DEEP LEARNING APPROACH FOR MANIPULATED IMAGE REGION LOCALIZATION USING CONVOLUTION NEURAL NETWORK

C.Rajalakshmi[1] Dr.M.Germanus Alex[2] Dr.R.Balasubramanian[3]

1. Research scholar Roll No:12332, Dept. of Computer science, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli 627012,Tamil Nadu, India.
2. Prof &Head, Dept. of Computer science,Government Arts College, Nagercoil.
3. Prof &Head, Dept. of Computer Science & Engg., Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli 627012

Abstract

When creating a forgery, a forger can modify an image using many different images editing process. In recent year, localization of forgery region has attracted more and more attention and many forensic methods have been proposed for identifying such image forensic operation. Up to now, most existing methods are designed for just forgery detection task but the most challenging task in digital image forensics is the localization of image forgery. In this paper, we proposed a new Convolution Newel Network (CNN) based method to locate the region of any type of forgery that made in an image. The extensive results show that the proposed method is a better alternative for recent forgery localization methods. Numerous experiments are conducted in the test images to prove the effectiveness and efficiency of the proposed method in detecting image forgery localization.

Key words

Image forensic, Image processing, Convolution, localization, Neural network.

I Introduction

With the rapid development of image processing technology, it is much easier to modify digital image without leaving any perceptible artefacts than ever before. Nowadays, the abuse of tampered images would lead to many potential serious moral, ethical and legal problems. Therefore, image forensics has attracted increasing attention.With free access to tools like GIMP (GNU image manipulation program) and an internet full of free resources, the use and abuse of photo editing software has exploded. Humorously doctored images are spread across image board and email inboxes while politically charged forgeries get blasted as new article headlines. With images being used to make decisions with heavy consequences, there exists a clear need for reliable forgery detection methods [1][6][7][28]. Within the realm of digital image forgery detection there exist many methods.

In practical forensic application, we are more interested in figuring out the tampered regions compared to forgery detection. Forgery localization becomes an important issue in image forensics. The different approaches have their own advantages and short comings, in localization of manipulated data depends on the type of detection and the method of forgery [4]. Over the past several years, researchers have developed a variety of information forensic techniques to determine the authenticity and processing history of digital image. Generally there are two main problems in image forensics, one is forgery detection, and the other one is forgery localization.

Forgery detection aims to discriminate whether a given image is pristine or fake. For instance, by exploiting some camera- related signals such as sensor pattern noise (SPN) and color filter array (CFA) properties, it is possible to reveal tempered images via camera source identification. By analyzing the JPEG compression artifacts one can expose JPEG decompressed images and detect JPEG recompressed images. Based on the distinctive artifacts left by a certain operation, it can identify contrast enhancement, reveal image re-sampling, detect median filtering, and so on. In practices, a key influential factor for forgery detection performance is the variety and uncertainty of tampering operations. Since most existing forensic methods assume that only one specific tampering operation investigation, they should not be used for a real forgery scenario independently. Usually it requires to analyzing the image with several forensic detectors and combining the detection result using some fusion schemes.

Some recent works applied fuzzy theory and to fuse the detection result, but these methods only considered JPEG compression artifacts, and might not be suitable for more general cases. An alternative solution is to seek for universal features that can identify as many tampering operation as possible. It has been observed from that, with a certain features, only a particular type of forgery is detected. So there is still a need to develop feature that can be used for multiple type of forgeries. A step towards this has been taken [29] in which a new form of convolution layer is proposed that will force the CNN to learn manipulation detection features.

The existing methods results are still far from satisfactory for practical forensics scenarios. So the improvement of existing method is significant. In this paper we construct a new CNN model for image forgery localization and checked the model with IFC-TC (IEEE information forensics and security technical committee) image forensics challenge set of images. The results are discussed finally to prove its efficiency.

II Background study

Much Research has been conducted in Image forgery field filed. Because of this, there exist many methods for detecting and localizing multiple different forms of image manipulation. Generally there are two main problems in image forensics, one is forgery detection and the other one is forgery localization. In practical forensic applications, we are more interested in figuring out the tampered regions compared to forgery detection. Forgery localization requires pixel level analysis [32] rather than Image level analysis as it faces more challenges compared to forgery detection.

Convolution neural network first appeared in the late 1980s with the handwritten zip code recognition [21] as an extended version of artificial neural networks (ANN). They have been also applied to handwritten digit recognition, image speech and time series data. A CNN is a special type of multilayer neural network used in deep learning that has recently gained significant attention in the computer vision and learning communicates [20,30]. In this paper, we proposed a forgery localization methods based on CNN, and tested the proposed method with the images in IEEE IFC test images. Finally experimental results are compared with other results to prove the efficiency of the proposed method.

