Image Splicing forgery detection using deep learning

Under the guidance of:
Prof. R. S. Chakraborty

Presented by:
Umang Chaturvedi
M.Tech (CSE)
17CS60R69

Types of image tampering

Image Splicing (copy – paste)

addition of new objects from different images

(a) (b) (c)

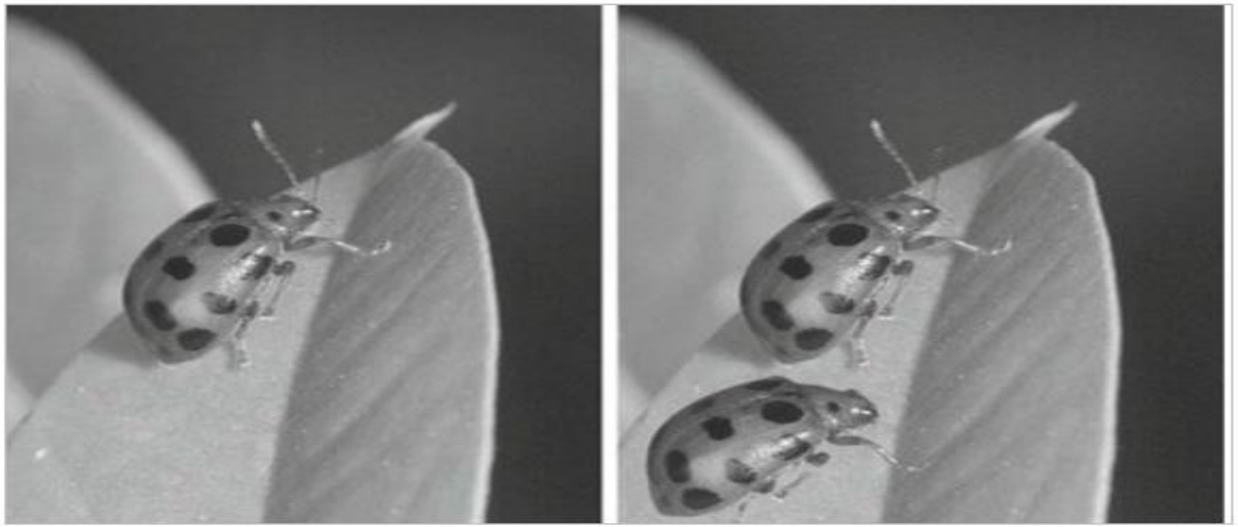
An example of image splicing. (A) and (B) are the genuine images (C) The resulted image.

Source : https://www.researchgate.net/Example-of-Copy-Move-Forgery-a-Original-Image-b-Tampered-Image-17_fig3_32257459

Types of image tampering

Image Cloning (copy – move)

tampering occurs within a single image



(a) (b)

An Example of Copy-Move Forgery (a) Original Image (b) Tampered Image.

Source: https://www.researchgate.net/An-example-of-image-splicing-A-and-B-The-genuine-images-C-The-resulted-image_fig3_316667407

Types of image tampering

Image Retouching

Changes in colour, contrast, brightness etc. of image

(a) (b)

An example of image retouching: (a) original, (b) retouched.

Source : https://www.researchgate.net/An-example-of-image-retouching-left-original-right-retouched_fig1_296472356

Literature survey

There are three methods that are mainly used :

- JPEG based methods
- Camera based methods
- Data – driven methods

JPEG based method

- The key point in this kind of approach is JPEG compression.
- Edition performed on an original JPEG image, will occur a double JPEG compression, which is an evidence to detect traces left on the image.
- Eg. Bianchi et al.[1] proposed a Bayesian approach to automatically calculate doubly compressed probability map of 8x8 DCT (Discrete Cosine transform)patches in an image.

