International Journal of Advanced Technology in Engineering and Science
Vol. No. 09, Issue No. 12, December 2021
www.ijates.com
ijates
ISSN 2348 - 7550

IMAGE MORPHING DETECTOR

1) Bharani K , 2) Bharath G, 3) Kishore R 4) Ms. Divya P

[1,2,3,] *Computer Science Engineering, Bannari Amman Institute of Technology, Sathyamangalam*

[4.] *Assistant Pr ofessor, Computer Science Engineering,*

Bannari Amman Institute of Technology, Sathyamangalam

Abstract

Photos are one of the most prevalent ways of media sharing on social media among users. Therefore, the monitoring of images found in social media is important. It has now become possible for individuals and small communities to create and widely disseminate these photos in a very short period, threatening the credibility of the news and public confidence in the means of social communication. Also, due to the large increase in population size, nowadays ID proofs like the Aadhaar card, Voter ID, etc. are verified automatedly. This may increase the possibility of submission of fake/doctored ID proofs and get approval. Likewise, forged images can also be submitted in court as proof. This may lead to the punishment of an innocent person or a guilty person may escape from punishment.

Keywords *– LSTM algorithm, VGG-16 network, CNN network, splicing mechanism, copy-move mechanism.*

1. Introduction

In this project, deep learning will be used to predict if an image is manipulated or not and the parts of the image where any kind of manipulation has been performed will be shown. The kind of manipulation will also be provided as an output along with the mask of tampered parts. Through this project the problem of detecting image forgery on digital images will be solved which is used to spread false news on social media platforms, used in manipulation of documents, manipulation of identity proofs which can lead to identity theft, etc. Detection of false news on social media platforms allows the administrators to take quick action by removing the particular image from spreading further. Using it in the court of law helps in identifying if people are submitting valid proofs or not. The benefits of integrating such an application in different places in our society has been the motivation to develop this project.

2. Modules

2.1. Data Preprocessing

In this module, we take the images from the CASIA dataset and perform pre-processing to obtain the types of manipulations, bounding box coordinates and ground truth mask for training the model. Bounding box is found from the ground truth mask. The dataset contains class labels as “Authentic” or “Tampered” which helps in training the classification model.

Pseudocode:

For each image:

Read AuthenticImage

Read TamperedImage

Convert both images to grayscale

Mask = AuthenticImage – TamperedImage

Save the generated mask

Generate contour for the mask

Save the contour

Generate bounding box coordinates for each image

End For

2.2. Neural Network

Here, a fully convolutional neural network will be developed which will be able to handle images of different dimensions along with identifying different types of known forgery types like copy-move, splicing, removal, enhancement, and other types. The network consists of two parts: first is the image manipulation trace feature extractor, and second is the local anomaly detection network.

Pseudocode:

- Create Bayar Convolutional layer
- Create SRM Convolutional Layer
- Create Conv2D layer with 5x5x10 filter
- Concatenate all the 3 outputs
- Create 10 Convolution layers with ReLU Activation function
- Perform 1x1 Convolution on output of previous step
- Perform BatchNormalization
- Perform ZPooling and pass the output to Conv2DLSTM layer.
- Perform 1x1x7 Convolution

2.3. Website to Check for Forgery

In this module, firstly, a website will be developed which will enable the users to upload an image from their local computers to the website. After the image has been uploaded, it will be tested by the Neural Network which will then generate the results that shows parts of the image that have been tampered in white while the original parts will remain black i.e., a mask will be presented to the user. In order to test the input image on the website, the neural network model will be integrated with the website in the backend.

3.Analysis and Design

The aim of the proposed system is to detect if an image is tampered or not, and detect the regions of tampering, if any. This is done by first taking an input image and uploading it to the website. The website submits the input image to the backend where the trained convolutional neural network is present. The CNN model is trained by passing tampered images as the input and the ground truth mask as the output. The model applies various filters based on the layers added to predict the mask. In each iteration, the loss value is calculated which is back

propagated to update the filters. The trained model is saved to be used in the website backend.The image is passed into the model in order to get the output mask which marks the tampered regions in a lighter colour. After processing, the input image and the predicted mask are displayed back to the user on the website.The proposed system consists of a website to upload tampered images and display the output,a CNN model that localises the regions of tampering, and a python backend that connects the website to the CNN model.

4. Architecture/Workflow

4.1 Neural Network

A deep neural network which will show the localized mask of the manipulated region. It first extracts image manipulation trace features for a testing image, and identifies anomalous regions by assessing how different a local feature is from its reference features. There are 2 networks here: the image manipulation trace feature extractor and deep anomaly detection.