The localization of image forgery is the most challenging tasks in digital image forgery detection image forgery localization attempts to detect the accurate tampered area [27]. In forgery localization there are several papers are published by researchers and suggests their ideas in detecting the localization of forged regions. These includes the photo response non uniformity noise (PRNN)[25], Image forgery localization via fine grained analysis of CFA artifacts[26], traces left by JPEG coding[17], to localized the tampered areas,[9][14][10] search for some relationships among the adjacent pixels which inevitably inherent during tampering operations.

The winner[11] in first IFS-TC Image forensics challenge[24] using the fusion of statistical features achieved in [16] which was based on color rich models[14] and ensemble classifier[2] (SCRM+CDA) Some other CNN based models are median filter Residuals features used [29], prediction error filters[8], residual-based feature[31], AC coefficients of DCT[22], DFT and log- scale transformation features[33], CNN- cross entropy scheme [5] deep learning based method[19] etc…In [3], CNNs are applied in median filtering image forensics In [34], a novel CNNs are adopted to detect multiple manipulations. In [18], a CNN with

SRM kernels [12] is adopted for forgery detection. In [13], they used residual based descriptors as a CNN which conduct forgery localization.

Numerous meaningful works have been done to improve the performance of image forensics by adopting[23]. In this paper we design CNN architecture and tested on the Image data set IEEE-IFS challenge [15]. This results shows that the proposed CNN architecture is one of the best tampering localization methods.

III Methodology

When a forensic investigator designs CNN architecture, they have at their disposal numerous possible choices of parameters such as the number of convolution layers, the choice of activation function etc. In this work we designed a CNN as shown in below Figure 1.

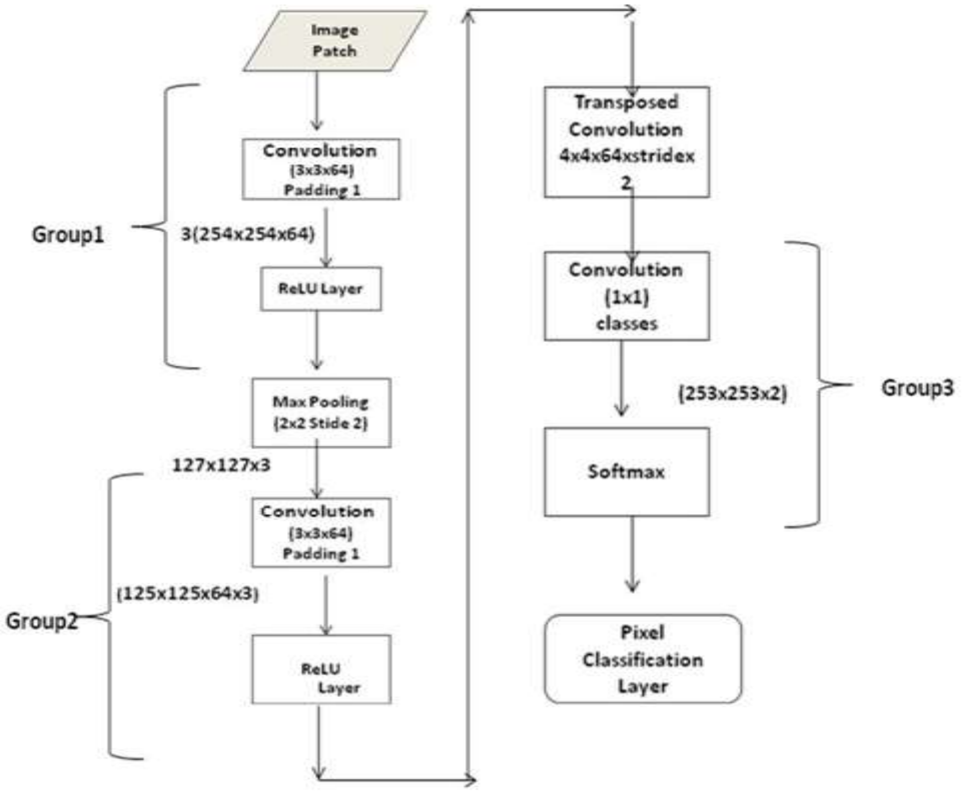


Image Patch
Convolution (3x3x64) Padding 1
Group1
3(254x254x64)
ReLU Layer
Max Pooling (2x2 Stide 2)
127x127x3
Convolution (3x3x64) Padding 1
(125x125x64x3)
Group2
ReLU Layer
Transposed Convolution 4x4x64xstridex 2
Convolution (1x1) classes
(253x253x2)
Group3
Softmax
Pixel Classification Layer

