IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

Image Forgery Detection using Error Level Analysis and Convolutional Neural Networks

B.Manikanth[1], N.S.V. Phani Pavan[2], K. Lokesh [3], M. Vamsi Krishna [4], K. Harsha Vardhan [5]

Assistant Professor, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt, Andhra Pradesh, India[1]

U.G. Students, Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur Dt, Andhra Pradesh, India[2,3,4,5]

ABSTRACT:Images play a vital role in our lives and they have evolved into an essential means of conveying information. Nowadays, image forgery has become a more significant problem and matter of concern. Many traditional techniques like DWT, histograms of robust local binary patterns, DCT, and many others are used to detect image forgery. Recently, Convolutional Neural Networks (CNN) have gained much importance in the field of image processing because of their ability to detect complex features and identify the patterns in the image. Error Level Analysis (ELA) is the digital forensic technique that is used to find forged images by recompressing the images and it is widely used in the many photos forensic sites on the internet to detect manipulated images. Here we propose an image forgery detection method that detects the image splicing forgery based on the Error Level Analysis (ELA) by emphasizing CNN architecture which classifies real and fake images.

KEYWORDS:Error Level Analysis, Convolutional Neural Networks, recompressing, photo Forensics, image splicing.

I. INTRODUCTION

According to the proverb “A picture isworth a thousand words”, this is certainly true in today’s visually driven culture. Nowadays, photographs are utilized widely in journalism, education, social media, and other fields, and they have developed into crucial tools for circulating information. In addition to all of this, the development of image editing tools has made it simpler to change an image with outstanding results, giving the impression that the viewer is viewing the real image. The image manipulation tools like Adobe Photoshop, GIMP, and other image editing tools are widely used to manipulate images easily and more accurately as real images. In this digitally oriented society and this world of internet and the smartphones, there are millions of images that are circulating in the world and the importance of images is increasing in our lives. In addition to that, manipulated images are circulating and misguiding people. This became a serious concern in society. The images are not only used for conveying information and also used as shreds of evidence and proof in the investigation of crimes. Videos and photographs have been used as evidence in court cases, making it possible to tamper the images and make decisions that could hurt the society. This makes it difficult for forensic analysts to differentiate between authentic and fake images.

Image tampering is classified into three types. one is image retouching, second one is copy-move and third one is image splicing. Image retouching is improving the specific quality of the image like the sharpness and smoothness of the image. It is usually used by magazine photo editors.Copy move forgery is we take some portion of the image and paste it on the same image. Image splicing is taking part of the image and pasting it on another image. It is usually combing two images. Due to the availability of image editing tools, these forgeries became easy to perform.

Convolutional Neural Networks (CNN) gained much importance in the field of image processing in recent times. CNN is good at identifying more complex patterns and features on the images and classifying them. It can become a common solution for image classification problems.Generally, the splicing introduces high contrast in the corners, smooth regions, and edges. So, it is possible to detect these forgeries using CNN.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

Fig 1: Original Image and Spliced Image

The main objective of our project is to build a CNN model which detects image splicing forgery using Error Level Analysis and classifies between real and fake images more efficiently and accurately.

II. LITERATURE REVIEW

The authors in [6] proposed a passive approach for detecting the image splicing forgery using deep learning with the Haar wavelet transform. The authors in [4] proposed a method that follows a deep learning CNN algorithm that is based on Resnet-50 which is a pre-trained residual network. This method uses three classifiers namely: Naive Bayes, K-Nearest Neighbors (KNN), and a multi-class model using SVM. The accuracy for all these classifiers is 70.26%, 59.91%, and 59.91% and MATLAB is the platform used in this experiment.In [3], two different datasets are used namely CASIAV2.0 and NC2016. Here also, the authors follow CNN approach based on two different models. They are VGG16 and VGG19 along with the Error Level Analysis. The accuracies obtained are 71.6% and 72.9%. The block-level approach is used in [2] using CNN. This method resulted in an accuracy of 91.1 % and reduced computational cost.In the paper [1], the authors followed a reliable deep learning approach and the Error Level Analysis (ELA) for image pre-processing. This method resulted in an overall accuracy of 92%.

