Geometrical Attack Classification using DCNN and Forgery Localization using Machine Learning

Abhishek Thakur, Neeru Jindal

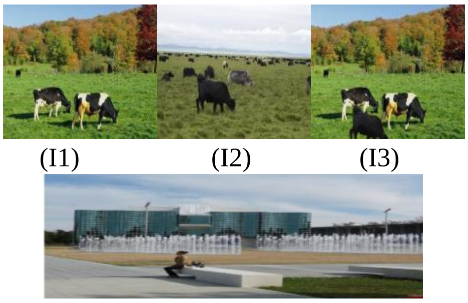
Abstract: ***Manipulation of images is frequently happening nowadays for false propaganda and also for illegal advantage. Only the manipulation of images are not sufficient as an evidence. These are considered only after valuable forensic investigation. The most common forgeries are copy move and splicing. It is very important to detect the realness of digital images which cause a grave threat to the society. This paper is about copy move, splicing forgery classification of various geometrical attacks. The deep convolution neural network is used to classify images into forged or not forged and also classify which type of forgery is present.***

Keywords: Image Forensics (IF), Deep Learning (DL), Convolution Neural Network (CNN), Color Illumination (CI), Copy-move Forgery (CMF), Splicing Forgery (SF).

I. INTRODUCTION

Nowadays digital camera is available in the market at very low cost, resulting in more usage of digital images on the social network. These images are downloaded and modified by onlookers with user- friendly software. It becomes very easy to modify these images and create false propaganda. In some cases, such images are created as proof during some legal hearing. But these images are only considered after forensic investigation [1]. The detection and localization of these types of forgery are a vital problem. Therefore, in order to make the forensic investigation more trustworthy, so we require an active research for value addition.

Copy-move forgery (CMF) and splicing forgery (SF) are created very easily, but it is very difficult to detect these type of forgeries. In CMF and SF some part of the image is copied and pasted on the other part. These forged images hide some useful information. These forgeries are created to spread false propaganda. In CMF copied object is from the same image, whereas in SF copied object is from multiple images. The main reason to create CMF is to hide useful information and create false propaganda [2]. Image splicing is the type of forgery in which two images are merged into a single image. In this type of image forgery items are composed from more than one picture.



(I1) (I2) (I3)

(I4)

Figure 1.Original images (I1), (I2). Spliced image (I3). Copy move forged image (I4).

Figure 1 depicts the splicing forgery in (I3) and CMF in (I4). Some objects from one image (I2) are copied and pasted on the other image (I1) which give the spliced image in (I3). In Figure 1 (I4) some objects from one location are copied and pasted to another location on the same image.

The novelty of this work is to develop the Deep Convolution Neural Network (DCNN) for the classification of forged or authentic images and also classify types of forgery as Copy-Move Forgery (CMF) and Splicing forgery (SF).

The rest of this paper is structured as follows. Section two is divided into two parts: first part is a classification of authentic and forged, second part is a classification between CMF and SF. In section three CMF attacks (JPEG, Scale and Rotation) classification is covered. Section four concludes the paper by highlighting the salient features of DCNN.

II. FORGERY CLASSIFICATION

The DCNN model is used for forgery classification [3]. The main reason to use classification in the first part is that there are a number of images on the internet and how to find which one is authentic or forged. This DCNN algorithm is utilized to classify authentic and forged images. This algorithm further classifies types of forgery, such as CMF and SF. This algorithm saves time which is the major advantage to use classification first.

Revised Manuscript Received on Janurary 25, 2019.

Abhishek Thakur,Department of Electronics and Communication, Thapar Institute of Engineering and Information Technology, Patiala, Punjab, India.

Neeru Jindal,Department of Electronics and Communication, Thapar Institute of Engineering and Information Technology, Patiala, Punjab, India.

