EasyChair Preprint

№ 10580

A Review on Image Forgery Detection Techniques Using Machine Learning

Yogesh Kumar, Ravi Kumar, Roshan Kumar, Rahul Kumawat, Nikhil Soren, Sachin Kumar Jangir and Tarun Singh

July 17, 2023

A Review on Image Forgery Detection Techniques Using Machine Learning

Yogesh Kumar[1, a)], Ravi Kumar[2, b)], Roshan Kumar[3, c)], Rahul Kumawat[4, d)], Nikhil Soren[5, e)], Sachin Kumar Jangir[6, f)], Tarun Singh[7, g)]

Department of Computer Science and Engineering, Lovely Professional University, Jalandhar – Delhi Grand Trunk Rd, Phagwara, Punjab, 144001

Email : [a)]everyogesh@gmail.com [b)]ravik.cs.19@gmail.com
[c)]roshan.kr.8207@gmail.com [d)]rahulkumawat835@gmail.com
[e)]sorennikhilshiv@gmail.com [f)]sachin23062001@gmail.com [g)]tarunsingh0502@gmail.com

Abstract Image forgery has evolved into common problem in the digital age, due to the extensive uses of digital image manipulation tools. In a variety of industries, including forensics, journalism, and arts, image fraud can have detrimental effects. Thus, it is crucial to provide trustworthy techniques for identifying image forgery. Using machine learning techniques to automatically spot indications of image modification is one promising strategy. We give a summary of current developments in machine learning-based image forgery detection in this review paper. We talk about many methods of forging images, including copy-move, splicing, and retouching. We also give an overview of common machine learning techniques used in picture forgery detection, including SVM, CNN and Random Forests. The performance of various features extraction techniques to capture the distinctive aspects of various types of image forgeries is then discussed, including the Scale-Invariant Feature Transform and convolutional neural network-based features. Several datasets that have been utilized to train and evaluate machine learning models for image forgery detection are also reviewed. Finally, we evaluate the shortcomings of current approaches and specify potential future research avenues. We stress the importance of creating reliable methods that can identify cutting-edge types of image forgery, such as deepfakes, as well as the necessity of creating real-time, practical solutions.
This review paper intends to be a helpful resource for scholars and practitioners working in this field by giving a thorough overview of recent developments in picture forgery detection using machine learning.

Keywords: Image Forgery Detection, ML, SVM, CNN, Copy- Move and Splicing Forgery

INTRODUCTION

Image forging is the practice of altering a digital image in such a way as to change its original content, frequently with the intention of misleading or deceiving viewers. The content of one image can be copied and pasted into another, objects or people can be added or removed, the colour or brightness can be changed, or even fully made-up images can be produced from scratch. The rise of advanced and powerful digital imaging equipment and procedures has raised both the incidence and difficulty of detecting picture forgeries, necessitating the development of automated algorithms for identifying and stopping image alteration [1].

Detecting digital image manipulation or alteration from its original form is known as "image forgery detection". In order to evaluate the image and find any indications of modification or tampering, such as irregularities in pixel values or adjustments to the lighting and colour, a variety of approaches and algorithms are used. Image forgery detection aims to offer a trustworthy and automated technique of identifying and blocking the usage of altered photographs in a variety of contexts, including forensic investigations, digital media, and social media platforms. As a result of its ability to distinguish patterns and attributes that differentiate real photographs from modified ones, machine learning algorithms are being used more frequently in the detection of image fraud.

It is used in forensics to spot manipulation with digital data, such as images, videos, and audio files. In order to maintain credibility and avoid spreading false information, it is helpful in journalism to confirm the authenticity of photos used in news pieces. When dealing with a high amount of photos, automated solutions can be more efficient in terms of time and resources than manual inspection.
There are various kinds of image forgeries, such as:
Copy-Move Forgery: A piece of a picture is copied and pasted into another image or within the original image in a process known as copy-move forgery. This is done to deceive viewers or modify the visual material. The copied region is frequently altered or altered in some other manner to blend in with the surroundings in order to lessen the visibility of the fraud [2].
Splicing: Splicing is the process of merging two or more distinct images into one another, frequently with the goal of

misleading the spectator. To accomplish this, copy and paste a few image components from one image onto another one. An object, a person, an environment, or any other element of an image can be copied [9].
Splicing can be used for a number of things, like fabricating information or propaganda, changing the context of an image, or concealing details or items that were once visible in the scene.
Watermark Removal: A watermark is a distinctive identifier added to a photograph to stop it from being used without permission. In order to utilize an image without permission, a watermark must be removed from it.
Object Removal: In order to alter the context or meaning of an image, an object may be removed from it. This could be used to get eliminate incriminating information from an image.

