A REVIEW ON IMAGE CLASIFICATION BY TEXTURE AND PATTERNS USING MACHINE LEARNING

K. NITYA SRI CHOWDARY[1] PRAGYA DUBEY[2]

[1] B. TECH Student, Dept of Computer Science Engineering-Data Science , KGReddy College of engineering & Technology, Chilkur, Moinabad, T.S, India

[2] B. TECH Student, Dept of Computer Science Engineering-Data Science , KGReddy College of engineering & Technology, Chilkur, Moinabad, T.S, India

ABSTRACT

With the rapid increase of deep learning technology, creating human face images with artificial intelligence (AI) is becoming easier. Those generated images are coming up to images that humans cannot distinguish from authentic ones. It is essential to realize an accurate method to detect such fake images to avoid abusing them. In this paper, we propose a fake image detection using an ensemble model of convolutional neural network (CNN) models that focus on deepfake detection of individual face parts. Our results show that a combination of deepfake detection based on different face parts is effective. This idea can be adopted on partially manipulated deepfake images/videos.

Biometric technology are now helpful in identifying a person's identity, but criminals alter their look, behaviour, and psychological makeup to trick identification systems. We are employing a novel method called Deep Texture Features extraction from photos to solve this issue, followed by the construction of a machine learning model using the CNN (Convolution Neural Networks) algorithm. This method is also known as LBPNet or NLBPNet because it largely relies on the LBP (Local Binary Pattern) algorithm for features extraction.

INTRODUCTION

The use of technology has grown significantly in the modern world, and one of the most popular methods of communication is the use of images. Images are now used frequently in publications like newspapers, magazines, websites, and advertising, and they may convey a variety of information. As images become more commonplace, people's belief in them grows every day. Image forgery is the alteration of certain information included in an image, and image forgery detection is the process of determining whether the altered image is authentic.

In the age of technology, a great number of people have fallen prey to photo fraud. Some criminals utilise software to manipulate and present images as proof in court as confusion.A huge number of people have become victims of photo forgery in this technological age. Some criminals use software to exploit and use pictures as evidence to confuse the courts of justice. To put an end to this, all photographs exchanged via social media should be labeled as true or fake. Social media is a great platform for knowledge sharing and dissemination. Yet If there is no caution, people may be fooled and even induced by unintended false propaganda. Though most image editing using Photoshop is clearly evident, some of these images may indeed appear really due to pixelization and shoddy jobs by novices . In particular, in the Policy arena, edited images can break the credibility of a politician. In this research using machine learning algorithms, the researcher will attempt to propose a classifier model via a convolutional neural network (CNN) that is capable of take advantage of knowledge to take an image from social media and then classify and detect it.

Local binary patterns (LBP) could be a variety of visual descriptors used for classification in laptop vision and could be an easy nonetheless terribly economical texture operator that labels the constituents of a picture by thresholding the neighbourhood of every pixel and considers the result as a binary variety. Because of its discriminative power and machine simplicity, the LBP texture operator has become a preferred approach in numerous applications. It is often seen as a unifying approach to the historically divergent applied mathematics and structural models of texture analysis. maybe the foremost necessary property of the LBP operator in real-world applications is its hardiness to monotonic gray-scale changes caused, as an example, by illumination variations. Another necessary property is its machine simplicity, which makes it doable to research pictures in difficult period settings.

This is actually done by assuming that changing the image changes the correlation between and within bit planes. Therefore, the quantized spatial correlation between the bit levels of the original image is different from the bit level correlation of the curved images. Once this is done, some features are extracted from the image measurements based on the bit-by-bit correspondence of the corresponding pixel locations in the two images, using an algorithm known as the Sequential Floating Forward Search (SFFS) algorithm to select. the best features and a linear regression classifier for classification.