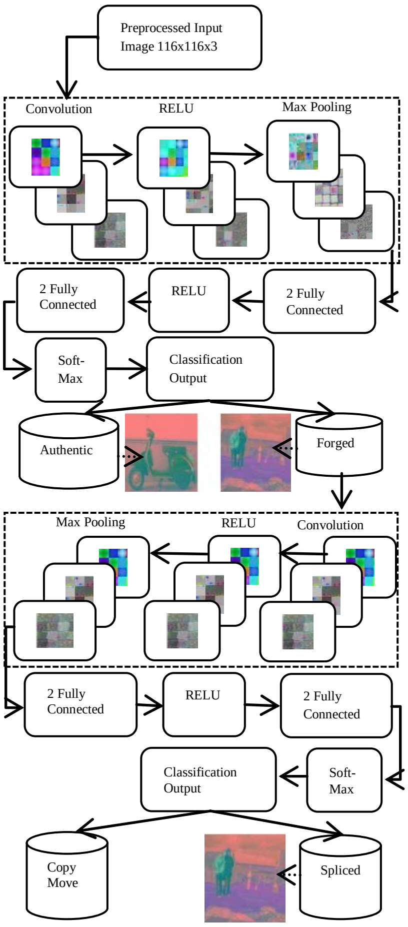


Figure 2. Block diagram of forgery classification using DCNN model and forgery localization using machine learning based Color Illumination method.

2.1 Forgery classification algorithm

In this paper the emphasis is given on copy- move, splicing image forgery classification of CMF under various geometrical attacks using DCNN method.

The major steps of the proposed forgery classification algorithm are given below.

2.1.1 Image preprocessing:

In this step all the images are resized and labeled into proper size (116×116×3). Color illumination [2] is applied to all the images. This step transforming an RGB image into identical blocks and illuminant maps, in order to detect sharp edges and traces in geometrical attacks.

2.1.2 Prepare training and validation dataset:

First step is to create two categories such as forged and authentic. In these two categories, copy-move and spliced images are placed. The CASIA-1 [5], CASIA-2 [5], DVMM [6], CoMoFoD [4] dataset of copy move and splicing are used to perform experiments. All these datasets are arranged in the proper size and labels. In the second step color information and category labels are extracted to generate training and validation dataset. This dataset is divided into authentic and forged categories (70% for training and 30% for validation).

2.1.3 Setup for CNN:

To create Convolution Neural Network [7] (CNN) input layer is taken with no data augmentation. The convolution layer has 32 filters of 5×5×3, the stride of one pixel and padding of four pixels. This network has RELU layer, max pooling layer with a 5x5 filter with a stride of two pixels. These layers create a CNN model for training.

2.1.4 Setup for Deep CNN:

Deep Convolution Neural Network (DCNN) is nothing but multiple layers of convolution, RELU and max pooling. In this step multiple convolution layer, RELU layers and max pooling layers are added. The max pooling layer has 5×5 filter with stride of two picture elements. These layers reduce the size of the image.

2.1.5 Setup for Fully Connected Layers:

Output categories decide the number of output neurons. In this experiment two categories are classified, therefore, fully connected layer is defined with two output neurons. Soft max loss layer is applied to cut the loss. Classification layer classifies the output categories. These layer learn the characteristic of the output classes with the help of updated network weights. These weights are updated by the loss function in training.

2.1.6 Train the Model:

The DCNN model is trained with the given dataset using training options. This training option consists of parameters such as stochastic gradient descent with momentum, initial learn rate, learn rate schedule, piecewise, drop factor, drop period, L2 regularization, maximum size of epochs, minimum batch size and verbose. These parameters are tuned to get good accuracy. The DCNN model is trained with these parameters. The first layer of the DCNN model is an image input of size 116x116x3 images with 'zero center' normalization. The second layer of the DCNN model is convolution which consists of 32 filters of size 5x5x3 with a stride [1 1] and padding [4 4 4 4]. The third layer of the DCNN model is ReLU-1. The fourth layer of the DCNN model is Max Pooling of 5x5 block with a stride [2 2] and padding [0 0 0 0]. The fifth layer is second convolution which consists of 64 filters of size 5x5x32 with a stride [1 1] and padding [4 4 4 4]. The sixth layer is ReLU-2. The seventh layer is max pooling of 5x5 block with a stride [2 2] and padding [0 0 0 0]. The eighth layer of DCNN model is third convolution which consists of 64 filters of size 5x5x64 with a stride [1 1] and padding [2 2 2 2]. The ninth layer is ReLU-3. The tenth layer is max pooling of 3x3 block with a stride [2 2] and padding [0 0 0 0]. The output of the input image across each layer is shown in Figure 3.