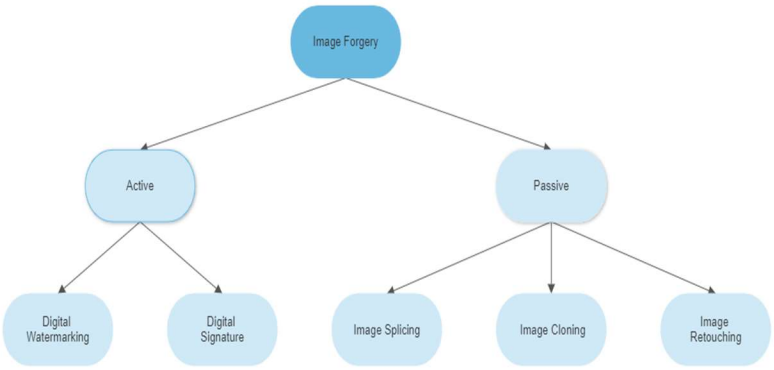

FIGURE 1. *Types of Image Forgery Detection*

There are numerous methods currently available to identify fake images illustrated in Figure 1:
Passive Techniques: Methods that utilize the intrinsic qualities of the image to identify forgeries include passive techniques that look for abnormalities in statistical variables, differences in colour and texture, and signs of double JPEG compression.
Active Techniques: To identify any changes made to the image, these approaches implant a digital watermark or signature in it.
Model-Based Techniques: These methods examine the image and look for any irregularities in its composition or structure using mathematical models [4].
Machine Learning Approaches: To identify any anomalies in an image, these techniques include training a machine learning model on a collection of real and altered images [5].
A machine learning system is trained using a sizable dataset of known fake and real photos. The algorithm gains the ability to spot patterns in the image features that distinguish the two types of photos apart.
After training, the system can be used to identify new photos as genuine or fake. To achieve this, the algorithm is fed the image, which examines the attributes and calculates a likelihood score for each class.

CONTRIBUTION

This paper contributes to the field of image forgery detection using machine learning by providing a comprehensive survey of existing approaches and identifying areas for future research. The paper highlights the strengths and weaknesses of different techniques, including traditional forensic methods and machine learning-based approaches.

1. Analysis of existing machine learning algorithms and scope of future enhancements.
2. identifies the need for benchmark datasets and evaluation metrics to facilitate fair comparisons between different approaches and guide the development of new techniques.
3. By providing an overview of existing datasets and evaluation metrics, the paper helps to establish a common ground for future research in the field.

LITERATURE REVIEW

Khudhair et al. [1] discuss how well CNN performs in different situations while detecting image forgeries. The CNN

model's performance can drop quite dramatically. Two datasets are chosen to train the CNN in order to test this presumption, with CASIA v2.0 being favored onto v1.0 due to its increased difficulty. To determine whether an image has been altered, CASIA v2.0 and NC2016 are used, followed by the training of three distinct models: ELA, VGG16 and VGG19. The results show that VGG19 outperforms the other models in detecting forged images, while VGG16 performs better for authentic images.

Mallick et al. [2] discuss how people attempt to duplicate portions of photographs and how to spot when they do so. To determine the methodologies being employed, the researchers examined numerous articles that were published between 2017 and 2020. One technique they discovered was to examine various areas of the image to determine whether they appear overly similar. In order to determine if the image was real or false, they also employed a machine learning technology called Random Forest. The researchers expect that their findings will aid in the development of better tools to capture picture cheaters. They discovered a variety of approaches to identify fraudulent photos

Wei et al. [3] how to design a system for identifying image splicing forgery, which entails taking a piece of one image and fusing it with another to make a new one. A coarse CNN and a refine CNN are two different forms of convolutional neural networks that are used in the suggested technique, which is based on deep learning. An image-level CNN is introduced to replace the initial patch level in order to simplify computation and speed up the process. The findings reveal that the proposed method works better than the existing detection methods, as shown by the results obtained from the testing dataset, which is based on real-world scenarios.