LITERATURE SURVEY

S. Beram, et al. proposed a way for identify Doctoring in digital images. Doctoring typically involves several steps, usually in the sequence of initial image-processing operations such as scaling, rotation, contrast shift, smoothing, and more. These methods used are dedicated to three categories of statistical features including binary similarity, image quality and wavelet Statistics. The three categories of forensic facilities are as follows:

1. Image quality measurements: These focus on the difference between the captured image and its source. If the original image is not available, it is simulated with a blurred version of the test image. 2. Higher order wavelet statistics: These are obtained from multilevel decomposition of the image. 3. Binary similarity measures: These measures capture correlation and textural features between and within less significant bit levels, which are more susceptible to manipulation. To influence the detection of physician effects, individual tools are first developed to identify the required image processing functions. These individual "weak" indicators were then added together to define a PhD in the expert fusion plan. Swaminathan et al. proposed a method to evaluate in-camera and post-camera fingerprints to verify the integrity of photographs. The new methodology is surgery. It mainly focuses on forensic

analysis and identification of digital camera images based on both indoor and outdoor imaging devices.

Raturi's 2018 architecture was proposed to identify counterfeit accounts in social networks, especially on Facebook. In this research, a machine learning feature was used to better predict fake accounts, based on their posts and the placement on their social networking walls. Support Vector Machine (SVM) and Complement Naïve Bayes (CNB) were used in this process, to validate content based on text classification and data analysis. The analysis of the data focused on the collection of offensive words, and the number of times they were repeated. For Facebook, SVM shows a 97% resolution where CNB shows 95% accuracy in recognizing Bag of Words (BOW) -based counterfeit accounts. The results of the study confirmed that the main problem related to the safety of social networks is that data is not properly validated before publishing.

Gaussian conditional domain pattern are then used to construct a heat map. A Random Walker segmentation method uses total areas. In the next system, for identification and localization, software resampling properties are passed on overlapping object patches over a long-term memory (LSTM)- based network. In addition, the detection/ localization performance of both systems was compared. The results confirmed that both systems are active in detecting and settling digital image fraud. Aphiwongsophon and Chongstitvatana, aimed to use automated learning techniques to detect counterfeit news. Three common techniques were used in the experiments: Naïve Bayes, Neural Network, and Support Vector Machine (SVM). The normalization method is a major step to disinfect data before using the automatic learning method to sort information. The results show Naïve Bayes to have a 96.08% accuracy in detecting counterfeit news. There are two other advanced methods, the Neural Network Machine and the Support Network (SVM), which achieve 99.90% accuracy. Neural network was successfully trained by analyzing the 4000 fake and 4000 real images error levels. The trained neural network has succeeded in identifying the image as fake or real, with a high success rate of 83%. The results showed that using this application on mobile platforms significantly reduces the spread of fake images across social networks. In addition, this can be used as a false image verification method in digital authentication, court evidence assessment, etc.

This study develops an approach that takes an image as input and classifies it using a CNN model. For a completely new task/problem, CNNs have very good properties. It extracts useful features from an already trained CNN and trained weights, feeding your data at each level and tuning the CNN slightly for a specific task. This means that a CNN can be retrained for new detection tasks, allowing it to rely on existing networks. This is called pre-training, where you can avoid training CNN from the beginning and save time. CNN can perform automatic feature extraction for a given task. This eliminates the need for manual extraction as the CNN learns the features directly. In terms of performance, CNNs outperform many methods in image recognition tasks and many other tasks where it provides high accuracy and accurate results. Another key feature of CNNs is weight distribution, which basically means that the same weights are used in the two layers of the model. Because of the aforementioned features and advantages, CNN is used in this study compared to other deep learning algorithms.

RESEARCH METHODOLOGY

This research explores a supervised machine learning classification problem [14,18], where the label or category of the input sample is known as the training phase. There are two labels or classes: the original image class and the fake image class. The researcher uses the deep learning technique via a conventional neural network (CNN).