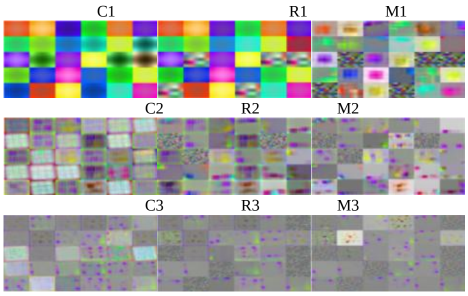


Figure 3. Feature extraction in Convolution, RELU and Max Pooling layers of DCNN model. C1, C2 and C3 represent Convolution layers. R1, R2 and R3 represent RELU layers. M1, M2 and M3 represent Max Pooling layers.

The 11th layer of the DCNN model is fully connected layer. The 12th layer is ReLU-4. The 13th layer is fully connected layer. The 14th layer is soft max. The 15th layer is the classification output with classes 'Authentic' and 'Forged'.

2.1.7 Validate the Model:

The trained model is validated with 30% of unseen images. These images are not present in the training phase. All these images are new for the model. To overcome under fit and over fit problem the equal proportion of each category images should be given to train the model. The training and validation of the DCNN model are performed on Dell, Intel fifth generation i7 processor of clock speed 2.4 gigabytes per second with 8 gigabyte of random access memory, NVIDIA graphic card of 4 gigabyte which is CUDA capable. The MATLAB software is used for the computation, training and validation of the DCNN network. The training time is very large and we have computed the time and curacy of 200 epochs with the number of iterations. Figure 4 shows the training process for CASIA-1.

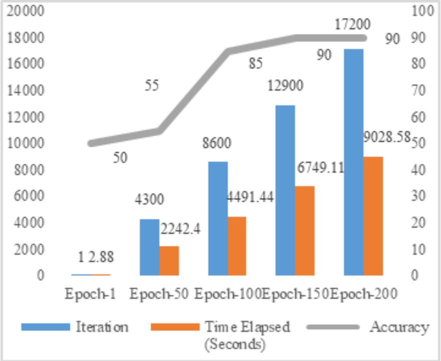


Figure 4.Bar graph of CASIA-1 training.

In CASIA-1 dataset 800 authentic images and 921 spliced images are given for training. The bar graph shown in figure 4 of CASIA-1 depicts the accuracy, iteration and time elapsed of the training process. The average accuracy achieved on the training data set is 97.26. We have 15/516 wrong classifications. The average accuracy on validation set is 0.9735.

Figure 5 depicts the training for the CASIA-2 dataset. In this dataset 7437 authentic images and 1638 spliced images are given for training. The bar graph of CASIA-2 shown in figure 5 depicts the accuracy, iteration and time elapsed of the training process. The average accuracy achieved on the training data set is 97.67. The average accuracy on the validation set is 97.93.

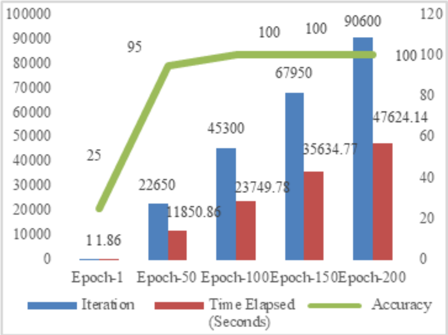


Figure 5.Bar graph of CASIA-2 training.

