Image Splicing Detection using Deep Learning

Master of Technology

in

Computer Science and Engineering

by

Umang Chaturvedi (17CS60R69)

Guided by

Prof. R.S. Chakraborty

Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

November 2018

Declaration

This is to certify that

1. The work contained in this thesis is original and has been done by myself under the general supervision of my supervisor.
2. The work has not been submitted to any other Institute for any degree or diploma.
3. I have followed the guidelines provided by the Institute in writing the thesis.
4. I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.
5. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.
6. Whenever I have quoted written materials from other sources, I have put them under quotation marks and given due credit to the sources by citing them in the text of the thesis and giving their details in the references.

Umang Chaturvedi
Department of CSE
IIT Kharagpur

Date : Nov 12, 2018

Certificate

This is to certify that the thesis titled **Image Splicing Detection using Deep Learning** submitted by **Umang Chaturvedi (17CS60R69)** to the Department of Computer Science and Engineering is a bonafide record of work carried out by him under my supervision and guidance. The thesis has fulfilled all the requirements as per the regulations of the Institute and, in my opinion, has reached the standard needed for submission.

Dr. R.S. Chakaborty
Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Nov 12, 2018

Abstract

The images often are manipulated with the intent and purpose to benefit one party. In fact, the picture is often seen as evidence of a fact or reality, therefore, fake news or any publication form using an image that is already manipulated in such a way have the capability and the potential to mislead a more large. To detect the falsification of the image, it takes large amounts of image data, and models that can process each pixel in the image. In addition, efficiency and flexibility in the training data are also needed to support it is used in everyday life. The concept of deep learning is the right solution for this problem. Therefore, we proposed the architecture of the Convolutional Neural Network (CNN) which utilizes the Error Level Analysis (ELA) to detect most popular image forgery i.e. image splicing forgery in and achieved 89.37% accuracy.

Acknowledgment

I would like to thank my supervisor Prof. R.S. Chakraborty, associate professor, dept. of CSE, IIT Kharagpur for his valuable guidance and consistent support. I would also like to thank Ms. Diangarti Tariang, PhD Scholar, dept. of CSE, IIT Kharagpur, who has been very much involved in this project. Without her tremendous support, this work might not be finished so early.

I am grateful to my parents for their unconditional love and support. I have learned a lot from the professors and my friends in IIT Kharagpur. Thanks to all of them.

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

With the availability of various image editing software, it has become possible to create visually plausible image forgeries with a minimal effort. Because of this, a large number of forged images are now available on the web. These images when used on different platforms, like the electronic and social media, may create tensions in the society. These concerns necessitate the development of image forensics techniques for checking the authenticity of images before using them as critical information.

While creating a forgery, the forged parts are often processed through different image editing operations to make them look visually plausible. For example, in image splicing forgery the spliced objects go through different image editing operations, e.g. resizing, rotating, smoothing, contrast enhancement, compression. Although imperceptible to human eyes, every image editing operation leaves a unique trace of manipulation. These traces are utilized by researchers to detect different types of editing operations performed on images. Different techniques have been proposed to extract features related to the traces left by different editing operations, and which are utilized to check the authenticity of images.

1.2 Types of Image forgery

Picture altering is characterized as adding, changing, or deleting some important features from an image without leaving any obvious trace. There have been different techniques utilized for forging an image. Taking into account the methods used to make forged images, digital image forgery can be isolated into three primary classifications: Copy-Move forgery, Image splicing, and Image resampling.

1.2.1 Copy-Move Forgery

In copy-move forgery (or cloning), some part of the picture of any size and shape is copied and pasted to another area in the same picture to shroud some important data as demonstrated in Figure 1.1. As the copied part originated from the same image, its essential properties such as noise, color and texture dont change and make the recognition process troublesome.

Figure 1.1: Example of Copy-Move Forgery
(a) Original Image (b) Tampered Image [1]

1.2.2 Image Splicing Forgery

Image splicing is the form of digital image forgery where the forger combines regions from multiple images into a single image, so as to form a natural looking composite image. However, such modifications are detectable by investigating inconsistencies in natural statistics of the image. Figure 1.2 shows the example of image splicing forgery.

