Available online at : http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 3, issue 1, pp.826- 830, Dec. -2023
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 **IBI IMPACT FACTOR 1.5** **DOI: 10.53633/IJMASRI**

RESEARCH ARTICLE

IMAGE FORGERY DETECTION

Apurv Jinda

Department of Information Technology, Maharaja Agrasen Institute of Technology, Rohini, Delhi

Abstract

We are living in an age of digital imagery. Everyone's identity in society is also judged by their digital persona. Therefore, digital identities of the people should/need to be protected. With the advancement of image editing tools, creating forged images has become easier. Methods need to be developed to recognise, flag and take action against these forgeries and restore people's faith in the digital content. Traditional methods of forgery detection simply rely on manually flagging content. But with the rise of various softwares such as photoshop, paint etc. using this method to get good results has become very difficult. Also, with the exponential growth of the number of images being uploaded in the cyber space using this method becomes impractical. A reliable method needs to be developed to automate this task.

Keywords: Image Forgery Detection, Machine Learning, CNN

Introduction

In the age of social media there has been a huge increase in the volume of image data generated in the last decade. Use of image (and video) processing softwares to create doctored images and videos is a major concern for politicians, celebrities, well-being of the public and even social networking apps and websites. These images are prime sources of fake news and are often used in malevolent ways such as for mob incitement or to accuse people of malicious behavior. Before action can be taken on the basis of a questionable image, we must verify its authenticity. By verifying if an image has been doctored or not we can prevent false defamations and also protect the social networking websites from getting sued by the above mentioned individual or groups for hosting falsified images.

There are majorly 2 types of image forgery detection techniques which are further divided into various sub-techniques.

Active Forgery Detection

This method is used when the generated image has been encoded with a digital signature, watermark

or some sort of hash value. For this detection technique, hardware information of the digital content's owner is required. These techniques are generally used in the court of law in most of the countries.

Passive Forgery Detection

In this detection technique no additional information is given about the image except the image. These detection techniques are also sometimes called 'blind' detection techniques. The two main types of forgery dependent can be classified as i) copy-move forgery ii) splicing.

These forgeries are difficult to make out from the naked eye.

i) Copy-Move Forgery

Here, the parts of an image are duplicated in the same image. A small section of an image might be copied and pasted into another section in the same image to create this forgery.

ii) **Splicing Forgery**

Here, two or more images are combined together to forge images. Some sections of one image might be cut/copied and pasted onto another image.

Some examples of forged images:

Fig 1: Forged and authentic image of Movistar

Fig. 2 and 3: Edited images of world leaders

Methodology:

Data Collection

The dataset used in this was taken from Kaggle. It hosts the CASIA v1 and v2 Datasets on it. These datasets are divided into two categories. Authentic and tampered. Authentic folder contains all the untampered images, similarly, tampered folder contains all the tampered images.

Some authentic images:

Fig. 4 and 5: Authentic images present in our dataset

Some tampered images:

Fig. 6 and 7: Examples of forged images i our dataset

Data Preprocessing:

First, we create a temporary JPEG of the image with quality nearly equal to the original image. After that we compare the JPEG to the original image. This gives the difference between the two images. The tampered image would have significantly more difference as the edges of the tampered region of the image wouldn't be consistent with the rest of the image.

Fig 8: Raw Image (Authentic)

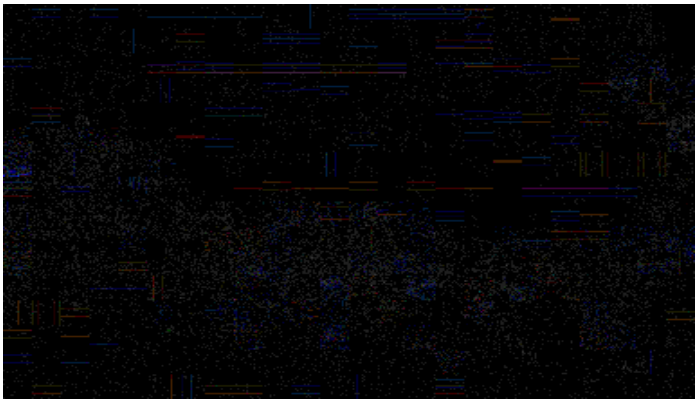

Fig 9: Processed

Fig. 10: Raw Image (Tampered)