2.1.8 Classify correct categories as Authentic and forged:

The classification output is obtained into two categories as authentic or forged. Figure 6 depicts the output of the wrong classification results. In this experiment 79/2722 wrong classifications detected whereas 2643/2722 are correct classification detected.

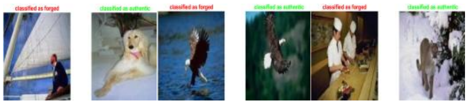


Figure 6.Wrong prediction during validation of DCNN model into two categories Authentic and Forged.

Using the forged image category the dataset is created into two categories as copy move and splicing. These two categories are preprocessed with geometrical attacks and applied for training and validation. The main reason to preprocess these images with geometrical attack is to increase data and test system for robustness.

2.2 Geometric Attacks Classification

2.2.1 Prepare Transfer Learning Dataset:

In this step forged images of copy move and splicing categories with various geometric attacks is collected from different dataset. The rotation and Scaling attacks are applied on CASIA-1[5], CASIA-2[5], CoMoFoD[4] and DVMM[6] datasets. The color information is extracted and all the images are passed through color illumination for better detection of edges [2]. The dataset is labeled into two categories as copy move and splicing. All the images are resized into the same size and channels. Then training and validation dataset is generated. This image dataset with Copy Move and Spliced Categories (80% for Training and 20% for validation) is given for our model.

2.2.2 Repeat steps 2.1.3, 4, 5, 6, 7:

In these steps all the process remains same. After these steps our system correctly classifies the type of forgery. In this phase of classification process is switched from small dataset to large dataset. There is the need for high speed processing so we changed our machine. As we can see from figure 4, 5 the epoch and iteration are less, but the time taken to complete the task is more. In this phase training is performed on Intel i7 CPU of base speed 2.90 GHz with 16 GB of RAM, two 1070 STRIX NVIDIA graphic cards of 8 GB each CUDA capable. The MATLAB software is used for the computation, training and validation of the DCNN network. In this software different MATLAB deep learning toolbox is used.

2.2.3 Classification of CM and SP images:

The classification of copy move and splicing images with scaling attack and rotation attack achieved good training and validation accuracy. The classification of copy move and splicing images are shown in figure 7, 9.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

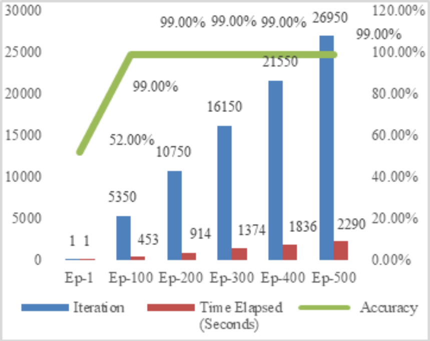


Figure 7.The training process, bar graph on copy move and splicing images under scale attack.

Figure 8 depicts the training plot between Accuracy v's Iteration and Loss v's Iteration on copy move and splicing images under scale attack. The total 2802 spliced images and 2658 copy move images under scale attack are given for training. The bar graph shown in figure 7 of scale attack depicts the accuracy, iteration and time elapsed of the training process. The average accuracy achieved on the training data set is 97.86 in which 96/4368 wrong classifications predicted. The average accuracy on the validation set is 97.86 in which 24/1092 wrong classifications predicted.

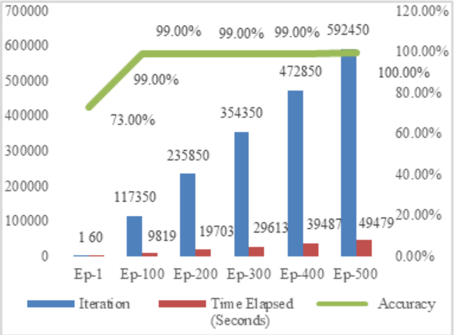


Figure 8. Training plot between Accuracy v's Iteration and Loss v's Iteration on copy move and splicing images under scale attack.