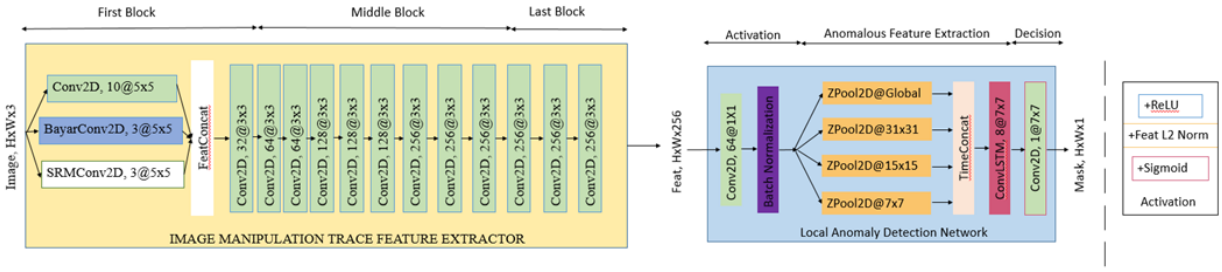


Fig. 1. Architecture of the Convolutional Neural Network

The backbone of the architecture is the VGG-16 network. An inception network is created with 3 different convolutional filters. The inception stack is then passed onto this VGG-16 network. Then we apply a 1x1 convolution filter and then apply Z-pooling. This is passed onto the ConvLSTM network.

4.2. Application Architecture

A website where users can upload an image. This image will be passed through the neural network and will check if that image has been manipulated or not.

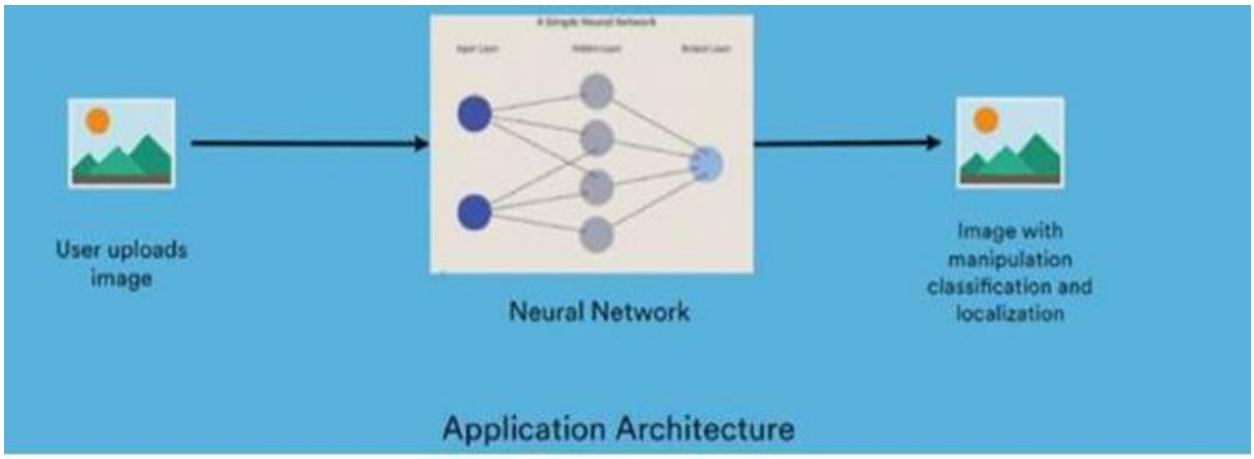
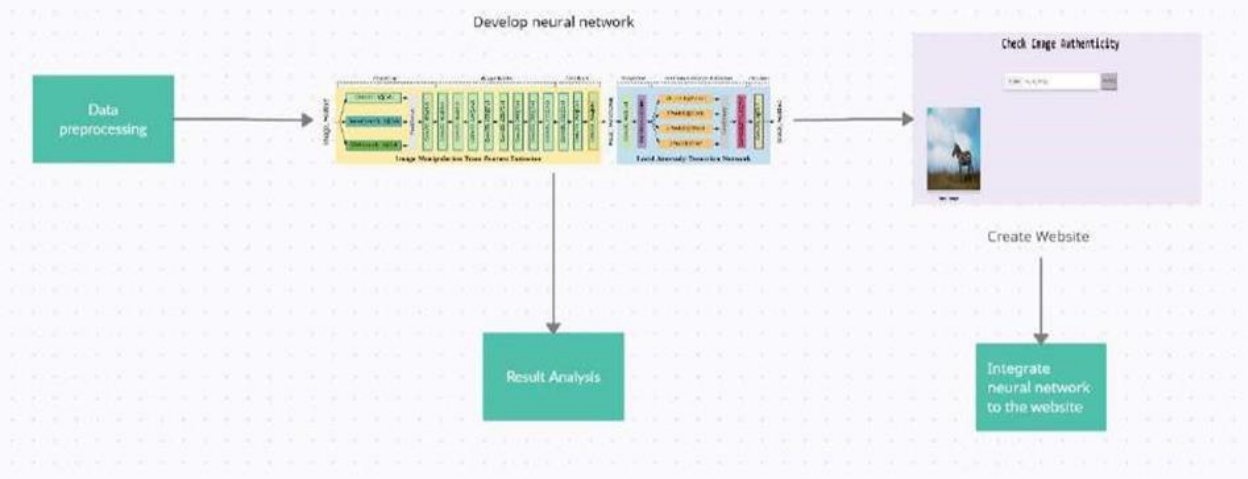