Doegar et al. [4] discuss CNN and pre-trained AlexNet architecture are used in this research to offer a unique method for spotting fake images using the MICCF220 benchmark dataset. Doegar et al. [4] suggests utilizing pre-trained AlexNet on the MICC-F220 dataset to identify image fraud using a CNN-based method. In order to differentiate between fake and legitimate photos, the method collects deep characteristics and trains an SVM classifier. The study's findings indicate that the given CNN-based method using pre-trained AlexNet on the MICC-F220 dataset achieves high accuracy of 93.94%, with Recall/TPR rate of 100%, Precision of 89.19%, and F-measure of 94.28%. The approach's average execution time is 4.86 seconds

Latha et al. [5] attempts to identify that uploaded and altered images are fake. The suggested technique finds fake images using KPCA and DWT vector block-by-block, and determine geometric changes by a detection Algorithm, new rotation detection algorithm. This strategy uses two methods: SCI identifies the source camera, and AFCED employs SVM to detect images that have been altered. It has the ability to categories both original and morphed pictures and disable accounts from uploading them. This study examines forensic splicing and determines the probability of finding fake pictures.

Ranjan et al. [6] detect the image Forgery using artificial Neural Network, GLEM, Support vector Machine algorithm. This process contained image six steps which included creation of datasets, pre-processing of image, segmentation, extraction of GLCM features, classification. and creation of GUI. In segmentation, K-means clustering segments image into k parts. Linear SYM was used initially dataset classification but ANN achieved higher accuracy (96.4%) on 220 images containing both original and morphed documents. GLCM feature extraction and SVM One to one classification achieved 96.4% accuracy compared to linear SVM.

Kuznetsov et al. [7] discuss that due to recent development and high growth of image forgery. In this paper, VGG-16 convolutional neural network used for both fine-tuned and zero staged trained using CASIA Dataset. In this paper to detect splicing, CNN is used to classify into original or distorted. Proposed approach tested as two- class classifier for original and forged images. Dataset split 80:20 for training and testing patches of 40× 40 pixel extracted and clarified by majority voting. It gave 97.8% accuracy for VGG-16 CNN algorithm for digital image distortion detection. Future work includes comparing with other works like Mobinet and Resnet-50 Models.

Goel et al. [8] discuss that for the purpose of identifying copy move forgery attempts in digital images, the current research suggests a novel dual branch CNN architecture. In two branches of the suggested design, feature extraction kernels of various sizes are implemented. The dominant characteristic for categorizing photographs as fake or real is then created by combining these attributes. Analyzing the suggested architecture against state-of-the-art research reveals that it can achieve high prediction accuracy and is lightweight. The architecture can be used to assess the robustness of the model, the architecture can be tried and reviewed in the future on more datasets with different image sizes.

Rao et al. [9] introduce a novel deep CNN-based method for detecting image forgery. The 30 basic high-pass filters used in the spatial rich model (SRM) for image analysis are used as initialization weights in the proposed CNN model, which uses specific specialized visual designs to detect tampering. By combining the extracted features, discriminative features for SVM classification are produced after dense features from the test images have been taken using the pre-trained CNN. Numerous tests on numerous open datasets show that our CNN-based strategy outperforms other cutting-edge image forging techniques.

Wang et al. [10] examine how the Mask R-CNN network behaves during the initial training stages. Wang et al. [10] notice from looking at the prediction mask of the mask branches that they frequently have hazy limits and occasionally do not follow the precise and complete contours of the original tamper-area mask. Wang et al. [10] to improve the precision of tamper localization, a parameter-free network head was added that employs the Sobel edge detection filter(SEDF) on the mask to figure out the L^2 loss between the predicted and ground-truth mask contours. Wang et al. [10] show that the suggested strategy outperforms other cutting-edge image tampering detection techniques. Future research will examine more aspects.