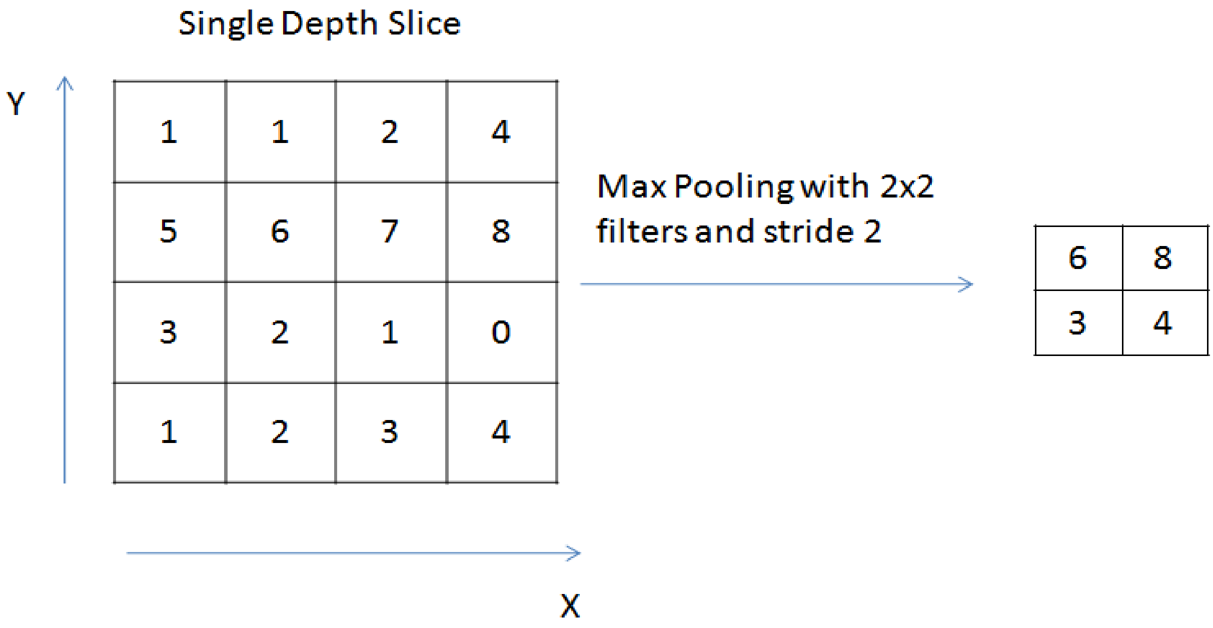
Figure 1.

A Proposed CNN experimental set up

There is still a need to develop features that can be used for multiple types of forgeries. A step towards this has been taken in this paper. A new form of Convolution layer is proposed that will force the CNN to locate multiple forgeries in an image. In this section, we describe the detection process of image manipulation using CNN. The proposed model comprises of various combinations of Convolution, pooling, and activation operations. The proposed module part with three groups of layers displayed as Group1, Group2 and Group 3 in Figure 1. Group 1 starts with a convolution layer that takes the input image. The Convolution layer is the main building block of a Convolution neural network. The proposed Convolution in a neural network is a product of a two dimensional matrix called an image and a kernel or mask. The filter size to be 3x3 and a stride of 2 is used. Stride is the number of pixels that jump or slide over the every iteration. Through this convolution, local features considering neighbor pixels can be extracted.

The number of channels, which is the depth of the image, since the images are in color the depth is 3 and padding 1. After this, we pass this layer in to the Rectified Linear unit (Relu) activation function. The purpose of this layer is to introduce non linearity to the system that basically has just been computing linear operations during the Convolution layer. Relu layers work far better because the network is able to train a lot faster without making a significant difference to the accuracy. Relu layers applies the function f(x) = max(0,x)to all the values in the input volume. In basic terms, this layer just changes all the negative activations to 0.

After Relu layer, we choose to apply a pooling layer which is a down sampling layer. Convolution neural networks generally have a very large number of neurons. It has been shown that this increases the complexity of learning problem. To solve this problem, We apply the pooling layer, such as Maximum pooling layer or average pooling. There are several layer options, out of which the most popular max pooling is being taken. Max pooling is such a sub sampling scheme that the maximum value of the input block is returned. Max pooling is used at the front of the proposed system, a max pooling layer is not only used to reduce the resolution of the input image patches but also used to make the network robust. We take a filter of size 2x2 and stride of length2. It then applies it to the input volume and outputs the maximum number in every sub region that the filter convolves around. Figure 2 shows an example of Maximum Pooling to select Maximum value.



1	1	2	4
5	6	7	8
3	2	1	0
1	2	3	4

6	8
3	4

Figure 2.

