ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 5, May 2023

ELSCNN: A Deep Learning Architecture for Image Counterfeit Detection

[1]Subrato Kumar, [2]Shruti Garg

[1][2] Department of Computer Science and Engineering, Birla Institute of Technology, Mesra,Ranchi-835215,India
[1] subratokumar5113@gmail.com, [2]gshruti@bitmesra.ac.in

Abstract*— This study presents a novel approach to detect image forgery using Error Level Analysis (ELA) with Sequential Convolutional Neural Network (SCNN) model named as error level sequential convolution neural network (ELSCNN). ELA is a widely-used technique in detecting image manipulation that exploits the variance in compression artifacts between authentic and manipulated images. The proposed method enhances the effectiveness of ELA by integrating it with SCNN models, which learn to classify authentic and manipulated images using a large set of training data. This models are trained to detect forgery in various image manipulation scenarios. Experimental results demonstrate that the proposed method outperforms than existing ELA-based methods in respecting of accuracy, robustness, and computational ability. The proposed method has potential applications in forensic investigation, media authentication, and content verification

Index Terms*— ELA, CNN, SCNN, Deep Learning.

I. INTRODUCTION

Image forgery[1] is a growing problem in digital age, where advanced technologies and image editing software have made it uncomplicated to manipulate images. The ability to manipulate images has raised concerns about the authenticity and reliability of visual information, particularly in situations where images play a significant role, such as in news reporting, legal proceedings, and scientific research[2]. As such, there is a pressing need for effective and efficient methods to detect image forgery and ensure the authenticity of digital images.

One of the most promising methods for detecting image forgery is the use of error level analysis(ELA), it is a technique that compares the error levels of different areas within an image to identify inconsistencies that may indicate manipulation[3]. It works by compressing an image at a known error rate, and then decompressing it again, resulting in a new image with areas of different error levels[3]- [4]. Comparing the authenticate image to ELA-generated image, it identifies areas that have been altered. Fig. 1 shows an example of ELA with 90% compression level.

Fig. 1 Authentic Image

Fig. 2 Output of ELA, Image generated after applying ELA

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 5, May 2023

While ELA is a powerful technique, it is not always accurate, particularly in cases where the manipulation is subtle or sophisticated. To address this issue, researchers have explored the utilisation of machine learning techniques in this areas too, like convolutional neural networks(CNNs), to enhance the accuracy and reliability of ELA-based image forgery detection[3]. CNNs are deep learning models that are tasks. In image forgery detection, a CNN can be trained to distinguish between original and manipulated images by learning to recognize patterns and features that are indicative of image manipulation.

The advantage of CNNs is that they can be highly accurate and can detect a wide range of manipulation techniques, including those that are more complex than those detectable by ELA. However, CNNs require a abundant of training data and can be computationally expensive to train and apply.

To train a CNN for image manipulated detection using ELA, a large dataset of both authenticate and manipulated images is required. The images in the dataset must be labelled as either original or manipulated, and the CNN is trained using backpropagation to minimize the error between the predicted and actual labels. Once the CNN is trained, it can be applied to new images to classify them as either original or manipulated.

Author of [5] proposed a technique to determine splicing image forgery using LBP and DCT. The method split the image chromatic component into blocks and transformed each block's LBP code into the DCT domain, using the standard deviation of DCT coefficients as features for classification with an SVM. The proposed method outperformed other color channels and achieved high accuracy on various datasets.

Author of [6] proposed technique for detecting forgery in images using two methods based on the Discrete Cosine Transform(DCT) and Scale Invariant Feature Transform(SIFT) algorithms. The proposed technique combines these methods to improve the accuracy of the detection. The experimental results show that the proposed technique can effectively detect both types of forgery with high accuracy.

II. TYPES OF IMAGE FORGERY TECHNIQUES

Digital image forgery is the act of altering or manipulating a digital image to deceive the viewer. This can be achieved through various techniques. Digital forgery is becoming more prevalent with the rise of digital technology and social media platforms. It can be used for malicious purposes, such as spreading fake news, creating propaganda, or even blackmailing individuals. Detecting digital image forgery is a challenging task, and researchers are constantly developing new methods and algorithms to address this issue.

