Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549811

IMAGE FORGERY DETECTION USING CNN

Rajashree
Assistant Professor, Dept of Computer Science and Engineering, Nitte (Deemed to be University) NMAM Institute Of Technology, rajashree@nitte.edu.in

Sunil Kumar Aithal S
Assistant Professor, Dept of Computer Science and Engineering, Nitte (Deemed to be University) NMAM Institute Of Technology, sunilaithal@nitte.edu.in

Abstract- Majority of images is widely spread in the virtual universe of online based social media entertainment. With the accessibility of numerous altering programming tools that permits us to alter images, evidently in various image processing applications there exist unidentified numerous falsification images. Scientifically using the error level analysis we can find out the pressure proportion between the first image and the phony picture, in light of the fact that the first image pressure and phony images are unique. Besides knowing whether the image is authentic or counterfeit we can drill down the metadata properties of the image, however the modification of metadata can be easily performed. Under these circumstances we apply deep learning to perceive controlled images via preparing the model utilizing dataset containing phony and genuine images through adopting error level analysis strategy on each image and fine tuning various parameters for accurate error rate analysis. In our research work random forest algorithm and CNN technique are compared for the effectiveness of image forgery detection task. Finally, the proposed CNN method witnesses the best precision of almost 99% compared to random forest algorithm for 50 epochs upon custom dataset consisting of 200 real and 100 fake images.

Keywords: CNN, Deep Learning, ELA, Random Forest, Image Forgery

I. INTRODUCTION

With the rapid development of technology in the current era has made it simpler for people to transmit fake information and falsified photos. With enormous availability of modern software tools for image manipulation, the public may easily modify images according to their need. Due to the proliferation of fraudulent photos on social media that might cause controversy, image forensics is enthusiastically employed to determine whether or not an image is authentic. Image forensics, in general, is the study of tracing an image's lineage and establishing its veracity.

Since large number of phony photographs that circulate on the internet and social media, an efficient technique is required to enable users to distinguish between real and fake images. Several techniques are used to determine the level of authenticity of the picture, one with determining the quality of the image compression level results.

Many modern techniques available under deep learning field are being utilized for this classification task. Many researchers have been found in their study for forgery frame detection from the video sequences using error level analysis, forensic approach. Hites C. Patel et al. in his research work detected fake images by counting the number of frames and contrasting the real and phony video frames through the analysis of several image properties including time duration, frame rate, number of frames, data rate, resolution, total bit rate, audio channel, audio sample rate, protected, video quality, and camera base editing video [1]. Meera Mary Isaac et al. performed image forgery detection by utilizing local phase quantization and gabor waves with the aid of the CASIA TIDE v.1 Dataset [2]. Birajfar et al. analyzed misleading pictures using a passive approach method [3].

In our research work error level analysis (ELA), forensic approach is utilized to gauge the degree of compression whereby the considered forensic technique uses varying degree of compression applied on the image for further analysis.

Due to the recent development of GPU acceleration technology, deep learning is a new emerging field of study in machine learning. Thus, in the proposed research work to identify photographs that have been digitally altered deep learning based system is implemented for effectively distinguish between authentic and fake images

Literature Survey

The purpose of this section is to critically summarize the cur- rent knowledge in the field of image forencis. Youseph et al. utilized the illuminant colour estimation approach to obtain the image's edge boundary by fusing canny detection with the HOG edge descriptor. Later, SVM training was performed with an accuracy value of 74% [4]. According to Mohhamad F.H incorporated a reliable and effective strategy that combined the undecimated wavelet transform and scale invariant feature transform for distinguishing real and fake image documents by considering accuracy, re-call, and false positive rate parameters [5]. Jie Zhao et al. applied the DCT and SVD algorithms to analyse picture forgeries based on DAR and FPR [6]. Wu-Chih Hu et al. examined image forgery based on the examination of alpha mattes and picture watermarking. [7].

Ghulam Muhammad et al. proposed the dyadic wavelet transform to analyse picture fraud [8]. Ashwini V. Malviya et al. analysed picture fraud using auto colour correlogram technique [9]. Susan Oommen et al. compared the real and false images, using fractal dimension and singular values [10]. Bunk et al. suggested two approaches to identify and localize fraudulent photos using a combination of resampling attributes and deep learning techniques [11].

Kuruvilla et al. demonstrated the effectiveness of both methods in identifying and resolving digital picture fraud [12].