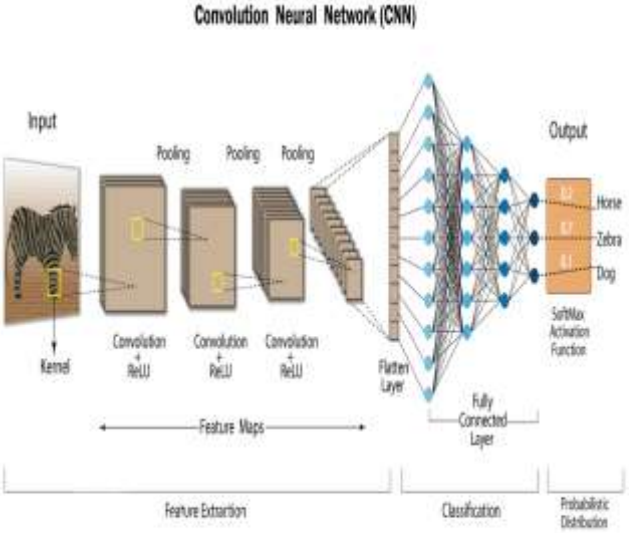
Build a CNN convolutional layer, the convolutional layer is responsible for extracting image features using standard mathematical operations. These circuit operations work as an application of two-dimensional digital filters. Assuming that the screen is 4x4 pixels and the normal filter is a 2x2 matrix filter, illustrates the normal operation where each screen block matrix with dimensions equal to the filter dimensions is multiplied by the filter matrix. Creating an activation function illustrates the activation function layer inside the yellow oval. The activation function layer is a layer between the traditional layer and the feature map, which, as with any traditional neural activation function, removes unwanted pixels, such as negative values.

(1) Error level analysis: Error level analysis is a forensic method for identifying parts of an image with different levels of compression. This technique can be used to determine if an image has been digitally altered. These result in poor quality compressed images. Error Level Analysis (ELA) allows you to identify areas in an image with different levels of compression. For JPEG images, the entire image should be approximately the same level. If part of the image has a significantly different level of error, this probably indicates digital alteration.

(2) Convolution Neural Network (CNN): In deep learning, a convolutional neural network is a class of deep neural networks most commonly used for visual image analysis. A convolutional neural network consists of input and output layers and several hidden layers. The hidden layers of a CNN typically consist of multiple convolutional layers convoluted using a convolutional product or other dot product.

(3) Layers used in this proposed model:

1. Convolution2D
2. Maxpooling2D
3. Flatten
4. Dropout
5. Dense



EXISTING SYSTEM

When an image is taken, hidden information necessary to prevent authentication and forgery is added to it. Passive technology does not rely on additional information, but instead analyzes some features extracted from the digital content of the image itself. Copy-move means manipulating a part of an image and pasting it to another place in the same image, while paste means taking a part of an image and pasting it to another.

DISADVANTAGES OF EXISTING SYSTEM

 Complexity in analyzing the data.

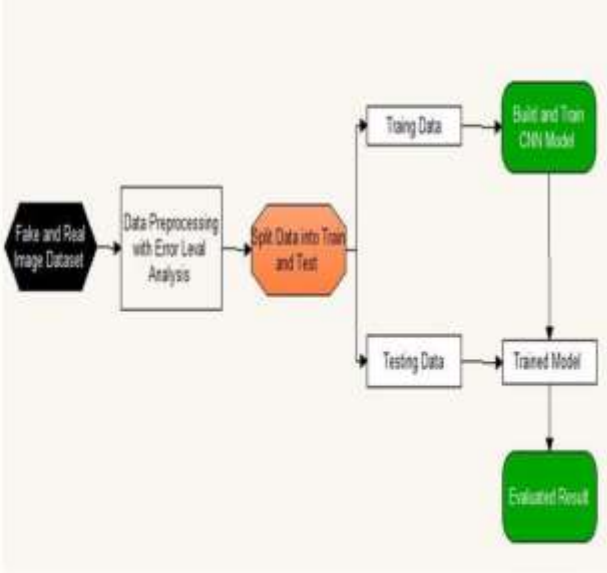
 Prediction is a challenging task working in the model

 Coding is complex maintaining multiple methods.

