International Journal of Innovative Research in Engineering
Volume 4, Issue 3 (May-June 2023), PP: 01-05.
www.theijire.com ***ISSN No: 2582-8746***

Fake Image Detection on Social Media usingCNN Algorithm

Aakash Singh[1], Deepak Verma[2], Km Annu Singh[3], Km Pinki Yadav[4], Sunil Yadav[5]
[1,2,3,4] B.Tech Students, Department of Computer Science & Engineering, Institute of Technology and Management, GIDA, Gorakhpur,India.
[5]Assistant Professor, Department of Computer Science & Engineering, Institute of Technology and Management, GIDA, Gorakhpur,India.

How to cite this paper:
Aakash Singh[1], Deepak Verma[2], Km Annu Singh[3], Km Pinki Yadav[4], Sunil Yadav[5], "Fake Image Detection on Social Media usingCNN Algorithm", IJIRE-V4I03-01-05.

Abstract: *In today's time, the common man is being fooled through fake pictures because they do not know whether the pictures are real or not.In this technological age, people have placed social media at a prominent level in their daily lives. Most of the people share their information or any important thing on social media through text message image and video like twitter, snapchat, Face book, WhatsApp telegram and many more. Biometric techniques are helpful now for identifying people, but criminals alter their look, behaviour, and psychology to trick the identification system. In order to solve this issue, we are employing a novel method called Deep Texture Features Extraction from Images, followed by the construction of a machine learning model utilising the CNN (Convolution Neural Networks) algorithm.As it largely relies on features extraction utilising the LBP (Local Binary Pattern) method, this technique is often referred to as LBP Net or NLBP Net. The sole purpose of this research is to create a model that can be used to classify social media content to detect any threats and fake images. This model was made using Deep Learning which is Convolutional Neural Network (CNN). 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, and then we will train the convolution neural network on the LBP descriptor images to produce the training model. Every time a newtest picture is uploaded, the training model will use that image to determine if the test image contains fraudulent images or not. Details regarding LBP are shown below. Now that the feature vector has been processed, it may be classified using a machine learning method such as the Support Vector Machine, extreme learning machines, or another one. The study of textures or the recognition of faces may both be done using these classifiers. The results of this research will be helpful in monitoring and trucking of images in social media to detect unusual material counterfeit images and protect social media from threats and fraudsters.*

Key Word: *Supervised Machine Learning Techniques,Local binary patterns (LBP), Convolution Neural Network (CNN); Support vector machine.*

I.INTRODUCTION

In this technological age, there have been many changes in the way people interact and move their lives forward and communicatively, it becomes very easy through social media.

Social media is based on the unique foundation that connects people and empowers them to present their interests and ideas by presenting themselves and forming new friendships with all others who share their interests. WhatsApp, Facebook, TwitterSnapchat and Instagram are among the most popular social network sites at the moment.

Sharing her images online through social networking services like Instagram is widespread and at least 90 million images are currently being shared via Instagram every single day. People upload and share billions of photos every day through social media.

In recent years, it has been common practise to synthesise the complete or partial photo- realistic content of a picture or video using generative models based on deep learning, such as the generative adversarial net (GAN). A very photorealistic image or video might also be created using GANs thanks to recent research, including Big GAN and the Progressive Growth of GANs (PGGAN) study, making it impossible for a human to tell if it is genuine or not in the short amount of time. The picture translation jobs may generally be completed using generative software. When the fabricated or artificial picture is utilised incorrectly on a social media site, though, it might become a severe issue. The phoney facial picture in a pornographic video, for example, is created using CycleGAN.

We provide a unique network architecture with a pairwise learning technique, dubbed the common fake feature network (CFFN), in order to address the enormous demand of the fake picture identification for GANs-based generator. The pairwise learning strategy may clearly address the drawbacks of supervised learning-based CNNs, such as those in, according to our earlier methodology. The performance of the false picture identification is substantially enhanced in this research by the use of a unique network design combined with pairwise learning.

We employ the suggested deep fake detector(Deep FD) to distinguish between fake faces and generic images in order to assess the efficacy of the system.

In this technological age, more and morepeople are falling prey to image counterfeiting. Many criminals use software and photographs to mislead the courts or to provide evidence [17]. Under this research, using machine learning Algorithm [6,7], the researcher will try to propose a class formodel through a convolutional neural network (CNN) which is able to take advantage of knowledge to take an image from social media and then this model Classified and is able to detect it.