D.-H. Kim et al. determines whether the image was real or phony by comparing the error levels of 4000 actual photos and 4000 false images which gave an impressive 83% of success rate by using digital forensics methods to identify alteration and phony photos used for criminal activities [13].

AlShariah et al. implemented overlapping picture adjustments to estimate the radon conversion of resampling parameters. In their research work a heat map is then created using deep learning classifiers and a gaussian conditional domain pattern. In their proposed system, software resampling attributes are communicated on overlapping object patches through an LSTM-based network for identification and localization.

According to their findings, spreading of false photos on social networks is dramatically decreased when using this software on mobile platforms. Evidently deep learning technology has produced impressive results in recent research on image forensic field. In various research works an altered neural network is used to process images first. In addition, hidden features rather than semantic data in the picture are sought for using a high pass filter [14].

Consequently in our proposed work CNN based algorithm upon real and fake image pictures are experimented for properly detect the fraudulent images.

II. System Design

In this research we make use of two level analyses for the image. At first level, it checks the image metadata. Image metadata is not that much reliable since it can be altered using simple programs. But most of the images we come across will have non-altered metadata which helps to identify the alterations. For example, if an image is edited with adobe photoshop, the metadata will contain even the version of the adobe photoshop used.

In the second level, the image is converted into error level analyzed format and will be resized to 100px x 100px image. Then these 10,000 pixels with RGB values (30,000 inputs) is given to the input layer of multilayer perception network. Output layer contain two neurons. One for fake image and one for real image. Depending upon the value of these neuron outputs along with metadata analyzer output, we determine whether the image is fake or not and how much chance is there for the given image to be tampered.

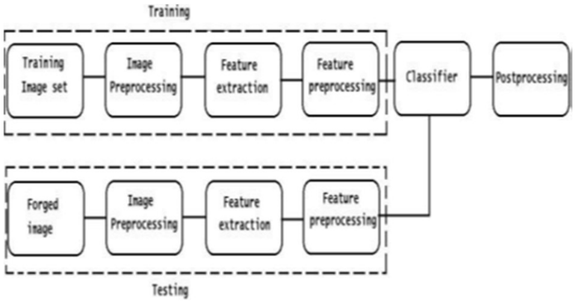


Fig 1: Methodology Used

Pre-processed images will then be subjected to several Machine Learning Techniques, in order to generate an optimal model. Due to the data being in the form of images, CNNs will be of importance in generating the model, whose layer by layer breakdown will be understood during the implementation. Multi-class Classifier is generated which will classify the data into one of the following classes: 0 – Fake, 1 – Real.

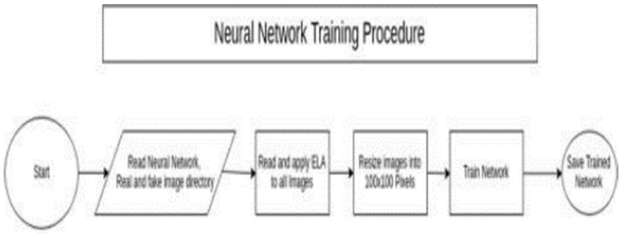

Neural Network Training Procedure
Start
Read Neural Network, Real and fake image directory
Read and apply ELA to all Images
Resize images into 100x100 Pixels
Train Network
Save Trained Network

Fig 2: Architecture of Image Forgery Detection

IV Implementation

STEP 1: DATASET CREATION

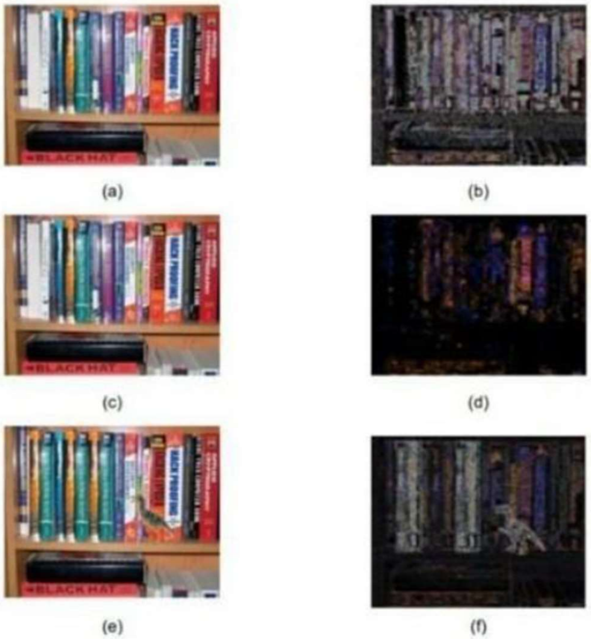
The dataset contains two categories of images i.e fake and real. The real images were captured through mobile phones and the fake images were photoshopped with the help of adobe photoshop tool. We created around 200 real images and 100 fake images. These two categories of images were stored in separate folders which was later supplied as input for the creation of .csv file. The data set contains two columns, “filepath” and “classification”. The filepath column contains the path where the images are stored and classification column contains two values 0 and 1 where 0 represents fake image and 1 represents real image