JPEG based method

A composite image, where the different parts have different JPEG compression levels

The same image with a uniform 90% quality JPEG compression

The difference between the two images shows a variation of the JPEG compression artifacts

An example of JPEG based tampering detection
Source : https//en.wikipedia.org/wiki/Error_level_analysis

Camera based method

- This method has also been explored where the detection is based on demosaicing regularity or sensor pattern noise where the irregularities of the sensor patterns are extracted and compared for anomalies.

- Eg. Lyu et al. [2] revealed the inconsistencies of local noises due to camera sensors or post-processing.

Data-driven method

- Specifically, this approach feeds a great deal of data into an Artificial Neural Network in order to automatically learn optimal features representing for the data.

- Eg. Rao et al. [3] proposed a CNN to detect splicing and copy-move forgeries. However, instead of using normal initialization, they assigned a Spatial Rich Model to the first layer to reduce image content while reserving artifacts.

Proposed methodology

- Used Error level analysis (ELA) to detect areas of an image that may have been tampered. A (Convolutional neural network CNN/Recurrent neural network RNN)is used to train a supervised model for classifying whether an image is authentic or tampered.

- Images are preprocessed by performing ELA to focus on the detection of JPEG compression artifacts instead of image feature extraction.

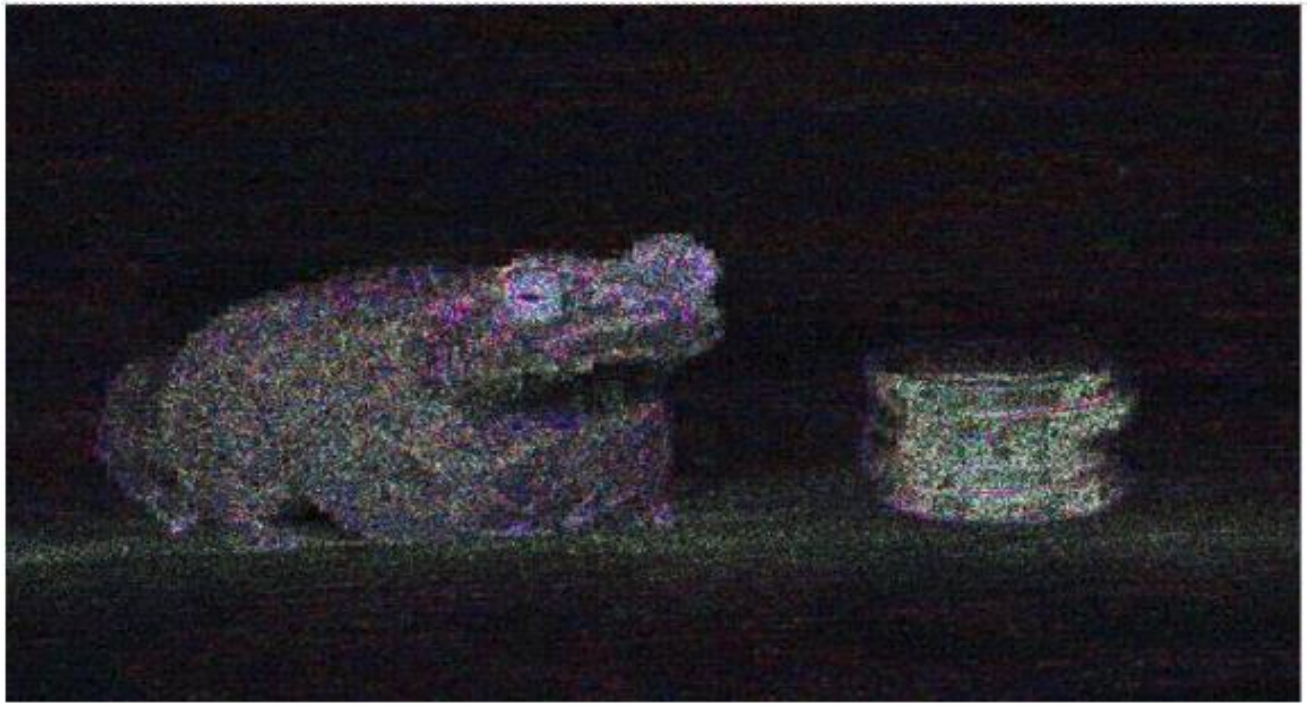
Error level analysis

- Error level analysis is the analysis of compression artifacts in digital data with lossy compression such as JPEG.

