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] Computer Science and Engineering, Institute of Technology and Management, Gorakhpur, India.
[5]Assistant Professor, Computer Science and Engineering, Institute of Technology and Management, Gorakhpur, India.

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, snap chat, face book, Whatsapp telegram and many more. It has become easy for the general public or for small groups to create these images and disseminate widely in a very shortperiod of time, threatening the world credibility of news and public confidence through social communication. 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). Networks in the model present more accurate detection of fake images than other techniques with around 97%. 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, Convolution Neural Network (CNN); Image forgery; Classification; Features extraction*

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 networking sites are currently being seen as a major media phenomenon, And has attracted ahuge number of people, the number of users [1] worldwide has exceeded 3 billion. The increase in the number of active subscribers in the Gulf region exceeds 70%. Saudi Arabia ranks fifth in the world when it comes to social media use, with an estimated 33 million people with more than76% active users of 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. Whats App, Face book, Twitter Snap chat 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 photosevery day through social media.

In this technological age, more and more people 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 for model 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 REVIEW

So far very little work has been done to detect fake audio image video. Yet, several studies and works are on the way to find What can be done 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 their research, two systems were present to detect and assign forgery images using a consist of 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 pictures corrections.

Deep learning classifiers and a Gaussian conditional domain pattern are used to generate 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 active in 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 of times 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 **Zheng et al.** To detecting of fake news and images is complex, Some existing models can be used to address these problems because upon improvement 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 text words and images in fake news. Wordsand 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] , It states 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 Face book news post. They were aggregate from three large Face book 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 the divergence of the data set in which only 4.9% were fake news.

In [13] by **Kuruvilla et al.,** a neural network by 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 are entered..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 CNN may be retrained to perform additional recognition tasks, allowing for the expansion of 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 machine learning classification issue [14, 18], where the training phase is the label or category of the input sample. The actual image class and the false image class are the two labels or classes. Additional necessary hidden information is attached toa picture at the time of capture for authentication and forgery protection reasons.

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

A. Neural network input features: The objective is to gather relevant data attributes. Through the creation of new features from the current ones, features seek to minimise the amount of features in a dataset (and then discarding the original features).

B. Developing Fake Image Detection Algorithm 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.
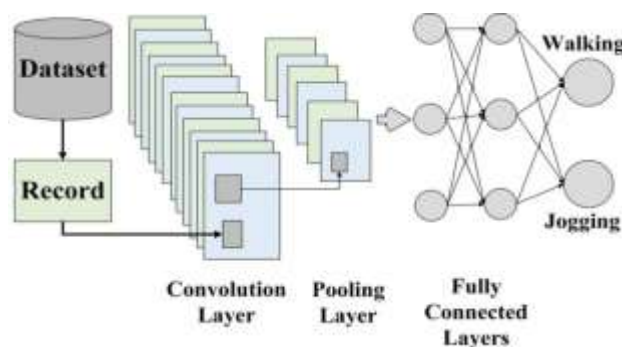

Fig. 1. Convolution Neural Network Architecture.

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

IV.CONCLUSION

Lately, There have been electronic attacks in Saudi Arabia also a large population country India faced threats and attacks. At this time we neither have a clear vision nor any unified frameworkto protect us from theft, 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 tothe rapid detection and rectification of forgery and fraud in the field of images in social media.

Similarly, to solve the problem of promoting fake news on social media networking sites, to protect their technical

infrastructure from theft and cyber threats and to strengthen their information security. Neural networks have some problems and limitations which are computationally very expensive, similarly necessitates the use of powerful and specialized processing units.

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 and deeper model for detectable problem. Integration of deep neural networks with the theory of enhanced learning.

Reference

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. 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. 3.Strigl, K. Kofler, & S. Podlipnig, (2010). Performance of GPU-based CNN model.
4. Li, W., Prasad, S., Fowler, J. E., & Bruce, L. M. (2012).Hyperspectral image analysisusing dimensionality reduction and classification with locality preservation.
a. Krizhevsky, I. Sutskever, & G. E. Hinton, (2012). Using deep convolutionalneural networks to classify images.
5. K. Ravi, (2018). Detecting fake images with Machine Learning. Harkuch Journal.
6.] J. Bunk, J. Bappy, H. Mohammed, T. M. Nataraj, L., Flenner, A., Manjunath, B., et al. (2017)Combining deep learning with resampling characteristics to recognise and locate fake images. Electrical and Computer Engineering Department from University of California at USA.
7. R. Raturi, (2018).Implementing Machine Learning to Spot Fake Accounts on Social Networks.50(4), 1185–1198 of the IEEE Transactions on Geoscience and Remote Sensing.
8. M. Villan, A. Kuruvilla, K. J. Paul, & E. P. Elias, (2017). Fake Image Detection Using Machine Learning.
9. D.-H. Kim, & H.-Y. Lee, (2017). Image Manipulation Detection using Convolutional Neural Network.