COMPARITIVE ANALYSIS

Year	Objective	Methodology/Algorithm	Performance and evaluation metrices	Limitation
2021 [1]	Copy-Move Image Forgery Detection Techniques and in-depth analysis of copy-move image tampering detection techniques from 2017 to 2020.	Mathematical morphological filter detector (2020), Attention DM for CISDL (2020), CNN (2020)	Accuracy of 94.89%,enhanced the computational speed and performance and It is extremely precise and resilient to image reduction (JPEG).	Complex mathematical function and time complexity.
2022 [2]	Detection of copy-move Image Forgery through CNN with ELA, VGG16, and VGG19 Models	The VGG16 is a Convolutional Neural Network (CNN) that comprises 22 neural layers and the VGG19 is the neural network that contains 24 layers.	Achieved training accuracy of 94.4% for VGG16 and the training accuracy of 95% for VGG19	The result between both the models shows that the overall accuracy of VGG19 is better than/similar of VGG16.
2018 [3]	Deep Learning-Based Approach for Splicing Image Detection	Convolutional Neural Network(CNN) and C2R NET	It is highly accurate than previous methods. F-Measure of the method was 68%.	The suggested technique has a more intricate structure.
2019 [4]	CNN based image forgery using deep learning features	CNN, Pre-trained AlexNet Model, SVM, Deep Learning	Accuracy using SVM classifier is 93.94% using CNN based pre-trained AlexNet Model.	Inefficient on working with large datasets
2022 [5]	techniques for detecting image forging using machine learning algorithms such as SVM and different methods such as active and passive.	SVM, Antiforensic contrait enhanced Detector (AFCED), source camera Identifier(SCI).	It is highly accurate for low quality image. SVM has high efficiency.	Complex Datasets and High computational time.

2018 [6]	Detecting forgery image using different Machine learning Algorithm copy - Move forger will be detected" using stationary Wavelet Transform(SWT)	Artificial Neural Network, Support vector Machine	SVM gave accuracy 87.67%. Compared to linear SVM,ANN has higher accuracy of 96.47%.	High complexity and Less Accuracy than CNN
2019 [7]	Detecting,one of t he most common image forgeriessplicing using Machine learing technique. and forgery dataset for zero stage tuned & fine tuned model	VGG-16 convolutional Neural Network, CASIA Dataset.	Accuracy of 96.4%. for Initial Stage for &=90 compressed accuracy is 67.1 and for comprened accuracy Q = 80, accuracy is 66.37%. for fine-tuned model accuracy is 97.8%	complex Mathematical functions, large Dataset, High computational Time
2020 [8]	Detecting forgery by Dual Branch CNN and MICCF-2000 Dataset	Dual Branch CNN and Deep Learning	It gave accuracy of 96% and sensitivity of 93% and precision of 89%.	complex Dataset, Less Precision
2016 [9]	detecting copy- move forgery of images using convolutional neural network (CNN).	The proposed method involves two major steps, feature learning and feature extraction, CNN	For CASIA v1.0 Accuracy came 98.04% and for DVMM accuracy came 96.38	Complex mathematical functions, High computational time
2019 [10]	Detection and localization of image forgeries using an improved CNN mask regional	Mask R-CNN and sobel filter, single mask R-CNN.	Accuracy of 95.7%,Sobel edge detection filter used to calculate the L^2.	Time complexity, Complex functions.

Table 1. *Comparative Analysis of Literature Review.*

PERFROMANCE ANALYSIS OF IMAGE FORGERY DETECTION

In this section ,the accuracy of Khudair et al. [1], Mallick et al. [2], Wei et al. [3], Doegar et al. [4], Ranjan et al. [6], Kuznetsov et al. [7], Goel et al. [8], Rao et al. [9], Wang et al. [10] will compared. We will examine their accuracy and compare them.

