Automated Detection of Image Forgery Based on Machine Learning: A Review

Muskan Mohd. Shabir[1], Dr. Manish Vyas[2]
VITM, Indore, India

***Abstract*—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.

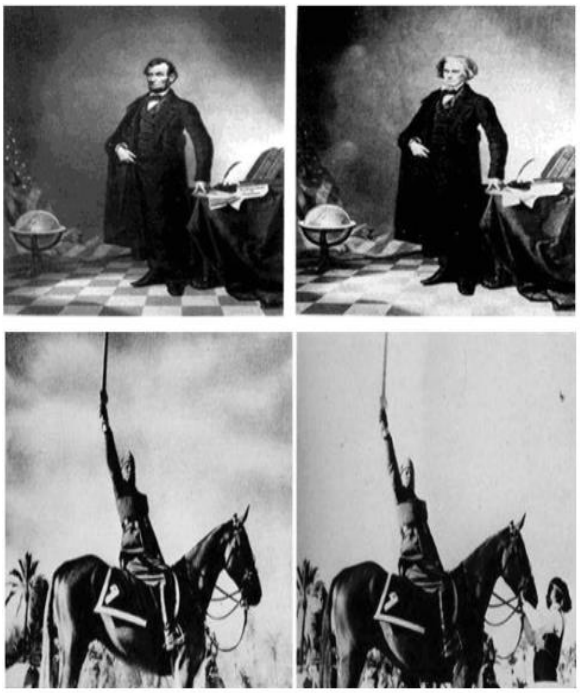

Fig.1 Illustration of typical image forgery

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.

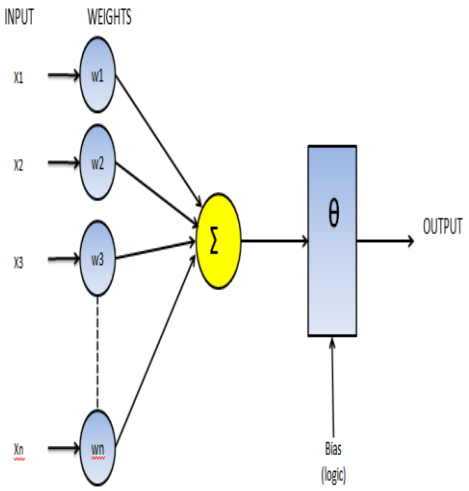

Fig.2 Mathematical Model of ANN

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:

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

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.

In [1], Araz Rajab Abrahim et al. in [1] proposed an approach for splicing image forgery detection. The image features used were colored and edge based features. The approach used a neural network for classification. It performance metric was the accuracy of classification.

In [2], Thales Pomari et al. in [2] proposed Image Splicing Detection employing Illumination Inconsistencies and Deep Learning. In this approach the neural network used was a deep neural network (DNN) and the learning approach used was a deep learning approach.

In [3], Jason Bunk et al. in [3] proposed an approach comprising of Resampling Features and Deep Learning for image forgery detection. The parts which were forged were localized using the Random Walker segmentation technique.

In [4], Clemens Seibold et al. proposed a convolutional neural network based deep learning approach for facial morphing tampering images. The parameter computed for the used dataset was the accuracy.

In [5], Yuan Rao et al. proposed the mechanism of deep neural networks and deep learning for the detection of splicing image forgery and copy-move image forgery. The approach uses a CNN for classification of image forgery from RGB images directly without going into the feature extraction. .

In [6], Belhassen Baya et al. proposed a Deep Learning based technique for the detection of Universal Image Manipulation. The proposed approach also used the convolutional neural network for classification.

In [7] Jiansheng Chen et al. proposed an amalgamation of Median Filter and CNN fir image forgery detection. The output of the medial filter is median filtering residual (MFR) is fed to the CNN for classification.

In [8], Chi-Man Pun et al. proposed the Adaptive Over segmentation and Feature Point Matching system for image forgery detection. The classifier was the fuzzy rule base classifier.

In [9], Jian Li et al. in [9] proposed segmentation prior to classification using neural networks. It was shown to attain higher accuracy compared to classification without segmentation.

In [10], Davide Cozzolino et al. proposed Image forgery detection through residual-based local descriptors and block-matching for image forgery detection. For the image forgery dataset. A comparative tabulation is presented next.

S.No	Paper Title	Authors	Approach used
1	"Robust Image Forgery Detection Against Transmission Over Online Social Networks"	H. Wu, J. Zhou, J. Tian, J. Liu and Y. Qiao	Stacked CNN Based Approach for automated detection of Image Forgery.
2	"Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation"	Abhishek, N Jindal,	Semantic Segmentation based Deep Neural Network based approach for copy and move image forgery detection.
3	"Splicing image forgery identification based on artificial neural network approach and texture features".	Araz Rajab Abrahim, Mohd Shafry Mohd Rahim, Ghazali Bin Sulong	Neural Network based approach for detection of splicing image forgery.
4	"Image Splicing Detection Through Illumination Inconsistencies and Deep Learning".	T Pomari, G Ruppert, E Rezende	Deep Neural Network and Deep Learing used for splicing image forgery detection.
5	"Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning".	J Bunk, JH Bappy, TM Mohammed	Resampling features used to differentiate forged images from unforged images using deep learning
6	"Detection of Face Morphing Attacks by Deep Learning".	C Seibold, W Samek, A Hilsmann, P Eisert.	Convolutional neural network (CNN) used for face image forgery detection
7	"A deep learning approach to detection of splicing and copy-move forgeries in images".	Yuan Rao, Jiangqun Ni.	Copy and move image forgery detection based on deep learning from RGB images.
8	"A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer".	Belhassen Bayar, Matthew C. Stamm,	Deep Learning based technique for the detection of Universal Image Manipulation.
9	"Median Filtering Forensics Based on Convolutional Neural Networks".	Jiansheng Chen ; Xiangui Kang ; Ye Liu ; Z. Jane Wang	Medial filter is median filtering residual (MFR) used a input layer of CNN for final classification
10	Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching"	Chi-Man Pun , Xiao-Chen Yuan , Xiu-Li Bi	Fuzzy based classification based on Segmentation and point to point matching.

Table.1 Comparative Analysis of different approaches used for image forgery detection

The 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] Abhishek, N Jindal, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation", Multimedia Tools and Applications, Springer 2021, vol.80., pp. pages3571–3599.

[3] Araz Rajab Abrahim, Mohd Shafry Mohd Rahim, Ghazali Bin Sulong "Splicing image forgery identification based on artificial neural network approach and texture features", Springer 2018

[4] T Pomari, G Ruppert, E Rezende "Image Splicing Detection Through Illumination Inconsistencies and Deep Learning", IEEE 2018

[5] J Bunk, JH Bappy, TM Mohammed, "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning", IEEE 2017

[6] C Seibold, W Samek, A Hilsmann, P Eisert., "Detection of Face Morphing Attacks by Deep Learning", Springer 2017

[7] Yuan Rao ; Jiangqun Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images", IEEE 2016

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

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

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

[11] Davide Cozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE 2014

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

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

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

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

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

[17] Neural Network and Learning Machines, 3rd edition, Pearson Publications.