When we pass one of these training images in to our first convolution layer, the dimensions reduced from 254x254 to 127x127. This is done with the help of padding. When we add 2 layers of Os on the outer layer of the image and pass it through the pooling layer, the output size is exactly reduced to half of the input. Then the output image of the Group 1 convolution layer allows passing through Group 2 layers. In Group 2 layers, a convolution layer with 3x3x64 dimension with padding 1 and an activation layer Relu are used. During this process, convolution layer of dimension 3x3x64 with padding converts the output of Group 1 with dimension 127x127x3 to 125x125x3.In the proposed CNN, transposed convolution of 4x4 filter size with slide 2 is used.

This transposed convolution layer carries out a regular convolution but revert its spatial transformation. It converts the input image of class 2 into the original image resolution finally the image passes in to Group III, where convolution layer of 1x1 with numerical classes 1 is used where input image is converted to dimension 253x253x2 image. The Softmax activation is applied to the very last layer in designed CNN, Softmax is used to converts the output of the last layer in our designed CNN in to essentially a probability distribution

B Tampered Region Mask generation

For each input image, it is analyzed by the sliding window of the scale s with a stride S based on CNN detectors described as above. The image set in IEEE IFS-TC is taken and stored in a folder while the ground truth image of the image set is taken in an another folder. These Folders are mentioned in the coding. Create class names as Fake and Original with condition. Then apply random affine geometric transform action using augment function for all training data set. Then all the set of images are process through proposed CNN architecture, take Epoach 1 to 100. The output of the proposed CNN architecture displays the mask region of the forged area along with ground truth image of all input images. Some results are shown in the Figure 3.

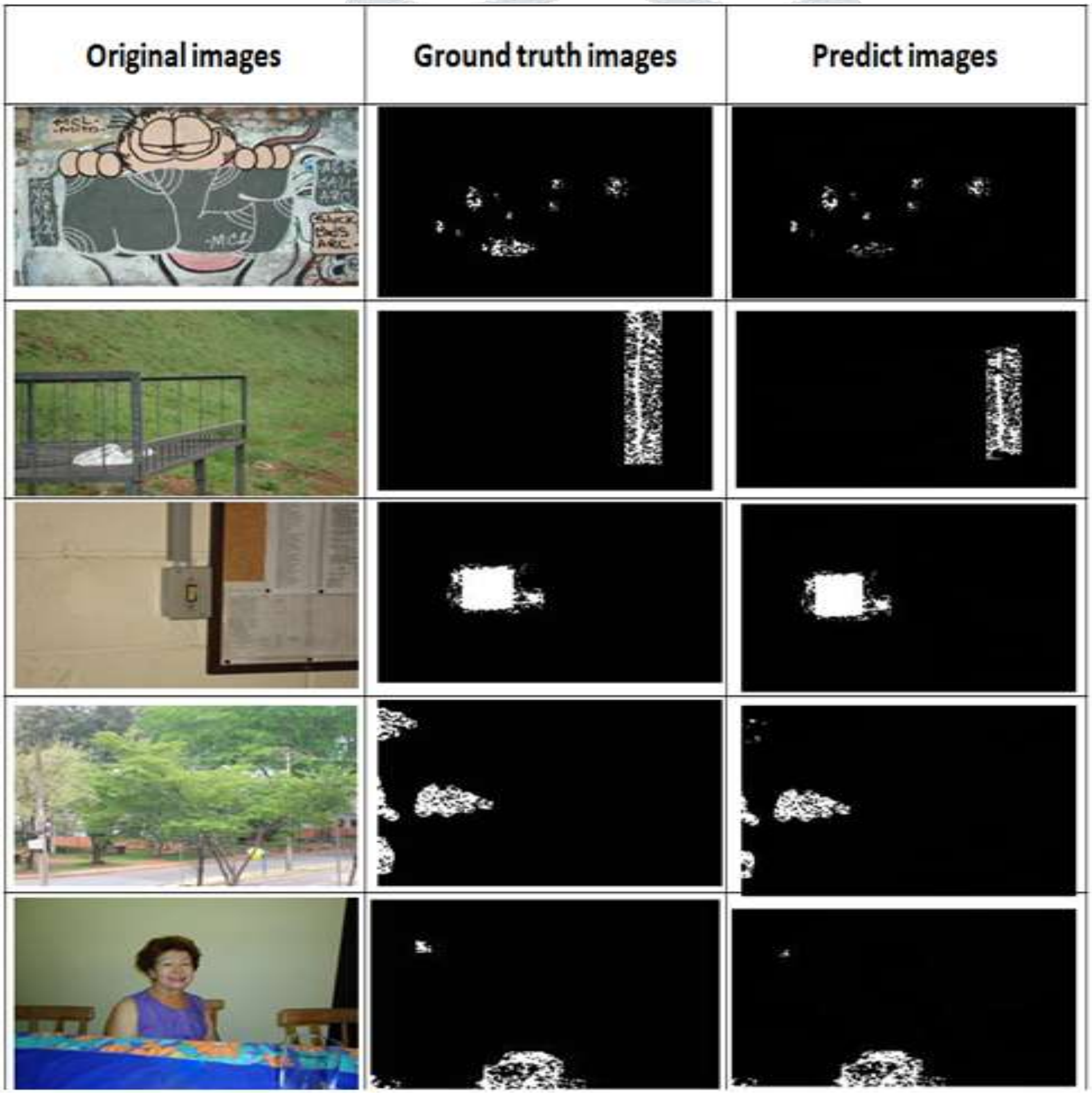


Figure 3.

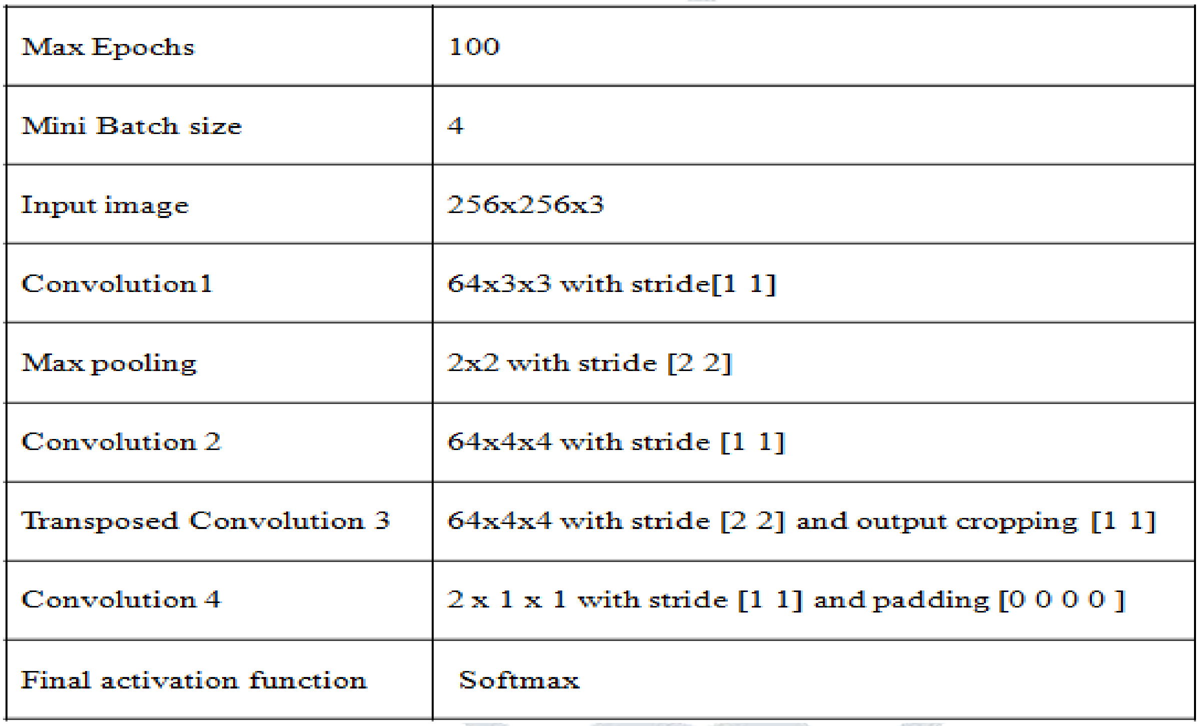
IV Experiment result and analysis

(i) Image Data Base

In our experiments, we use images taken from IEEE IFS.TC, first image forensics challenge. This comprises several original images captured from different digital cameras with various scenes either indoor or outdoor. The images are divided in to pristine and forged images. All the pristine and fake images are divided into training and testing set. In the training set the images are along with its corresponding class and mask and in the testing set, the images are without any class or mask. Fake images are manipulated by copy/pasting or image splitting.