Fig. 1. Architecture of the Application

4.3Workflow Diagram

The workflow diagram below divides the entire project into separate modules which are being worked upon and are then combined to get the final results.



5. Literature Survey

In the field of image forensics, there are many types of manipulations like copy-move, splicing, removal etc. Over the years many methods have been proposed to detect manipulations. Before the rise of neural networks, researchers were trying to utilize the JPEG compression algorithm [1,2] to detect whether an image is manipulated or not. One such method is error level analysis [1]. But this method would work only on JPEG images and was able to detect only one or two types of manipulations.

The authors of [3] have proposed a methodology which performs detection of splicing and copy-move forgery at the same time using the statistical properties of the AC components of the block DCT coefficients and the changes that occur in them. The authors of [4] have worked on only copy-move image forgery as it is the most common type of forgery and is very easy to forge. The proposed method involves using the Gaussian-Hermite moments. The RANSAC algorithm is used to filter the outliers from the inliers by taking into account scaling. The evaluation is done at both the pixel-level and the image-level.

6. RESULTS AND DISCUSSION

The data preprocessing was performed successfully on the CASIA dataset and the ground truth mask was generated and saved for each pair of original and tampered images. Afterpre-processing, the CNN model was trained to detect image forgery. The tampered image and the corresponding ground truth masks were used to train the model. The layers that were added to the model made sure that the dimensions of the input and output image remain the same.

7. Accuracy and F1 Score

The accuracy and the F1-score are calculated by comparing the ground truth masks with the predicted masks. These results are obtained by comparing both the images pixel-wise to see if the pixel is classified correctly or not. The comparisons are done after applying image thresholding to the predicted mask in order to get better

results. On the CASIA dataset, we obtained an accuracy of approximately 88.5% while the F1-score came out to be 0.33. These were the best results that we obtained by applying different thresholds to the predicted mask.

8. ADVANTAGE AND DISADVANTAGE:

Advantages

- Through this project,the problem of detecting image forgery on digital images will be solved, which is used to spread false news on social media platforms, used in manipulation of documents, manipulation of identity proofs which can lead to identity theft, etc.
- Forged images can also be submitted in court as proof. This may lead to the punishment of an innocent person or a guilty person may escape from punishment. Using it in the court of law helps in identifying if people are submitting valid proofs or not.
- We can prevent the possibility of submission of fake/doctored ID proofs .

Disadvantage:

- This project doesn't give 100% accurate results.
- Needs GPU for faster processing while running on localhost.

9. Conclusion

In this project, we have used the deep-learning method of Convolutional Neural Networks to train a model that can detect and highlight the areas of an image that are forged. These forgeries can belong to different classes and the model is trained to detect all of them. The model applies various filters to the base image in order to apply manipulations that can generate the desired output mask highlighting the regions of forgery. The experimental tests were performed on the CASIA dataset which is a commonly used dataset for detecting image forgeries. The model marks the forged parts in a brighter colour while the original parts remain dark. Along with this, the mask of an image with dimensions 384x256 can be generated within 7-8 seconds. The performance can be drastically improved if GPU support is enabled when using the TensorFlow library as GPUs have a higher memory bandwidth and number of cores, but consume a lot more power than CPUs. This will further allow the model to be trained on new datasets and calculating the accuracies of the models.

References

[1].Huang, DY., Huang, CN., Hu, WC. et al. Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimed Tools Appl 76, 1509–1530 (2017).

[2].S.Devi Mahalakshmi, K.Vijayalakshmi, S.Priyadarshini, Digital image forgery detection and estimation by exploring basic image manipulations(2017)

[3]Shilpa Dua, Jyotsna Singh, Harish Parthasarathy, Image forgery detection based on statistical features of block DCT coefficients,Volume 171,(2020)

[4]. Hui-Yu Huang & Ai-Jhen Ciou Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation (2019)