International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

FAKE IMAGE IDENTIFICATION USING MACHINE LEARNING

[1] Mohammed Azmatullah [2] Sykam Hemanth [3] Ummadi Arun Vineel raj [4] G Durvasi Kiran
[1,2,3] Department of Information Technology, Andhra Loyola Institute of Engineering and Technology
[4] Associate professer, Department of Information Technology, Andhra Loyola Institute of Engineering and Technology

Abstract:

Biometric techniques 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 since it largely relies on the LBP (Local Binary Pattern) algorithm for features extraction.

LBPNET, a machine learning convolution neural network, is the name of the network we created for this research to identify fraudulent face photographs. Here, we will first extract LBP from the photos before training the convolution neural network on the LBP descriptor images to create a training model. Every time we submit a new test picture, the training model will be applied to that test image to determine if it includes a false image or not. Details regarding LBP are shown below.

keywords: Biometry, Identity, Recognition, Detection, Fake face.

I. INTRODUCTION

Local binary patterns (LBP) are a class of visual descriptors used for classification in computer vision. They are a simple yet incredibly efficient texture operator that identifies the individual pixels in an image by thresholding the area around each one and treating the result as a binary number. The LBP texture operator has gained favour in many applications due to its strong discriminative ability and machine simplicity. It is frequently viewed as a unifying strategy for the structural models of texture analysis and the historically disparate applied mathematics. The LBP texture operator has emerged as a favoured strategy in a variety of applications because to its discriminative capability and machine simplicity. It is frequently viewed as a unifying strategy for the structural models of texture analysis and applied mathematics that have historically been in conflict.

II. LITERATURE SURVEY

The combination of audio, picture and video detection has not received much attention. To find out what can be done to curb the startling proliferation of false photos online, several research and activities are being carried out. Adobe realizes how Photoshop is misused, therefore it has made an attempt to offer a type of antidote. [8]. The phrases that follow provide summaries of a handful of these studies: According to research [9] by Zheng et al. (2018), it is very difficult to identify false news and photographs since there are few models for doing so and it is impossible to validate content on a pure basis. can be utilized to resolve the problem. It has been suggested that the issue of "detecting false news" be studied. After a comprehensive examination, it is found that the content, phrases, and images utilised in false news have many positive qualities. The phrases and visuals used in false news may be utilised to detect some hidden traits using a set of hidden attributes produced from this model over multiple layers. There has been talk about the TI-CNN trend. By displaying distinct and embedded characteristics in a same area, TI-CNN is trained using both text and picture data at the same time. For the purpose of identifying phoney accounts on social media, primarily Facebook, Raturi's 2018 architecture [10] was proposed. In this study, a machine learning feature was used to better reliably forecast phoney accounts based on postings and where they were placed on social networking walls. To assess content based on text categorization and data analysis, Complement Nave Bayes (CNB) and Support Vector Machines (SVM) were used. The major subjects of the data analysis were the list of objectionable terms and how frequently they were used. Based on the Bag of Words (BOW) algorithm, SVM shows a 97% resolution for Facebook while CNB shows a 95% accuracy for detecting bogus accounts.

The study's conclusions confirmed the idea that the main problem with social networks' safety is that content is not properly checked before posting. In a 2017 paper, Bunk et al. [11] proposed two algorithms to locate and identify fraudulent photos utilising resampling characteristics and deep learning. In the first system, the Radon conversion of resampling attributes is calculated using overlapping picture adjustments. using a classifier with deep learning. The development of a heat map is then achieved using Gaussian conditional domain patterns. Total areas are used in a With a Random Walker segmentation method, all areas are employed. For identification and localization in the following system, Over an LSTM-based network, software resampling attributes are communicated on overlapping object patches. It was also contrasted how well both systems were at localization and detection. The results showed how well both systems performed in spotting and stopping digital picture fraud. Using automated learning approaches, Aphiwongsophon and Chongstitvatana's [12] objective was to recognise bogus news. Nave Bayes, neural networks, and support vector machines were three techniques that were often employed in the trials (SVM). The normalisation approach must come first in the data cleaning process before utilising the artificial learning method to sort the data. The results show that Naive Bayes has an accuracy rate of 96.08% in detecting false news. The Support Network (SVM) and the Neural Network Machine are two more complex methods that attain 99.90% accuracy. Kuruvilla et al. successfully trained a neural network in [13] by contrasting the mistake rates of 4,000 authentic photos and 4,000 phoney ones. The trained neural network was able to distinguish between a real and false picture with an astounding 83% success rate. The results showed that the spread of false photos on social media is dramatically reduced when this software is used on mobile platforms. Also, this may be used as a method of false picture verification in digital authentication, the assessment of evidence in court, etc. The CNN model is used in this study's strategy to categorise the input photos. For brand-new jobs or issues, CNNs make outstanding feature extractors.