III. METHODOLOGY

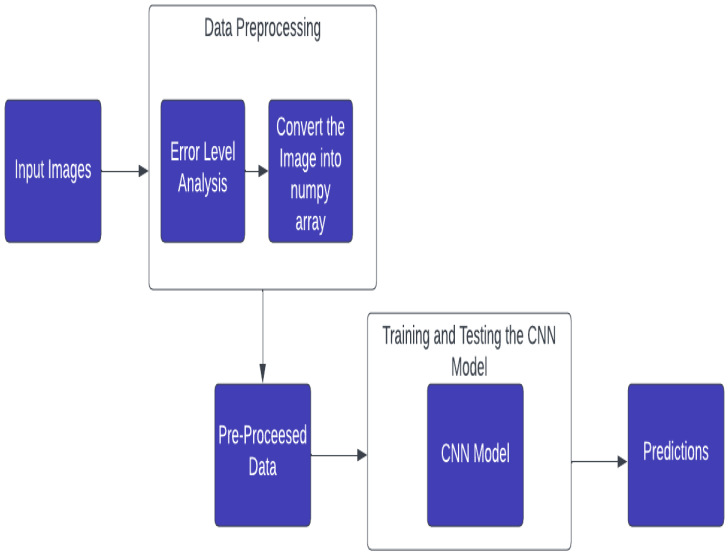

Fig 2: Methodology

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

In this method, we have used the CASIAV2.0 dataset because it is an open-source dataset for image splicing detection. This CASIA dataset contains two versions namely CASIAV1.0 and CASIAV2.0. Here, we have used the CASIAV2.0 dataset because it contains more images when compared to CASIAV1.0. Since the neural networks are data-hungry, it is good practice to train the model with greater number of images if possible.

Dataset Version	Type	Size	Real	Spliced
CASIAV1.0	JPG	384 *256	800	921
CASIAV2.0	JPG PNG TIF	240 *160 To 900*600	7491	5123

The CASIAV2.0contains a good number of real and spliced images.So, we have chosen CASIAV2.0 for this method. These images of the CASIAV2.0 are the input images and these images will undergo further data pre-processing.

Error Level Analysis:

Error Level Analysis is one of the techniques of photo forensics to detect image manipulation by storing the images at a certain quality level or by recompressing the images and calculating the difference in the compression levels. The differences in the compression levels are called errors. This is a lossy compression technique performed on the frames. Most image editing tools like Adobe Photoshop, GIMP, etc. support JPEG compression. Generally, when we click an image with the camera and save it, then the image was compressed. when the image was edited with these tools, then the image was compressed again. JPEG image type is used to extract this data.Resaving a JPEG removes high-frequency information, resulting in less contrast between high-contrast edges, textures, and surfaces. A low-quality JPEG will appear extremely dark.A picture's high-contrast edges can be enhanced by scaling it down, making them appear brighter under ELA. Similar to this, when you save a JPEG using an Adobe product, high-contrast edges, and textures are automatically sharpened, making them appear considerably brighter than low-texture surfaces. So, these are used to calculate the errors.

Consider the original image with the compression value as A_i and the compressed image compression value as A_j, then the difference between the two is taken as $(A_i - A_j)$ or $(A_j - A_i)$ and the pixels where the error rate was higher will be highlighted as shown in Fig 4. These highlighted portions are the pixels that contain high differences in the error rate and the portions of manipulated images are highlighted.

Fig 3: Original Image and Corresponding ELA Image

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

Fig 4: Fake Image and Corresponding ELA image where the spliced portions are highlighted

The image has reached the minimum local error value for this quality level if the change is not significant. If the difference is substantial, it has not reached the local minimum value. The PIL library in python is used to perform error-level analysis. The system first captures photos of the highest quality.The image will be forwarded to the neural network for additional processing. All the Images are converted into ELA images and then, the ELA images are converted into the NumPy array by adding the corresponding labels. This is the data preprocessing stage of our methodology.

Convolutional Neural Networks:

Convolutional Neural Networks (CNN) are the backbone of image classification. It is a deep learning technique that was widely used in image classification, segmentation, speech recognition, and natural language processing.CNN is a network of multiple layers which perform mathematical operations on the input data. The CNN consists of multiple layers. They are convolutional layers, pooling layers, and fully connected layers.

The convolutional layer applies filters to the input image to extract the features. Filter slides over the input image and perform the dot product between its values and resulting a single feature map. Let us assume N filters of size F x F, then output computation O is computed as

$$O(i, j, k) = AF(\Sigma\Sigma\Sigma\, I(x, y) * W(a, b, k) + b(k))$$

Where AF is the activation function, (i,j) are the indices of the feature map, (a,b) are the indices of the filter, W(a,b,k) weight of the filter at position (a,b) and index k, I(x,y) are the input value of the image, b(k) is the bias.

The pooling layer reduces the spatial dimensions and also extracts the most specific features. The max pooling is the pooling layer that finds outs the maximum value from a region. The output of the max pool layer is computed as O'.

$$O'(i,j,k)=Max(O(i+a,j+b,k))$$

Where (a,b) are the indices of the pooling region.