Digital image forgery techniques, includes various types:

A. Copy-move forgery: In this type forgery in which portion of an image is duplicated and pasted onto another part of the same image, with the intention of deceiving the viewer. This technique is often used to conceal or duplicate important information, such as a watermark or object within the image[6].

B. Splicing: In this type of forgery, different parts of different images are integrated to create a different image, which can be used to create a false narrative or deceive viewers[7].

C. Image retouching: This is the process of altering an image's colours, brightness, contrast, or other properties to make it look more appealing or convincing. Image retouching can be used to manipulate the appearance of people, objects, or locations in an image[8].

D. Image Inpainting: This type of forgery involves changing the colour of an object or area in an image to create a different impression or to hide something[9].

E. Image resizing: This is the process of enlarging or reducing an image's size, which can be used to crop out unwanted details or add new content to an image.

F. Object removal: This type of forgery, an portion or a person is removed from an image using photo editing tools. This can be done to change the context of an image or to create a false narrative.

G. Metadata manipulation: Image metadata contains details of the camera, location, and other details of an image. Manipulating this metadata can change the context of an image or create a false impression[10].

III. METHODOLOGY

The methodology for image forgery detection using ELSCNN is shown in Fig. 2:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 5, May 2023

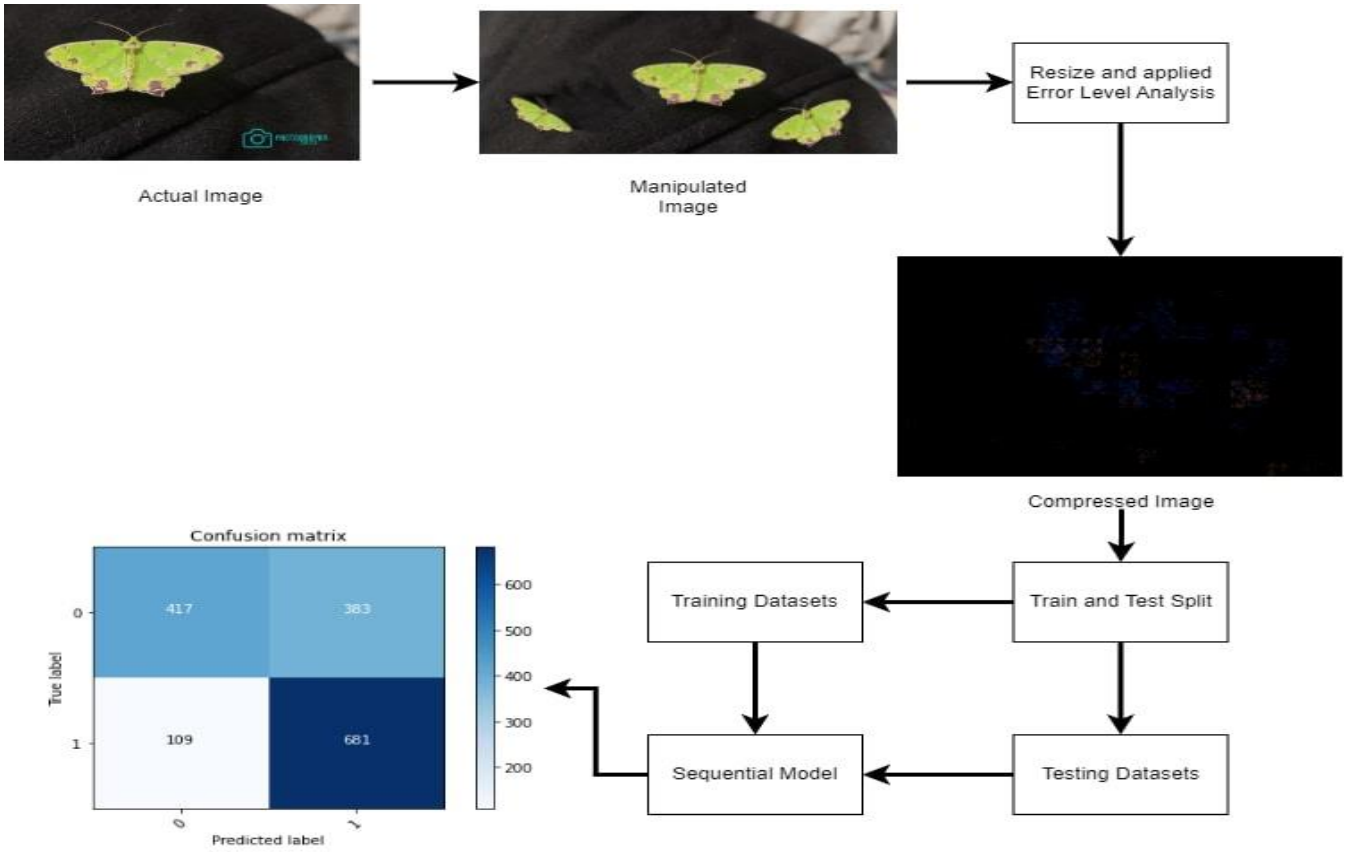

Fig. 3 Overall proposed methodology for image forgery detection with the use of error level analysis and CNN

The methodology describe in Fig 3 consist of following steps:

