

FORGERY IMAGE DETECTION USING NEURAL NETWORK

¹Silpa P M, ¹Aloknath U, ²Divya R V

¹UG Scholar, Department of Computer Science and Engineering,

²Asst.Prof, Department of Computer Science and Engineering,

Dr. APJ Abdul Kalam Technological University, Kerala, India.

ABSTRACT: Digital imaging has experienced tremendous growth in recent decades and computer generated images are employed in many applications. Now a days, several software's are available to manipulate image so the image appear to be as original. Detecting these kinds of forgeries has become significant issue at present. To see whether a digital image is original or doctored may be a big challenge. Forging images and identifying such images are promising research during the digital era. Detection of such fake images is inevitable for the revealing of the image based cybercrimes. There's a necessity for developing techniques to distinguish the computer generated images from the manipulated ones. In this paper, an efficient method based on convolutional neural network (CNN) for the image forensic problem is introduced. The objective of the proposed system is to 1) detect the tampered images using neural network Convolutional Neural Network (CNN), 2) the neural network will learn features of an image and predict whether the given image is real or fake. It enhance the security of image frameworks, by adding assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment.

Keywords: Convolutional Neural Network, Image Forgery Detection, Deep Learning.

I. INTRODUCTION

Digital image forgery has become a widespread phenomenon in today's world. Digital images are easy to control and edit with the assistance of editing software. It possible to feature or remove important features from a picture without leaving any obvious traces of tampering. The detection of image manipulation is essential because a picture can be used as legal evidence, in forensics investigations, and in many other fields. Digital forgery is now horrible to individuals (e.g. fake images of celebrities and public figures), societies, journalism, scientific publication etc. Different types of image forgeries, including copy-move, splicing, and object removal, often implement resampling as part of the forgery workflow. Recently, the interest about deep learning has increased and lots of remarkable results are emerging. Hence, forensic researchers try to apply deep learning to detect the manipulation of images without human intervention. In this paper, an image manipulation detection algorithm using deep learning technology is introduced. The proposed method uses a Convolutional Neural Network (CNN) for feature extraction.

This paper provides a deep-learning method for distinguishing computer enhanced graphics from real photographic images. The CNN, amongst other deep neural networks, have the potential to obtain higher order features automatically and efficiently decrease its complexity and dimensionality. The method make high accuracy predictions on images exhibiting the robustness of the trained model. The problem with existing fake image detection system is that they will be used detect only specific tampering methods like splicing, colouring etc. Active techniques, like watermarking, are proposed to unravel the image authenticity problem, but those techniques have limitations because they require human intervention or specially equipped cameras. Thus an experimental set-up of a neural testing platform is implemented to overcome this limitations. The problem is solved using machine learning and neural network to detect almost all kinds of tampering on images.

II. RELATED WORK

In this paper, an image manipulation detection algorithm using deep learning technology is introduced. This system based on a convolutional neural network (CNN). The convolutional layer is consists of 2 layers having maximum pooling, ReLU activation, and local response normalization. The fully connected layer consists 2 layers. The convolution layer computes the image matrix that are connected to local regions in the input, each computing a dot product between their weights and a small receptive field to which they are connected to in the input. The convolutional layer consists of various combination of convolution, pooling, and activation functions. The computation of convolution in a neural network is a product of a two-dimensional matrix called a kernel or filter matrix. Through this convolution, local features can be extracted. Each computation is used for the extraction of a feature map from the input image. As a result, we will get a single number that represents all the values of the images. This layer is used for filtering which are multiplied by the values outputted by the convolution [3].

Another techniques of subsampling is max pooling. With this technique, the highest pixel value is selected from a region depending on its size. The pooling layer appearing after convolution layer is to pick a pixel value having a particular characteristic among pixels in a very specific region, such as maximum pooling and average pooling. It can be minimized to improve the time performance. However, in aspect of detecting image manipulation, there is a chance to lose important traces to determine the modifications. Through this pooling, the size of input data. The aim of the fully connected layer is to provide the high-level features that are extracted by convolutional layers and combining all the features. It passes the flattened output to the output layer where you use an activation functions to predict the input class label. Once the model is created, images are trained and store them in a list. The neural network model is compiled and predict the accuracy of image and identify the fakeness and realness of loaded image. Here Jupyter Notebook is the platform for system development. The basic image processing functions and feature extractions done by OpenCV and python. The Convolutional Neural Network is constructed by the support of TensorFlow 2.2.0.

III. PROPOSED SYSTEM

In the proposed system, the tampered images are detected using neural network and it can be implemented on Android platform and hence made available to common users. This proposed strategy directs an image manipulation detection algorithm using deep learning technology.

The experimental dataset was used to verify the image forgery detection. Here we have two datasets named as fake and real. Both fake and real image dataset contains 1000 images each. Fake image dataset contains only digitally enhanced images or Google images. Real images contains only computer generated images. Quantitative performance analysis is performed to check the performance of the proposed algorithm. Even with a complex neural network, it is not possible to determine whether an image is fake or not without identifying a common factor across almost all enhanced images. So, instead of giving direct raw pixels to the neural network, it is resized and RGB conversion is done in images. The input image into convolution layer. Choose parameters, apply filters with strides, apply padding if requires. Perform convolution on the image and apply activation functions to the matrix. Then perform pooling to reduce dimensionality size and flatten the output and feed into a fully connected layer (FC Layer) [2].