The training graph between iteration v's accuracy of CM and SP images under rotation attack is shown in figure 10. The total 86508 spliced images and 32028 copy move images under rotation attack are given for training. The bar graph shown in figure 9 of ROTATION attack depicts the accuracy, iteration and time elapsed of the training process. The average accuracy achieved on the training data set is 99.23 in which 827/94828 wrong classifications predicted. The average accuracy on the validation set is 99.29 in which 210/23708 wrong classifications predicted.

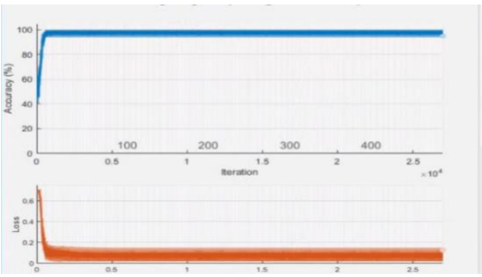


Figure 9.Training on copy move and spliced images under rotation attack.

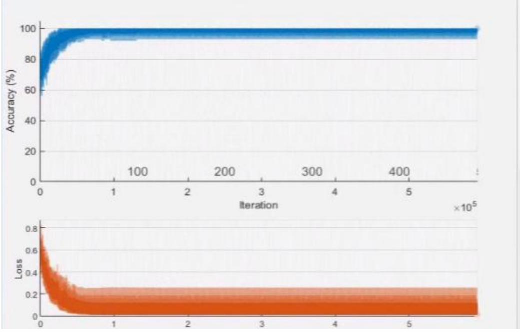


Figure 10.Training plot between Accuracy v's Iteration and Loss v's Iteration on CM and SP images under ROTATION attack.

III. FORGERY LOCALIZATION

Copy move forgery and splicing forgery localization is carried out using machine learning based method. The following steps are given below:

3.1 Data preprocessing:

In this step all the images are applied to color illumination algorithm. This algorithm change image color formation as described in [2].

3.2 SIFT feature extraction:

In this step all the color illuminated images are processed using SLICO algorithm which divide image into blocks. SIFT feature detector is used to detect features of each blocks. These detected SIFT features are matched throughout image using sliding window. If the SIFT features match with other block in the same image, then these extracted pixels are set to one otherwise set to zero. With the help of morphological operation forged regions are highlighted with white color. Figure 11 and 12 shows the copy move forgery detection results.

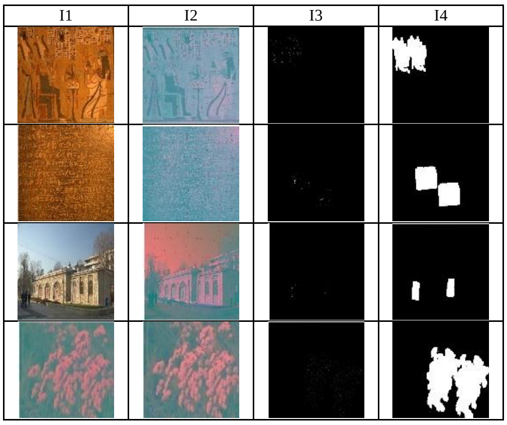
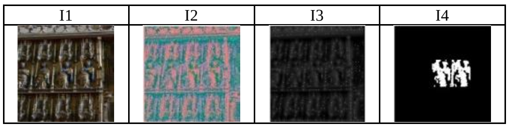


Figure 11.Copy-move forgery detection.I1-Forged Image, I2-Color Illuminated Image, I3-SIFT Feature and I4-Detected Forgery for dataset [4].



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

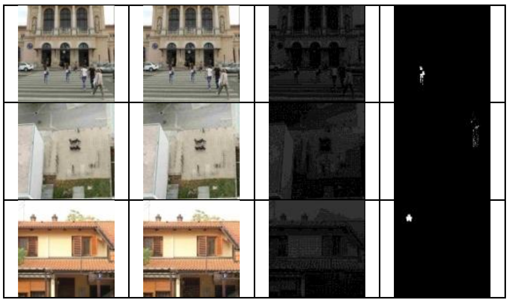


Figure 12.Copy-move forgery detection.I1-Forged Image, I2-Color Illuminated Image, I3-SIFT Feature and I4-Detected Forgery.

