DETECTING IMAGE MANIPULATION USING DEEP LEARNING IN TENSORFLOW

[1]Prithvija.M,[2]Dr.IlangoKrishnamurthi
[1]UG Student,[2]Professor & Dean
DepartmentofComputerScienceand Engineering
SriKrishnaCollegeofEngineeringandTechnology,Coimbatore,India
[1]15epcs013@skcet.ac.in,[2]ik@skcet.ac.in

Abstract—**Multimediaisoneof theprincipal meansof communicationinthesedays.Whenanimageorvideo is obtainedasevidence,itcanbeusedasprobativeonlyifi t isauthentic.Determiningtheauthenticityof thesekindsof multimediasuchasimageshasbeenanactiveresearch areaforpastfewyears.Herewepproposeasystemusing deeplearningalgorithm withTensorFlowasback end,to identifytheforgeriesonanimage.Inthis paper,weuse predictionerror filter thatmendsthealteredrelationship among the pixels of the image. Experimental results showed thatmanipulationslikemedianfiltering,Gaussian blurring, resizing and cut and paste forgery can be detectedwithanaverageaccuracyof96%.**

Keywords—Convolutional Neural Network, Artificial Neural Network,DeepLearning,ImageForgery,Te nsorFlow

I. INTRODUCTION

Overthepasttwodecades withtheincreasingamounts of databecomingavailablethereisalwaysa goodreason to believethatsmartdataanalysis willbemuch pervasiveasa necessary element for technology progress. In machine learning, thevanishinggradientproblemis adifficultyfoundin trainingartificialneuralnetworkswithgradient-basedlearning methodsandbackpropagation.Deeplearningovercomest he vanishinggradientproblemofANNbyanewconceptdropo ut, inwhichtheparticularPerceptronis removedfromthenetwork basedon thethresholdvalues.Itworkswith thesystem of interconnectedartificialneuronsthatareconnectedandtun ed duringthetrainingofthenetwork.Convolutional neural networks as well as traditional multilayer perceptron were beingunduly appliedtocharacterrecognitionandhandwritten digitrecognition.Trainingwasinitiallybasedon errorback propagation andgradientdescent. Theoriginal convolutional neuralnetworkisbasedonweightsharingwhichwas proposed in1986.Recentimplementationsmakeuseof other regularization techniquesasforexampledropout. The ConvolutionNeural Network(CNN)hasshownexcellent performanceinmany computervision andmachinelearning problems.When animageisgiven directly to thenetwork the rawpixel oftheimageistakenasinputforthefeature extraction which is obtained by the convolution operation. Inputis convolvedwithkernelvaluetoextractthefeaturemap.The obtained outputisthen given to theNon-linearlayerthat usesvariety ofNon-Linearfunctionstosignal distinct identification oflikelyfeatureinhiddenlayers.Initially the convolutionlayerextracttheinformationlikeedges,linean d corners thenextractthehigherlevelfeatureswiththehelp extractedlowlevelfeatures.Theextractedfeaturemapsare then given to the Pooling layer. Pooling is an aggregation action oftheinputby averagepoolingorbymaxpoolingand retainingtheonevalueperwindow. Thepooledvalueisfeed tothefullyconnectedlayerin whicheveryneuronsof the previouslayerisconnected to theevery nodein thenextlayer. ImageForensicsisanactofidentifyingtheforgedimageby tracesleftbymanipulation operation.Forensicsapproach uses thealgorithmicapproachforidentifyingtheforgedoperati on .When theforgermademultipleeditingoperationsthen the forensicinvestigatorhavetoapply multiple algorithmsfor detection.Sometimesthismay causesomenewproblemsor increasethefalsealarm rate.ToovercomethisissuetheDeep Learningbasedapproach [1]isintroduced whichlearn the featuresdirectlyfrom thegivenimage.Image classification, Identificationandnumerousoperations caneasilybedonewith the

TensorFlowasbackend.TensorFlowisanopensource pythonsoftwarelibraryfornumericalcomputationwitht he helpof dataflowgraph.Therestof thepaperisorganizedas following. Section II discusses about the related works in imageforgery detection.SectionIIIandIVdescribesthe implementationandexperimentalresults. SectionVsummarize andconcludethepaper.

