International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-12 Issue-1, October 2022

Detecting Forged Images using Deep Learning

Pranav Sharma, Pooja Santwani, Rachit Narula

Abstract: ***This availability and requirement of data calls for the credibility and authenticity of the data. One such domain is images where tampering creates concern , leading to wide spread of misinformation and fake news. Images are transferred to initiate propagandas on social handles and other platforms. Most of these images are tampered from the authentic original content to allude people and miscommunicate malicious information. In this application, our main work is to modify the existing MobileNetV2 family of neural networks to a more relevant version, so that we can identify and differentiate tampered images from authentic images. We will further create our own convolutional neural network, to create an application which can help us to identify and differentiate tampered images from authentic images and compare our model with MobileNetV2.***

Keywords: Images, Application, MobileNetV2, Neural Network, Detecting, Deep Learning

I. INTRODUCTION

Image processing and its uses within the consumer industry have been rising since the last decade. This is attributed due to numerous changes and evolutions in parallel processing and the ease to access of high-usage and performing hardwares.Another new space which has emerged in the last decade has been the availability of user smartphones. Now, the user has exceptional computational power in their hands.Newer and more advanced Neural Networks have been able to solve harder problems even on cheaper and low powered resources.An example of such Neural Network is MobileNetV2.As know, we have numerous resources at our hands to edit images with the need to verify the authenticity of the images being at an all time high.Methods of tampering content have become so subtle as to be unrecognisable to the human eye with many resing methods used to tamper images for the purpose of imposing propagandas. By means of this project we have trained existing MobileNetV2 using transfer learning and have trained it for image forgery analysis. This model has been trained on the CASIA 2 dataset which consists of tampered and authentic images.

Manuscript received on 18 August 2022 | Revised Manuscript received on 27 August 2022 | Manuscript Accepted on 15 October 2022 | Manuscript published on 30 October 2022.
*****Correspondence Author
Pranav Sharma*, Department of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore. (Tamil Nadu), India. E-mail: pspranavsharma9@gmail.com
Pooja Santwani, Department of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore. (Tamil Nadu), India. E-mail: poojasantwani9@gmail.com
Rachit Narula, Department of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore. (Tamil Nadu), India. E-mail: vrachit456@gmail.com

The images are converted into 224x224x3 sized images which undergo ELA analysis.These images are fed into the MobileNetV2 model to get the outputs. Similarly we have also trained these images on our own Convolutional Neural Network using 128x128x3 sized images which undergo ELA analysis. Finally, we use our custom Neural Network which is deployed in our Flask Web App which prompts user to upload an image and further examines it and tells the authenticity of the image.

II. CORE TECHNOLOGIES

A. Convolutional Neural Networks

Convolutional Neural Networks are a kind of neural network that use different layers to examine unstructured data such as images which are processed through different layers and are used to detect patterns such as edges in the starting layers and other objects like face , mouth , etc in the subsequent layers. They use filters over the input images and these filters match the pattern over the image. The image is then sent through max pooling and normalized .These filters are matrices that are applied on the input images which are collections of different values of pixels.

B. MobileNetV2

MobileNetV2, introduced by Google in 2018, is the second generation of a series of light- weight neural networks that produce results comparable to those of other resource-intensive systems. These neural networks were created with the goal of creating a realistic and clever resource-accuracy trade-off in constrained resource contexts. In fact, this trade-off is so favorable that mobileNetV2.The MobileNetV2 accomplishes this by breaking down a full convolution process into two layers. The former layer uses a depth wise convolution method, in which each input channel receives a single sliding filter, whereas the latter uses a point wise convolution method. The processing resources required to perform the convolution operation can be reduced by dividing it down into two smaller phases.

C. Error Level Analysis (ELA)

Introduced in 2007 by Dr. Neal Krawetz which works on lossy-compression. ELA works by taking the original image and re-saving that image as a new image with slightly less quality compression and then both the images are subtracted from each other using Image Chops in python PIL. In case the image has been tampered, it is easily detected using ELA analysis since different parts of the images have different levels of compression.

D. Flask

Flask is a miniature system offering essential highlights of web application. This structure has no conditions on outer libraries.