1. Aquisition of data is done from CASIA V2.0 [10] dataset containing 7491 authenticate images and 5123 manipulated images and added few more from my own image folder for better training the model.
2. In order to convert all images of similar size the images are rescaled to 128*128 pixel using python resize() function.
3. Pre-process the images using ELA to generate an error map.
4. Segregate the dataset into two distinct subsets:training sets(80%) and testing sets(20%).
5. Train the SCNN on the training set using the error maps generated by ELA
6. Validate the trained SCNN with the validation set.
7. Test for trained SCNN with the testing set.
8. Evaluate the attainment of the method using metrics through accuracy, precision, recall.
9. Check in which portion image has been manipulated.

IV. EXPERIMENTS AND RESULTS

The experiments are performed in Jupyter Notebook with GPUv512.78 enabled Pythonv3.9.12.

In this experiment a python function called convert_to_ela_image() is required that takes two parameters

path and quatity. Path defines the location of image file and quality is an integer that represents the quality of the JPEG compression that will be used to create a temporary file.

This function first creates a temporary JPEG file from our input image with the specified quality. Then, it opens both original image as well as the manipulated image and computes the ELA image by taking the difference between the two images using the ImageChops.difference() function.

After computing the ELA image, the function normalizes the pixel values to a range between 0 and 255 by calculating the extrema of the pixel values using the getextrema() method, and then scales the brightness of the image using ImageEnhance.Brightness() and the enhance() method. Finally, the function returns the resulting ELA image as a python imaging library image object.

After pre-processing, the SCNN is applied using the Keras library of Python architecture shown in Fig 4.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 5, May 2023