II. BACKGROUNDSTUDY

Chen,J.Kang,X.,Liu,Y.,&Wang,Z.J.in[2],introduce d anewapproach usingdeeplearningforperforming theimage editingdetectionthatiscapableofautomaticallylearningt he tracesleft.Deeplearningapproach learnsby representing the conceptsin such away thathigherlevel conceptsarebeing learnedfromthelowerlevelconcepts.CNNmodelswitht he rawimagepixels asinputs does notyieldgoodperformance,so oneadditionalfilterlayerisaddedto theconventional model. Throughthisfilterlayer,theMedianFilteredResidual(M FR) of animageisobtained.Medianfilteringandcutandcopy imageforgeriescanbeeasilydetectedbythismethod.Inor der todetecttheforgery, thecompositeimagewasfirstsegmented into64x 64 pixelblocks,and theneachblockwasthen tested forevidenceoflocallyappliedmedianfiltering.Eachdete ction methodwastrainedusingcorrespondingimages.Bayar,B ,and

Stamm,M.C.in [3],proposeda methodforidentifyingthe universal imagemanipulation by applying theprediction error filterwhichiscapableof suppressingtheimagecontentand retrievingthepixelrelationshipamongthepixels.

Popescu,A.C.,andFarid,H.in [4]hasproposed amethod thatpinpoints themanipulationbythetraces leftbyresampling operations.Adatabasecontaining200gray scaleimagesinthe TIFFformatwhichareof 512x512pixelsizeiscreated.These imageswerecroppedfromlargerimagestakenwithacame ra in ordertocaptureandstorein uncompressedTIFFformat usingthebi-cubicinterpolation,theseimagesare thenup sampled,downsampled,andthenrotatedby changingthe amount.When resamplingisdonein aparticularimageit introduces theperiodiccorrelationsandthesecorrelationscan bespottedwith theExpectation/Maximization (EM) [8] algorithm.

In[4]twomodelswereconsideredinwhichfirst method takes thesamplesthatarecorrelatedtotheirneighbors,andin second methodsamples thatarenot.TheEM algorithmis iterativeinwhichtheE-stepis theprobabilitythateachsample belongstoeach model isestimatedandin the M-step,the specificform ofthecorrelationsbetweensamplesisestimated. When animageisresampled theeven columnsand odd rows willbethelinearcombination ofhorizontal neighborsand the verticalneighborsformthelinearcombinationforevenro ws and oddcolumns.Based on this,theprobabilitymapcanbe developedthatembodythespatialcorrelationsoftheimag e.

TheEMalgorithmestimatesthesetofperiodicsample s thatarecorrelated to theneighborswhichidentify thebroad rangeofresamplingrates.Thenewmedianfilteringforen sic techniquesisproposedin[5]thatidentifythemedianfilter ed imageinfoursteps.Initially theMedianFilterResidue(MFR) extractsthemedianfilteringfeaturesandsuppresstheima ges edgecontentandthenobtainsthestatisticalfeaturebyfitti ng theMFR totheAutoregressive(AR).TogetthesingleAR model,take theaverage ofthecorrespondingARcoefficients. These coefficients are used to train the SVM and in turn classifythemedianfilteredorunalteredimages.