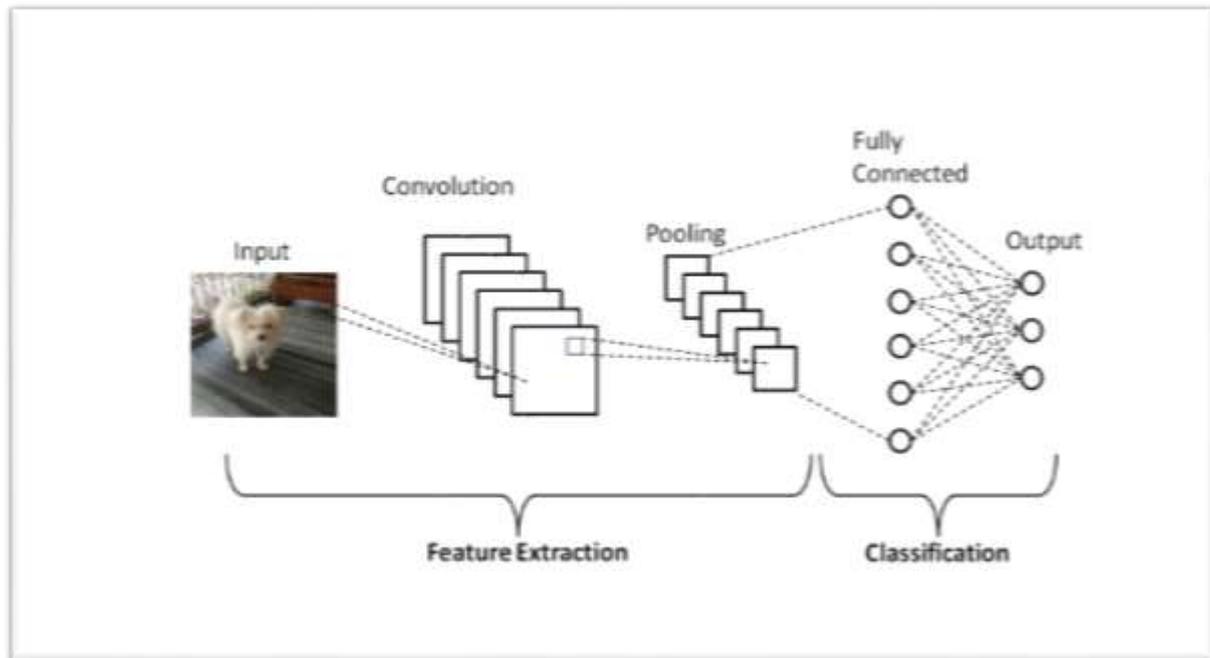


Figure 1. Process in Convolutional Neural Network

The input layer holds the raw input of image with width 32, height 32 and depth 3 and the convolutional layer computes the output volume by computing dot product between all filters and image patch. Activation layer will apply element wise activation function to the output of convolution layer. Some common activation functions are RELU: $\max(0, x)$, Sigmoid: $1 / (1 + e^{-x})$, Tanh, Leaky ReLU, etc. The volume remains unchanged hence output volume will have dimension $32 \times 32 \times 12$. output of convolutional layer is send to the pooling layer. Pool layer is periodically inserted in the convnets and its main function is to reduce the size of volume. There are two types of pooling layers are max pooling and average pooling. Here we use a max pool with 2×2 filters and stride 2, the resultant volume will be of dimension $16 \times 16 \times 12$. After the operation in the ReLU layer the output of this send to the fully connected layer. Which takes input from the previous layer and computes the class stores and outputs the 1-D array of size equal to the number of classes. If the 1-D array stores the value 0 our system will take it as a real image, if the value is 1 our system will take it as a fake image [3].

