Image Forgery Detection Based on Parallel Convolutional Neural Networks

Dr. Praveen T. Blessington, Prof. Ravindra Mule,
Aditya Pandit, Vedant Pawar, Kavyashree Chimbulkar, Janhavi Patil
Zeal College of Engineering And Research, Narhe

Abstract— **Due to the availability of deep networks, progress has been made in the field of image recognition. Images and videos are spreading very conveniently and with the availability of strong editing tools the tampering of digital content become easy. To detect such scams, we proposed techniques. In our paper, we proposed two important aspects of employing deep convolutional neural networks to image forgery detection. We first explore and examine different preprocessing method along with convolutional neural networks (CNN) architecture. Later we evaluated the different transfer learning for pre-trained ImageNet(via-fine-tuning) and implement it over our dataset CASIA V2.0. So, it covers the pre-processing techniques with basic CNN model and later see the powerful effect of the transfer learning models.**

Keywords— ***image tampering, convolution neural network (CNN), error level analysis (ELA), transfer learning, sharpening filter, fine-tuning***

I. Introduction

The development of approaches to authenticating the source of documents bring curiosity in the research community in the recent years, because the amount of information available to ordinary people such as videos and images, which can be easily tampered with to in order to produce deceitful information. Tampered, modified, fake content is used and spread inappropriately over media through every platform. As the modification tools are easily available, which made it challenging to accurately authenticate the multimedia content.

The study emphasizes on drawing a comparison between the CNN and its pre-processing stages improvements along with CNN and another comparison drawn between transfer learning models. Different tables and figures of comparison all together represents the stats of performance and efficiency.

The objective to carry out this research is to bring forth the improvements either through pre-processing stage or by simply using the better algorithms. The evaluation metrics which is used is the accuracy and loss function i.e mean squared error (MSE). Accuracy could be calculated using the confusion matrix[41],where summation of true positive and true negative over the summation of true negative, true positive, false negative , false positive. The terms true positive means observed positive and predicted positive, true negative means observed negative and predicted negative only whereas false negative means observedpositive and predicted negative, likewise false positive is observed negative and predicted positive. MSE is the squared difference of predicted output and observed output.

The rest of the paper is organized as follows. Section II briefly review related work in the field of image tampering using neural networks. Section III explains in details the examined methodology and explanation of techniques. Experimental results, visualization and discussion are presented in section IV, continue with section V which consists of conclusion, followed by section VI of further work and improvement might possible.

II. Related Work

Zankhana J. Barad, Mukesh M. Goswami, in “Image Forgery Detection using Deep Learning: A Survey”, [1] The information is shared in form of images through newspapers, magazines, inter- net, or scientific journals. Due to software like Photoshop, GIMP, and Coral Draw, it becomes very hard to differentiate between original image and tampered image. Traditional methods for image forgery detection mostly use handcrafted features. The problem with the traditional approaches of detection of image tampering is that most of the methods can identify a specific type of tampering by identifying a certain features in image. Nowadays, deep learning methods are used for image tampering detection. These methods reported better accuracy than traditional methods because of their capability of extracting complex features from image. In this paper, we present a detailed survey of deep learning based techniques for image forgery detection, outcomes of survey in form of analysis and findings, and details of publically available image forgery datasets

NAM THANH PHAM AND CHUN-SU PARK in “Toward Deep-Learning- Based Methods in Image Forgery Detection: A Survey”, [2] In the last decades, deep learning (DL) has emerged as a powerful and dominant technique for solving challenging problems in various fields. Likewise, in the field of digital image forensics, a large and growing body of literature investigates DL- based techniques for detecting and classifying tampered regions in images. This article aims to provides a comprehensive survey of state-of-the-art DL-based methods for image-forgery detection. Copy-move images and spliced images, two of the most popular types of forged images, were considered. Recently, owing to advances in DL, DL-based approaches have yielded much better results as compared to traditional non-DL-based ones. The surveyed techniques were proposed by developing or fusing various efficient DL methods, such as CNN, RCNN, or LSTM to adapt to detecting tampered traces.

Anushka Singh, Jyotsna Singh in "Image forgery detection using Deep Neural Network", [3] Due to the availability of deep networks, progress has been made in the field of image recognition. Images and videos are spreading very conveniently and with the avail- ability of strong editing tools the tampering of digital content become easy. To detect such scams, we proposed techniques. In our paper, we proposed two important aspects of employing deep convolutional neural networks to image forgery detection. We first explore and examine different preprocessing method along with convolutional neural networks (CNN) architecture. Later we evaluated the different transfer learning for pre-trained Image Net (via- fine-tuning) and implement it over our dataset CASIA V2.0. So, it covers the pre-processing techniques with basic CNN model and later see the powerful effect of the transfer learning models.

Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi in "Pixel-Based Image Forgery Detection: A Review" [4] With the advancement of the digital image processing software and editing tools, a digital image can be easily manipulated. The detection of image manipulation is very important because an image can be used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. There are many ways for tampering an image such as splicing or copy-move, resampling an image (resize, rotate, stretch), addition and removal of any object from the image. In this paper we have discussed various pixel-based techniques for image forgery detection, mainly copy-move and splicing techniques.

Micah K. Johnson, Hany Farid in "Exposing Digital Forgeries by Detecting Inconsistencies in Lightning", [5] When creating a digital composite of, for example, two people standing side-by-side, it is often difficult to match the lighting conditions from the individual photographs. Lighting inconsistencies can therefore be a useful tool for revealing traces of digital tampering. Borrowing and extending tools from the field of computer vision, we describe how the direction of a point light source can be estimated from only a single image. We show the efficacy of this approach in real-world settings.

Arati Chougala, Gayatri Patil, Sathisha Kumar in "A Review on Copy Move Forgery Detection in Document Images", [6] With billions of digital images folding the internet which are widely used and re- gards as the major information source in many fields in recent years with the high advance of technology it may seen to fraud the image. In digital images copy moveforgery is the most common image tempering objective of copy move forgery may be to conceal some unwanted features, or to add some local feature which are otherwise absent. In the technological development in digital world has led to a huge increase in the popularity of digital images all domains of life. Thus, there need to authenticate images especially in legal matters. Copy move forgery involves copying a portion of an image and pasting it to different location in same image. With a purpose to conceal facts. This paper presents a study of various image forgery techniques and datasets. A Comparative analysis of major techniques is also presented.

Syed Sadaf Ali, Iyyakutti Iyappan Ganapathi, Ngoc-Son Vu, Syed Danish Ali, Neetesh Saxena and Naoufel Werghi in "Image Forgery Detection Using Deep Learning by Recompressing Images.", [7] Capturing images has been increasingly popular in recent years, owing to the widespread availability of cameras. Images are essential in our daily lives because they contain a wealth of information, and it is often required to enhance images to obtain additional information. A variety of tools are available to improve image quality; nevertheless, they are also frequently used to falsify images, resulting in thespread of misinformation. This increases the severity and frequency of image forg- eries, which is now a major source of concern. Numerous traditional techniques have been developed over time to detect image forgeries. In recent years, convolutional neural networks (CNNs) have received much attention, and CNN has also influencedthe field of image forgery detection. However, most image forgery techniques basedon CNN that exist in the literature are limited to detecting a specific type of forgery(either image splicing or copy-move). As a result, a technique capable of efficientlyand accurately detecting the presence of unseen forgeries in an image is required. Inthis paper, we introduce a robust deep learning based system for identifying image forgeries in the context of double image compression. The difference between an image's original and recompressed versions is used to train our model. The pro- posed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches.

III. Methodology

A. Method 1

The basic image recognition neural network called convolution neural network (CNN), has been used. Images as input is given and significant features from an image is taken out. It is a multi-layered neural network, hence at each layer it extracts certain features. As move deeper into network, it can identify even complex features.

The CNN architecture, as shown in fig.2. is divided into 2 parts: Feature-Extraction and Classification. It consists of following layers:

- Input layer: Here the images from the dataset is fed.

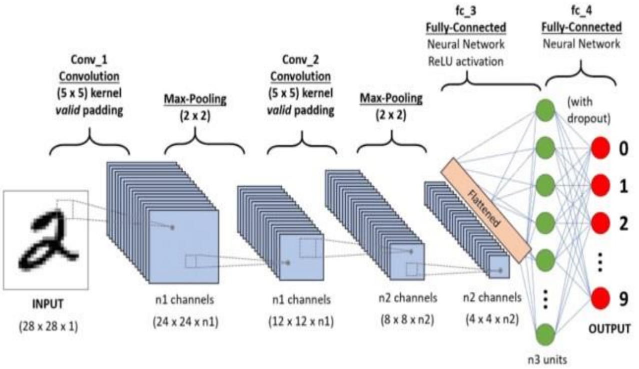


Fig.2. Architecture of Convolution neural network

- Convolution layer: Identification of features takes place here. With each layer certain feature is/are extracted, from simple to complex, which further help in processing.
- Pooling layer: It reduces the content by keeping the significant features which are required. Decrease the computation power, by reducing the spatial size of convolution layer.
- Fully-connected layer: Construct a single column vector by flattens the image. After series of epochs, using softmax classification technique [14,15,16], model could able to distinguish between dominating and weak features in images and classify them.