YanjunCao,TiegangGao,Li Fan,QuntingYang[9] proposedamethod todetect thecutandmoveforgery.In this paperthey dividedtheinputimageintofixed-sizeblocks, appliedDCTtoeachblocktogenerate thequantized coefficientsafterrepresentingeach quantizedblockby a circle block and extracting appropriate features from each circle block.Performthesearchingforsimilarblockpairs. Finding correctblocksandthenoutputthem.Theaboveapproache s willleads toadvancementinforensics butitraisesseveralnew problemsifmultipleeditingis doneontheparticularimage.To overcomethisproblemnewideaisproposedwith referenceto thepixelrelationship.Inordertoobtainhigherperforman ce andimprovedefficiencyinidentifyingtheforgedimage we

haveimplementedimageforgerydetectionusingdeeplearning withthehelpofTensorFlow III.

III.FORGERYDETECTIONWITHDEEPLEARNING USINGTENSORFLOW

ConvolutionalNeural Networksarecapableoflearning the contentoftheimagetoclassifythegivenimage.Itrecoups the contentof theimagewhichisnotsuitableforidentifyingthe alterations.Toovercome thisissue,BelhassenBayar[6] proposedthefilterlayercalledpredictionerrorfilterwhich willsuppressthecontentoftheimageand helpstoretrieve thelocalstructuralrelationshipthatexistbetweenpixels.

To get greater performance [7] we implemented theforgerydetectioninTensorFlowwhichyieldshigherlevelof flexibilityandfastercomputation.Ifrawpixelsaregiveto thenetworkthentheoutputwillnotbeefficient.Thealtered relationshipbetween thepixelsand theoutputisthen directly fedintothe convolutionallayerwhere theconvolution operationisperformedbetween thekernel andtheretrieved pixels. Andthefeaturemapswillbeextractedasaresult. Thesefeaturemapsarethengivenasinputtothenextlayer, Rectified Liner Unit (ReLU) and the output is given for pooling where we prefer max pooling operation. When poolingoperationiscompleted,itwillresultinproducingthe reducedfeaturemaps,andthesevaluesarethendirectly fed intothefully convolutionallayerwherethesoftmaxoperation isbeingperformedand the classification willbedonedepends ontheclassscorethenetworkwillbeabletopredictthegiven imageismanipulatedornotmanipulated.

Theintroducedpredictionlayerhastobe placedbefore the convolutionlayer,whichwillbeabletopredicttheerrorby subtractingthecentralvaluefrom thecenterofthefilter window.Predictionerrorfilterisof size512x512kernels which resultsin223x 223x12featuremaps. Thisconvolution isnotstepped tonon–linearfunctionmappingbecauseit containsthetracesof themanipulatedimage.Intheabove architecturewehavetaken twoconvolutionlayersin which firstlayerhas64kernelsofsize7x 7x 12withstridevalue2 thatyields112x112x64featuremaps.Thesecondlayer has 48kernelswithstridevalue1.Thesizeofthekernelis5x5x 64.

ThetrainingalgorithmforConvolutionallayerwillbeas follows

Initializeweights randomly
i=1
While*I*<max_iteration

Set $(w_k)^1(0,0) = 0$ (1) Normalize weights in suchawaythat

$$\sum_{l=0}^{row-1}\sum_{m=0}^{col-1}(w_k)^1(l,m) = 1$$

$$(w_k)^1(0,0) = 0$$

Set (2)

Performaforwardpass
Updatetheweights usingSGDalgorithm,applyback propagation
i=*i*+ 1

oftrainingvalues reaches theaccuracy exit
end

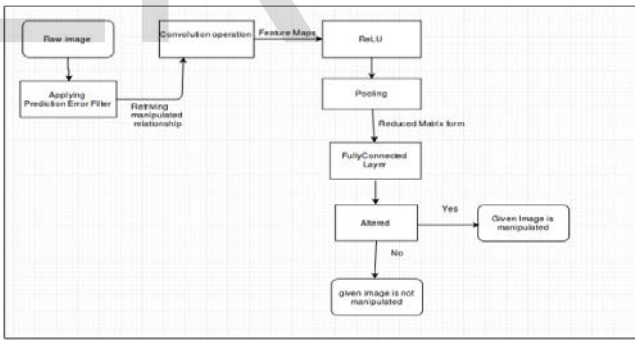

Fig.1.DataflowgraphofImageManipulationDetection

IV.EXPERIMENTALRESULTS

Thedatasetcontains 100images ofsize256x256andeach image were undergone manipulationslikemedianfiltering, resizingandcutandpasteforgery.Wehavealsocreated a trainingdatasetofimagesofthesize227x227bycropping down using 100 images each and testing dataset with 50 imageseach.Table1showsthedetection rateforvarious forgeries.WecanunderstandfromthistablethatCNNisable todistinguishbetween unalteredandmanipulated imageswith atleast96%accuracy.