The structure offers expansions for structure approval, object-social mappers, open verification frameworks and easy access to routes.

III. LITERATURE SURVEY

This section provides an overview on the previous work done for Image Forgery Detection and related works which use Neural Networks for detecting tampered images and their drawbacks. In[1] Michael Zimba Focuses only on the strategy of first copy and then move Image forgery detection. [2] Uses only the RGB spectrum and hence results are less accurate as compared to existing works which are similar.[3] explains the MobileNet along with its advantages but doesn't have the specific case of detecting tampered images or faked images along with having high computation cost.[4] explains MobileNet and its advantages but doesn't have the specific case of detecting tampered images.

In [5]H K. V.& Nguyen surveys various IFD techniques, used to decide on the most efficient method.The technique used is quite expensive and the computations involved are also complex.[6] is applicable for a very wide range of formats and has high accuracy but is too time consuming and complex to train and implement. In [7] again error level analysis takes images and uses a Computationally cheap CNN called VGG16 with 16 hidden layers but produces worse results and is only good for spliced images. In [8] the model yields a comparable result, Alex-net for the purpose is computationally expensive although only 8 layers deep but the operation cost of each layer is much higher than MobilenetV2.

In [9] Results are not as accurate as MobileNetV2 uses VGG19 with 19 hidden layer and still not effective as VGG16 in certain cases while also being only effective on copy and move forgery. BusterNet is a proprietary Neural Network [10] but due to being based for a different purpose it is not well suited for this application and is computationally expensive and less accurate as well.

IV. EXPERIMENTAL RESULTS

We used images from the CASIA 2 dataset which were labeled as authentic and tampered respectively. The images were pre processed using ELA analysis and were converted into 224X224X3 sized images before being trained with MobileNetV2 which used Adam optimizer for optimization and later these images were resized to 128X128X3 images and were sent to our own CNN to be trained to compare the results.Accuracy was used as the key metric since we required our model to give correctly predicted results. The accuracy results are as follows.

Table - I: Accuracy Results

Neural Network	Training Data	Validation Data
MobileNetV2 model	98.5%	93%
Convolutional Neural Network	97%	92%

We thus inferred that MobileNetV2 outperformed our Convolutional Neural Network giving us a higher accuracy. Although MobileNetV2 outperformed our model , our model additionally gave highly accurate results and we thus used it in our Flask WebApp.

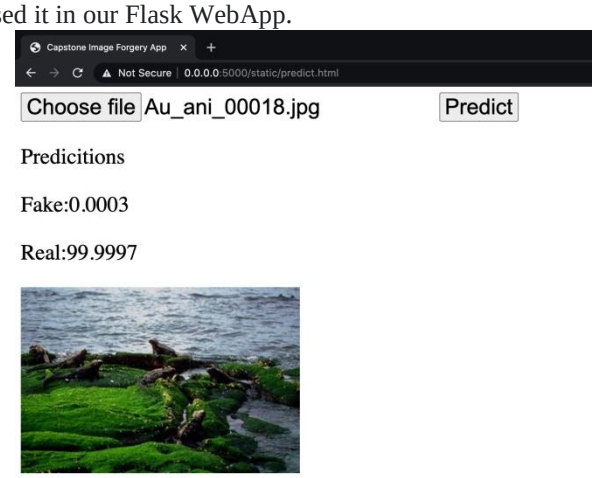

Figure 1: Flask WebApp Demo 2

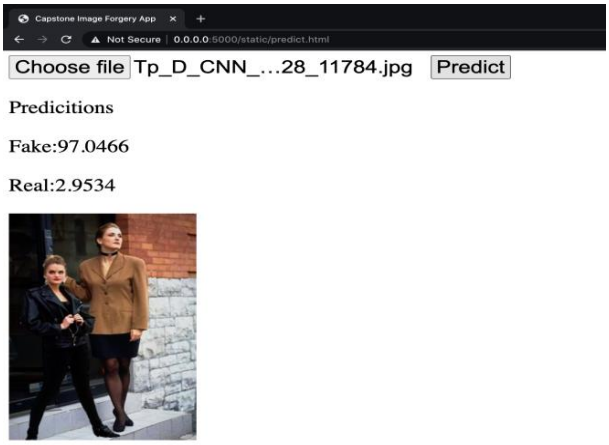

Figure 2: Flask WebApp Demo 2

Thus we can see that the Flask WebApp successfully predicts the authenticity of an image and can be used to differentiate authentic images from tampered images.