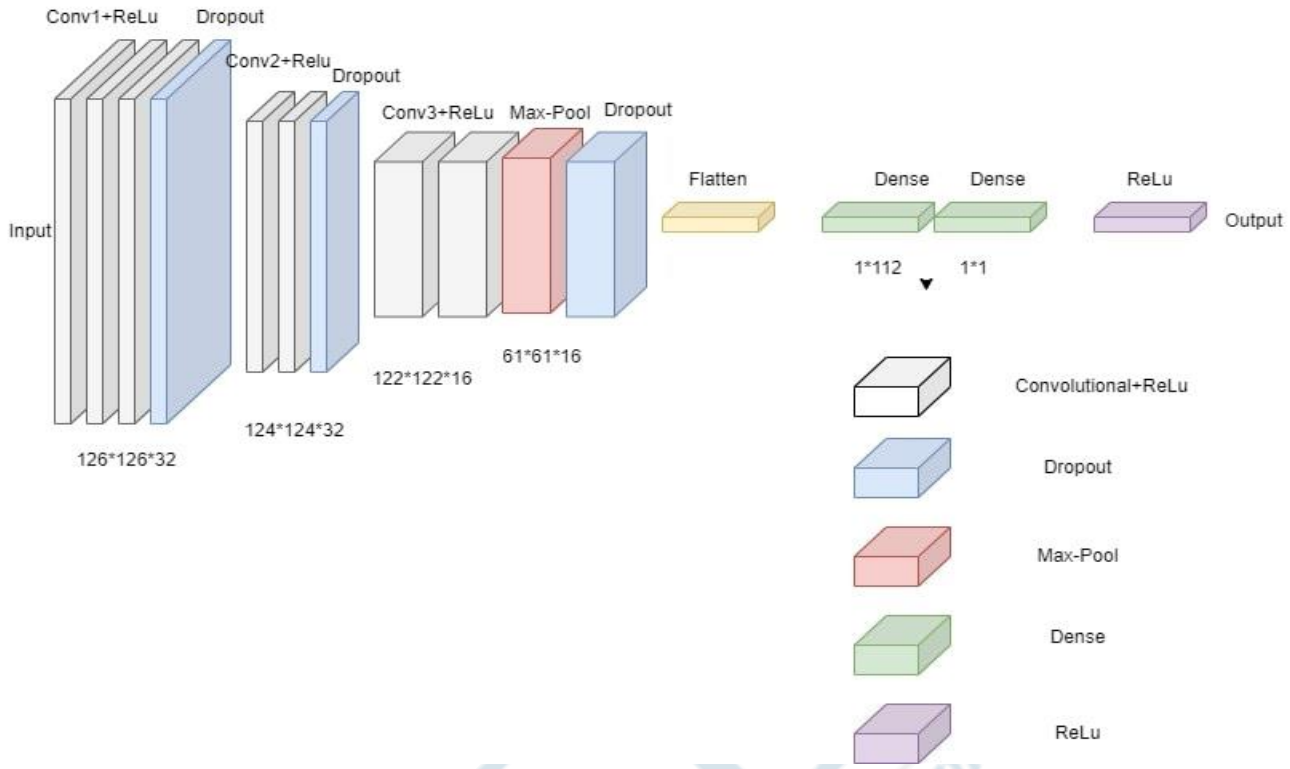

Fig.4 Sequential convolutional architecture of our model.

The network consists of 3 convolutional layers with increasing numbers of filters and a kernel size of 3x3. Each convolutional layer is stalked by a Rectified Linear Unit (ReLU) which is a activation function, which adds non-linearity to the model. The first layer of convolutional also takes input shape of 128x128x3, where 3 is number of colour channels in the image.

The model includes a max pooling layer with pool size of 2x2, which reduces the dimensionality of feature maps produced by the each convolutional layers. This is followed by a dropout layer with a rate of 0.25, which randomly drops out 25% of the neurons to prevent overfitting.

The output of the dropout layer is then flattened into 1D array and then again passed through fully connected layer with 112 neurons and a ReLU activation function. Another dropout layer with a rate of 0.5 is added to this fully connected layer to further prevent overfitting. Finally, the output layer consists of a single neuron, with no activation function specified, which makes this a regression problem as shown below.

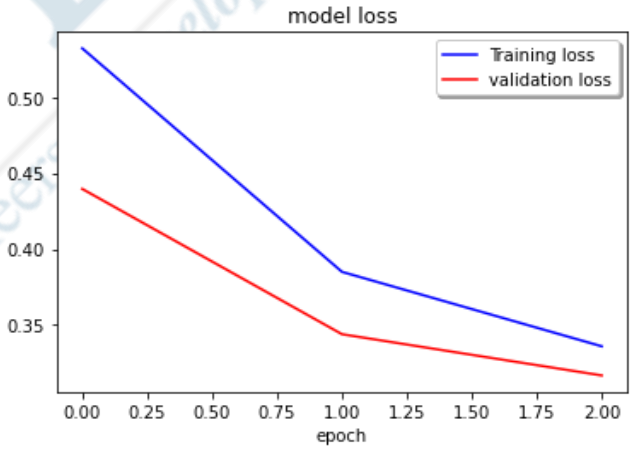

Fig. 5 Plot between loss vs epoch in the CNN model

The function returns the compiled Keras model, which can be used to train and evaluate the performance of the SCNN on a specific dataset. The new model variable is assigned to the

output of this function, allowing the user to access and manipulate the model as needed.

After fitting the model the test accuracy is observed as 69.24% after 10 epochs. Fig. 4 shows the plot between loss and epoch for 10 epoches.

It is observed from Fig 5 that validation loss and training loss

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 5, May 2023

have the minimal gap that tells there is very less chance for overfitting.

Overfit occurs when the model is trained too well on training data, to the point where it starts to memorize the data instead of learning patterns from it. This results in poor performance on new, unseen data.

