A Literature Review on IMAGE FORGERY DETECTION

1st Adams Mathew
Computer Science and engineering
St. Joseph's College of Engineering
Palai, India
adamsmathew@gmail.com

2nd Adithya Sanil
Computer Science and engineering
St. Joseph's College of Engineering
Palai, India
adisanil11@gmail.com

3rd Akhil J Medackal
Computer Science and engineering
St. Joseph's College of Engineering
Palai, India
akhiljmedackal@gmail.com

4nd Nikhil J Medackal
Computer Science and engineering
St. Joseph's College of Engineering
Palai, India
nikhiljmedackal@gmail.com

Dyni Thomas
Computer Science and engineering
St. Joseph's College of Engineering
Palai, India
dyni@sjcetpalai.ac.in

***Abstract*—Taking pictures has grown in popularity recently as cameras are so widely accessible. Since they are so rich in information, images are crucial to daily life.Pictures frequently need to be enhanced in order to gain more information due to their wealth of data. Although there are many technologies available to enhance picture quality, they are also regularly used to alter photos, which leads to the dissemination of false information. This makes picture forgeries more severe and frequent, which is now a major cause of worry. To identify fake images, several conventional methods have been developed over time. CNNs have drawn a lot of interest recently, and CNN has also had an impact on the area of picture forgery detection.**

In recent years, CNNs have gained great attention, and CNN has also affected the field of picture fraud detection. The majority of CNN-based picture forgery detection methods, however, are only capable of spotting one kind of fraud (either image splicing or copy-move). Hence, a novel method that can quickly and precisely identify any hidden forgeries in a picture is needed. In the context of double image compression, the suggested system is a strong deep learning-based system that is introduced for detecting picture forgeries. The suggested model is trained using the variation between the original and recompressed versions of a picture.

***Index Terms*—IoT (Internet of Thing), Sensors, Image processing, Microcontroller, GSM module**

I. Introduction

Due to technological advancements and globalization, electronic equipment is now widely and inexpensively available. As a result, digital cameras have grown in popularity. There are many camera sensors all around us and they are used to collect a lot of images. Images are required in the form of a soft copy for various documents that must be filed online, and a large number of images are shared on social media every day. The amazing thing about images is that even illiterate people can look at them and extract information from them thus images are an integral component of the digital world, and they play an essential role in storing and distributing data. There are numerous tools accessible for quickly editing the images.

These tools were developed in order to enhance and enhance the photographs. Unfortunately, some individuals abuse their ability to distort photographs and spread myths rather than improving the image. This poses a serious risk since falsified photographs often result in severe and often irreparable harm. Image splicing and copy-move are the two fundamental kinds of image forgeries, and they are both covered below:

- Image splicing: involves copying a section of a donor image into a source image. The final forged picture may also be constructed from a series of donor photos.
- Copy-Move: There is just one picture in this scenario. A piece of the picture has been duplicated and placed inside of it. Other things are routinely hidden using this technique. There are no elements from other photographs in the final forged image.

II. Overview of Image Forgery Detection

The examination of existing studies and materials on a particular topic is crucial to any research endeavor. In this case, the term "review" pertains to the investigation of systems for detecting image forgery detection. These works provide valuable insights and information on the various methods used for observing, keeping track of, and identifying wildlife in various surroundings.

In a study by Deepika Jaswal et al. [2014][1],proposed a notion to use Convolutional neural networks (CNNs), a Deep Learning technique, in picture classification. The system is evaluated on a number of common datasets, including scene photographs from the SUN database and remote sensing data of aerial images (UC Merced Land Use Dataset). Based on classification accuracy and the quality parameter known as MSE, the algorithm's performance is assessed. Based on MSE versus the number of training epochs, a graphical depiction of the experimental data is provided. The classification accuracy provided by the algorithm (CNN) for all of the studied datasets is demonstrated by the experimental result analysis

based on the quality metrics and the graphical depiction.

J.Malathi et al.[2019][2] proposed a two phase imperative altering way to deal with oversee direct learn features in referencing to see changed pictures in various picture formats.The concept illuminant color inconsistency and machine learning classifiers are used for forgery detection. The method mainly consists of the following steps:estimation of illuminant color,extraction of face, Extraction of highlights,Histogram of Oriented Gradients.

Wei Yu et al.[2022][3] presented a method to understand the internal work mechanism of CNNs by probing the internal representations in two comprehensive aspects, i.e., visualizing patches in the representation spaces constructed by different layers, and visualizing visual information kept in each layer. The architectures of VGG-16 and AlexNet and comparison between VGG and AlexNet were also discussed in the paper.

Falko Matern et al.[2019][4] presented a physics-based forensic descriptor to characterize 2-D lighting environments of objects. The integral over a gradient field of an object, which specifies the direction of incident light in the picture plane, is the fundamental concept. The suggested method, as opposed to other 2-D lighting techniques, acts on the entire object area rather than just the object outlines, making it astonishingly resilient to changes in object colour and human input. Moreover, the suggested method is unaffected by picture downsizing or compression, making it feasible to evaluate photos that are not currently amenable to statistical analysis using state-of-the-art techniques.

Weiqi Luo et al.[2010][5] presented method for detecting double JPEG compression, which is a common technique used to manipulate images.They demonstrate that determining whether an image has been compressed twice may be done by looking at the error distribution in the discrete cosine transform coefficients. The results demonstrate that the suggested method outperforms existing methods for double compression identification. The method is empirically evaluated on a dataset of real-world photographs. The work proves the use of JPEG error analysis in digital picture forensics. In this study, JPEG error analysis is the method utilised to spot fake images. The first step is to convert coloured photos to grayscale ones.Then using the MATLAB JPEG Toolbox, perform JPEG compression and decompression. After that, apply IDCT to the resultant.Finally compute $\%$ resulting pixel values that are larger than 255 and smaller than 0.