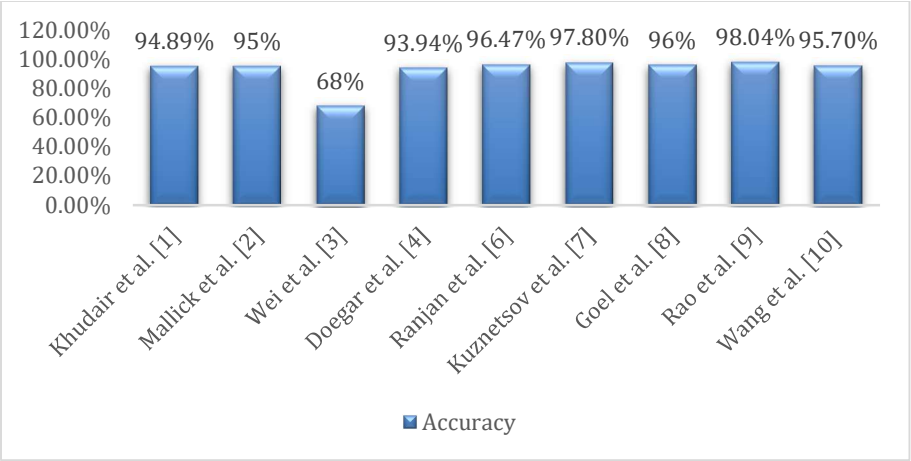

FIGURE 2. *Graph of Accuracy for Various Methods.*

Analysing the Figure 2, CNN has the highest accuracy but it has some limitations of time complexity, complex mathematical functions. For CASIA v1.0, accuracy is 98.04% which is higher than other machine learning algorithm like SVM, Naive bayes, Random Forest, etc.. For Kuznetsov et al. [7] accuracy is 97.80% which used VGG-16 CNN having slightly less accuracy than Rao et al. [9].

CONCLUSION

Machine learning techniques have shown great potential in detecting image forgery. The ability of these techniques to learn from large datasets and detect subtle patterns and anomalies in images make them effective in detecting even the most sophisticated forms of image manipulation. While various ML- based methods have been proposed, there is still room for improvement, particularly in terms of addressing the challenges of real-world scenarios such as detecting forgeries in compressed or low- quality images. As shown in Fig. 2 there are many Machine learning algorithm which are being used to detect the forgery like SVM, CNN, etc. but CNN is proved to be the most accurate amongst the other. With the continued advancement of ML techniques and the availability of larger datasets, it is expected that image forgery detection using machine learning will continue to evolve and become more accurate and effective in the future. Furthermore, more robust methods that can recognize complex forging methods are required.
Despite these difficulties, the use of machine learning to the detection of image forgery has already produced encouraging results, and it is anticipated that continued study in this field will result in more precise and effective detection methods. Therefore, future research and development efforts will focus on the creation of efficient machine learning approaches for identifying forgeries in images.

REFERENCES

1. Khudhair, Z.N., Mohamed, F. and Kadhim, K.A., 2021, April. A review on copy-move image forgery detection techniques. In Journal of Physics: Conference Series (Vol. 1892, No. 1, p. 012010). IOP Publishing.
2. Mallick, D., Shaikh, M., Gulhane, A. and Maktum, T., 2022. Copy Move and Splicing Image Forgery Detection using CNN. In ITM Web of Conferences (Vol. 44, p. 03052). EDP Sciences.
3. Wei, Y., Bi, X. and Xiao, B., 2018, August. C2r net: The coarse to refined network for image forgery detection. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1656-1659). IEEE.
4. Doegar, A., Dutta, M. and Gaurav, K., 2019. Cnn based image forgery detection using pre-trained alexnet model. International Journal of Computational Intelligence & IoT, 2(1).
5. Latha, K., Kavitha, D., Hemavathi, S. and Velmurugan, K.J., 2022, December. Image Forgery Detection Using Machine Learning. In 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS) (pp. 1-6). IEEE.
6. Ranjan, S., Garhwal, P., Bhan, A., Arora, M. and Mehra, A., 2018, May. Framework for image forgery detection and classification using machine learning. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1-9). IEEE.
7. Kuznetsov, A., 2019, November. Digital image forgery detection using deep learning approach. In Journal of Physics: Conference Series (Vol. 1368, No. 3, p. 032028). IOP Publishing.
8. Goel, N., Kaur, S. and Bala, R., 2021. Dual branch convolutional neural network for copy move forgery detection. IET Image Processing, 15(3), pp.656-665.
9. Rao, Y. and Ni, J., 2016, December. A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE international workshop on information forensics and security (WIFS) (pp. 1-6). IEEE.
10. Wang, X., Wang, H., Niu, S. and Zhang, J., 2019. Detection and localization of image forgeries using improved mask regional convolutional neural network. Mathematical Biosciences and Engineering, 16(5), pp.4581-4593.