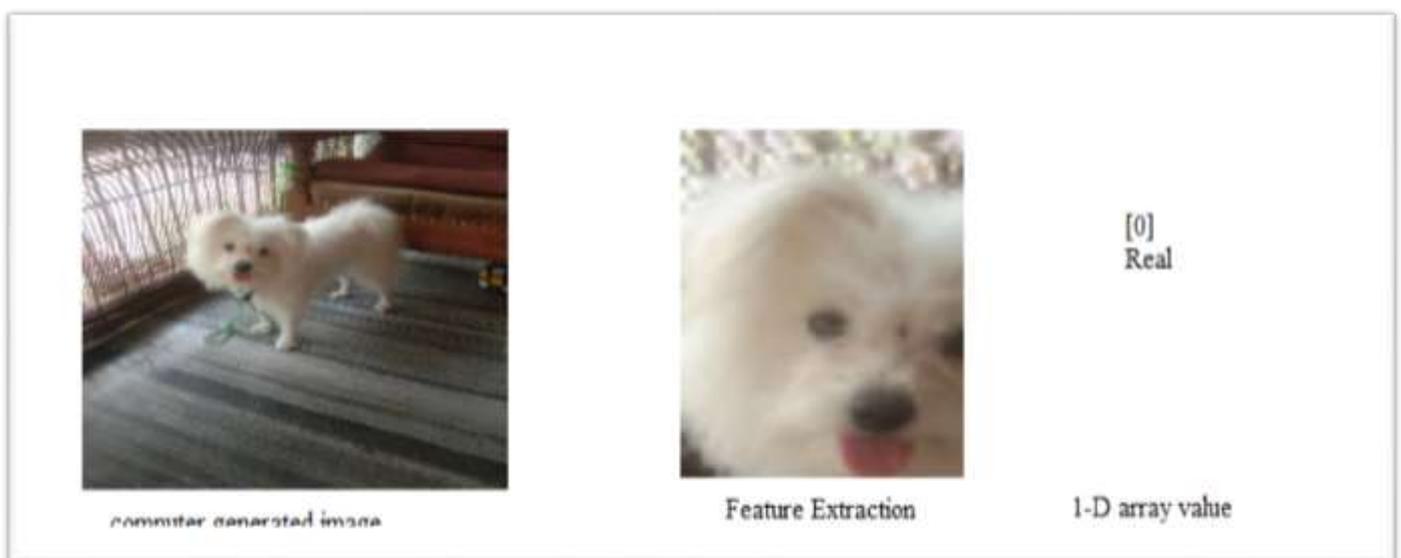


Figure 2: Output of CNN process

IV .CONCLUSSION

Neural network has been successfully trained using the image dataset with 2000 fake and 2000 real images. The trained neural network was able to recognize the image as fake or real at a maximum success rate of 89%. The use of this application in mobile platforms will greatly reduce the spreading of fake images through social media. This project can also be used as a false proof technique in digital authentication, court evidence evaluation etc. By using the results of neural network output a reliable fake image detection program is developed and tested. This system enhance the security of image frameworks, by making assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment.

V. ACKNOWLEDGEMENT

We express our wholehearted thanks to everyone who had contributed to the successful completion of this project. We would like to express deepest appreciation towards our project guide Mrs.Divya RV, Assistant professor in Computer Science and Engineering Department who gave valuable suggestion and guidance for our project. We sincerely thank Dr. Ramani K, Head of the Department, Computer Science and Engineering for providing necessary information regarding the project and also her support in completing it. We also thank our project Co-ordinator, Prof. Jithin Jacob, Computer Science and Engineering Department who gave expert supervision, encouragement and constructive criticism amidst his busy schedule throughout the project. We also grateful to all authors of books and papers which have been referred to publish this paper.

REFERENCES

- [1].R. Salloum, Y. Ren, and C.-C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (MFCN)," *J. Vis. Commun. Image Represent.* vol. 51, pp. 201–209, Feb. 2018.
- [2]. L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering detection and localization through clustering of camera-based CNN features," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jul. 2017, pp. 1855–18.
- [3]. D. Cozzolino and L. Verdoliva, "Camera-based image forgery localization using convolutional neural networks," in *Proc. 26th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2018, pp. 1372–1376.
- [4]. M. Huh, A. Liu, A. Owens, and A. Efros, "Fighting fake news: Image splice detection via learned self-consistency," in *Proc. Eur. Conf. Comput. Vis.*, 2018, pp. 101–117.
- [5]. G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–480, Dec. 2003.
- [6]. F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 1251–1258.
- [7]. K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.
- [8]. 4] Y. Wu, W. Abdalmegeed, and P. Natarajan, "ManTra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features," in *Proc. IEEE/CVF Con f. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 9543–9552.
- [9] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. de Rezende Rocha, "Exposing digital image forgeries by illumination color classification," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1182–1194, Jul. 2013.
- [10]. J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath, and A. K. Roy-Chowdhury, "Hybrid LSTM and encoder–decoder architecture for detection of image forgeries," *IEEE Trans. Image Process.*, vol. 28, no. 7, pp. 3286–3300, Jul. 2019.
- [11]. B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," *Image Vis. Comput.*, vol. 27, no. 10, pp. 1497–1503, Sep. 2009.
- [12]. P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of CFA artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1566–1577, Oct. 2012.
- [13]. S. Ye, Q. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Proc. IEEE Multimedia Expo Int. Conf.*, Jul. 2007, pp. 12–15.
- [14]. T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.
- [15]. M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 74–90, May 2008.
- [16].G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "A Bayesian-MRF approach for PRNU-based image forgery detection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 554–567, 2014.
- [17]. M. Kirchner and J. Fridrich, "on detection of median filtering in digital images," in *Proc. SPIE, Electron. Image. Media Forensics Security*, vol. 7541, pp. 101–112, Oct. 2010.
- [18]. D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5297–5301.
- [19]. S. Lyu and H. Farid, "How realistic is photorealistic?" *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 845–850, Feb. 2005.