It takes advantage of an already trained CNN's taught weights to extract important features by giving it your data at each level and slightly adjusting the CNN for the specific purpose. A CNN may therefore be retrained to carry out fresh recognition tasks, enabling it to build on current networks. Pre-training is the technique of saving time by not training a CNN from start. CNN may carry out automated feature extraction for the given job. Manual feature extraction is not required because the CNN immediately learns the features. CNNs exceed several approaches in terms of performance for image recognition tasks and many other tasks where it offers high accuracy and accurate results. Another crucial feature of CNNs is weight sharing, which simply entails utilising the same weight for two layers of the model. The CNN algorithm is chosen in this study above other deep learning algorithms because of the aforementioned advantages and characteristics.

III.METHODOLOGY

A. EXISTING SYSTEM

At the time of capture, a picture is given the additional concealed information it needs to be authenticated and protected against fabrication. Instead than depending on supplementary data, the passive approach analyses specific elements that are obtained straight from the digital content of the image. You copy a portion of one picture and paste it into another when you copy-move. Contrary to splicing, which requires removing a section of one picture and replacing it with another similar image,.

Disadvantages of the Existing System:

➢ Complexity in analyzing the data.

➢ Prediction is a challenging task working on the model

➢ Coding is complex maintaining multiple methods.

➢ Library's support was not that much familiar.

B. TOOLS USED:

I. SOFTWARE REQUIREMENTS:

Operating system: Windows 10

Coding Language: python

HARDWARE REQUIREMENTS:

System : Pentium IV 2.4 GHz.

Hard Disk: 40 GB.

Ram: 512 Mb.

C. PROPOSED SYSTEM

In this research, we want to identify fraudulent face photos using a convolution neural network called LBPNET, which is based on LBP. Here, we'll first extract LBP from photos, then use those images to train a convolution neural network to produce a coaching model. In order to determine whether or not a new test contains a phoney examination, the exam will be utilised on a coaching model when it is transferred. Here, we'll examine some LBP details.

Advantages:

➢ Libraries help to analyze the data.

➢ Statistical and prediction are very easy compared to existing technologies.

➢ Results will be accurately compared to other methodologies.

IV.CODE

#{'Fake': 0, 'Real': 1} from tkinter import * import tkinter from tkinter import filedialog import numpy as np from tkinter.filedialog import askopenfilename import pandas as pd from keras.optimizers import Adam from keras.models import model_from_json from tkinter import simpledialog

from keras.models import Sequential from keras.layers import Convolution2D from keras.layers import MaxPooling2D from keras.layers import Flatten from keras.layers import Dense,Activation,BatchNormalization import os from keras.preprocessing import image from keras.preprocessing.image import ImageDataGenerator from tkinter import messagebox import cv2 from imutils import paths import imutils import cv2 import numpy as np main = tkinter.Tk() main.title("Fake Image Identification") #designing main screen main.geometry("600x500")

V.OUTPUT SCREENS

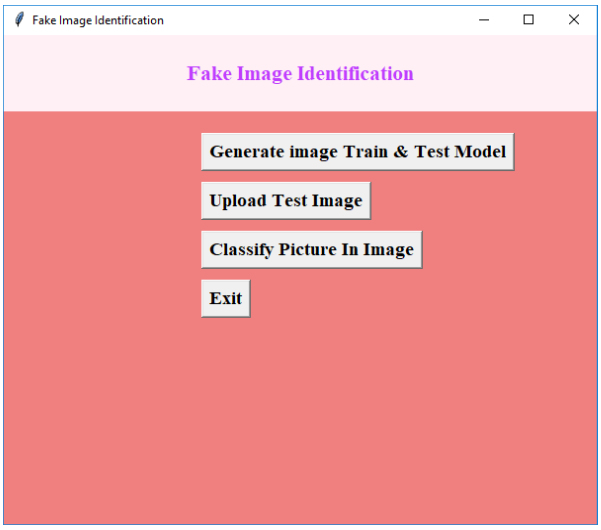
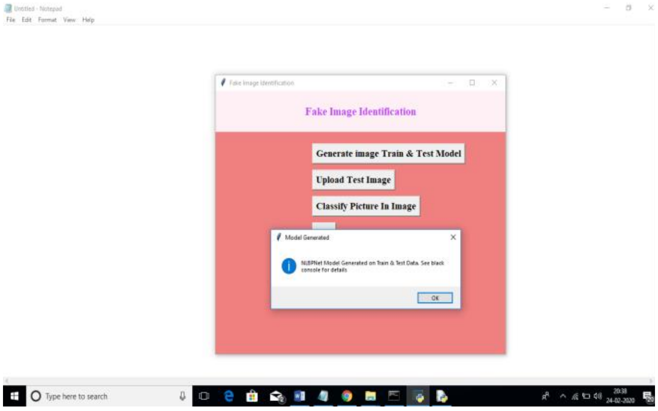

Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Exit

Fig. 1 Output screen 1


Untitled - Notepad
File Edit Format View Help
Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Model Generated
OK
Type here to search

NLBPNet Model Generated on Train & Test Data. See black console for details

Fig. 2 Output screen 2

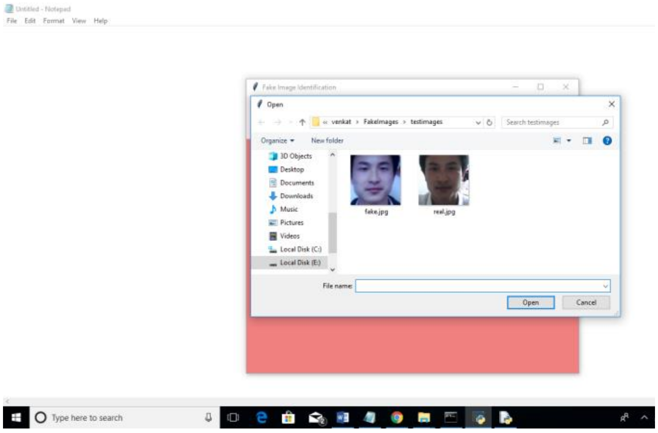


Fig. 3 Output screen 3

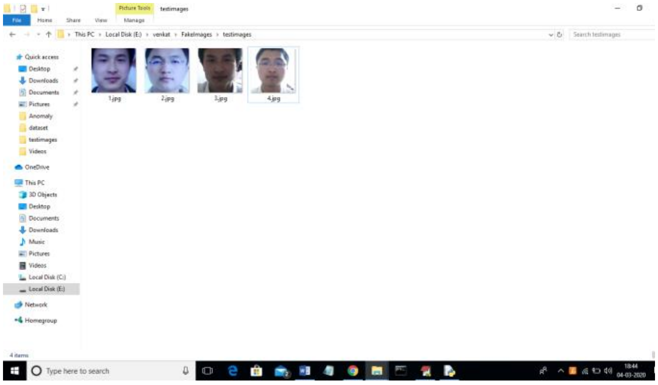


Fig. 4 Output screen 4

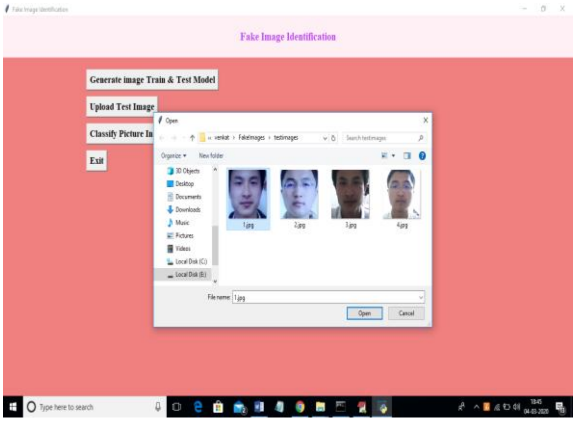


Fig. 5 Output screen 5

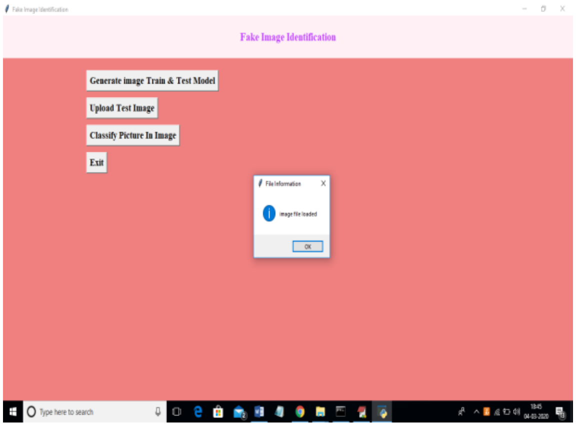

Fake Image Identification
Fake Image Identification
Generate image Train & Test Model
Upload Test Image
Classify Picture In Image
Exit
File Information
OK
Type here to search

