A Survey on Machine Learning Based Approaches for Detection of Image Forgery

Madhu Malviya[1], Prof. Sanmati Jain[2]

Image Forgery has been a very prevalent incidence in the recent times. With the rise in usage of the digital platforms and proliferation of digitization and social media in social and corporate sphere, images and multimedia have become indispensable. The image data generation has been enormous and its applications have also been quite vast. Consequently, it has led to misuse as well. Image Forgery has become a very grave concern in the world. Forged images can lead to major and innumerable problems and incur critical damages. So, Image Forgery detection is a very important mechanism to combat such incidents. The Image Forgery detection system has to very robust and yield accuracy and precision as it has to deal with large and complex data sets of images [1]. Therefore, the use of Artificial Neural Networks is a very sophisticated method for the same. This paper discusses the ANN approach for the Image Forgery Detection.

Keywords—Image Forgery, Artificial Neural Network (ANN), Accuracy, Precision.

I. INTRODUCTION

Images generally are comprised of two dimensions namely x and y[2].The use of images has increased rapidly in the recent times. Due to the high use of images and multimedia in the technological space, the image security has become a paramount aspect of concern. Encryption of images is also very important because of the different security related threats that are rampant. Image Forgery is one of such illegal activity that has made Image Forgery Detection a necessary measure to guard against such incidents. The Image Forgery generally refers to tampering of the image and visual data and modifying it. Such incidents have become very prevalent in these days. Encryption is a way of safeguarding the image data. Manipulation of the image data and altering it for unlawful purposes is Forgery of images and is a part of Image Forensics. The authenticity and integrity aspects of an image are of crucial importance[3]-[5]. The authentic verification of digital images is mandatory in various purposes. Henceforth, the branch of image forensics deals with the detection of the tampering of digital images. Here an accurate image forgery detection system proves to be very useful. Image Forgery can be of many kinds. It can be a simple tampering of some of the image properties. It can also be forging the image in a very sophisticated way. Forgery that entails the altering of the digital image properties and features to render it modified. Forgery is of a very major concern Enlisted below are the types of Image Forgery that take pale commonly today.

II. IMAGE FORGERY COMMON TYPES

For detection of the type of image modification and tampering, awareness about the types of Image Forgery is required. So below are the common types of approaches:-

Image Forgery Active Approach: - In this kind of approach, some traces of the activity are visible. Preprocessing methods such as watermarking etc are done at the time of the creation of the image.

Image Forgery Passive Approach: - In this Passive approach and method, the traces of tampering are not obvious about the picture. Some very prevalent types of passive methods are as follows:-

Copy-Move Forgery method: In this copy move method, a part of the original image itself is taken and then copied and .pasted in the same image itself. In this method, the process is done to hide any information or may change any revealing information.

Splicing: In the Image Splicing method, portions of different images are taken and then replaced the fragment of the original picture. This is one of the most common forms of forgery.

Image Retouching: This method involves using any advanced Image editing tool to edit and modify the images in any manner and as required. This method makes the look and feel of the image as authentic as possible. This is like a polishing of the forger image by bringing fine modification in the color, illumination etc.

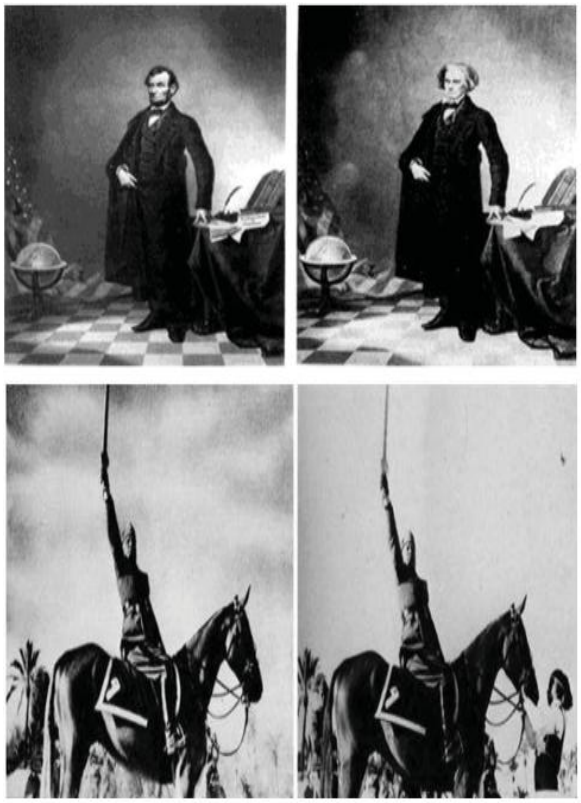

Fig.1 Illustration of typical image forgery

The Image Forgery is a kind of tricky and complex. The detection mechanism needs to be strong enough to comprehend the different types of the Image Forgery. Hence this requires the help of Artificial Intelligence approach. The machine learning mechanisms are high end and robust techniques that can deal with large sets of data to classify them and also are more accurate and precise than the manual methods. This is beneficial in the domain of Image Forensics.