The fully connected layer in CNN is the layer that generates the predictions. Each neuron in this layer computes the weighted sum of the input multiplied by the output of the preceding layer to the activation function.

$$Y = AF(\Sigma\, W(i) * x(i) + b)$$

Where W(i) is the weight of the input neuron, x(i) is the input from the preceding neuron, AF is the activation function and b is bias.

We propose a CNN model for image splicing detection using CASIAV2.0 which consists of 3 Convolutional layers,3 max-pool layers,2 dense layers, and 2 dropout layers.Since we have used the 3 Convolutional layers, we are calling it CNN3 Model. This CNN3 model is a custom sequential model which was built by adding layers to the sequential model. We have conducted experiments by optimizing the filters, strides, and other parameters. From our experiments, we propose this CNN3 model with the optimized parameters.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

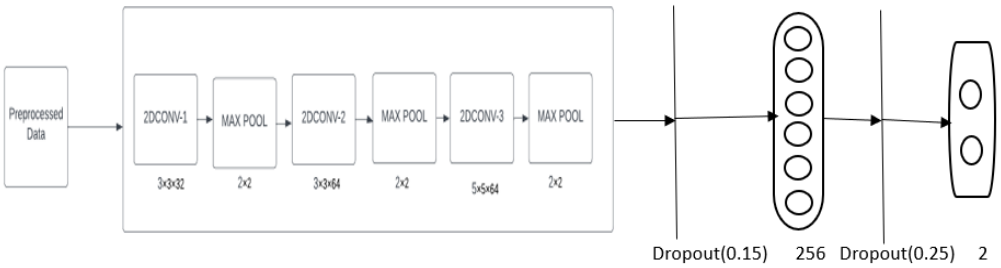

Fig 5: CNN3 Model

1st convolutional layer consists of 32 filters which are of size 3 x 3
2nd convolutional layer consists of 64 filters which are of size 3 x 3
3rd convolutional layer consists of 64 filters which are of size 3 x3.

Each convolutional layer is followed by a max-pool layer of pool size 2 x 2. These convolutional layers are activated by the activation function RELU.Fully connected layers consist of a dropout layer, followed by a flatten layer, followed by a dense layer of size 256 with the activation function of RELU, and another dropout layer, followed by a dense layer of size 2 with the activation function of SoftMax.

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 126, 126, 32)      896

 max_pooling2d (MaxPooling2D  (None, 63, 63, 32)       0
 )

 conv2d_1 (Conv2D)           (None, 61, 61, 64)        18496

 max_pooling2d_1 (MaxPooling  (None, 30, 30, 64)       0
 2D)

 conv2d_2 (Conv2D)           (None, 26, 26, 64)        102464

 max_pooling2d_2 (MaxPooling  (None, 13, 13, 64)       0
 2D)

