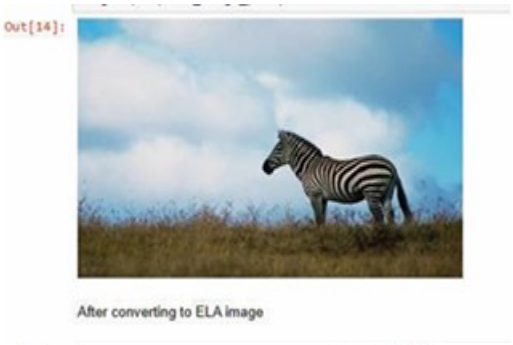

Fig. 7. Result

Figure 7 displays the outcome of the user-provided picture, which in turn displays the model's confidence, or the degree to which the model believes our image to be genuine or phony. This means that the model has a 99% certainty that the photograph is authentic.

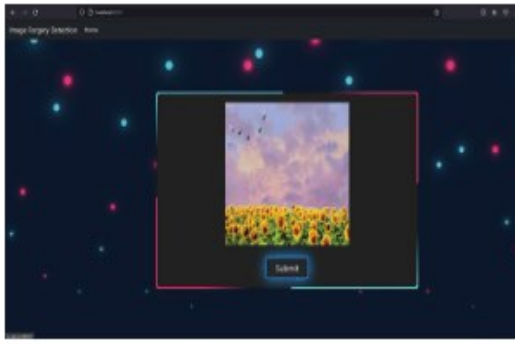

Fig. 8. Uploading Fake Image

Figure 9. Findings Figure 9 displays the outcome of the user-imputed false picture with a confidence level of about 93%, indicating that the model is 93% certain that the image is fake.

Conclusion

In summary, Finally, a CNN-based picture forgery detection and localization system is an encouraging development in this area. Its speed, precision, and adaptability make it useful in many contexts, and its ability to boost the trustworthiness of digital photographs is immense. The picture forgery system makes a significant contribution to the battle against digital fraud, since image modification remains a major threat in today's digital environment.

REFERENCES

[1]. Ranjan, Shruti, Prayati Garhwal, Anupama Bhan, Monika Arora, and Anu Mehra. ”Framework for image forgery detection and classification using machine learning.” In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1 9. IEEE, 2018.

[2]. Ali, S. S., I. I. Ganapathi, N. S. Vu, S. D. Ali, N. Saxena, and N. Werghi. ”Image Forgery Detection Using Deep learning by Recompressing Images. Electronics 2022, 11, 403.” (2022).

[3]. Amit Doegara , Maitreyee Duttaa , Gaurav Kumarb. ”CNN based Image Forgery Detection using pre-trained AlexNet Model” 2018.

[4]. Boubacar Diallo, Thierry Urruty, Pascal Bourdon, Christine Fernandez- Maloigne. ”Robust forgery detection for compressed images using CNN supervision” IForensic Science International: Reports,Volume 2,2020,100112.

[5]. Sarma, Barnali, and Gypsy Nandi. ”A study on digital image forgery detection.” International Journal of Advanced Research in Computer Science and Software Engineering 4, no. 11 (2014).

[6]. Barad, Zankhana J., and Mukesh M. Goswami. ”Image forgery detection using deep learning: a survey.” In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 571-

[7]. 576. IEEE, 2020. Kuznetsov, A. ”Digital image forgery detection using deep learning approach.” In Journal of Physics: Conference Series, vol. 1368, no. 3, [9] p. 032028. IOP Publishing, 2019.

[8]. Doegar, Amit, Maitreyee Dutta, and Kumar Gaurav. ”Cnn based image forgery detection using pre-trained alexnet model.” International Journal of Computational Intelligence IoT 2, no. 1 (2019)

[9]. Ganguly, Shreyan, Aditya Ganguly, Sk Mohiuddin, Samir Malakar, and Ram Sarkar. ”ViXNet: Vision Transformer with Xception Network for deepfakes based video and image forgery detection.” Expert Systems with Applications 210 (2022)

[10]. ”Forensically Beta”, https://29a.ch/photo-forensics/forensic-magnifier (accessed on : Jan 16, 2023)

[11]. ”FotoForensics”,https://fotoforensics.com/ (accessed on : Jan 17, 2023)

[12]. [14] ”Amped Authenticate”, https://ampedsoftware.com/authenticate (accessed on : Jan 17, 2023)

[13]. ”CASIA 2.0”, https://www.kaggle.com/datasets/divg07/casia-20 image- tampering-detection-dataset/code (accessed on Jan 15, 2023)

[14]. “MICC F200”, http://lci.micc.unifi.it/labd/2015/01/copy-move forgery-detection-and-localization/ (accessed on feb 15, 2023)