III. INTRODUCTION TO ARTIFICIAL NEURAL NETWORKS

Artificial Intelligence and Machine learning have become an increasingly sought after domain in this recent time. Its popularity and dependence can be attributed to the fact that it is very advanced and strong approach. Below are some of the associated concepts of artificial intelligence. Artificial Neural Networks are the mechanism of artificial intelligence that implements it:

Computational Intelligence: This refers to the intelligent machines and using machines for high computational work that usually requires huge amounts of human efforts. Here the machine can perform such high end tasks better and more accurately.

Artificial Intelligence: It can be defined as the design of computational systems which can perform tasks generally needing human intervention.

Machine Learning: This is a branch of computer science that involves making the machine learn akin to humans for problem solving and performing variety of advanced and complex tasks.

Neural Networks: Neural Networks can be described as the neuron connection counterpart of the human brain. It has the ability to replicate the functions of human intelligence. The main features of machine learning are given below:-

- The ANN is type of self learning network that can be trained to perform tasks accurately.
- There consists of millions of neurons that are connected to each other. This aids the brain to perform complex tasks and process lots of information. But with ANN, the ANN has the feature of saving the previous input data.
- And this way ANN trains itself based on the data and information that input to it previously.
- This way ANN learns and adapts according to the previously fed data. This is achieved through training and testing of the neural network. This is a crucial aspect as the accuracy of the classification depends on this process.

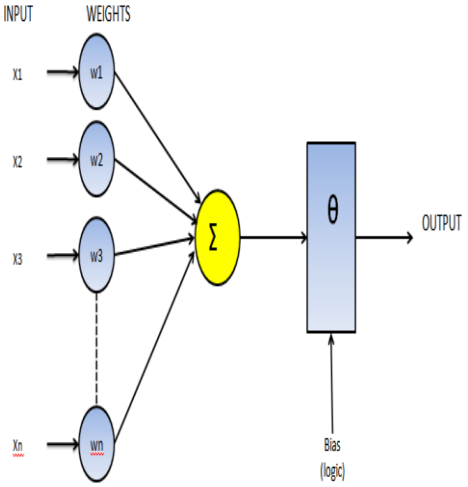

Fig.2 Mathematical Model of ANN

Artificial neural networks are effective in the following problems:

1) Forecasting problesms
2) Classification Problems
3) Optimization Problems

In this present case, the ANN is used as a classifier for a classification problem in which the ANN has to decide whether the image is forged or not. The mathematical formylation for the output of the neural network is given by:

$$Y = f(\sum_{i=1}^{n} X_i W_i + \theta) \quad (1)$$

Here,
X is the parallel input stream fed to the neural network
W is the weights updated as per the changing inputs
Y is the final output or decision of the neural network
Θ is the bias

III. PREVIOUS WORK

The previous work section presents the contemporary work in the domain.

This section presents the previous work done in the domain. It highlights the salient features of the approach as well as mentions the limitation found in the approach.

Wu et al. in [1] proposed a a novel robust training scheme is proposed. Firstly, we design a baseline detector, which won the top ranking in a recent certificate forgery detection competition. Then we conduct a thorough analysis of the noise introduced by OSNs, and decouple it into two parts, i.e., predictable noise and unseen noise , which are modelled separately. The former simulates the noise introduced by the disclosed (known) operations of OSNs, while the latter is designed to not only complete the previous one, but also take into account the defects of the detector itself. We further incorporate the modelled noise into a robust training framework, significantly improving the robustness of the image forgery detector. Extensive experimental results are presented to validate the superiority of the proposed scheme compared with several state-of-the-art competitors, especially in the scenarios of detecting OSN-transmitted forgeries

Dhivya et al. in [2] proposed a peeded Up Robust Feature (SURF) feature extraction, and the specific object is recognized with the help of the support vector machine. When copy-move forgery was performed, some modifications were done to the image. For instance, turning, scaling, darkening, compression, and noise addition are applied to make effective impersonation forgeries. Here, feature matching process uses the image rotate function, which consists of bicubic and crop operations, and calculates the difference using the blend, scale and joint operation. The results show that forged images are extracted from a given set of test images. The test results exhibit that the proposed technique can get noteworthy and impressive results.

Jason Bunk et al. in [3] proposed a technique that used Resampling Features and Random Walker segmentation to train a deep neural network. The approach tries to segment out the parts of the image which seem to be morphed based on the Random Walker segmentation approach. This part is followed by the computation of resampling features. The segmentation and resampling feature computation from the segmented parts are fed to the deep neural network to classify the image. The major limitation of the approach is the necessity of segmentation of the image parts with apparent or visible modifications. While this can lead to satisfactory results for active forgery approaches, the passive approaches may clearly bypass such a segmentation based approach or render false positive or false negative values. Additionally, segmentation may result in fringing of the edges of segmenting parts which can result in plummeting values of accuracy of classification.