STEP 2: CONVERT TO ELA

By storing photos at a certain quality level and then determining the difference from the compression level, error level analysis is one method for identifying photographs that have been altered. Most editing programmes, including adobe photoshop, gimp, and adobe light room, support JPEG compression. When JPEG is initially saved, it will compress the picture for the first time. When utilising image editing tools, the picture can be rescheduled before being compressed once more.

As a result, it is evident that the original picture has through two compression processes—once using the camera and once using editing software—when the initial image is shot using a digital camera. When viewed with the naked eye, the image seems identical, however when employing this approach, it will appear that a fake image and the genuine image are different. Calculation of the quantization tables Y (luminance) and CrCb (chrominance)'s average difference. The image is not optimised by the digital camera for a particular camera quality setting (high, medium, low, etc.). High ELA values should be present in the original digital camera photos. The possible mistake rate will drop with each subsequent saving.

As seen in Figure 2, original photographs contain high ELA values that can be seen through white on the ELA picture. When the image is saved, using standard human vision, there is little to no difference visible, but ELA displays the predominant black and dark colours. The image quality will be reduced if this file is saved repeatedly. ELA will indicate the changed region has a colour with a greater ELA level if the original image is modified after that.



Error level analysis compression: (a) original image, (b) ELA original Image, (c) resave image, (d) ELA resave image, (e) tampered image, (d) ELA tampered image

STEP 3: DATA PREPROCESSING

1. Apply image preprocessing techniques such as resize, reshape and normalization.
2. Use the power of vectorization by converting images into NumPy arrays and pandas data frame whenever it's necessary.
3. Convert the images into NumPy arrays using OpenCV and make the output as categorical using pandas.

STEP 4: SPLITTING DATASET

Split the data set into the train and validation set. So that we can check whether the model is overfitted to the training dataset or not using the validation dataset.

Step 5: BUILD THE MODEL USING CONVOLUTIONAL NUERAL NETWORK(CNN)

A convolutional Neural Network (ConvNet/CNN) is a deep learning algorithm that can take in an input image, assign importance (learnable weights and biases) to various aspects/objects in the image, and be able to differentiate one from the other. The pre-processing required in a ConvNet is much lower as compared to other classification algorithms. While in primitive methods filters are hand engineered, with enough training

STEP 6: TRAINING THE MODEL

Now it's time to train our model. Training is nothing but a learning loop. here we define hyperparameters such as the number of epochs, batch size, and learning rate.

V RESULTS

Result using CNN:-

Even though the proposed model has been trained on combined dataset, it has been successful to achieve validation accuracy of 99% with epoch value 50. This model has succeeded to maintain higher and nearly equal classification rate for each class. The proposed system delivers a firm classification output.

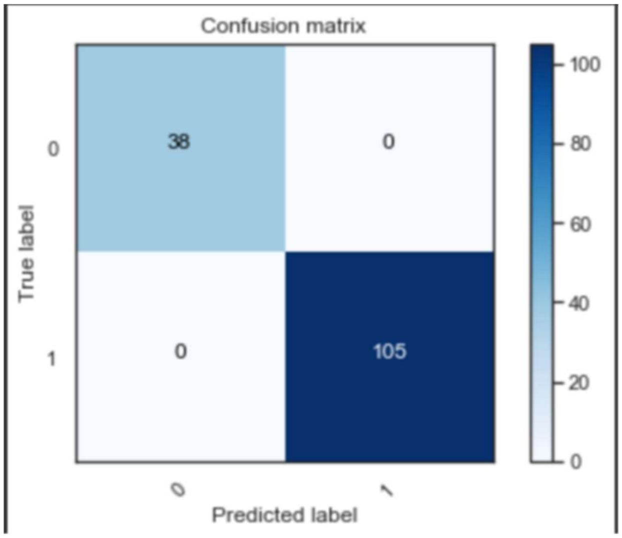


Fig 3: Confusion matrix for CNN

Result using Random Forest Algorithm:-

Applying data augmentation on the dataset and successfully building the model using random forest algorithm gave an accuracy of 97%, which is comparatively lesser than what was achieved using CNN.

