Fake Image Detection

S. Shalini¹, A. Sowmya², G. Rohith Raj³, Mrs. J. Matha⁴, Mr. B. Ramji⁵

¹, ² B. Tech Student, ³ Assistant Professor, ⁴ Assistant Professor, Dept of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana, India

Abstract: In this technological generation, social media plays an important role in people’s daily life. Most of them share text, images and videos on social media (Instagram, Facebook, Twitter, etc.). Images are one of the common types of media share among users on social media. So, there is a chance for monitoring of images contained in social media. So most of the people can fabricate these images and disseminate them widely in a very short time, which treats the credibility of the news and public confidence in the means of social communication. So here this research has attempted to propose an approach which will extract image content, classify it and verify that the image is false or true and uncovers the manipulation. There are many unwanted contents in social media such as threats and forged images, which may cause many issues to the society and also national security. This approach aims to build a model that can be used to classify social media content to detect any threats and forged images.

Keywords: Convolution Neural Networks, Fake image Detection.

I. INTRODUCTION

Many fake images are spreading through social media nowadays. Identification of such fake images is inevitable for the unveiling of the image based cybercrimes. Forging images and identifying such images are promising research areas in this technological era. The forged images are a detected using Convolutional Neural Network (CNN). This research aims to build a model that can be used to classify Social media content (images) to detect any threats and forged images. The model was built using deep learning algorithms which is Convolutional Neural Network (CNN), Alexnet network and transfer learning using Alexnet. The results occurred from the proposed Alexnet network offers more accurate Identification of fake images compared to the other techniques with 97%. The results of this research will be helpful in monitoring and tracking in the shared images in social media for unusual content and forged images detection and to protect social media from electronic attacks and threats. This model provides facility to upload the images and get to know which is fake and which is real. This project uses machine-learning methods and computer vision to identify fake images from pictures. First, we use a convolutional neural networks to classify image key features for each image. We then compare a number of classification algorithms that use certain features to predict the image whether it is fake or real.

II. LITERATURE SURVEY

In the proposed model we are using new technique called Deep Texture Features extraction from images and then building train machine learning model using CNN (Convolution Neural Networks) algorithm. This technique refer as LBPNet or NLBPNet as this technique 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 training model. Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-fake image. 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 about counterfeit pictures online. The following provide a summary of a few of these studies:

A. Locality-preserving dimensionality reduction and classification for hyperspectral image analysis.
B. ImageNet Classification with Deep Convolutional Neural Networks.
C. CNN: Convolutional Neural Networks for Fake News Detection.
D. Machine Learning Implementation for Identifying Fake Accounts in Social Network.
E. Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning.
III. PROPOSED SYSTEM AND ARCHITECTURE

The aim of proposed system is to identify the fake images. The system provides higher accuracy and reduces the classification work. The existing system has several disadvantages and many more accuracy issues. The proposed system tries to eliminate or reduce these issues up to some extent. To overcome these limitations an advanced method is proposed which is deep learning algorithm which is Convolutional Neural Networks (CNN). This Convolutional Neural Networks algorithm will be first trained and generate the train and test model. Once the model has generated we need to upload the test image on that model, upon uploading the test image the generated model will classify that image and identifies whether the image is fake or real.

The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features:

A. It provides the strong quality and low cost.
B. It will extract the hidden features from the images.
C. It gives better and accurate result and minimum time requirement.

A system architecture is very important to understand the flow of the project. It describes the step-by-step procedure of the complete project. Here, firstly we will import the dataset which is a process of loading and reading data from various resources. Then, the data will be preprocessed it is a step in which the data gets transformed, or Encoded, to bring it to such a state that now the machine can easily parse it. In other words, the features of the data can now be easily interpreted by the algorithm. Next we will read all LBP images from LBP folder and then train CNN model with all those images to generate training model. Once the training model has generated we will upload test image from ‘testimages’. Application will read this image and then extract Deep Textures Features from this image using LBP algorithm. Finally, we need to apply test image on CNN train model to predict whether test image contains spoof or non-spoof face.

IV. IMPLEMENTATION

A. Module and its Description

1) Generate Image Train and Test Model: The first step in this process is generate image train and test model. In this step, we will read all LBP images from LBP folder and then train CNN model with all those images. 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 training model.

2) Upload Test Image: In this module we will upload test image from ‘testimages’ folder. Application will read this image and then extract Deep Textures Features from this image using LBP algorithm. Whenever we upload new test image then that test image will be applied on training model to detect whether test image contains fake image or non-spoof face.