B. Block Diagram

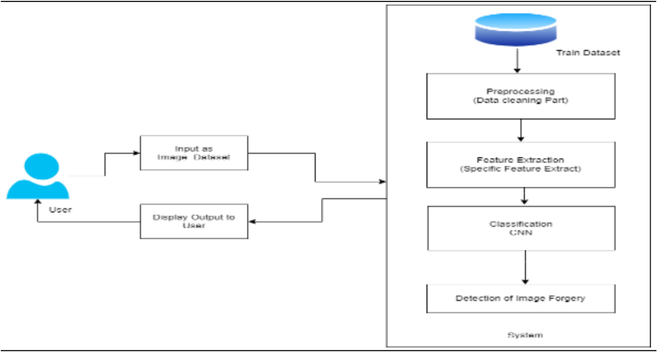


Fig.1. System Architecture

Admin

In this module, the admin has to log in by using valid user name and password. After login successful he can do some operations, such as View All Users and Authorize.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users**.**

End User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will best or to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Manage Account.

C. Data Flow Diagram

In Data Flow Diagram, we Show that flow of data in our system in DFD0 we show that base DFD in which rectangle present input as well as output and circle show our system. In DFD1 we show actual input and actual output of system input of our system is text or image and output is rumor detected likewise in DFD 2 we present operation of user as well as admin.

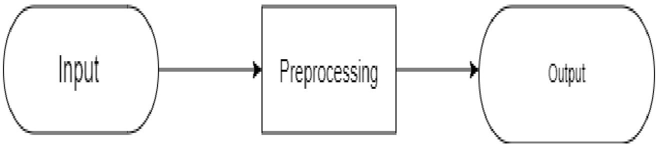


Fig.2. Data Flow(0) Diagram

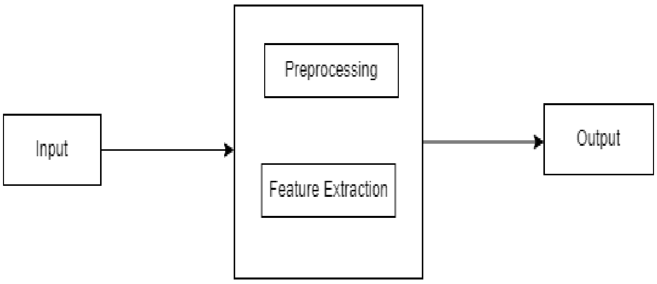


Fig.2. Data Flow(1) Diagram

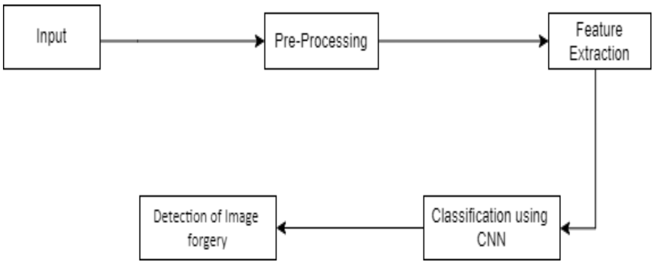
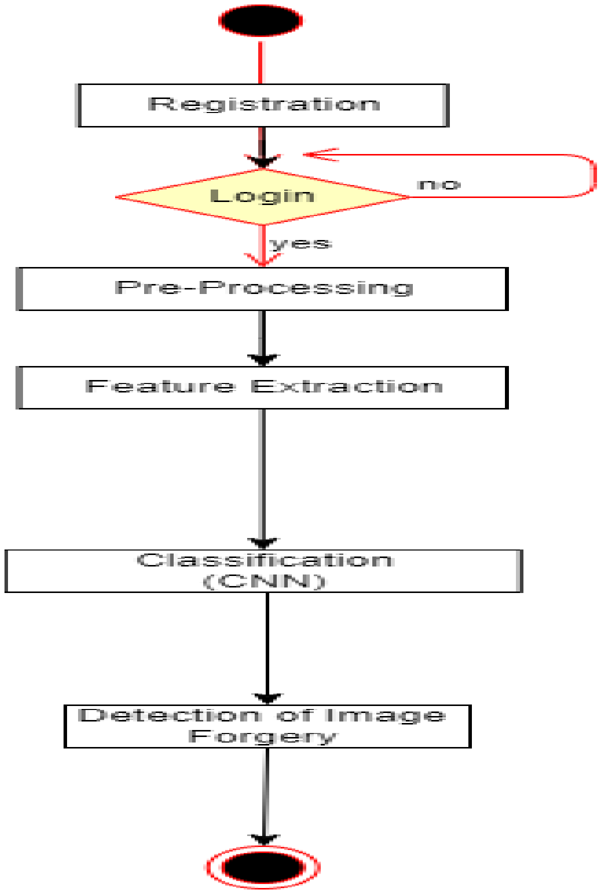