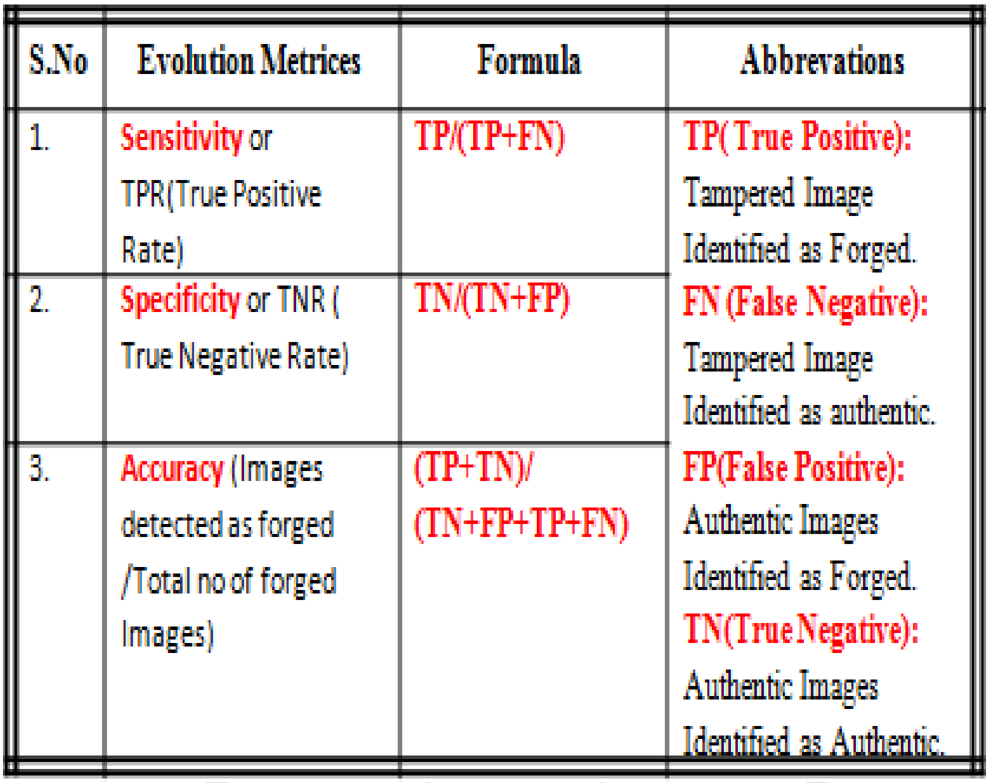
(ii)Experimental Result

The parameters of operations used in the experiment are shown in Table1. The proposed CNN is tested on IEEE FC data sets and drawn the results as shown in Table 2. Epoch and Accuracy are shown in Table 3.



Max Epochs	100
Mini Batch size	4
Input image	256x256x3
Convolution1	64x3x3 with stride[1 1]
Max pooling	2x2 with stride [2 2]
Convolution 2	64x4x4 with stride [1 1]
Transposed Convolution 3	64x4x4 with stride [2 2] and output cropping [1 1]
Convolution 4	2 x 1 x 1 with stride [1 1] and padding [0 0 0 0]
Final activation function	Softmax

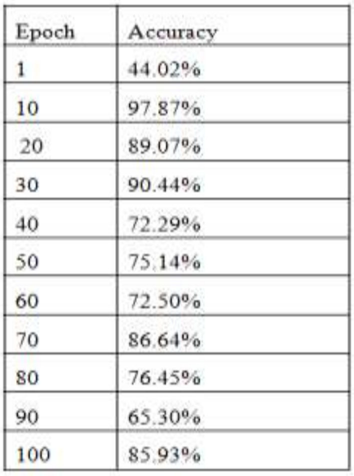
Table 1.



S.No	Evolution Metrices	Formula	Abbrevations
1.	Sensitivity or TPR(True Positive Rate)	TP/(TP+FN)	TP(True Positive): Tampered Image Identified as Forged.
2.	Specificity or TNR (True Negative Rate)	TN/(TN+FP)	FN (False Negative): Tampered Image Identified as authentic.
3.	Accuracy (Images detected as forged /Total no of forged Images)	(TP+TN)/ (TN+FP+TP+FN)	FP(False Positive): Authentic Images Identified as Forged. TN(True Negative): Authentic Images Identified as Authentic.

Method	Measure	Value
Proposed Method	Accuracy	73.3122
	Sensitivity	76.5375
	Specificity	73.4687

Table 2.



Epoch	Accuracy
1	44.02%
10	97.87%
20	89.07%
30	90.44%
40	72.29%
50	75.14%
60	72.50%
70	86.64%
80	76.45%
90	65.30%
100	85.93%

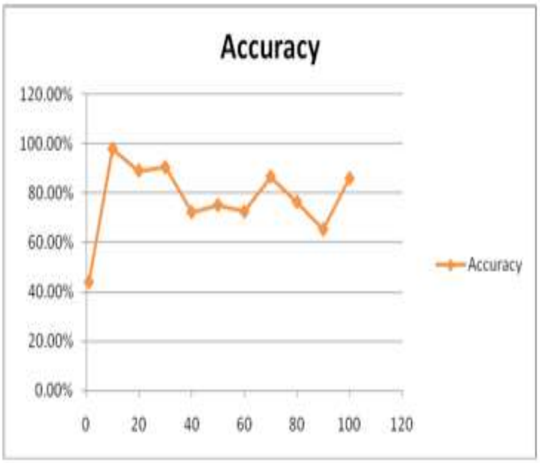


Table 3.