II.LITERATURE SURVEY

So far very little work has been done to detectfake audio image video. Yet, several studies and works are on the way to find What can bedone about the spread of fake photos online and around credible dissemination. Adobe software that detects the way Photoshop is abused and tries to provide a way to [8]. The following provide a relating to of a rare of these literatures:

By **Bunk et al** [11] in 2017 during theirresearch, two systems were present to detect and assign forgery images using a consistof examining properties and deep learning. Deep learning classifiers and a Gaussian conditional domain pattern are then used to construct a heat map. In the beginning system, the Radon conversion of examining properties is founded on overlapping picturescorrections.

Deep learning classifiers and a Gaussian conditional domain pattern are used togenerate heat map. A Random Walker segmentation method uses total fields. Further system, Knowing and Detecting it, Software resampling properties are proceed on turn overing object patches over a long- term memory (LSTM)based network.

Explore it with Both detection systems have been compared. The result ensures that activein detecting and committing image fraud in both systems.

In 2018 **Raturi's** systems [10], was present to find out Whatever is the latest social website nowadays, most of the fake accounts are on Facebook social media. Machine learning feature was used in this experiment to better found fake accounts based on their and their information on social networking wall. Focused on analyzing data and collecting offensive words and the number oftimes they were used. The results of this research ensure that the main problems related to the security of social networks are that the data is not treated properly before it is posted.

According to a survey [9] proposed by **Zhenget al.** To detecting of fake news and images is complex, Some existing models can beused to address these problems because uponimprovement we know that finding the element of news remains a major problem. This proposal describes the problem of "detecting false news." Through internal investigation of fake news, Many good features are evidenced by appropriate textwords and images in fake news. Words and images used in fake news have hidden features, whereby individual layers means can be identified through the collection of hidden information obtained from this structure. A pattern called TI-CNN has been proposed.

By **Mykhailo Granik et.** in his study [3] , Itstates that using naïve Bayes classifier is the easiest way to detect fake news using simple. This usage was implemented in the form of a software system and data set comprehension used on a Facebook news post. They were aggregate from three large Facebook pages each from the right and from the left, Its above Three big mainstream political news pages (Politico CNN ABC News). They all achieved a classification accuracy of about approx.74%.This may be due to thedivergence of the data set in which only 4.9%were fake news.

In [13] by **Kuruvilla et al.,** a neural networkby examining the error levels of 4000 false notes and 4000 genuine photos, a neural network of this type was effectively trained. An impressive 83% of the time, the given neural network correctly determines if a picture is real or phoney. With 60% of the neural network output and 40% of the analysis, this metamodel creates and evaluates trustworthy simulated image recognition systems.

By **Kim's and Lee's** survey [15] To identify fraud and phoney photographs used for criminal purposes, digital forensic methods are required. In this manner, the researchers doing this study are developing an algorithm to identify fraudulent photos using deep learning methods. where fresh study has uncovered surprising facts.

This study creates a method that uses the CNN model to classify images once they areentered.. CNNs are excellent feature extractors for tasks or problems that are entirely new. It feeds your data at each level, trains the CNN with its taught weights, and then extracts usable properties from the CNN for the given job. Accordingly, a CNNmay be retrained to perform additional recognition tasks, allowing for the expansionof existing networks. This process of saving time and not having to train a CNN from scratch is known as pre-training.

III.METHODOLOGY

This study investigates a supervised machinelearning classification issue [14, 18], where the training phase is the label or category of the input sample. The actual image class andthe false image class are the two labels or classes. Additional necessary hidden information is attached to a picture at the timeof capture for authentication and forgery protection reasons.

For authenticity and forgery protection reasons, additional necessary concealed information is attached to a picture when it iscaptured. The researcher used a traditional neural network in conjunction with deep learning (CNN).

A. Neural network input features

The objective is to gather relevantdata attributes. Through the creation of new features from the current ones, features seek to minimise the amountof features in a dataset (and then discarding the original features).

B. Devloping Fake Image DetectionAlgorithm Architecture Figure 1 depicts the architecture of a convolution neural network (CNN).

• Target photographs, which serve as the dataset relevant to answering the research questions, testing the hypothesis, and evaluating the outcomes, will be taken from the Instagram programme.