Splicing forgery detection results are shown in figure 13 and 14. In figure 13 forged image is shown in first column, authentic image in second column and detected forgery is shown in third column.

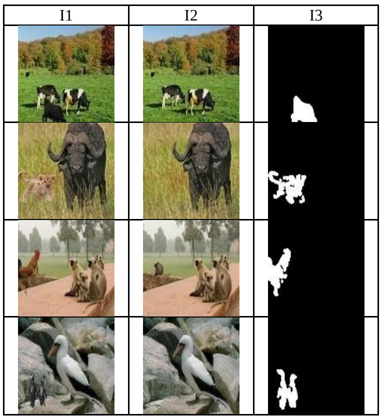


Figure 13.Splicing forgery detection.I1-Forged Image, I2-Original Image, I3-Detected Forgery for dataset [5].

Figure 14 shows the results for splicing forgery detection. In this machine learning based saliency algorithm is used for image forgery localization. In figure 14 forged image is shown in first column, authentic image in second column and detected forgery is shown in third column.

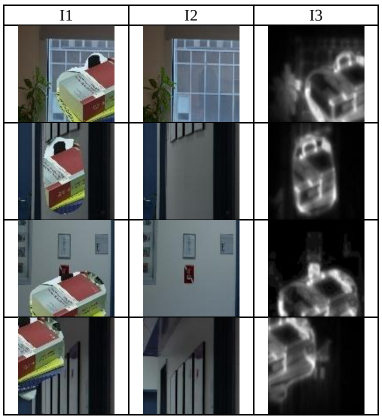


Figure 14.Splicing forgery detection.I1-Forged Image, I2-Original Image, I3-Detected Forgery for dataset [6].

IV. CONCLUSION

In this paper DCNN model is used to classify between forged and authentic image categories, copy move and splicing image categories and copy move and splicing image categories with different attacks. The DCNN model consist of multiple layers of hidden neurons, which share weights to learn the features and classify image categories automatically. From experiment, it is clear that if we train DCNN model with large dataset of these categories its performance improve from 90% to 99%. The classification accuracy between Authentic and Forged for the training data set is 97.26% and for validation set is 97.67%. The classification accuracy between Copy Move and Spliced for the training data set is 99.23 % and for validation set is 99.29 %.

REFERENCES

1. T.J. Carvalho, C. Riess, E. Angelopoulou, E. Pedrini, H., & A., Rocha, IEEE Transactions on Information Forensics and Security, Exposing Digital Image Forgeries by Illumination Color Classification, (2013); 8:1182-1194.
2. A. Thakur, & N. Jindal, Multimedia Tools and Application, Image Forensics Using Color Illumination, Block and Key Point Based Approach, (2018); 77: 26033.
3. C.S. Prakash, A. Kumar, S. Maheshkar et al., Multimedia Tools and Application, An integrated method of copy-move and splicing for image forgery detection, (2018).
4. D. Tralic, I. Zupancic, S. Grgic, M. Grgic, 55th International Symposium ELMAR, CoMoFoD - New Database for Copy Move Forgery Detection, (2013); 49-54.
5. P. Gao, H. Zhang, R. Guo, J. Liu, L. Ma, J. Zhang and Q. He., National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, CASIA Image Tempering Detection Evaluation Database (CAISA TIDE) V1.0 and v2.0, http://forensics.idealtest.org.
6. A. Nadig and W. Harwell George et al., DVMM Laboratory of Columbia University, Columbia Image Splicing Detection Evaluation Dataset, http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm.
7. Y. Rao, J. Ni. A., IEEE Int. Workshop on Information Forensics and Security, Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images, (2016).

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication