

Fake Image Detection Using Machine Learning

**V.VenkataReddy¹, P.Priyanka², D.Kavya Supriya³, P.R.Vishnu⁴,
A.Dinesh Kumar⁵, Srihari Babu Gole⁶**

Student, Computer Science And Engineering, KL University, Guntur, India^{1,2,3,4}

Associate professor, Assistant professor Computer Science And Engineering, KL University, Guntur, India^{5,6}

Abstract: Nowadays biometric systems are useful in recognizing a person's identity, but criminals change their appearance in behaviour and psychological to deceive recognition system. To overcome this problem we are using a new technique called Deep Texture Features extraction from images and then building train machine learning model using CNN (Convolution Neural Networks) algorithm. This technique refers as LBPNet or NLBPNet as this technique is heavily dependent on features extraction using LBP (Local Binary Pattern) algorithm.

In this project, we are designing LBP Based machine learning Convolution Neural Network called LBPNET to detect fake face images. Here first we will extract LBP from images and then train LBP descriptor images with Convolution Neural Network to generate a training model. Whenever we upload a new test image then that test image will be applied to the training model to detect whether the test image contains a fake image or a non-fake image. Below we can see some details on LBP.

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

I.INTRODUCTION

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 hardness 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.

II.LITERATURE SURVEY

Very little work has been finalized around detecting forge audio, images, and videos. Yet, several studies and tasks are underway to identify what can be done around the incredible proliferation of counterfeit pictures online. Adobe recognizes the way in which Photoshop is misused and has tried to offer a sort of antidote [8]. The following provides a summary of a few of these studies: According to a study [9] conducted by Zheng et al. (2018), the identification of fake news and images is very difficult, as fact-finding of news on a pure basis remains an open problem and few existing models can be used to resolve the problem. It has been proposed to study the problem of "detecting false news." Through a thorough investigation of counterfeit news, many useful properties are determined from text words and pictures used in counterfeit news. There are some hidden characteristics in words and images used in fake news, which can be identified through a collection of hidden properties derived from this model through various layers. A pattern called TI-CNN has been proposed. By displaying clear and embedded features in a unified space, TI-CNN is trained with both text and image information at the same time.

Raturi's 2018 architecture [10] 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. In a 2017 study by Bunk et al [11], two systems were proposed to detect and localize fake images using a mix of resampling properties and deep learning. In the initial system, the Radon conversion of resampling properties is determined on overlapping pictures corrections. Deep learning classifiers and a



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 [12], 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. In [13] by Kuruvilla et al., a 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 research develops an approach that takes an image as input and classifies it, using the CNN model. For a completely new task/problem, CNNs are very good feature extractors. It extracts useful attributes from an already trained CNN with its trained weights by feeding your data at each level and tuning the CNN a bit for the specific task. This means that a CNN can be retrained for new recognition tasks, enabling it to build on pre-existing networks. This is called pre-training, where one can avoid training a CNN from the beginning and save time. CNN can carry out automatic feature extraction for the given task. It eliminates the need for manual feature extraction since the features are learned directly by the CNN. In terms of performance, CNNs outperform many methods for image recognition tasks and many other tasks where it gives high accuracy and accurate result. Another key feature of CNNs is weight sharing, which basically means that the same weight is used for two layers in the model. Due to the above features and advantages, CNN is used in this research in comparison to other deep learning algorithms.

III.METHODOLOGY

A. EXISTING SYSTEM

When capturing an image, additional required hidden information is associated with it for authentication and forgery protection purposes. The passive technique does not rely on extra information, but it analyzes some features extracted from the digital content of the image itself. Copy-move means coping a part of an image and pasting it into another place of the same picture whereas splicing is about taking a part of an image and pasting it into 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.

B. TOOLS USED:

I. SOFTWARE REQUIREMENTS:

Operating system : Windows 10

Coding Language : python

Tool : PyCharm

II. HARDWARE REQUIREMENTS:

System : Pentium IV 2.4 GHz.

Hard Disk : 40 GB.

Ram : 512 Mb.

C. PROPOSED SYSTEM

In this project, we have a tendency to area unit planning LBP primarily based machine learning Convolution Neural Network known as LBPNET to sight pretend face pictures. Here 1st we'll extract LBP from pictures and so train LBP descriptor pictures with Convolution Neural Network to get coaching model. Whenever we have a tendency to transfer new take a look at the image then that take a look at image are going to be applied on coaching model to sight whether or not take a look at image contains pretend image or non-fake image. Below we will see some details on LBP.

**Advantages:**

- Libraries help to analyze the data.
- Statistical and prediction is very easy compared to existing technologies.
- Results will be accurate 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

Fig. 1 Output screen 1

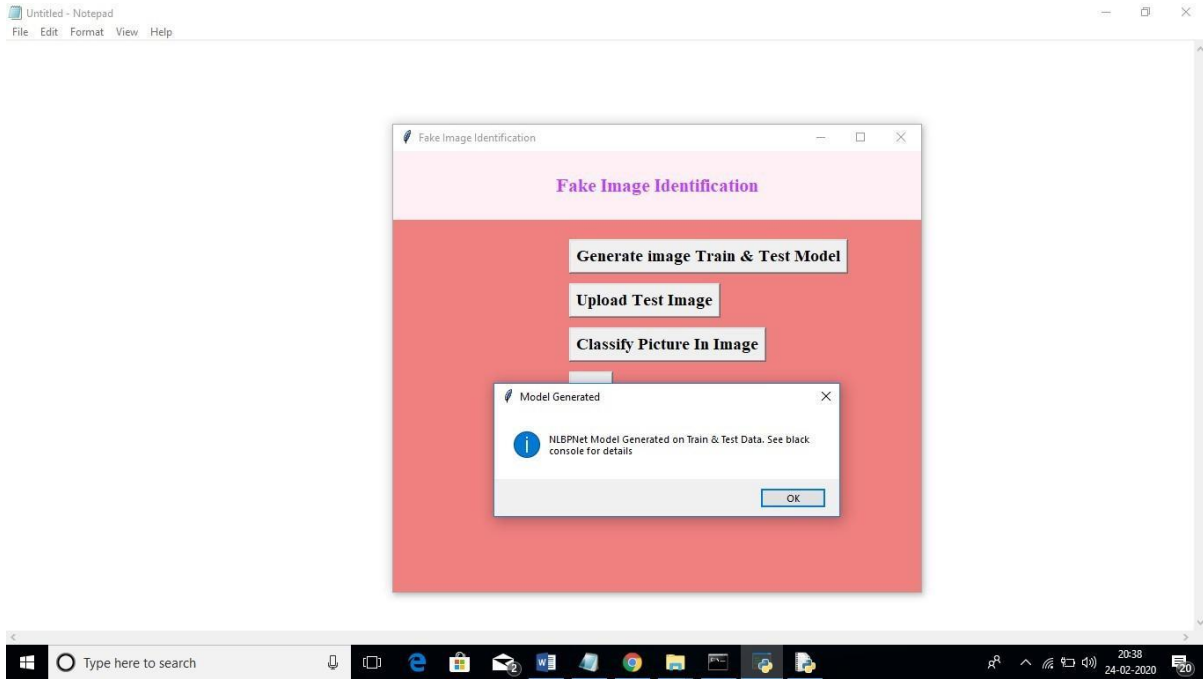


Fig. 2 Output screen 2

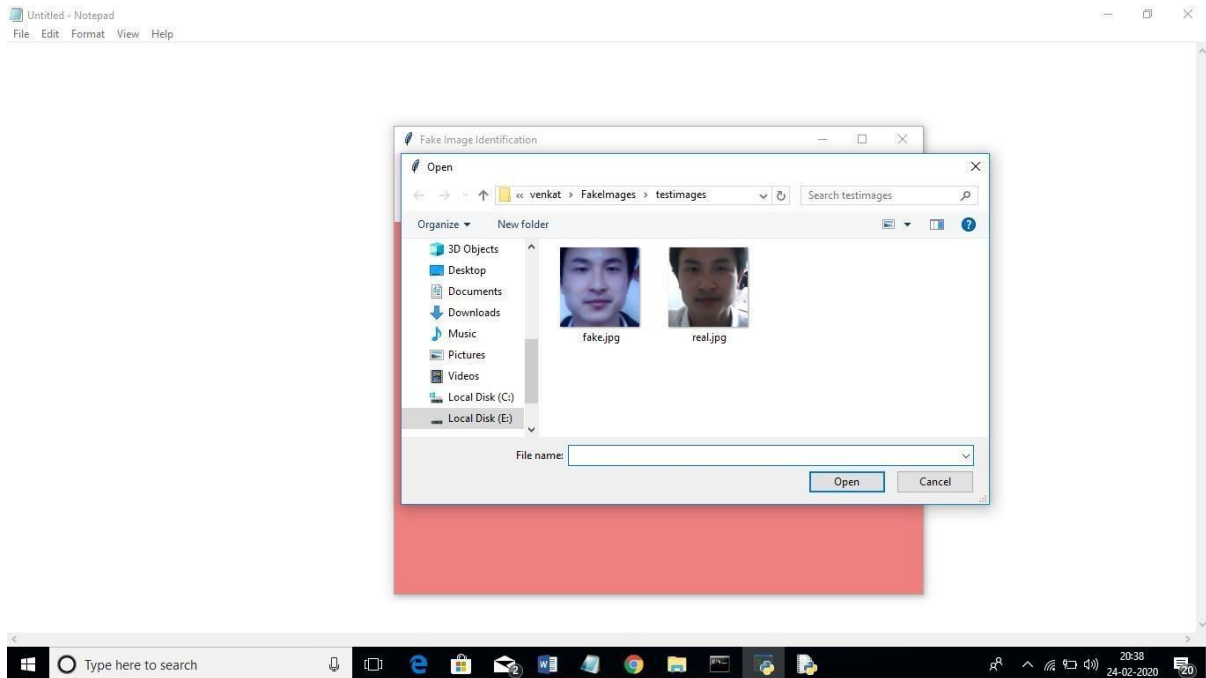


Fig. 3 Output screen 3

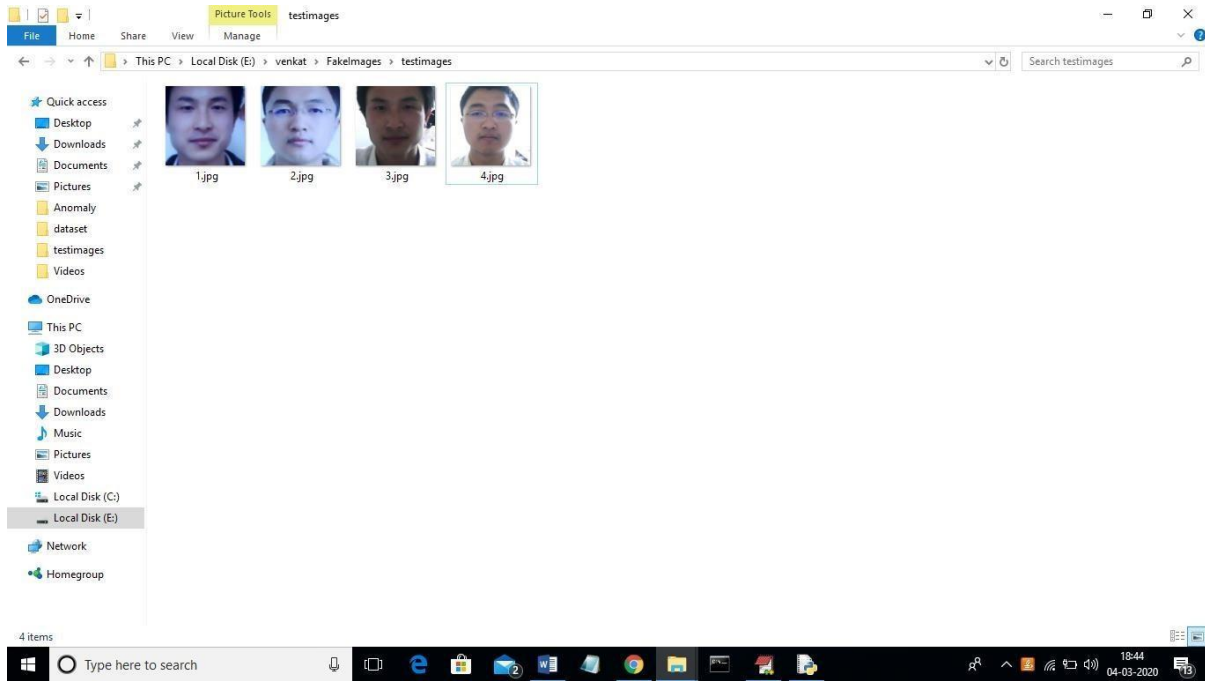


Fig. 4 Output screen 4

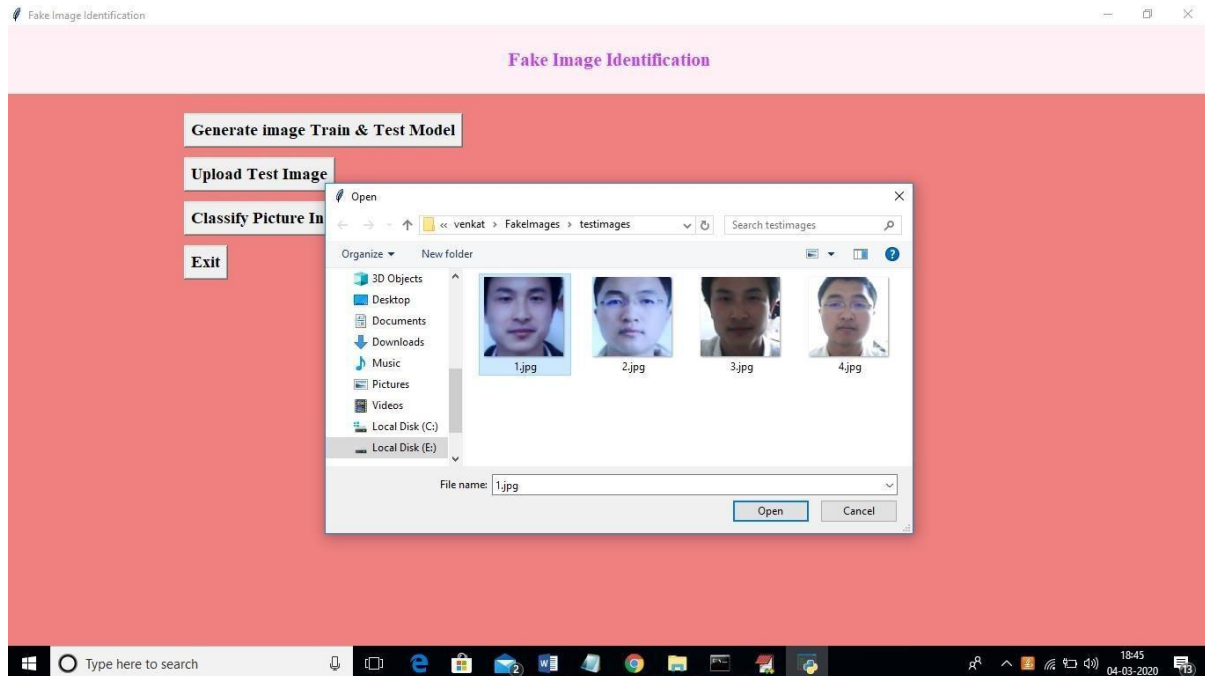


Fig. 5 Output screen 5

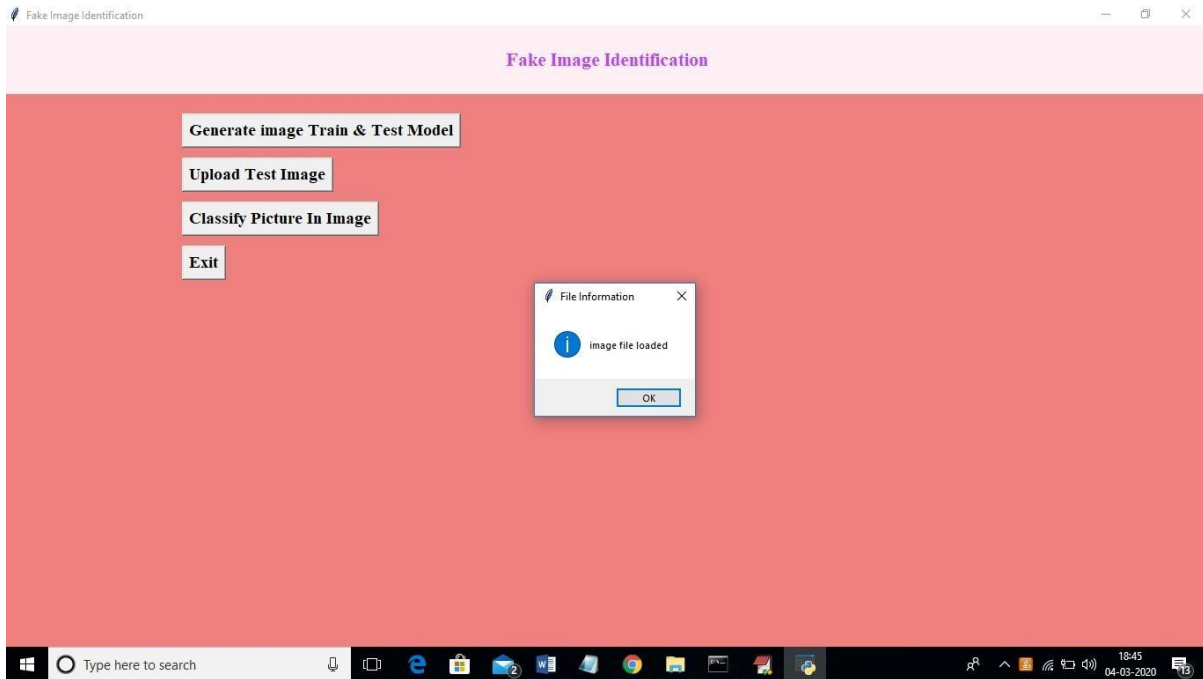


Fig. 6 Output screen 6