Figure 1.2: An example of image splicing
(A) and (B) are the genuine images (C) The resulted image. [2]

1.2.3 Image Retouching Forgery

Image Retouch refers to making small changes to your photos in order to improve them using any photo editing software. Retouching may be in various ways, such as color change, background remove, making shadow, liquify shapes, fix imperfection of photos, etc. Figure 1.3 shows the example of image retouching.

(a) (b)

Figure 1.3: An example of image retouching : (a) original, (b) Retouched image. [3]

Chapter 2

Literature Survey

2.1 Types of Image Forgery detection methods

Digital image forgery detection techniques are grouped into two categories such as active approach and passive approach. In the active approach, certain information is embedded inside an image during the creation in form of digital watermark. Drawback of this approach is that a watermark must be inserted at the time of recording, which would limit to specially equip digital cameras. In the passive approach, there is no pre-embedded information inside an image during the creation. This method works purely by analyzing the binary information of an image. Passive image forgery detection techniques roughly grouped into four categories.

2.1.1 Pixel-based image forgery detection

Pixel-based techniques accentuate on the pixels of the digital image. These techniques are generally classified into four sorts such as copy-move, splicing, resampling and statistical.

2.1.2 Format-based image forgery detection

Format based techniques are another kind of image forgery detection techniques. These are mainly based on image formats, in which JPEG format is preferable. Statistical correlation introduced by specific lossy compression schemes, which is helpful for image forgery detection. These techniques can be partitioned into three sorts such as JPEG quantization, Double JPEG and JPEG blocking. If the image is compressed then it is exceptionally hard to identify fraud however these techniques can detect forgery in the compressed image.

2.1.3 Camera-based image forgery detection

Whenever we take a picture from a digital camera, the picture moves from the camera sensor to the memory and it experiences a progression of processing steps, including quantization, color correlation, gamma correction, white adjusting, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may shift on the premise of camera model and camera antiques.
These techniques work on some standards. These methods can be separated into four classes such as chromatic aberration, color filter array, camera response and sensor noise.

2.1.4 Physical environment-based image forgery detection

These techniques basically based on three dimensional interactions between physical object, light and the camera. Consider the creation of a forgery showing two movie stars, rumored to be romantically involved, strolling down a nightfall shoreline. Such a picture may be made by grafting together individual pictures of each movie star. In this manner, it is frequently hard to exactly match the lighting effects under which each individual was initially captured.
Contrasts in lighting across an image can be utilized as proof of altering. These techniques work on the basis of the lighting environment under which an article or picture is caught. Lighting is very important factor for capturing an image. These techniques are

isolated into three classifications such as light direction (2-D), light direction (3-D) and light environment.

2.2 Image Splicing forgery detection techniques

Image splicing forgery technique involves composition or merging of two or more images changing the original image significantly to produce a forged image. In case images with differing background are merged then it becomes very difficult to make the borders and boundaries indiscernible.
Splicing detection is a complex problem whereby the composite regions are investigated by a variety of methods. The presence of abrupt changes between different regions that are combined and their backgrounds, provide valuable traces to detect splicing in the image under consideration. This section reviews some of the existing techniques to detect image splicing forgery.

1. **Lin et al.** [4] proposed an integrated technique for splicing and copy-move image forgery detection in 2011. First, the authors converted an image into the YCbCr colour space. For splicing detection, the image is divided into sub-blocks and DCT is used for feature extraction. For copy-move detection, SURF is used. The algorithm works well in both splicing and copy-move image forgery detection.

2. **Lin Z et al.** [5] proposed an approach that computes the response functions of the camera by selecting appropriate patches in different ways. The splicing forgery is found on the basis of whether the response functions are abnormal or inconsistent to each other. The normality of the response functions is classified by a trained support vector machine (SVM). This method was effective for high-contrast images only.