Comparison with existing methods

For a fair comparison, all of the result obtained for the testing images is submitted to the evaluation system of the challenge. According to the result of the challenge, the forgery localization performance is evaluated with the F1 score as follows.

$$F_1 = 2\,\frac{\text{Precision. Recall}}{\text{Precision+Recall}} = \frac{2TP}{2TP+FN+FP}$$

Where TP (true positive), FN (false negative), and FP (false positive) mean the number of detected fake pixels, undetected fake pixels, and wrongly detected pristine pixels, respectively. The experimental results are evolutes based on average F_1 –score [1] and comparison of the results are shown Table 4. and Figure 4. Result on the IFS-TC testing set2.

Method	FIScore
S3+SVM[17]	0.1115
S3+LDA[16]	0.1737
PRNU[33]	0.2535
SCRM+LDA[16]	0.3458
Proposed CNN	0.3962

Table 4.

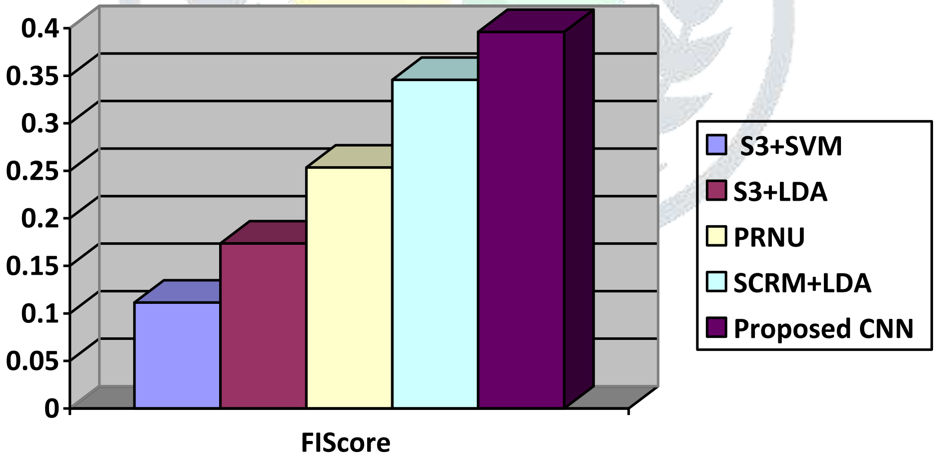


Figure 4.

Conclusion

In this paper, we proposed a forgery localization method based on Convolution Neural Network. We demonstrate the effectiveness of our detection method with a series of experiments on IFS-TC images. Although a state of the art result has been achieved, the proposed frame work is still in fant for real applications. In the next step we will further improve the performance by combining it with certain other techniques such as image segmentation computer vision and others. Although the proposed method can achieve the state of the art performance, it still has a long way to go for real applications.

Reference

[1] Asghar.K, Habib.Z, and Hussain.M, "Copy-move and splicing image forgery detection and detection and localization techniques: a review," Australian Journal of Forensic Sciences, vol.49.no.3,pp. 281-307,2017.DOI:10.1080/00450618.2016.1153711.

[2] Bayar B, Stamm MC. A deep learning approach to universal image manipulation detection usinga new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security - IH&MMSec '16; 2016, pp. 5–10.

[3] Belhassen Bayar andMatthew C Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in *The 4th ACMWorkshop on Information Hiding and Multimedia Security*. ACM, 2016, pp. 5–10.

[4] Chen.M, Fridrich.J, Golijan.M, and Lulas.J, "Determining image origin and integrity using sensor noise," IEEE Transcations on Information Forensics and Security, vol.3, no.1,pp.74-90, mar.2008, ISSN: 1556-6013. DOI :10.1109/TIFS.2007.916285.

[5] Choi, H, et al. Detecting composite image manipulation based on deep neural networks. Int. Conf. Syst. Signals Image Process; 2017.

[6] Cozzolino. D, Poggi.G, and Verdoliva.L, "Splicebuster : a new blind image splicing detector," in 2015 IEEE International Workshop on Information Forensics and Security(WIFS),Nov.2015, pp. 1-6 DOI: 10.1109/WIFS.2015.7368565.

[7] Cozzolino. D, Gragnaniello. V, and Verdoliva. L, "Image forgery detection through residual-based local descriptors and block-matching," in 2014 IEEE International Conference on Image Processing (ICIP), Oct. 2014, pp. 5297-5301.DOI: 10.1109/ICIP.2014.7026072.