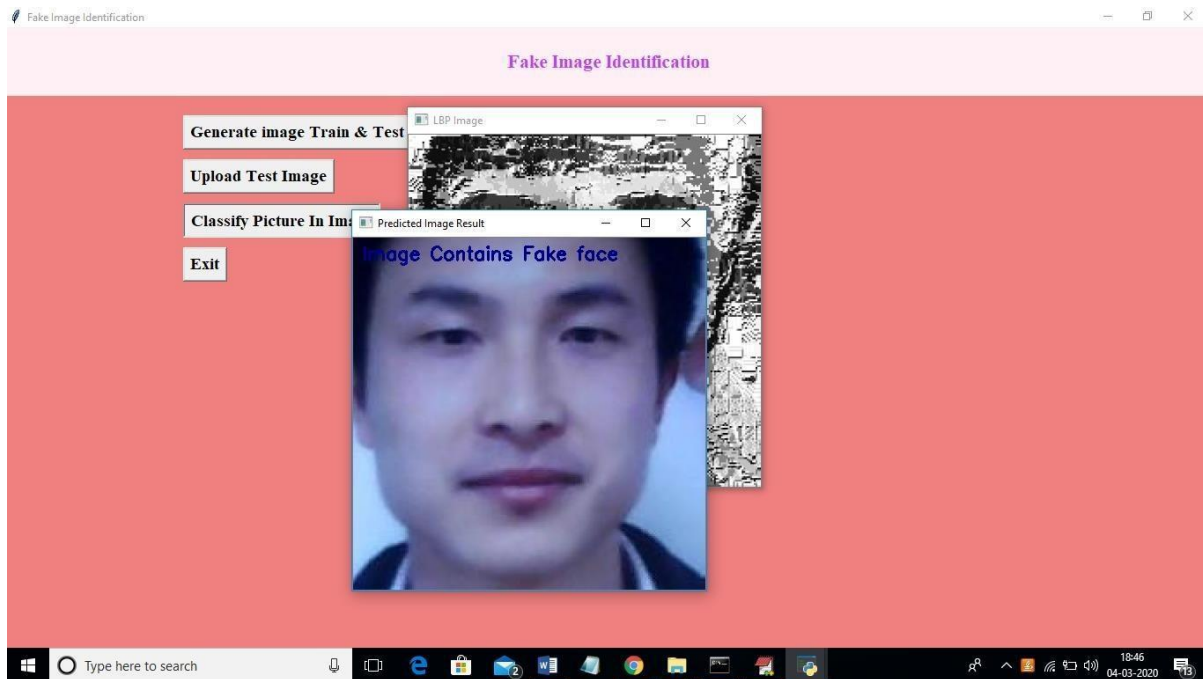


Fig. 7 Output screen 7

VI.CONCLUSION AND FUTURE ENHANCEMENT

In this study, we have proposed a novel common fake feature network-based pairwise learning, to detect the fake face/general images generated by state-of-the-art GANs successfully. The proposed CFFN can be used to learn the middle- and high-level and discriminative fake features by aggregating the cross-layer feature representations into the last fully connected layers. The proposed pairwise learning can be used to improve the performance of fake image detection further. With the proposed pairwise learning, the proposed fake image detector should be able to have the



ability to identify the fake image generated by a new GAN. Our experimental results demonstrated that the proposed method outperforms other state-of-the-art schemes in terms of precision and recall rate.

For future, work square measure for instance employing an additional complicated and deeper model for unpredictable issues. Integration of deep neural networks with the idea of increased learning, wherever the model is simpler. Neural network solutions seldom take under consideration non-linear feature interactions and non-monotonous short-run serial patterns, that square measure necessary to model user behavior in thin sequence information. A model is also integrated with neural networks to unravel this downside. The dataset can be inflated and another variety of images can be used for coaching, for instance, gray-scale pictures.

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/323185146_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-billion-images-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.