- In JPEG, each resave intoduces more error.

- 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.

(a) Original image (b) Tampered image



Ela output of tampered image.
Source : https://sites.google.com/site/elsamuko/forensics/ela

Ela example

The Error Level Analysis gives a hint for the manipulations at the toad's head and the coins.

Error level analysis

Methodology :

- Resave the image with 95% (or 90%) JPEG quality.

- Compare each (8 x 8) blocks of corresponding original and new resaved image.

- If image is unmodified, then all 8x8 squares should have similar error potentials.
- else, modified areas will appear with a higher potential error level.

Ela output of images from dataset used

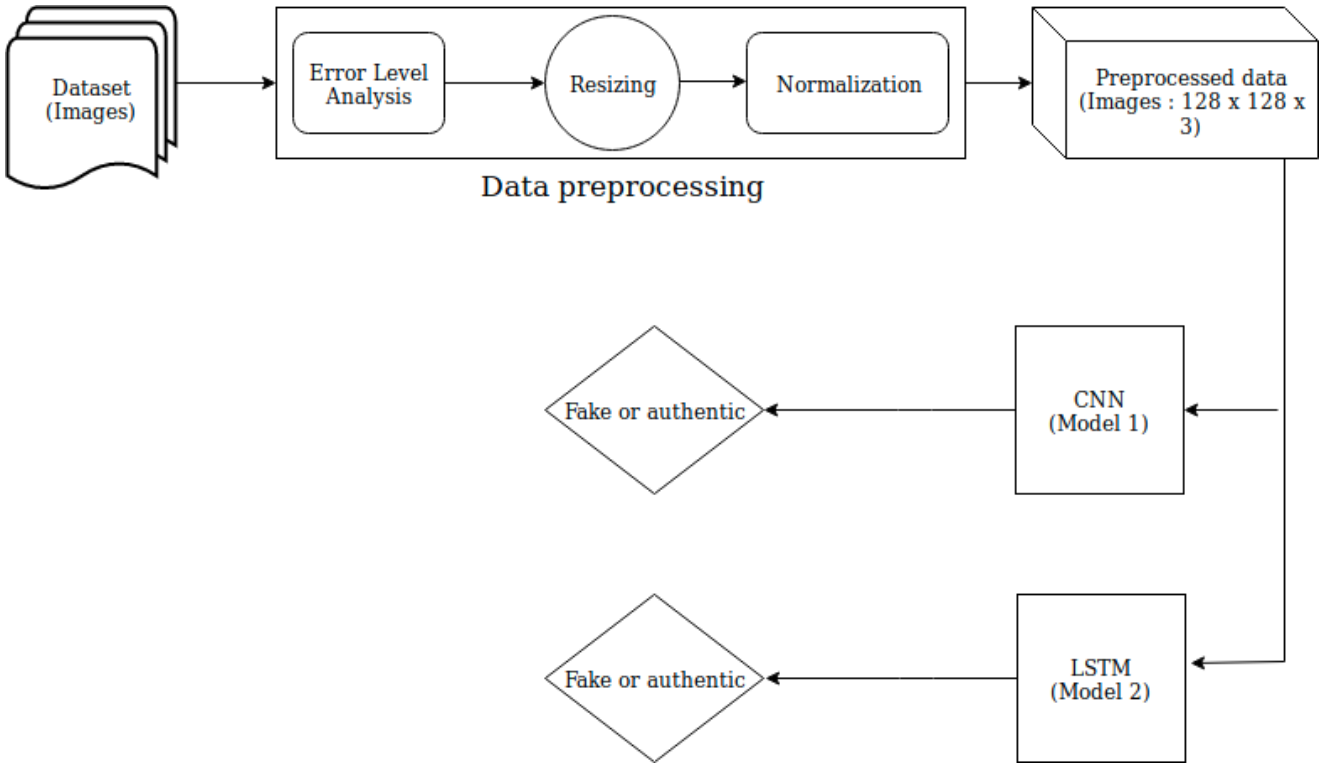
ELA OF AUTHENTIC IMAGE

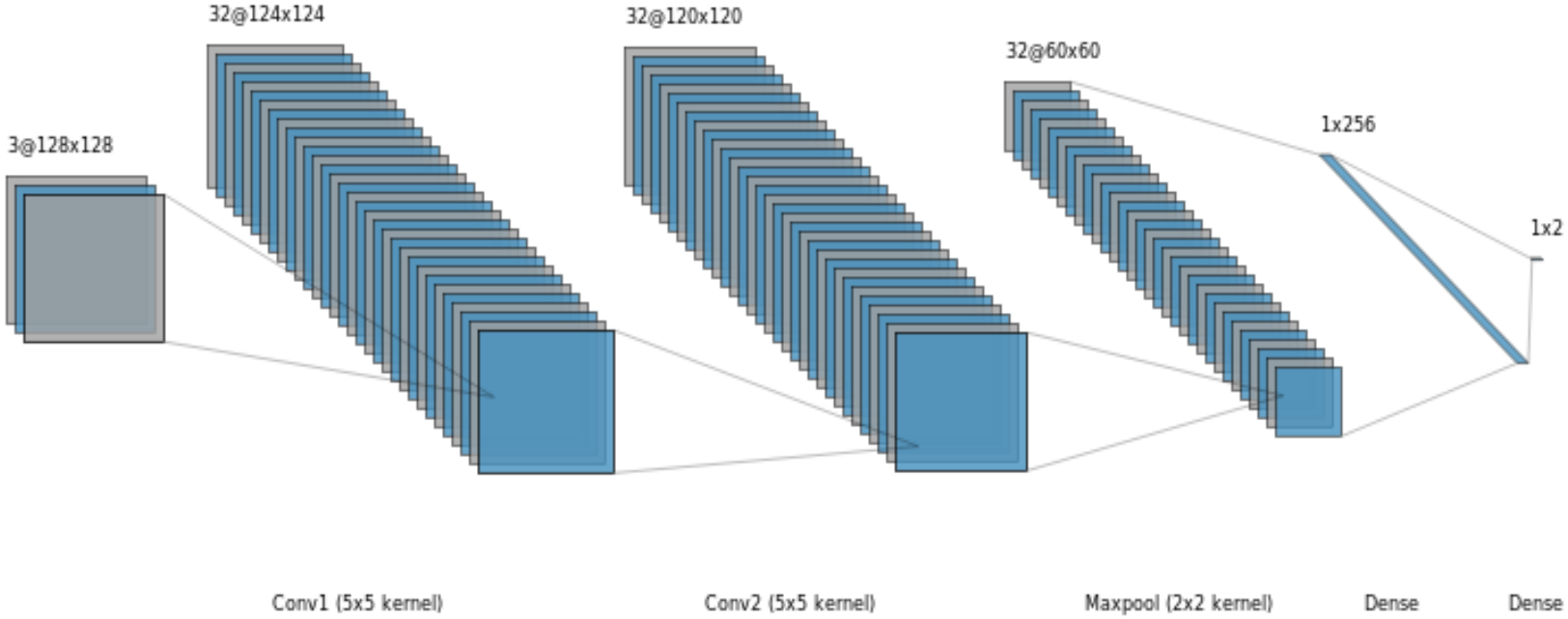
Original image ELA output

ELA OF TAMPERED IMAGE