 dropout (Dropout)           (None, 13, 13, 64)        0

 flatten (Flatten)           (None, 10816)             0

 dense (Dense)               (None, 256)               2769152

 dropout_1 (Dropout)         (None, 256)               0

 dense_1 (Dense)             (None, 2)                 514

=================================================================
Total params: 2,891,522
Trainable params: 2,891,522
Non-trainable params: 0
_________________________________________________________________
```

Fig 6: Summary of CNN3 Model

The Fig 6 shows the summary of our custom-created CNN3 model to classify real and fake images. After the data preprocessing, the data was divided into the training and validation data and this CNN3 model will be trained by the training data. And further validated using the validation data. After the training, the model will be used to classify the real and fake images.This is our proposed methodology for Image forgery detection using Error Level Analysis along with Convolutional neural networks.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

IV. EXPERIMENTAL RESULTS

From our proposed methodology, We have obtained a Validation accuracy of 93% and a training accuracy of 96%.

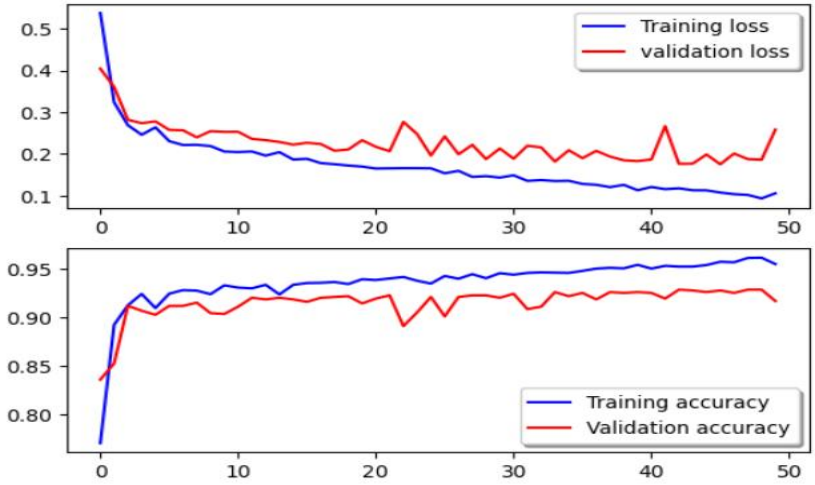

Fig 7: Loss and Accuracy Curves

Fig 7 Shows the loss and the accuracy curves obtained by training our CNN3 model over 50 epochs. We have obtained a model accuracy of 96% during this training process. After Training Process, we have obtained an accuracy of 93% by validating the CNN3 model.

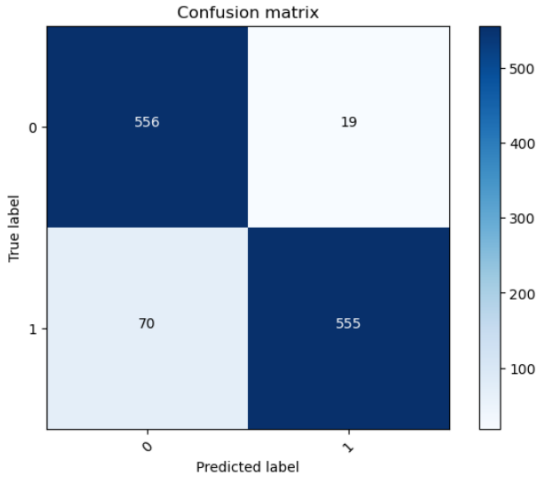

Fig 8: Confusion Matrix

The above Fig 8 is the confusion matrix that we have obtained by validating the CNN3 model. True positive (TP) is 555, TrueNegative (TN) is 556, False Positive (FP) is 19, and False Negative (FN) is 70. Here, 0 represents Fake image and 1 represents Real image.

Fig 9 is the classification report of our model which has the detailed performance of our model on the real and fake images. From the classification report, we can conclude that we have obtained an F1 score of 93%, accuracy of 93% ,precision for fake and real images are 89% and 97% respectively and recall for the fake and real images are 97% and 89% respectively.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

	precision	recall	f1-score	support
0	0.89	0.97	0.93	575
1	0.97	0.89	0.93	625
accuracy			0.93	1200
macro avg	0.93	0.93	0.93	1200
weighted avg	0.93	0.93	0.93	1200

Fig 9: Classification Report

We have tested the model with some real and fake images. Below are some predictions of our CNN3 model on real and fake images.

```
1/1 [==============================] - 0s 14ms/step
Class: real Confidence: 99.98
```

Fig 10: Prediction of Real Image

```
1/1 [==============================] - 0s
Class: fake Confidence: 84.28
```

Fig 11: Prediction of Fake Image

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

||Volume 12, Issue 3, March2023||

|DOI:10.15680/IJIRSET.2023.1203080|

V. CONCLUSION

Aiming to detect the image splicing forgery and classify the real images and the images which undergone the splicing forgery (fake) images.This paper proposes a method based on the error level analysis and convolutional neural networks with the optimized convolutional and dropout layers.From this method, we have obtained less training time and cost with increased efficiency by increasing the complexity of the model.From our experiments, we conclude that we have obtained a Training accuracy of 96% and Validation Accuracy of 93% on the CASIAV2.0 dataset using Error Level Analysis with our CNN3 model.

REFERENCES

[1] S.S. Ali, I.I. Ganapathi, N.S. Vu, S.D. Ali, N. Saxena, N. Werghi, Image ForgeryDetectionUsingDeepLearningbyRecompressingImages,Electronics11(3),403,2022
[2] Castillo Camacho, I.; Wang, K. A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. J. Imaging 2022
[3] Devjani Mallick1, Mantasha Shaikh2, Anuja Gulhane and Tabassum Maktum, Copy Move and Splicing Image Forgery Detection using CNN,2022
[4] Ankit Kumar Jaiswal, Rajeev Srivastava, Image Splicing Detection Using Deep Learning,2020
[5] Y. Rao, J. Ni, Deep learning local descriptor for image splicing detection and localization, IEEE access, vol. 8,2020
[6] Eman I. Abd El-Latif, A. Taha, Hala H. Zayed, A passive approach for detecting image splicing using Deep Learning and Haar Wavelet Transform, Arabian journal for science and engineering, vol. 6,2020
[7] Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.
[8] Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. Image Vis. Comput. 2020, 104, 104004.
[9] Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399.
[10] Mirsky, Y.; Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Comput. Surv. 2021, 54, 1–41.
[11] Luo, W.; Huang, J.; Qiu, G. JPEG Error Analysis and Its Applications to Digital Image Forensics. IEEE Trans. Inf. Forensics Secur. 2010, 5, 480–491.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details