Jun-Liu Zhong et al. [2020] [6] suggested using deep learning to identify copy-move image forgeries. In order to extract features from the input image, the authors suggest an end-to-end Dense-InceptionNet that combines the dense block and Inception module. This network is being proposed. meant to discover a representation of a discriminative feature for copy-move forgeries. The suggested method surpasses state-of-the-art algorithms for copy-move forgery detection in terms of accuracy, precision, recall, and F1 score, according to the evaluation of the approach on two common datasets. The study shows how well deep learning works for spotting copy-move forgeries in photos. The PFE, FCM, and HPP modules make up the three core components of the DenseInceptionNet framework model that this study proposes.The main advantage is that it can achieve the best efficiency while keeping high detection performance.

Younis Abdalla et al. [2019] [7] A deep learning method for identifying copymove picture forgeries is proposed in this paper. Several convolutional and pooling layers are used by the authors' proposed CNN architecture to extract features before fully linked layers are added for classification. Using a sizable dataset of fake and real images, the proposed network is trained to develop a feature representation that can distinguish between the two. The suggested method surpasses state-of-the-art algorithms for copy-move forgery detection in terms of accuracy, precision, recall, and F1 score, according to the evaluation of the approach on two common datasets. The study shows how well deep learning, in particular CNNs, can be used to find copy-move forgeries in photos. The CNN architecture uses a total of 15 layers.

In a study published by Gustavo Botelho de Souza et al. [2018] [8], a deep learning method for identifying fingerprint spoofing attempts is suggested . The authors suggest an approach to feature extraction based on CNN, which is trained on a sizable dataset of real and fake fingerprints. A SVM classifier is subsequently trained to distinguish between authentic and fake fingerprints using the retrieved features. In terms of accuracy, precision, recall, and F1 score, the suggested methodology surpasses state-of-the-art algorithms for fingerprint spoofing detection, according to evaluation results on two common fingerprint spoofing datasets. The work reveals how well CNNs, in particular, may be used to identify fingerprint spoofing assaults. This research employs a restricted Boltzmann machine methodology. Energy-based neural networks called Restricted Boltzmann Machines are utilised to build probabilistic deep learning architectures.

Yue Wu1 et al.[2022] [9] suggested a deep learning method for localising the source and target of copy-move picture forgeries. To identify the copied and pasted portions of the image, the authors suggest a brand-new network design dubbed BusterNet that combines a feature extraction network with a source/target localization network. The suggested network is intended to provide a feature representation of the input image's disparities between the source and target regions. The suggested method surpasses state-of-the-art algorithms for copy-move forgery detection in terms of accuracy, precision, recall, and F1 score, according to the evaluation of the approach on two common datasets. The paper shows that copy-move fraud with source/target

localisation in photos may be detected using deep learning, in particular the suggested BusterNet architecture.

Nguyen et al. [2019] [10] created a CNN that uses a multi-task learning approach to both locate the forged regions and detect manipulated pictures and videos. When knowledge from one activity is shared with the second, both tasks are improved. The network is made more generable by using a semi-supervised learning approach. The network includes an encoder and a Y-shaped decoder.

The results of the experiments demonstrate that the suggested strategy exceeds current splicing detection methods in terms of precision and computing effectiveness.

CONCLUSION

In recent years, photography has gained popularity due to the increasing accessibility of cameras. As the general population readily comprehends images, they have developed into a vital mode of information transmission. Pictures play a significant part in life. There are several tools available to edit photographs; while their primary purpose is to enhance them, these technologies are routinely abused to alter the images in order to distribute false information. Hence, picture forgery has grown to be a serious issue. The suggested method offers an original solution for spotting fake images that is based on deep learning and neural networks, with a focus on CNN architecture. The recommended approach makes use of a CNN architecture that includes several picture compression techniques to get good results.The model is trained using the difference between the original and recompressed pictures. The suggested method effectively detects copy-move and picture splicing forms of image forgeries.

REFERENCES

[1] D. Jaswal et al (2014) *Image Classification Using Convolutional Neural Networks International Journal of Scientific Engineering Research 2014. [Online]. Available.*

[2] J. Malathi et al (2017) Image Forgery Detection by using Machine Learning, International Journal of Innovative Technology and Exploring Engineering.

[3] W. Yu et al (2014) "Visualizing and Comparing AlexNet and VGG using Deconvolutional Layers ,International Research Journal of Engineering and Technology.

[4] Falko Matern et al (2019) Gradient-Based Illumination Description for Image Forgery Detection August ,IEEE Transactions on Information Forensics and Security.

[5] W. Luo et al (2010) JPEG Error Analysis and Its Applications to Digital Image Forensics ,IEEE Transactions on Information Forensics and Security.

[6] Jun-Liu et al (2019) An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection ,IEEE Transactions on Information Forensics and Security.

[7] Abdalla Y et al (2019) Neural Network for Copy-Move Forgery Detection. ,IEEE Transactions on Information Forensics and Security.

[8] Gustavo Botelho de Souza et al. [2018] Deep features extraction for robust fingerprint spoofing attack detection , International Journal of Engineering Research in Electronics and Communication Engineering.

[9] Yue Wu , Wael Abd-Almageed , and Prem Natarajan (2020) "BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization ,Proceedings of the European Confrence on computation.

[10] Nguyen, H.H.; Fang, F.; Yamagishi, J.; Echizen (2019) Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos.International Conference on Biometrics Theory, Applications and Systems