3. **Alahmadi et al.** [6] proposed a technique based on features extracted from the chromatic channel. After chrominance component is extracted, image is divided

into overlapping blocks. Then, LBP is calculated for each block and transformed into 2D DCT. Further the frequency coefficients are evaluated to find the standard deviations for all blocks and those acts as features. For classification support vector machine (SVM) is used.

4. **Liu et al.** [7] presented image splicing detection based on multiresolution histogram to detect the splicing between two images for this two factors are considered one is the feature that characterize image and other is the classifier which gives result of detection techniques in this the multiresolution histogram of the image act as feature which provides the spatial information of the image, and then subjected to SVM classifier to find out the image forgeries and to check whether the digital image is spliced or unspliced.

5. **Chen et al.** [8] proposed a median filtering detection method based on convolutional neural networks (CNNs), which can automatically learn and obtain features directly from the image. They used first layer of CNN framework as a filter layer that accepts an image as the input and outputs its median filtering residual (MFR). Then, via alternating convolutional layers and pooling layers to learn hierarchical representations. The results show that the proposed method achieves significant performance improvements, especially in the cut-and-paste forgery detection.

6. **Rao et al.** [9] proposed CNN which is specifically designed for image splicing and copy-move detection applications. Rather than a random strategy, the weights at the first layer of our network are initialized with the basic high-pass filter set used in calculation of residual maps in spatial rich model (SRM), which serves as a regularizer to efficiently suppress the effect of image contents and capture the subtle artifacts introduced by the tampering operations. The pre-trained CNN is used as patch descriptor to extract dense features from the test images, and a feature fusion technique is then explored to obtain the final discriminative features for SVM classification.

Chapter 3

Implementation

3.1 Method used

To classify tampered and authentic images, we used deep learning architecture to extract features automatically. Specifically, We used error level analysis (ELA) to detect areas of an image that may have been tampered then, Convolution Neural Network (CNN) / (Recurrent Neural Network (RNN) is used to train a supervised model for classifying whether an image is authentic or tampered. Below figure 3.1 is the flow chart of model used.

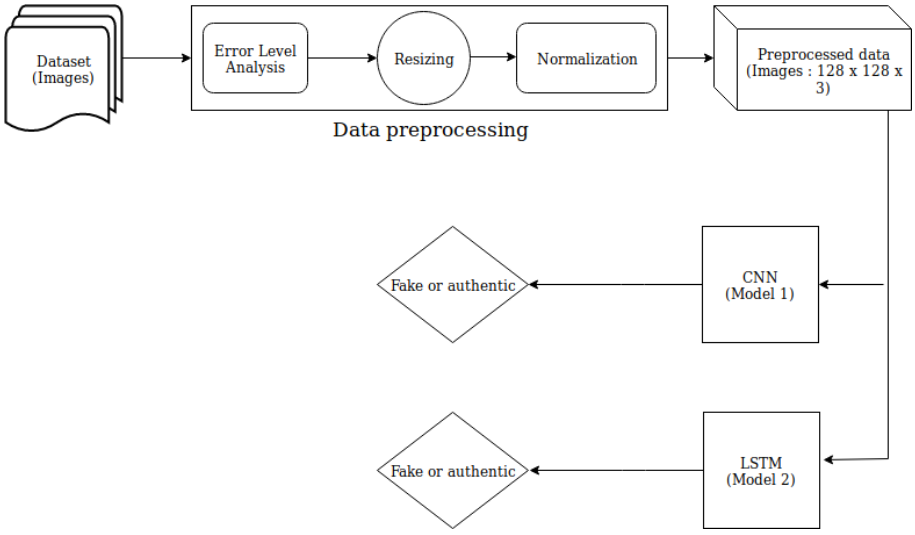

Figure 3.1: Flow chart of model

3.2 Error level analysis

Error Level Analysis is one of the techniques used for detecting image manipulation by way of storing pictures on the anniversary of a certain quality level and calculating the comparison between its levels. In General, this technique is performed on an image that has a lossy format (lossy compression). Picture type used in mining this data is JPEG. On JPEG images, compression is done independently for each 8 x 8 pixels in the image. If an image is not manipulated, each 8 x 8 pixel on the image must have had the same error level.