Further, a plot between accuracy and epoches is shown in Fig. 6. From Fig. 6 it is observed that the training and validation accuracy curve are moving in same direction that rules out the chances of overfitting.

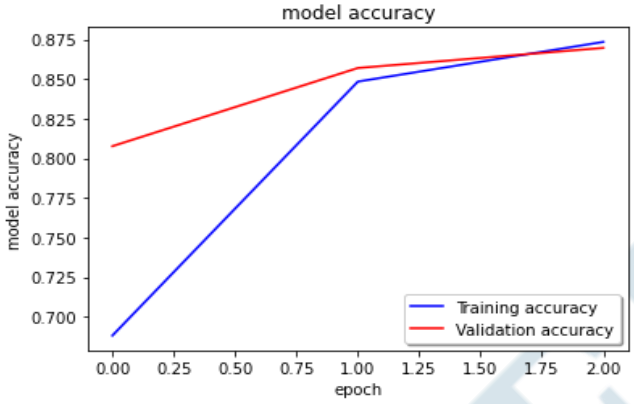

Fig. 6 Plot between model accuracy vs epoch in the CNN model

A comparison of proposed ELSCNN model is performed with the MobileNet model for the same datasets is calculated in terms of accuracy and loss, shown in Table 1.

TABLE I

Comparision of accuracies obtained by diffent models.

Datasets	**Model Name**	**Accuracy(in%)**	**Loss(in%)**
Casia V2+Our datasets	ELSCNN	69.25	76.04
Casia V2+Our datasets	MobileNet	64.4	66.07

V. CONCLUSION

The research work presented here is found important in various type of image forgery that can help to artist, photographers, lawyers and different other professionals to find counterfiet images automatically. The accuracy of counterfiet is dependent on type of operations performed. For example, when the forgery was a simple copy-paste operation or any one type of manipulated image the accuracy was over 90%. However, when the forgery involved more complex manipulation or combination of different of forgery such as image splicing, retouched image, the accuracy dropped to around 69%. This suggests that more complex forgery task such as digital watermark, digital signature are need to researched in future. To improve accuracy in complex forgery task an efficient preprossing method need to be devised. The simplicity of proposed model increases it applicability in various domain.

REFERENCES

[1] H. Farid, "Image forgery detection," *IEEE Signal Process Mag*, vol. 26, no. 2, pp. 16–25, 2009, doi: 10.1109/MSP.2008.931079.

[2] T. Qazi *et al.*, "Survey on blind image forgery detection," *IET Image Process*, vol. 7, no. 7, pp. 660–670, Oct. 2013, doi: 10.1049/IET-IPR.2012.0388.

[3] I. B. K. Sudiatmika, F. Rahman, Trisno, and Suyoto, "Image forgery detection using error level analysis and deep learning," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 2, pp. 653–659, Apr. 2019, doi: 10.12928/TELKOMNIKA.V17I2.8976.

[4] "Image Forensics : Error Level Analysis." http://www.errorlevelanalysis.com/ (accessed Dec. 08, 2022).

[5] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in *2013 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2013 - Proceedings*, 2013, pp. 253–256. doi: 10.1109/GlobalSIP.2013.6736863.

[6] M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," *AASRI Procedia*, vol. 9, pp. 84–91, 2014, doi: 10.1016/j.aasri.2014.09.015.

[7] M. K. Alshwely and S. N. AlSaad, "Image splicing detection based on noise level approach," *Al-Mustansiriyah Journal of Science*, vol. 31, no. 4, pp. 55–61, Dec. 2020, doi: 10.23851/mjs.v31i4.899.

[8] A. Kaur and J. Rani, "Digital Image Forgery and Techniques of Forgery Detection: A brief review," 2016, Accessed: Mar. 25, 2023. [Online]. Available: www.ijtrs.com

[9] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, and X. Sun, "A robust forgery detection algorithm for object removal by exemplar-based image inpainting," *Multimed Tools Appl*, vol. 77, no. 10, pp. 11823–11842, May 2018, doi: 10.1007/S11042-017-4829-0/TABLES/7.

[10] "What is image metadata and how is it used?" https://www.techtarget.com/whatis/definition/image-metadata (accessed Mar. 25, 2023).