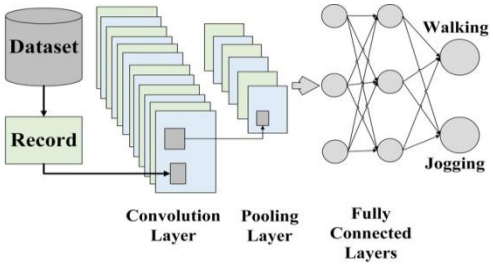

Fig. 1. Convolution Neural Network Architecture.

Testing and Results: Following the dataset's testing after the neural network hascompleted its training, we retrieve a confusion matrix, which comprises a numberof factors used to calculate the accuracy of the neural network.

IV.PROPOSED SYSTEM

The two main contributions of the suggestedtechnique are as follows:

- To increase the false image's representative power, we suggest a fake face image detector built on theinnovative CFFN and composed of anumber of dense blocks.
- In order to enhance recommendations. Deep FD's standardisation property, the paired learning strategy is initially implemented.

Tools Used

Software Requirements

- Operating System : Windows 10
- Coding Language : Python
- Tool : PyCharm, VS Code

Hardware Requirements

- System : Pentium IV 2.4 GHz
- Hard Disk : 40 GB
- Ram : 512 Mb

V.IMPLEMENTATION

With the aid of Deep Learning Toolbox, youmay execute transfer learning using a pretrained model or create your own CNN from start. The technique you use will rely onthe resource you have, the kind of applicationyou are building, and the programme'sintended use. The number of layers and filtersmust be chosen, and the other conditionsmust be modified, in order to train the network from scratch. It can take a while to gather the vast quantities of data based on millions of samples necessary to train a particular model from scratch. Using a pre- trained model to automatically extract attributes from a fresh dataset is a suitable substitute for CNN training from scratch.

A test dataset and a training dataset are present. Additionally, there are instances where training data is used to generate test data and vice versa. In this experiment, we used two datasets. 100 photos are included inthe testing dataset, while 100 images are included in the training dataset. 100 photos make up the second dataset's training set,while 40 images serve as the test set. For eachoriginal picture in the second dataset, three fake photos were created. The false images inthe training data were extracted from the original photographs. By adding, removing, and altering colors, the researcher altered the original photos. Following are the processes for the dataset training using the CNN network.

1) Load sample data as a data storage for the image, then load it foranalysis. Data is stored as an object ofthe picture datastore and automatically labelled photos depending on the name of the folder. When training a convolution neural network, an image datastore allows you to effectively analyse batches of images and store massive amounts ofpicture data.

2) Establish the network architecture:Establish network layers and theconvolutional neural networkarchitecture.

3) Training option definition: After designing the network's architecture, the training choices are defined. the quantity of epochs, the learning rate, the batch size, and the momentum.

4) Train the network: Use the training choices, training data, and layer- defined architecture to train the network.

5) Determine the new data's labels inadvance and evaluate the categorization accuracy.
Using the trained network, make predictionsabout the data's labels, and then assess the final accuracy.

Fig. 1. Image Classification

Fig. 2. Image Classification

Test Datasets

In this phase, the researcher selected a picturefrom among the photographs using codes, and then, as shown in Figures 1 and 2, determined whether the image was real or a fake.

VI.RESULT AND DISCUSSION

There includes a thorough discussion of the suggested methodology's performance metrics. This research's main objective is to accurately distinguish between real and false photographs. In this study, a convolution neural network is employed for this purpose.

To categorise the provided image as authentic or fraudulent, the output's probability is calculated. Here, the method created in this study is assessed in relation tothe available methodologies and on the basisof performance criteria.

Performance Measures

Various performance indicators, including sensitivity, specificity, accuracy, precision,and recall, are used to assess the performanceof the projected approach.

Performance Analysis

The tables below tabulate and display the effectiveness of the suggested strategy. It has been demonstrated that different networkshave varying degrees of result accuracy.

accuracy score of 83%, a recall score of 82%,and a f1 score of 81.5% were attained using the LBN.