[8] Cozzolino D, Poggi G, Verdoliva L. "Recasting Residual-based Local Descriptors as Convolutional Neural Networks: an Application to Image Forgery Detection", in 5th ACM Workshop on Information Hiding and Multimedia. Security. 2017;159–164.

[9] Davide Cozzolino and Luisa Verdoliva, "Singleimage splicing localization through autoencoder-based anomaly detection," in *IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2016, pp. 1–6.

[10] Davide Cozzolino, Diego Gragnaniello, and Luisa Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in *IEEE International Conference on Image Processing (ICIP)*. IEEE, 2014, pp. 5302–5306.

[11] Davide Cozzolino, Diego Gragnaniello, and Luisa Verdoliva,"Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques,"in *IEEE International Conference on Image Processing (ICIP)*. IEEE, 2014, pp. 5302–5306.

[12] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva, "Recasting residual-based local descriptors as convolutional neural networks: an application to image forgery detection," in *The 5th ACM Workshop on Information Hiding and Multimedia Security*. ACM, 2017,pp. 159–164.

[13]Guanshuo Xu, Han-Zhou Wu, *Student Member, IEEE*, and Yun-Qing Shi, *Fellow, IEEE*"Structural Design of Convolutional Neural Networks for Steganalysis" IEEE SIGNAL PROCESSING LETTERS, VOL. 23, NO. 5, MAY 2016.

[14] Haodong Li, Weiqi Luo, Xiaoqing Qiu, and Jiwu Huang, "Image forgery localization via integrating tampering possibility maps," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1240– 1252, 2017.

[15] IFS-TC, "The 1st ieee ifs-tc image forensics challenge", http://ifc.recod.ic.unicamp . br/fc.website/index.py,2013

[16] Jan Kodovsky, Jessica Fridrich, and Vojtˇech Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2012.

[17] Jan Kodovsky, Jessica Fridrich and Vojtech Holub, Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no.2, pp. 432-444, 2012.

[18] Jessica Fridrich and Jan Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp.868–882, 2012.

[19] Jiansheng Chen, Xiangui Kang, Ye Liu, and Z Jane Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1849–1853, 2015.

[20]Krizhevsky.A, Sutskever.I, and Hinton.G.E., Imagenet classification with deep convolutional neural networks. In Advances in neural information processing systems, pages 1097–1105, 2012.

[21] LeCun.Y, Boser.B, Denker.D,Henderson. J.S., Howard. R. E., Hubbard. W, and Jackel. L.D.. Backpropagation applied to handwritten zip code recognition. Neural computation, 1(4):541-551,1989.

[22] Liu A, Zhao Z, Zhang C, Su Y. Smooth filtering identification based on convolutional neural networks. Multimed Tools Appl. 2016:1–15.

[23] Lorenzo Gaborini, Paolo Bestagini, Simone Milani, Macro Tagliasacchi, and Stefano Tubaro, "Multicule image tampering localization", in IEEE International Workshop on Information Forensics and Security(WIFS).IEEE, 2014,pp.125-130.

[24] Miroslav Goljan, Jessica Fridrich, and R´emi Cogranne, "Rich model for steganalysis of color images," in *IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2014, pp. 185–190.

[25] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Luk´as, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[26] Pasquale Ferrara, Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva, "Image forgery localization via finegrained analysis of cfa artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1566–1577, 2012.

[27] Paweł Korus and Jiwu Huang, "Multi-scale analysis strategies in prnu-based tampering localization," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 809–824, 2017.

[28] Qureshi. M.A. and Deriche.M, "A bibliography of pixel-based blind image forgery detection techniques," Signal processing : Image Communication, vol.39,part A, pp. 46-74, 2015,ISSN: 0923-5965.

[29] Savita Walia & Krishan Kumar "Digital image forgery detection: a systematic scrutiny", Australian Journal of Forensic Sciences. 2018.

[30]Szegedy. C, Liu.W, Jia.Y, Sermanet.P, Reed.S, Anguelov.D, Erhan.U, Vanhoucke.V, and Rabinovich.R Going deeper with convolutions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 1–9, 2015.

[31] Wang Q, Zhang R. "Double JPEG compression forensics based on a convolutional neural network". EURASIP J Inf Secur. 2016;2016:23.

[32] Yaqi Liu, Qingxiao Guan, Xianfeng Zhao, and Yun Cao, "Image Forgery Localization based on Multi-scale Convolutional neural Networks",Computer Vision and patten recognition. 7 Feb 2018.

[33] Yu J, Zhan Y, Yang J Xiangui KB. A multi-purpose image counter-anti-forensic method using convolutional neural networks. In International Workshop on Digital Watermarking. 2017:3–15.

[34] Yuan Rao and Jiangqun Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2016, pp. 1–6.