V. CONCLUSION

Thus we can use the proposed system to successfully differentiate between images and use relevant information which is communicated from these images. We further used MobileNetV2 for detecting tampered images by using transfer learning and preprocessed the images from CASIA2 dataset using ELA Analysis and we were successful in building another Convolutional Neural Network which was nearly as accurate as with MobileNetV2. Real world application of this project could be further improved by using more advanced dataset and also by using different preprocessing methods which could work on lossless images as well.

REFERENCES

1. Michael Zimba, Sun Xingming "DWT-PCA (EVD) Based Copy-move Image Forgery Detection" International Journal of Digital Content Technology and its Applications. Volume 5, Number 1, January 2011 [CrossRef]

2. Rao, Y., & Ni, J. (2016) "A deep learning approach to detection of splicing and copymove forgeries in images" IEEE International Workshop on Information Forensics and Security (WIFS), 2016 [CrossRef]
3. Andrew G. Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, Hartwig Adam "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications", 2018
4. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., & Chen, L.-C. (2018) "MobileNetV2: Inverted Residuals and Linear Bottlenecks" IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018 [CrossRef]
5. Huynh, T. K., Huynh, K. V., Thuong Le-Tien, & Nguyen "A survey on Image Forgery Detection techniques." The 2015 IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for Future (RIVF), 2015 [CrossRef]
6. Ying Zhang, Jonathan Goh, Lei Lei Win, and Vrizlynn Thing "Image Region Forgery Detection: A Deep Learning Approach" Cyber Security & Intelligence Department, Institute for Infocomm Research, Singapore, 2016
7. Ida BagusKresnaSudiatmika, Fathur Rahman, Trisno, Suyoto " Image forgery detection using error level analysis and deep learning" Magister Teknik Informatika, Universitas Atma Jaya Yogyakarta, Indonesia
8. Amit Doegar, Maitreyee Dutta, Gaurav Kumar "CNN based Image Forgery Detection using pre-trained AlexNet Model" Department of Computer Science and Engineering, NITTTR
9. Yue Wu, Wael Abd-Almageed, and Prem Natarajan "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network" Information Sciences Institute, University of Southern California
10. Yue Wu1, Wael Abd-Almageed, and Prem Natarajan, "BusterNet: Detecting Copy- Move Image Forgery"USC Information Sciences Institute, Marina del Rey

AUTHORS PROFILE

Pranav Sharma, Bachelors of Technology (B.Tech), School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore. Consistently involved in the field of Data Science and Machine Learning. Actively researching about applications of AI in our day to day lives rand strive to inculcate them in quotidian applications. Enrolled in Natural Language Processing, Data Visualization, Data Structures & Algorithms, Machine Learning as part of my academic curriculum. Core Interests: Machine Learning, Deep Learning, Natural Language Processing, Computer Vision. Mail ID- pspranavsharma9@gmail.com

Pooja Santwani, Bachelors of Technology (B.Tech), School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore. Enthusiastic about Computer Vision & Machine Learning and leveraging the use of Deep Learning to solve challenges related to Image Processing. Actively involved in research about Neural Networks and Image Segmentation/Classification. Pursued Data Visualization, Artificial Intelligence and Data Structures & Algorithms as part of my academic curriculum. Core Interests: SAP, Machine Learning, Vanilla Java Script. Mail ID- poojasantwani9@gmail.com

Rachit Narula, B.Tech, School of Computer Science Engineering, Vellore Institute of Technology (VIT), Vellore. Worked extensively on model deployments and creating end to end data pipelines. Developed applications and websites supporting ML models and pipelines. Actively research about Social & Information Networks, Image Processing and Machine Learning models. Pursued Pursued Data Visualization, Artificial Intelligence and Data Structures & Algorithms as part of my academic curriculum. Core Interests: Machine Learning , Android App Development , Java.. Mail ID-vrachit456@gmail.com