Original image ELA output

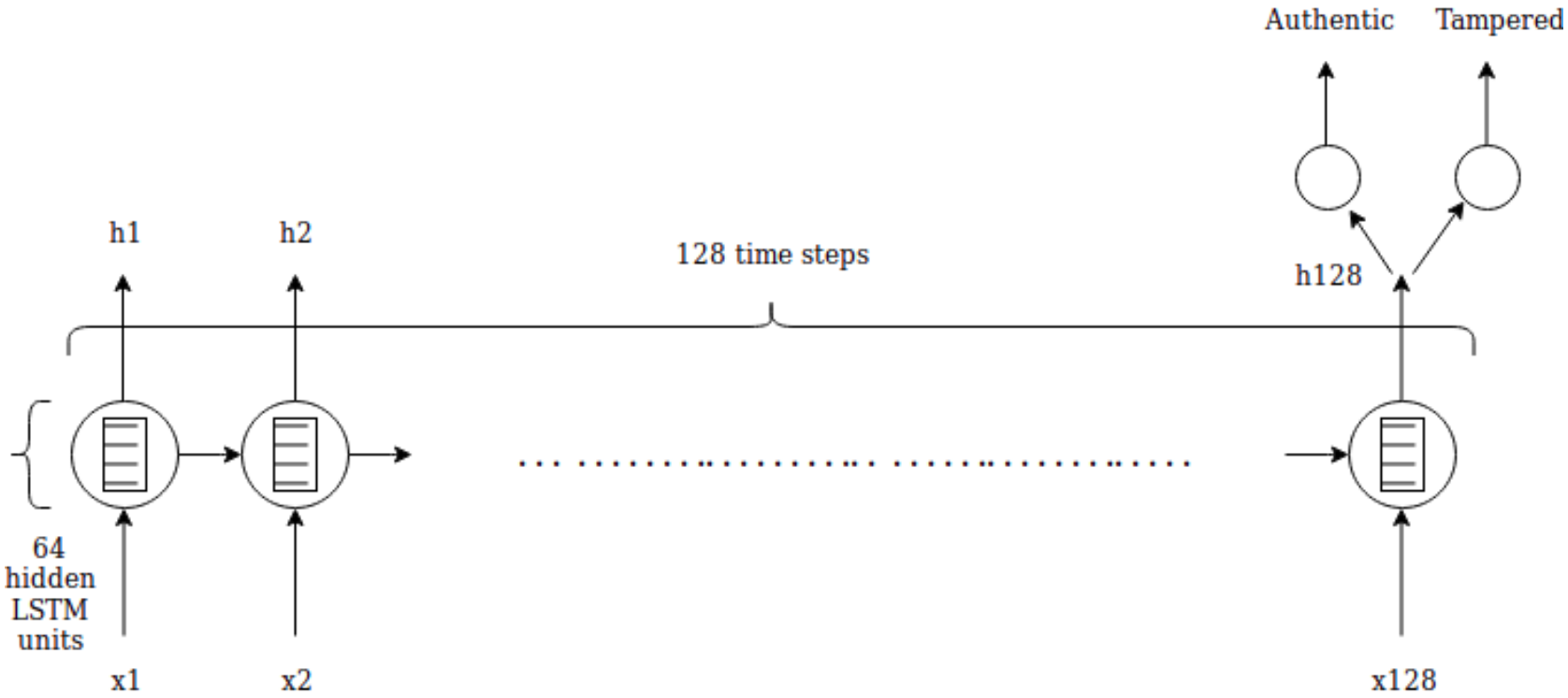
Flow chart


Dataset
(Images)
Error Level
Analysis
Resizing
Normalization
Preprocessed data
(Images : 128 x 128 x
3)
Data preprocessing
Fake or authentic
CNN
(Model 1)
Fake or authentic
LSTM
(Model 2)



- Learning rate : 0.005
- Optimizer : RMSprop
- Loss : categorical crossentropy
- Epoch : 100
- Batch size : 32
- Early stopping with patience 10