Clemens Seibold et al. in [4] proposed a technique for detecting facial morphing using the deep learning approach of convolutional neural networks (CNN). This approach uses the concept of one shot learning for the convolutional neural networks. The major limitations of the proposed work are the absence of distinctive pre-processing techniques which can remove the chances of noise and disturbance effects. Moreover, once shot learning doesn't rely on the separate computation of features and simply relies on the CNN based features. This happens since this neural network approach doesn't use the orientation of the image based features and the neurons do not have the capability to handle this type of feature analysis. This approach also tries to carry out a search for a specific or particular type of feature extraction and based on it, the classification is done. This means that if the features compatible with the CNN are not present, the image classification suffers heavily which is clearly undesirable.

Yuan Rao et al. in [5] proposed a technique utilizing the convolutional neural network for the detection of splicing image forgery and copy-move image forgery. The approach again uses no separate image pre-processing

technique and uses the one-shot CNN learning approach. The limitations of this approach again stems from the fact that low level details regarding to the image are sent for analysis to high level neurons which again pass it forward to the next level of neural layers with the process of thresholding the features in the previous layer before passing it on the subsequent layer. This thresholding process often reduces the accuracy of the features retained for the classification process. Moreover, the lack of encapsulated neurons that can analyse the low level orientation features reduces the classification accuracy of the system. The certain neural layers that are not receptive of the low level features or even non-receptive to the thresholded feature values affect the classification accuracy adversely.

comparative analysis renders insight into the basic methodologies used. The salient features have also been discussed. The performance metrics are now presented.

IV. PERFORMANCE METRICS

The performance of the approaches are accuracy and sensitivity since it's a classification problem that is being dealt with. The performance metrics are discussed below:

$$Se = \frac{TP}{TP+FN} \quad (2)$$

$$Ac = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

Here,

Se indicates sensitivity

Ac indicates accuracy

TP indicates true positive

TN indicates true negative

FP indicates false positive

FN indicates false negative

CONCLUSION

It can be concluded from previous discussions that image forgery detection is a challenging task due to the fact that the number of images circulating in social media applications is very large and they are complex to analyze with the eye due to the scene complexity and the perfection with which images can be forged with image editing tools. Hence it becomes almost mandatory to use artificial intelligence to detect image forgery. The previous discussions illustrate the basics of image forgery and artificial intelligence based techniques. The salient features of the previously existing techniques have been discussed which can impart insight into techniques which can further improve the classification accuracy.

REFERENCES

[1] H. Wu, J. Zhou, J. Tian, J. Liu and Y. Qiao, "Robust Image Forgery Detection Against Transmission Over Online Social Networks," in IEEE Transactions on Information Forensics and Security, 2022, vol. 17, pp. 443-456

[2] S Dhivya, J Sangeetha, B Sudhakar, Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique", Journal of Soft Computing, 2021 vol.24, pp.14429–14440

[3] Jason Bunk et al., "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning", IEEE 2020

[4] Clemens Seibold et al., "Detection of Face Morphing Attacks by Deep Learning", Springer 2019

[5] Yuan Rao ; Jiangqun Niet, "A deep learning approach to detection of splicing and copy-move forgeries in images", IEEE 2018

[6] Belhassen Bayar, Matthew C. Stamm et al.,"A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer", IEEE 2016.

[7] Jiansheng Chen ; Xiangui Kang ; Ye Liu ; Z. Jane Wang, "Median Filtering Forensics Based on Convolutional Neural Networks", IEEE 2015.

[8] Chi-Man Pun , Xiao-Chen Yuan , Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching",IEEE 2015.

[9]Jian Li et al., "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE 2014

[10]Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching", IEEE 2014

[11] GK Birajdar, VH Mankar, "Digital image forgery detection using passive techniques: A survey", Elsevier 2013

[12] G Lynch, FY Shih, HYM Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Elsevier 2013

[13] M Hussain, G Muhammad, SQ Saleh, AM Mirza, "Image forgery detection using multi-resolution Weber local descriptors", IEEE 2013

[14] MF Hashmi, AR Hambarde, "Copy move forgery detection using DWT and SIFT features", IEEE 2013

[15] G Muhammad, M Hussain, G Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Elsevier 2012

[16] W Fan, K Wang, F Cayre, Z Xiong, "3D lighting-based image forgery detection using shape-from-shading", IEEE 2012

[17] M Hussain, G Muhammad, SQ Saleh, "Copy-move image forgery detection using multi-resolution weber descriptors", IEEE 2012

[18] H Yao, S Wang, Y Zhao, X Zhang, "Detecting image forgery using perspective constraints", IEEE 2011

[19] G Muhammad, M Hussain, K Khawaji, "Blind copy move image forgery detection using dyadic undecimated wavelet transform", IEEE 2011

[20] H Yao, S Wang, Y Zhao, X Zhang, "Detecting image forgery using perspective constraints", IEEE 2011