Fig.2. Data Flow(2) Diagram

C. Flow Chart



The flowchart describes the sequence of image detection, which requires input of the image by the user. The system starts with subtraction, follows the KNN algorithm, uses hash sense and encodes the image using a bit encoder. The enc oded data is then saved and the system checks whether the input images are duplicates.

FUTURE WORK

- According to the complexities of the datasets, the number of convolution and pooling layers could be increased.
- Could apply the approaches on different and variety of dataset or modified the current model with simple changes in the area of training algorithms and/or at pre-processing stage.
- To broaden the approaches could be applied on videos which are the collection of frames.

IV. Conclusion

Image Forgery Detection Based On Parallel Convolutional Neural Networks (CNNs) represents a cutting-edge approach to addressing the pressing challenges posed by image manipulation and forgery in the digital age. This technology harnesses the power of parallel CNN models to achieve accurate, robust, and versatile forgery detection, with applications spanning across various domains, including digital forensics, content verification, media integrity, and more. With its ability to adapt to evolving forgery techniques and deliver accurate results, this technology represents a significant advancement in ensuring the trustworthiness of digital media in an increasingly image-driven world..

V. REFERENCES

[1] Mushtaq, S., &, Mir, A. H. (2021). “Image Copy Move Forgery Detection: A Review”. International Journal of Future Generation Communication and Networking, 11(2), 11-12.

[2] Xiaoqiang zhang and Xuesong wang, (November 2020), “Digital Image Encryption Algorithm Based on Elliptic Curve 2. 2. Public Cryptosystem.” IEEE Access, Vol.6

[3] Shwetha B and S V Sathyanarayana, (2021), "Digital image forgery detectiontechniques: a survey." ACCENTS Transactions on Information Security, Vol.2(5).

[4] Charmil Nitin Bharti and Purvi Tandel, (2016) "A Survey of Image ForgeryDetection Techniques", IEEE WiSPNET.

[5] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches" IEEE Transactions on information forensics and security, vol. 7, no. 6, pp. 1841– 1854, 2021.

[6] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy move forgery in digital images”, in in Proceedings of Digital Forensic Research Workshop, Citeseer, 2021.

[7] M. K. Johnson and H. Farid "Exposing digital forgeries in complex lighting environments", IEEE Transactions on Information Forensics and Security, vol.2, no. 3, pp. 450-461, 2020.

[8] K. Asghar, X. Sun, P. L. Rosin, M. Saddique, M. Hussain, and Z. Habib " Edge–texture feature-based image forgery detection with cross-dataset evaluation," Mach. Vis. Appl., vol. 30, nos. 7-8, pp. 1243-1262, Oct. 2021.

[9] Xiao, B.; Wei, Y.; Bi, X.; Li, W.; Ma, J. "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering." Inf. Sci. 2020, 511, 172–191. [CrossRef]

[10] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini and A. de Rezende Rocha "Exposing Digital Image Forgeries by Illumination Color Classification" in IEEE Transactions on Information Forensics and Security, vol. 8, no.7, pp. 1182-1194, July 2021, doi:10.1109/TIFS.2013.2265677.

[11] Khudhair, Z. N., Mohamed, F., Kadhim, K. A. (2021) "A Review on Copy-Move Image Forgery Detection Techniques". In Journal of Physics: Conference Series (Vol. 2021). IOP Publishing Ltd. https://doi.org/10.1088/1742-6596/1892/1/012010.

[12] N. Kanwal, J. Bhullar, L. Kaur, and A. Girdhar “A Taxonomoy and Analysis of Digital Image Forgery Detection Techniques”, Journal of Engineering, Science & Management Education, vol.10, pp. 35-41, 2019