Figure 3.2: An example of ela output of authentic image from dataset used

With JPEG, saving a picture causes the colors to change a little. The ELA results highlight the areas in the image that are most prone to color degradation during a resave. Edits typically stand out as being a region with a higher degradation potential compared to the rest of the image. ELA saves the image at a specified JPEG quality level. This resave introduces a known amount of error across the entire image. The resaved image is then compared against the original image. If the image is completely unmodified, then all 8x8 squares should have similar error potentials. If the image is unmodified and resaved, then every square should degrade at approximately the same rate. If an image is modified, then every 8x8 square that was touched by the modification should be at a higher error potential than the rest of the image. Modified areas will appear with a higher potential

error level. Figure 3.2 and 3.3 show the ela output of authentic and tampered images from the dataset used respectively.

Figure 3.3: An example of ela output of tampered image from dataset used

3.3 Convolutional Neural Network (CNN)

3.3.1 Architecture used

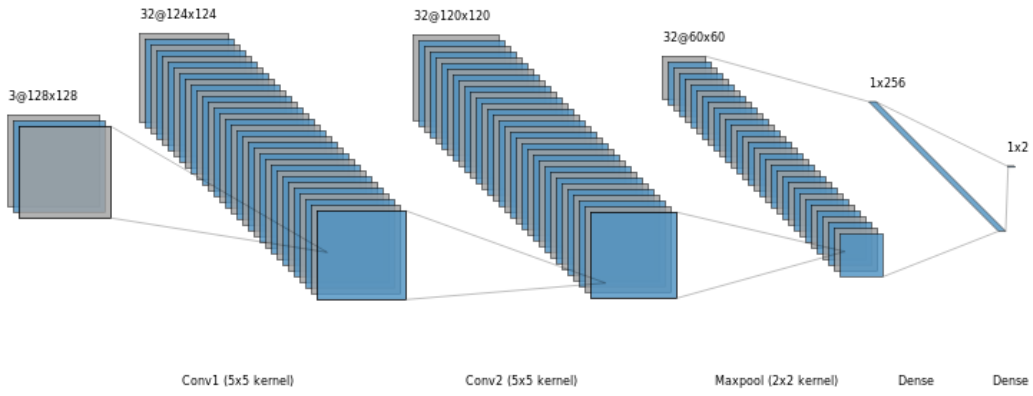

Figure 3.4: Architecture of proposed CNN

3.3.2 Parameters' value

Learning rate	0.005
Optimizer	RMSprop
Loss	Categorical crossentropy
Batch size	32
epochs	100