 Library's support was not that much familiar.

PROPOSED SYSTEM

Here, we tend to project the regional units of LBP into a mainly machine learning-based convolutional neural network, known as LBPNET, to see apparent face images. Here, we first extract LBP from the images and train the LBP images with Convolution Neural Network to obtain a training model. Every time we tend to move a new aspect, that aspect is applied to the training model to determine whether the aspect image contains a fake image or a non-fake image. Below we will see some details about LBP.


Fake and Real Image Dataset
Data Preprocessing with Error Leval Analysis
Split Data into Train and Test
Traing Data
Build and Train CNN Model
Testing Data
Trained Model
Evaluated Result

MODELING AND ANALYSIS

1. COLLECTION OF DATA

Download a dataset of real and fake faces from Kaggle. It has 1288 faces - 589 real and 700 fake. The fake faces were created using StyleGAN2, which makes them difficult to classify correctly.

2. PRE-PROCESSING OF IMAGES

To create an efficient neural network model, you must carefully consider the input data format. The most common parameters for entering image data are the number of images, the height and width of the image, and the number of channels. There are typically three channels of data corresponding to red, green and blue (RGB) colors, and pixel levels are typically [0.255]. Create a function that accepts an image path, reads it from disk, performs all the preprocessing steps, and returns it. Use OpenCV library for reading and resizing images and NumPy for normalization.

3: SHARE INFORMATION

Partitioning datasets is an important but often overlooked step in the ML process.

This helps avoid overfitting, which occurs when the model learns from the noise in the training data instead of the underlying pattern. This can lead to a model that performs well on training data, but poorly on testing data. By partitioning the data set, you can evaluate the model's performance based on unseen data and avoid overfitting. Another reason for splitting is to ensure that the model is generalizable. A model trained on a specific data set may not perform well with new, unseen data. By splitting the data set into a training and test set, you can train the model on one data set and evaluate its performance on another set, making sure it can handle new data.

4. **MODEL ARCHITECTURAL DRAWING**

It is possible that a model architecture that worked well for one problem formulation may work well for other problem formulations. This is because the underlying concepts and techniques of ML are often applicable to different domains and problem statements. After a lot of research and testing, I designed my own model architecture that I use in all my projects (with minor modifications): It consists of a sequential model with five convolutional layers and four density layers. The first convolutional layer has 32 filters and the kernel size is 2x2. In each subsequent convolution layer, the number of filters and the size of the kernel are doubled by one. To reduce overfitting and computational cost, max-pooling layers are introduced after each convolution layer. The output of the convolutional layer is smoothed and passed to the density layers. The first dense layer has 512 neurons, and the next two dense layers have half the number of neurons. Dropout layers are introduced throughout the model to randomly ignore some neurons and reduce overfitting. ReLU activation is used in all layers except the output layer, which has two neurons (one for each class) and softmax activation.

5. **MODEL TRAINING**

Building an ML model involves configuring its settings for training. The three main devices to consider are: LOSS FUNCTION: This measures the difference between the model's predicted return and the actual return. The choice of loss function depends on the type of problem to be solved. Since you are doing classification and the training labels are presented in categorical form (0,1), sparse_category_crosspoint is a logical choice. OPTIMIZATION: It updates the model weights during training to minimize the loss function. Some popular optimization algorithms include stochastic gradient descent, Adam, and RMSprop. The choice of optimizer depends on the complexity of the problem and the size of the data set. Adam Optimizer works well in most cases, so "when in doubt, go with Adam!" Evaluation: It measures the performance of the model during training and validation. Since your dataset is fairly balanced, this won't hurt accuracy.