CNN Model architecture & its parameters



- Cell type : LSTM
- Hidden units : 64
- Time steps : 128
- Input size = 128
- Learning rate : 0.01
- Optimizer : RMSprop
- Loss : categorical crossentropy
- Epoch : 200
- Batch size : 32
- Early stopping with patience 10

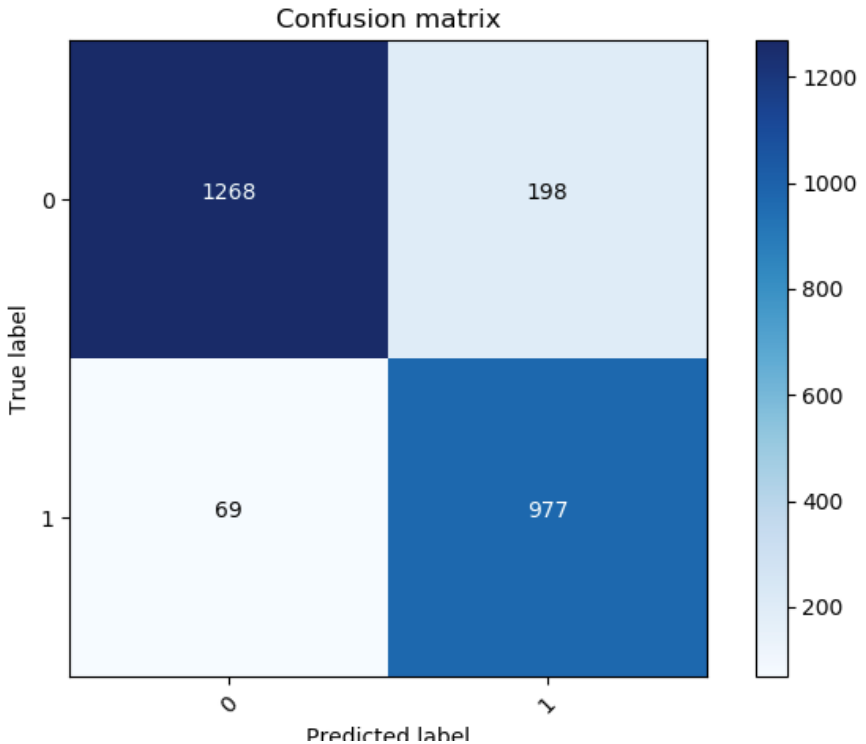
RNN model architecture & its parameters

Dataset used

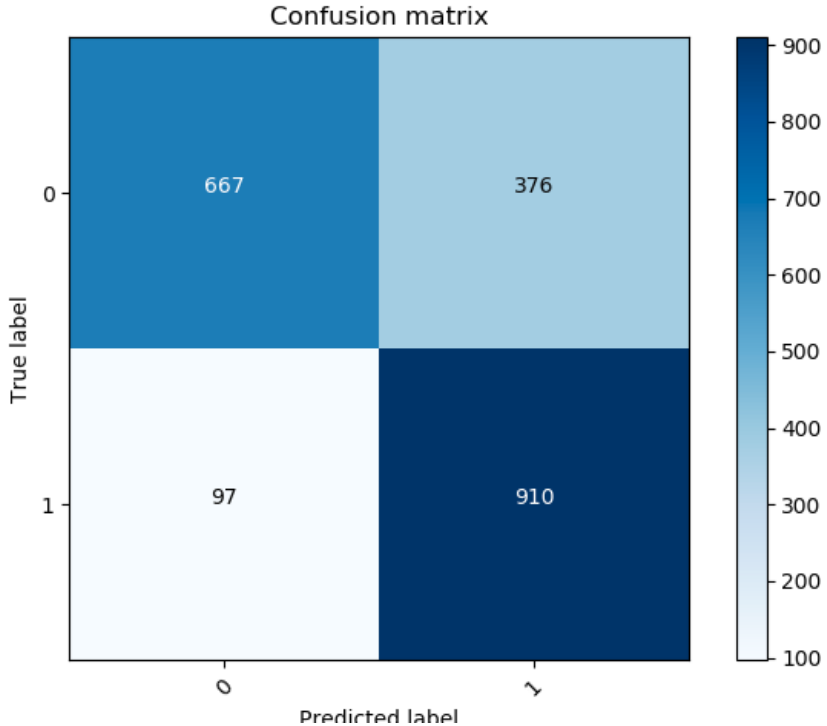
- We used CASIA-v2 database [4]. It consists of 7437 authentic and 5123 tampered images of various sizes from 240x160 to 900x600 with JPEG, BMP, and TIFF formats.
- For training, used 80% of dataset and rest for testing.