image file loaded

Fig. 6 Output screen 6

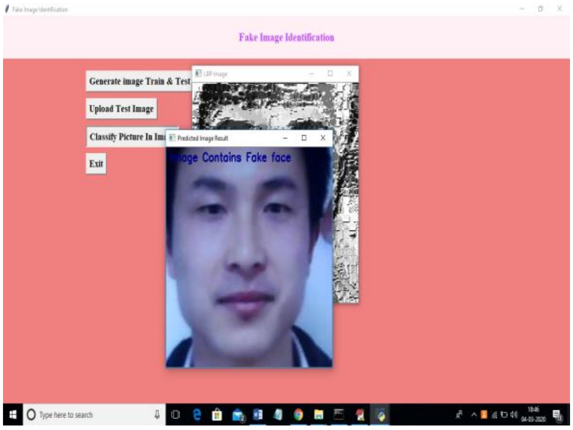


Image Contains Fake face

Fig. 7 Output screen 7

VI.CONCLUSION AND FUTURE ENHANCEMENT

The convolution neural network LBPNET, which is based on LBP, will be used in this research to identify false face photos. Here, we'll first separate LBP from photos, after which we'll train a convolution neural network with examples of LBP to develop a coaching model. When a new test is transferred, the exam will be utilised on a coaching model to assess whether or not it contains a phoney exam. Next, we'll look over some LBP details. With the aid of the proposed pairwise learning, the recommended fake image detector should be able to recognise the false picture generated by a new GAN. Our test findings demonstrated that the recommended technique outperforms other state-of-the-art plans in terms of accuracy and recall rate. Future work may, for instance, use an extensive and detailed model to account for unanticipated issues. Deep neural networks are incorporated whenever the model is made simpler with the goal of enhancing learning. Neural network approaches seldom ever take into consideration the non-linear feature interactions and non-monotonic short-run serial patterns necessary to explain user behaviour in thin sequence information. Neural networks are also incorporated into a model to remedy this flaw. If the dataset were expanded, another form of picture, such grayscale photographs, may be used for coaching.

REFERENCES

[1]. G.Mohamed Sikandar, "100 Social Media Statistics You must know," [online] Available at:https://blog.statusbrew.com/social-mediastatistics-2018-for-business/ [Accessed 02 Mar 2019].

[2]. Damian Radcliffe, Amanda Lam, "Social Media in the Middle East,"[online]Available:https://www.researchgate.net/publication/32318 5146_Social_Media_in_the_Middle_East_The_Story_of_2017 [Accessed 06 Feb 2019].

[3]. GMI_BLOGGER,"Saudi Arabia Social Media Statistics," GMI_ blogger. [online] Available at:https://www.globalmediainsight.com/ blog/saudi-arabia-social-media-statistics/ [Accessed 04 May 2019].

[4]. Kit Smith,"49 Incredible Instagram Statistics,". Brandwatch. [online] Available at: https://www.brandwatch.com/blog/instagram-stats/ [Accessed 10 May 2019].

[5]. Selling Stock. (2014). Selling Stock. [online] Available at: https://www. selling-stock.com/Article/18-billionimages-uploaded-to-the-web-everyd [Accessed 12 Feb 2019].

[6]. Li, W., Prasad, S., Fowler, J. E., & Bruce, L. M. (2012). Localitypreserving dimensionality reduction and classification for hyperspectral image analysis. IEEE Transactions on Geoscience and Remote Sensing, 50(4), 1185–1198.

[7]. A. Krizhevsky, I. Sutskever, & G. E. Hinton, (2012). Imagenet classification with deep convolutional neural networks. In Advances in Neural Information Processing Systems, 1097–1105.

[8]. K. Ravi, (2018). Detecting fake images with Machine Learning. Harkuch Journal

[9]. L. Zheng, Y. Yang, J. Zhang, Q. Cui, X. Zhang, Z. Li, et al. (2018). TICNN: Convolutional Neural Networks for Fake News Detection. United States

[10]. R. Raturi, (2018). Machine Learning Implementation for Identifying Fake Accounts in Social Network. International Journal of Pure and Applied Mathematics, 118(20), 4785-4797. [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. The University of California, Department of Electrical and Computer Engineering, USA.

[12]. S. Aphiwongsophon, & P. Chongstitvatana, (2017). Detecting Fake News with Machine Learning Method. Chulalongkorn University, Department of Computer Engineering, Bangkok, Thailand.

[13]. M. Villan, A. Kuruvilla, K. J. Paul, & E. P. Elias, (2017). Fake Image Detection Using Machine Learning. IRACST—International Journal of Computer Science and Information Technology & Security (IJCSITS).

[14]. S. Shalev-Shwartz, & S. Ben-David, (2014). Understanding Machine Learning: From Theory to Algorithms. New York: Cambridge University Press.