6. **MODEL EVALUATION**

Evaluating the performance of an ML model is critical to assessing its ability to generalize to new, unseen data. Reload it with the load_model() function of the Keras library.

7. **CONSTRUCTION OF THE OPERATING SYSTEM**

Evaluating a model's performance alone may not be sufficient to demonstrate its capability. End users may not have the skills or time to write the code and use the trained model. One solution is to create a user interface (UI) that allows users to interact with the model.

CONCLUSION

Due to the rapid development of the Internet in modern society, there are many social networking services such as Facebook, Instagram and so on, which have not only been used for good reasons, but some people take them away by using them for negative purposes. In these circumstances, crimes against images occur for illegal purposes. Digital forensics must detect such illegal targets. In this paper, we proposed image manipulation detection techniques using error rate analysis. After a brief observation of related works, the proposed model was explained in detail. An intensive experiment analyzed the proposed model and showed that at least 95 % accuracy was achieved. The proposed model can be used to determine whether an image has been manipulated or not, and can be used to detect more manipulation techniques if a better model is obtained in subsequent studies. In addition, it can be applied to various multimedia and videos in further research. In these circumstances, crimes against images occur for illegal purposes. Therefore, digital forensics must identify these illegitimate targets. In the background of the project, we built a deep learning algorithm, which is CNN and ELA in the data processing stage, where we used real and fake real and fake images as a dataset to train and validate the model. For further ease of the interface, we have saved this model in json format. And the Android app was built using Android Studio code and connected to the previously built model using Firebase. This app works as a platform where we can upload a live image to determine whether the uploaded image is genuine or fake.

FUTURE WORKS

Here are a few more approaches we are trying to get more accuracy:

1. more aggressive data entry
2. more aggressive suspension

3 Use of L1 and L2 regulation (also known as "weight loss")

4. Configure another convolution block (with more regularization).

Recommendations for future work include, for example, using a more complex and deeper model for unpredictable problems. Integrating deep neural networks into reinforcement learning theory where the model is more efficient. Neural network solutions rarely consider nonlinear feature interactions and nonmonotonic short-term sequential patterns, which are necessary to model user behavior in sparse serial data. The model can be integrated with neural networks to solve this problem. The material could be expanded and other types of images, such as grayscale images, could be used for training.

REFERENCES

[1] H. Farid, “Image forgery detection,” IEEE Signal Processing Magazine, Vol. 26, no. 2, pp. 16–25, 2009

[2] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation de taction with binary similarity measures,” in Proc. European Signal Processing Conf., Turkey, 2005

[3] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation detection,” J. Electron. Imaging, vol. 15, no. 4, p. 41102, 2006.

[4] Alessandro. Piva, “An overview on image forensics,” ISRN Signal Processing, pp. 1–22, 2012.

[5] G. W. Meyer, H. E. Rushmeier, M. F. Cohen, D. P. Greenberg, and K. E. Torrance, “An experimental evaluation of computer graphics imagery,” ACM Transactions on Graphics, vol. 5, no. 1, pp. 30–50, 1986.

[6] T. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. Rocha, “Exposing digital image forgeries by illumination color classification,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1182–1194, 2013.

[7] ATHERTON, P., AND CAPOREAL, L. A subjective judgement study of polygon based curved surface imagery. CHI’85 Conference on Human Factors in Computing Systems (San Francisco, Calif., Apr. 14-18). ACM/SIGCHI, New York, 1985.

[8] A. Piva, “An Overview on Image Forensics,” ISRN Signal Processing, vol. 2013.

[9] Yi-Lei Chen and Chiou-Ting Hsu, “Detecting Doubly Compressed Images Based on Quantization Noise Model and Image Restoration”, 2009 IEEE International Workshop on Multimedia Signal Processing, 23 October 2009, 978-1-4244-4652-0/09.