3) Classify Picture In Image: This step apply test image on CNN train model to predict whether test image contains spoof or non-spoof face. Local binary patterns (LBP) is a type of visual descriptor used for classification in computer vision and is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. Due to its discriminative power and computational simplicity, LBP texture operator has become a popular approach in various applications. It can be seen as a unifying approach to the traditionally divergent statistical and structural models of texture analysis. Perhaps the most important property of the LBP operator in real-world applications is its robustness to monotonic gray-scale changes caused, for example, by illumination variations. Another important property is its computational simplicity, which makes it possible to analyze images in challenging real-time settings.
The LBP feature vector, in its simplest form, is created in the following manner:
Divide the examined window into cells (e.g. 16x16 pixels for each cell).
For each pixel in a cell, compare the pixel to each of its 8 neighbors (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise.
Where the center pixel's value is greater than the neighbor's value, write "0". Otherwise, write "1". This gives an 8-digit binary number (which is usually converted to decimal for convenience).
Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center). This histogram can be seen as a 256-dimensional feature vector.
Optionally normalize the histogram.
Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window.
The feature vector can now be processed using the Support vector machine, extreme learning machines, or some other machine learning algorithm to classify images. Such classifiers can be used for face recognition or texture analysis.
A useful extension to the original operator is the so-called uniform pattern, which can be used to reduce the length of the feature vector and implement a simple rotation invariant descriptor. This idea is motivated by the fact that some binary patterns occur more commonly in texture images than others. A local binary pattern is called uniform if the binary pattern contains at most two 0-1 or 1-0 transitions. For example, 00010000 (2 transitions) is a uniform pattern, but 01010100 (6 transitions) is not. In the computation of the LBP histogram, the histogram has a separate bin for every uniform pattern, and all non-uniform patterns are assigned to a single bin. Using uniform patterns, the length of the feature vector for a single cell reduces from 256 to 59. The 58 uniform binary patterns correspond to the integers 0, 1, 2, 3, 4, 6, 7, 8, 12, 14, 15, 16, 24, 28, 30, 31, 32, 48, 56, 60, 62, 63, 64, 96, 112, 120, 124, 126, 127, 128, 129, 131, 135, 143, 159, 191, 192, 193, 195, 199, 207, 223, 224, 225, 227, 231, 239, 240, 241, 243, 247, 248, 249, 251, 252, 253, 254 and 255.

V. RESULTS AND ANALYSIS
This project is an application that develops and tests reliable fake image detection program by combining the results of metadata analysis (40%) and neural network output (60%). This research explores a supervised machine learning classification problem where the label or category of the input sample is known as the training phase. There are two labels or classes: the real image class and the fake image class.

A. Output Screens

![Fake Image Identification](image)

Fig 2: Main page

In above screen click on ‘Generate Image Train & Test Model’ button to generate CNN model using LBP images contains inside LBP folder.
In above screen we can see CNN LBPNET model generated. Now click on ‘Upload Test Image’ button to upload test image.

In above screen we can see four faces are there from same person but in different appearances, we can see all real face will have normal light and in fake faces has some editing to avoid detection but this application will detect whether face is real or fake. In above screen I am uploading 2.jpg and after upload click on open button to get below screen.

In the above screen we can see that image file has been uploaded successfully. And now click on ‘classify Picture in Image’ to get below details.
In above screen we are getting result as image contains Fake face. Similarly you can try other images also. If you want to try new images then you need to send those new images to us so we will make CNN model to familiar with new images so it can detect those images also.

VI. CONCLUSION
The overall objective of our project is to identify the fake images present in social media. This is done by implementing large, deep convolutional neural network which is capable of achieving a record-breaking results on a highly challenging dataset using supervised learning where the results of this approach achieved high accuracy of up to 97%. The results of this approach will be helpful in monitoring and tracking social media content and in discovering fraud on social networking sites, especially in the field of images. There are many unwanted contents in social media such as threats and forged images, which may cause problems to society and national security. This is the most effective model to detect the fake images. This project could detect more complex images by extracting the hidden features from images by using a new technique called Deep Texture Feature Extraction from images.

VII. FUTURE ENHANCEMENTS
Future enhancement and scope related to the fake image detection are listed below:
The recommendations for future work are for example using a more complex and deeper model for unpredictable problems. Integration of deep neural networks with the theory of enhanced learning, where the model is more effective. Neural network solutions rarely take into account non-linear interactions and non-monotonous short-term sequential patterns, which are necessary to model user behavior in sparse sequence data.
A model may be integrated with neural networks to solve this problem. The dataset could be increased and another type of images could be used for training, for example gray-scale images. Like a neural network, CNN and its variants can also be optimized to large datasets, which is often the case when classifying objects.

VIII. ACKNOWLEDGEMENT
We take this opportunity to express our gratitude to PRC Coordinator Mr. B. Ramji, and Mrs. J.Matha, Department of CSE, CMR Technical Campus, for their guidance and support at every stage of the project. We would like to extend our gratitude to HOD Dr. K. Srujan Raju, Department of CSE, CMR Technical Campus for his support. We also take this opportunity to thank Dr. A. Raji Reddy, Director CMR Technical Campus, for providing us with all the facility that was required.
REFERENCES

[1] G. Mohamed Sikandar, "100 Social Media Statistics You must know,"[online] Available at: https://blog.statusbrew.com/social-media-statistics-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-every-d [Accessed 12 Feb 2019].

[6] Li, W., Prasad, S., Fowler, J. E., & Bruce, L. M. (2012). Locality-preserving 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). TI-CNN: 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.