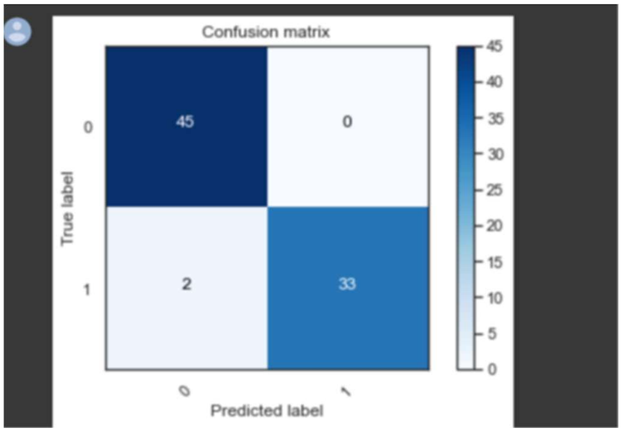


Fig 4:Confusion matrix for Random forest

VI. CONCLUSION

We experimented the dataset with random forest and CNN. The result of our experiment is that we get the accuracy of training 99% by going through 50 epoch using CNN and the

Random Forest algorithm on the dataset gave us an accuracy of 97 percent .Thus CNN offered better accuracy than Random Forest algorithm. In our subsequent investigation, we'll use a CNN architecture version to get the greatest accuracy and use other image-processing techniques to distinguish between the original image and a fake image.
Using deep learning, we have developed a model to identify authentic photos from fake ones. To address the aforementioned issues, we suggest a novel approach that combines error level analysis with convolutional neural network in machine learning.

REFERENCES

[1] Patel HC, Patel MM. Forgery Frame Detection From The Video Using Error LevelAnalysis.IJAERD. 2015; (6): 242–247.
[2] Isaac MM, Wilscy M. Image Forgery Detection Based on Gabor Wavelets and Local PhaseQuantization. Procedia Computer Science. 2015; 58: 76–83.
[3] Birajdar GK, Mankar VH. Digital image forgery detection using passive tech- niques: Asurvey. Digital Investigation. 2013; 10(3): 226–45.
[4] Youseph SN, Cherian RR. Pixel and Edge Based Illuminant Color Estimation for ImageForgery Detection. Procedia Computer Science. 2015; 46: 1635–42.
[5] Hashmi MF, Anand V, Keskar AG. Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant FeatureTransform. AASRI Procedia. 2014; 9: 84–91.
[6] Zhao J, Guo J. Passive forensics for copy-move image forgery using a method based onDCT and SVD. Forensic Science International. 2013; 233(1–3): 158–66.
[7] Hu WC, Chen WH, Huang DY, Yang CY. Effective image forgery detection of tam- pered foreground or background image based on image watermarking and alpha mattes. MultimediaTools and Applications. 2015; 75(6): 3495–516.
[8] Muhammad G, Hussain M, Bebis G. Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital Investigation. 2012; 9(1): 49– 57.
[9] Malviya AV, Ladhake SA. Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram. Procedia Computer Science. 2016; 79: 383–90.
[10] Oommen RS, Jayamohan M, Sruthy S. Using Fractal Dimension and Singular Values forImage Forgery Detection and Localization. Procedia Technology. 2016; 24: 1452–9.
[11] J. Bunk, J. Bappy, H. Mohammed, T. M. Nataraj, L., Flenner, A., Manjunath, B., et al. (2017). Detection and Localization of Image Forgeries using Resampling Features and Deep Learning. University of California, Department of Electrical and Computer Engineering, USA.
[12] M. Villan, A. Kuruvilla, K. J. Paul, & E. P. Elias, (2017). Fake Image Detection Us- ing Machine Learning. IRACST—International Journal of Computer Science and InformationTechnology & Security (IJCSITS) .
[13] D.-H. Kim, & H.-Y. Lee, (2017). Image Manipulation Detection using Convolutional NeuralNetwork. International Journal of Applied Engineering Research, 12(21), 11640- 11646
[14] AlShariah, Njood & Khader, Abdul. (2019). Detecting Fake Images on Social Media using Machine Learning. International Journal of Advanced Computer Science and Applications. 10. 10.14569/IJACSA.2019.0101224.