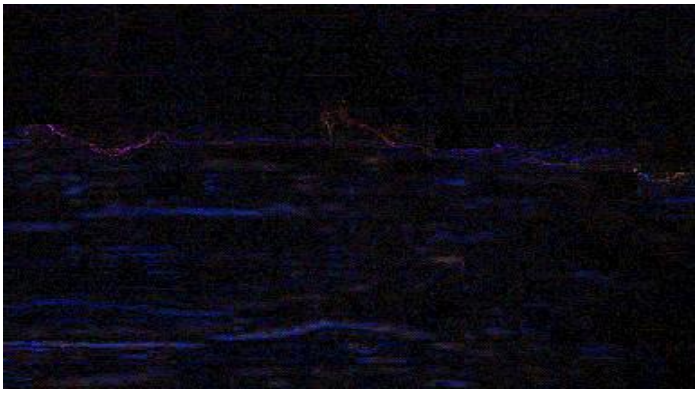

Fig. 11: Processed

These images were stored in an array and categorically given label 1 as authentic and 0 as tampered.

Algorithm

After preprocessing, we used CNN (Convolutional Neural Network) as it would be the best model to take spatial surroundings into consideration and also works best when the image is divided into smaller blocks. The CNN model used had following layers: We used CNN with several layers. They are:

- Conv2D: This layer creates a convolution kernel that is convolved with the layer input to produce a tensor of outputs. We use it with different filters by hyper tuning the parameters model.
- Average Pooling: Averages the pool of matrices. We gave it a size of 2x2.
- Flatten: Converts the array into one dimension.
- Dense: It tells us how dense the relationship would be between the preceding layers.
- Dropout: The Dropout layer is a mask that nullifies the contribution of some neurons towards the next layer and leaves unmodified all others.
- Batch Normalization: Batch Norm is a normalization technique done between the layers of a Neural Network instead of in the raw data. It is done along mini-batches instead of the full data set. It serves to speed up training and use higher learning rates, making learning easier.

Result

My model has a max accuracy of 0.9778 over 30 epochs.

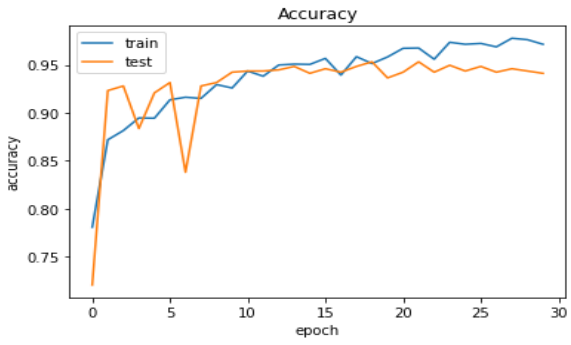

Fig. 12: Plot of accuracy vs epoch

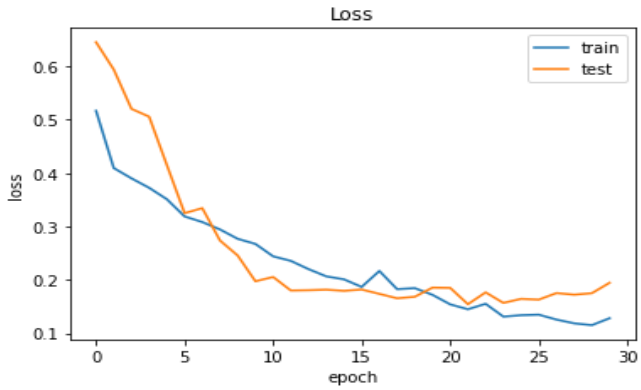

Fig. 13: Plot of Loss vs epoch the confusion matrix obtained was:

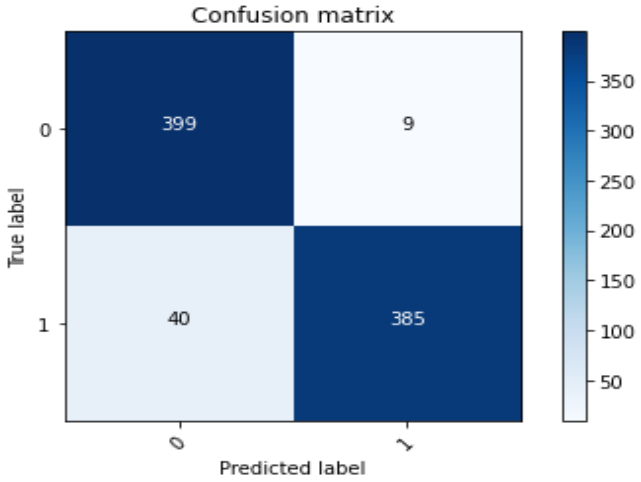

Fig. 14: Confusion matrix

Conclusion:

In the current proposal, we gave a model to detect image forgery. Proposed method was applied on the given dataset and found to be fairly accurate with minimal losses.

References:

1. Passive Image forgery detection using DCT and binary pattern. https://link.springer.com/article/10.1007/s11760-016-0899-0.
2. Image forgery detection based on statistical features of block dct coefficients by Shilpa et al. https://www.sciencedirect.com/science/article/pii/S1877050920310048

3. A novel forgery detection algorithm based on mantissa distribution in digital images by Arman et al. https://ieeexplore.ieee.org/document/9349611
4. A passive blind approach for image splicing detection based on dwt and lbp histograms by Mandeep et al. https://link.springer.com/chapter/10.1007/978-981-10-2738-3_27.
5. A robust forgery detection method for copy–move and splicing attacks in images by Mohammad et al. https://www.mdpi.com/2079-9292/9/9/1500.
6. Digital image forgery types and its methods by C. RajaLakshman https://www.iraj.in/journal/journal_file/journal_pdf/3-554-156136845314-18.pdf.
7. Birajdar, G.K and Mankar, V.H. (2013). Digital image forgery detection using passive techniques: a survey. Digit Investig. 2013;10(3):226–245.
8. Ali, M and Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. Signal Process Image Commun. 2015; 39:46–74.
9. Mahmood, T., Nawaz, T. Ashraf, R. Shah, M. Khan, Z. Irtaza, A and Mehmood, Z. (2015). A survey on block-based copy move image forgery detection techniques. International Conference on Emerging Technologies (ICET), 2015.
10. Thirunavukkarasu, V., Kumar, J.S. Chae, G.S and Kishorkumar, J. (2017). Non-intrusive forensic detection method using DSWT with reduced feature set for copy-move image. Wirel Pers Commun. 2017:1–19. https://doi.org/10.1007/s11277-016- 3941-1.
11. Redi, J.A., Taktak, W and Dugelay, J.L. (2011). "Digital image forensics: a booklet for beginners," Multimedia Tools and Applications, vol. 51, no. 1, pp. 133–162, 2011.
12. Kaushal, V., Garg, B. Jaiswal, A. Sharma, G.K (2015). Energy aware computation driven approximate DCT architecture for image processing. In: Proceedings of 28th International Conference on VLSI Design and 14th International Conference on embedded systems, pp. 357–362 (2015)
13. Mahmood, T., Mahmood, Z. Shah, M. Saba, T. (2018). A robust technique for copy–moves forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. J. Vis. Commun. Image Represent. 53, 202–214 (2018).
14. Kanan, C., Cottrell, G.W. (2012). Color-to-grayscale: does the method matter in image recognition. PLoS ONE 7(1), 1–7 (2012).
15. Parveen, A., Khan, Z.H. Ahmad, S.N. (2018). Identification of the Forged Images using Image Forensic Tools. In Proceedings of 2nd International Conference on Communication and Computing Systems, CRC-Press, Taylor and Francis (2018)

*****