3.4 Recurrent Neural Network (RNN)

3.4.1 Architecture used

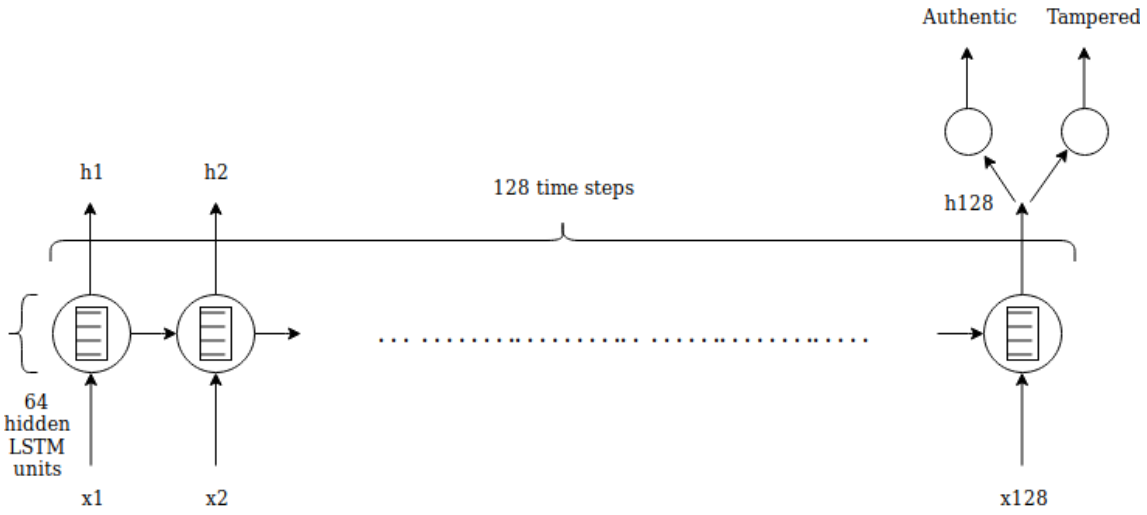

Figure 3.5: Architecture of proposed RNN

3.4.2 Parameters' value

Cell type	LSTM
Hidden units	64
Time steps	128
Input size	128
Learning rate	0.01
Optimizer	RMSprop
Loss	Categorical crossentropy
Batch size	32
epochs	200

3.5 Dataset used

We used CASIA-v2 database [10]. It consists of 7437 authentic and 5123 tampered images of various sizes from 240x160 to 900x600 with JPEG, BMP, and TIFF formats.
For training and testing purpose, we kept 80% of data for training and rest for testing.

Chapter 4

Results

4.1 Performance matrix for CNN and RNN

	CNN Model	RNN Model
Accuracy	89.37%	76.92%
Precision	83.14%	70.76%
Recall	93.40%	90.36%
F1 score	0.879	0.795