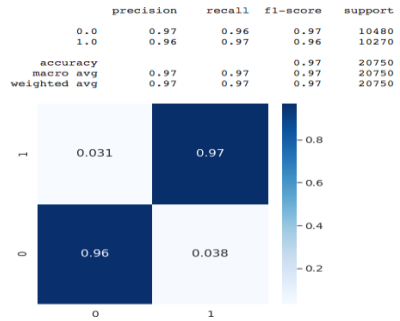

Fig. 3. Diagram for precision, recall, fi-score, support

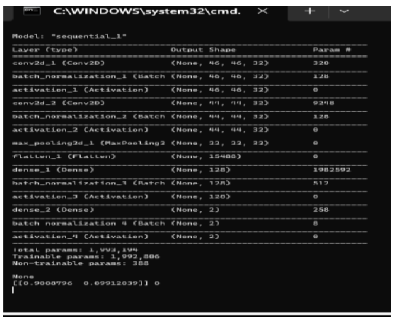

Fig. 4. Table for parameters i.e. Trainable params andNon-Trainable params (Layer, normalization, activation)

The total accuracy of the LBN classifier was81.8%. This means that in terms of accuracy,the LBN design outscored the vision transformer architecture by 1.1%. An overall

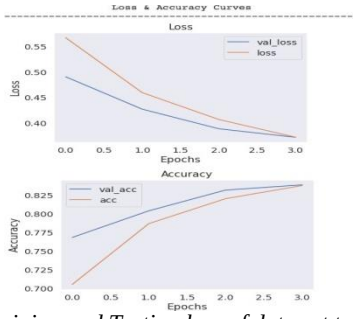

Fig. 5. Training and Testing loss of data set to givento the model

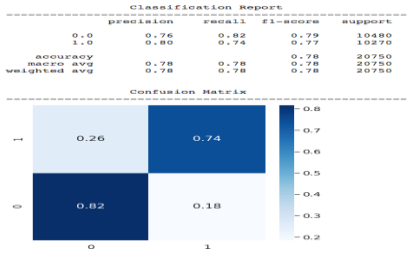

Fig. 6. Classification Report and Confusion matrixfor result of the model

By computing the value of True positive,True Negative, False positive, and False Negative, the values of precision, recall, accuracy, specificity, and sensitivity are recovered from the confusion matrix after thecode has run.

VII.CONCLUSION

Lately, There have been electronic attacks in Saudi Arabia also a large population country India faced threats and attacts.

At this time we neither have a clear vision norany unified framework to protect us fromtheft, counterfeiting and big threats, social media is a very wide area in today's time where the spread of false accounts is concerned.

This research is particularly contributing to the rapid detection and rectification offorgery and fraud in the field of images in social media.

In order to properly detect the false face/general pictures produced by cutting-edge GANs, we have suggested a unique common fake feature network based on paired learning in this research. By aggregating the cross-layer feature representations into the final fully connectedlayers, the proposed CFFN may be utilised tolearn the middle- and high-level and discriminative fake features. The suggested paired learning may be utilised to furtherenhance the effectiveness of false picture detection. The suggested false image detectorought to be able to recognise the fake pictureproduced by a new GAN with the help of thepairwise learning that is being proposed. Ourtest findings showed that, in terms ofprecision and recall rate, the suggestedstrategy exceeds other cutting-edge plans.

Like a neural network, CNN and its deviation can also be optimized to large datasets, which is often the case when classifying objects.

For future task recommended by this research are for example using more complex anddeeper model for detectable problem.Integration of deep neural networks with thetheory of enhanced learning.

Reference

1. *G.Mohamed Sikandar, "100 SocialMedia Statistics You must know,"[online] Available at: https://blog.statusbrew.com/social-mediastatistics-2018-for-business/ [Accessed 02 Mar 2019].*
2. *Kit Smith,"49 Incredible InstagramStatistics,". Brandwatch. [online] Available at:https://www.brandwatch.com/blog/inst agram-stats/ [Accessed 10 May 2019].*
3. *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.*
4. *K. Ravi, (2018). Detecting fake imageswith Machine Learning. HarkuchJournal*
5. *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*
6. *S. Aphiwongsophon, & P. Chongstitvatana, (2017). DetectingFake News with Machine Learning Method. Chulalongkorn University, Department of Computer Engineering, Bangkok, Thailand.*
7. *M. D. Ansari, S. P. Ghrera, & V. Tyagi,(2014). Pixel-based image forgery detection: A Review. IETE Journal of Education, 55(1), 40–46.*
8. *Y. Li, & S. Cha, (2019). Face Recognition System. arXiv preprint arXiv:1901.02452.*
9. *R. Saracco, (2018). Detecting fakeimages using artificial intelligence. IEEE Future Directions.*