Results

CNN MODEL



RNN (LSTM) MODEL



Results

CNN MODEL

Accuracy	89.37 %
F1 score	0.879
Recall	93.40%
Precision	83.14%

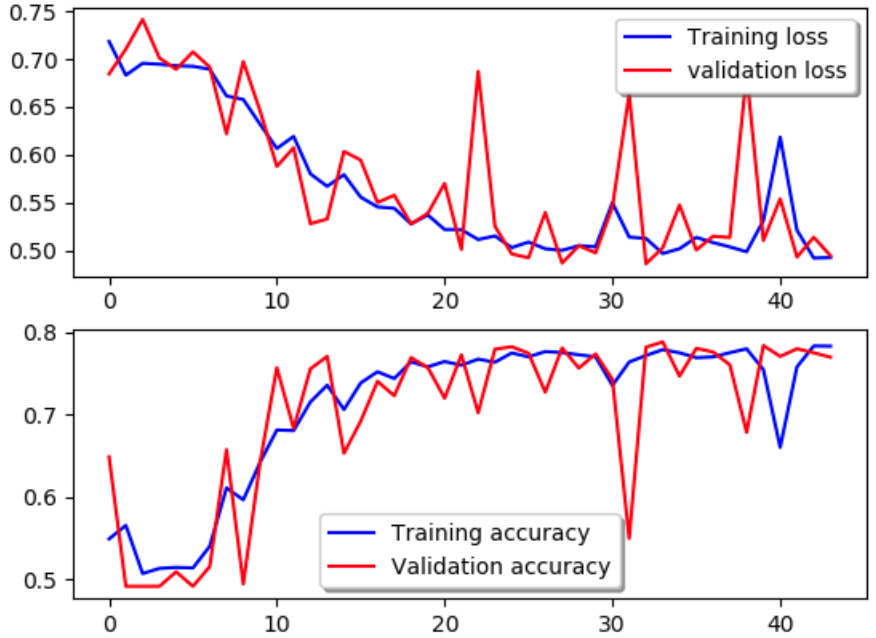
RNN (LSTM) MODEL

Accuracy	76.92 %
F1 score	0.795
Recall	90.36%
Precision	70.76%

Learning curve comparision

CNN MODEL

RNN (LSTM) MODEL



Future work

- Will work on localization of tampered region.
- Work on all kind of forgery detection that also includes different filtering mechanism of images.
- Include all formats of image.
- Will work on improving accuracy.

References

1. T. Bianchi, A. Piva, “Image forgery localization via block-grained analysis of JPEG artifacts”, IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, ISSN: 1556-6013, pp. 1003-1017, June 2012.

2. S. Lyu, X. Pan, and X. Zhang, “Exposing Region Splicing Forgeries with Blind Local Noise Estimation,” International Journal of Computer Vision, vol. 110, no. 2, pp. 202–221, 2014.

3. Rao Yuan, Ni Jiangqun, “A deep learning approach to detection of splicing and copy-move forgeries in images”, IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi-United Arab Emirates, 2016, ISBN: 978-1-5090-1139-1.

4. Jing Dong, Wei Wang, and Tieniu Tan. CASIA image tampering detection evaluation database. In Proceedings of the IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP 2013), pages 422–426, Beijing, China, July 2013. IEEE.

Thank You.