4.2 Outcomes

4.2.1 Confusion matrix of CNN

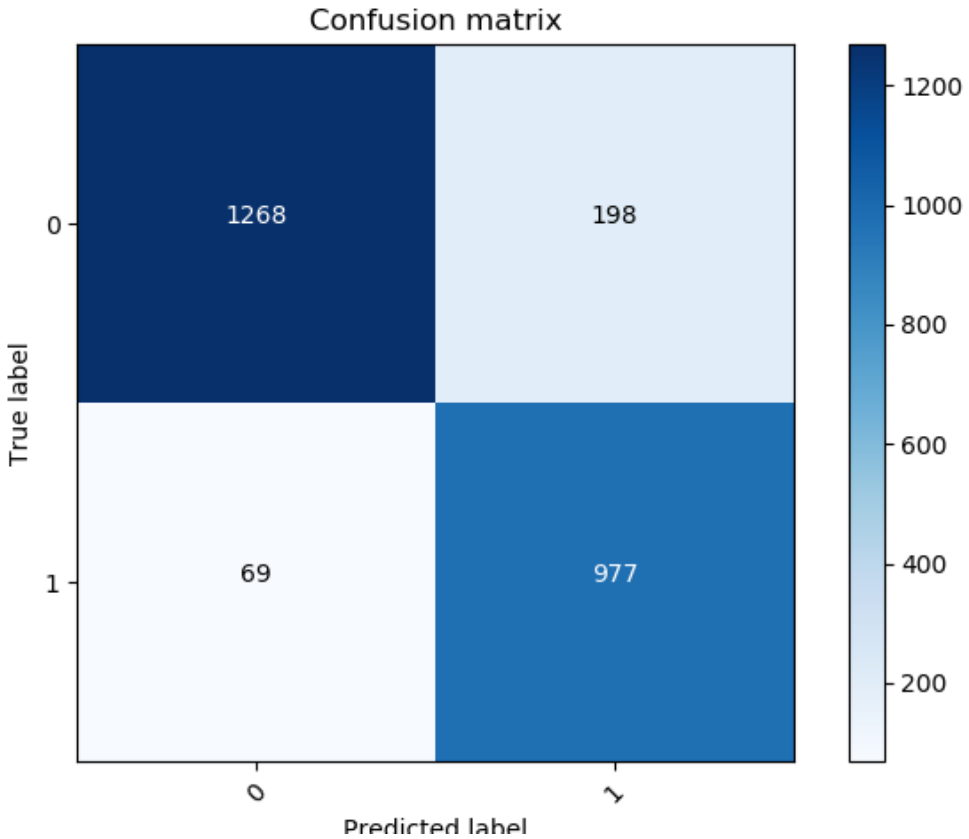

Figure 4.1: Confusion matrix of results of CNN on testdata

4.2.2 Confusion matrix of RNN

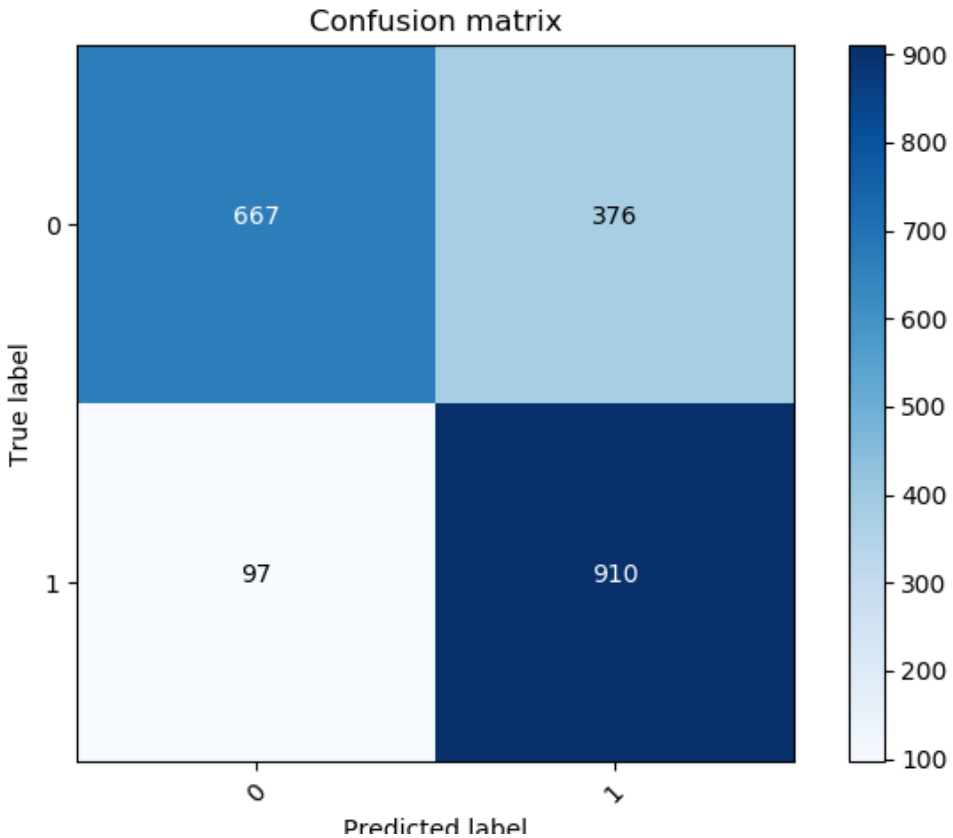

Figure 4.2: Confusion matrix of results of RNN on testdata

4.3 Performance curves

4.3.1 Performance curve of CNN

Figure 4.3: Performance curve of results of CNN on testdata

4.3.2 Performance curve of RNN

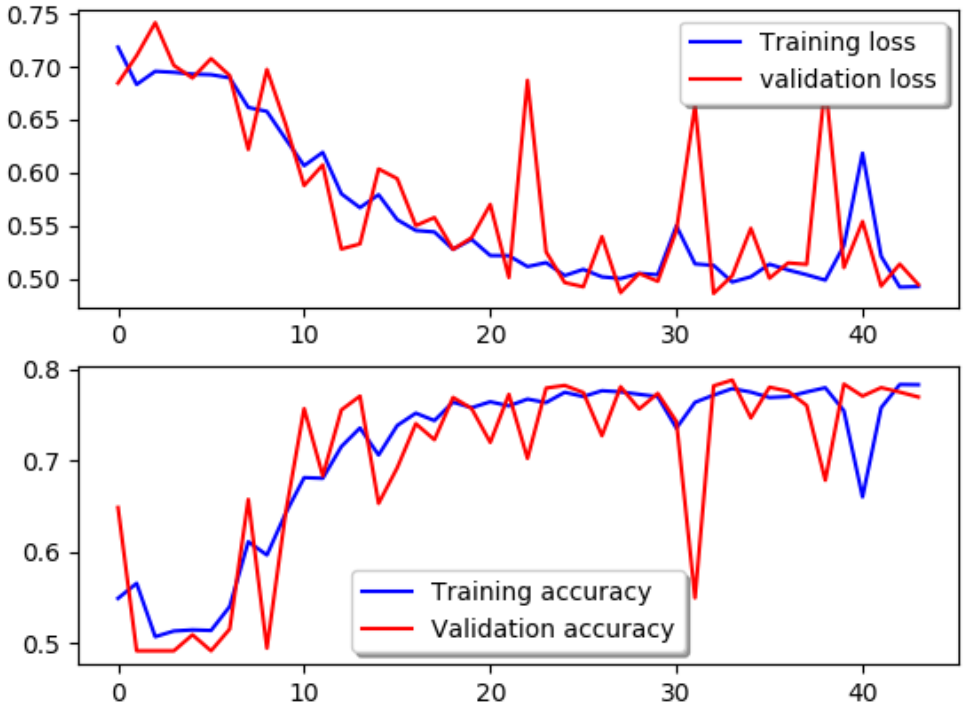

Figure 4.4: Performance curve of results of RNN on testdata

Chapter 5

Conclusions and Future Work

5.1 Conclusion

In this research, there are several things that can be inferred from the results of using ELA with (CNN/ RNN).

1. CNN outperforms the RNN (LSTM) model and achieved accuracy of 89.37% while RNN got 76.92%.
2. ELA usage can increase the efficiency and reduce the cost of computing the training process.

5.2 Future Scope of Work

1. We will work on localization of tampered region.
2. Work on all kind of forgery detection that also includes different filtering mechanism of images.
3. Include all formats of image.
4. Will work on improving accuracy.

Bibliography

[1] Scientific Figure on ResearchGate. Blind approach for digital image forgery detection, 2018. [Online; accessed Nov 12, 2018].

[2] Scientific Figure on ResearchGate. Copy-move forgery detection using integrated dwt and surf, 2018. [Online; accessed Nov 12, 2018].