Images	***Original***	***Median***	***Resized Image***	***Cut and past***
Original Image	***96.04%***	***0.23%***	***0.3%***	***0.4%***
Median Filte	***0.21%***	***96.3%***	***97.01%***	***96.8%***
Resized Image	***0.02%***	***0.18%***	***0.14%***	***0.04%***
Cut and past	***0.03%***	***0.04%***	***0.15%***	***0.23%***

Table.1:Accuracydetectionofdifferentmanipulatedimages

V. CONCLUSION

In thispaperwehaveimplementedanimagemanipulation detectioninTensorFlowframeworkwith thehelpofdeep learningwhichhasanabilitytoautomaticallylearnfeatures and tospot theimagemanipulationslikeMedian filtering, resizingandcutandpasteforgery.Wehavealsoplacedan errorfiltertoget only thepixel relationshipinstead oflearning features ofimagecontent.Throughexperiments,wehavealso demonstratedthataconvolutionalneuralnetworkbasedd eep learningapproachwasabletospottheforgerywithanaver age accuracy of96%.Wecanalsoplan totestournetworkby increasingthesizeofthedatasettoimproveaccuracy of detectioninthefuture.

REFERENCES

[1] Bayar,B.,&Stamm,M. C.ADeepLearningApproachtoUniversal Image ManipulationDetectionUsingaNewConvolutional Layer.In Proceedingsof the4thACMWorkshoponInformationHiding and MultimediaSecurity(2016), pp. 5-10, ACM.

[2] Chen,J.,Kang,X.,Liu,Y.,&Wang,Z.J.Medianfilter ingforensics based on convolutional neural networks. IEEE Signal Processing Letters, 22(11), (2015), pp.1849-185.

[3] Stamm,M.C.,&Liu,K.R.Forensicdetectionofimag emanipulation usingstatistical intrinsicfingerprints.IEEETransactionsonInforma tion Forensicsand Security, 5(3), (2010), pp.492-506

[4] Popescu, A.C.,&Farid, H. Exposingdigitalforgeriesbydetecting traces of resampling. IEEE Transactions on signal processing, 53(2),(2005), pp.758-767.

[5] Kang,X.,Stamm,M.C., Peng,A.,&Liu,K.R.Robustmedianfiltering forensicsusinganautoregressive model.IEEETransactionson Information Forensicsand Security, 8(9), (2013), pp.1456-1468.

[6] Bayar,B.,&Stamm,M. C.ADeepLearningApproachtoUniversal Image ManipulationDetectionUsingaNewConvolutional Layer.In Proceedingsof the4thACMWorkshoponInformationHiding and MultimediaSecurity(2016), pp. 5-10, ACM.

[7] Shi,S.,Wang,Q.,Xu,P.,&Chu,X.BenchmarkingState-of-the-Art Deep Learning Software Tools. arXivpreprint arXiv: (2016),pp. 1608.07249.

[8] A. Dempster, N.Laird, and D.Rubin, Maximumlikelihoodfrom incompletedataviatheEMalgorithm,Journalofthe RoyalStatistical Society, (1977)vol. 99, no. 1, pp.1–38.

[9] YanjunCao,TiegangGao,LiFan,QuntingYang , ARobustdetection algorithmforcopy-moveforgery indigitalimage,(2012),Forensic scienceinternational, Vol. 214, Issues1-3, pp 33–43 .