[3] Scientific Figure on ResearchGate. Color-enriched gradient similarity for retouched image quality evaluation, 2018. [Online; accessed Nov 12, 2018].

[4] S.D.Lin and T. Wu. An integrated technique for splicing and copy-move forgery image detection. In *IEEE 4th International Congress on Image and Signal Processing (CISP)*, 2011.

[5] Lin Z , Wang R , Tang X and Shum H-Y. Detecting doctored images using camera response normality and consistency. In *IEEE conference on computer vision and pattern recognition (CVPR)*, 2005.

[6] A. Alahmadi , M. Hussain , H. Aboalsamh , G. Muhammad and G. Bebis. Splicing image forgery detection based on dct and local binary pattern. In *Global Conference on Signal and Information Processing (GlobalSIP)*, 2013.

[7] Jin Liu , Hefei Ling , Fuhao Zou and Zhengding Lu. Image splicing detection using multi - resolution histogram. In *"Springer", pp.858-866*, 2009.

[8] J. Chen , X. Kang , Y. Liu and Z. J. Wang. Median filtering forensics based on convolutional neural networks. In *IEEE Signal Processing Letters, vol. 22, no. 11, pp. 1849-1853*, 2015.

[9] Rao , Yuan 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)*, 2016.

[10] Jing Dong , Wei Wang and Tieniu Tan. Casia image tampering detection evaluation database. In *IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, 2013.