Image Copy Move Forgery Detection

Harikrishnan S
Computer Science and Engineering
Amal Jyothi College of Engineering
Kottayam, India
harikrishnans2023@cs.ajce.in

Joel M Shaji
Computer Science and Engineering
Amal Jyothi College of Engineering
Kottayam, India
joelmshaji2023@cs.ajce.in

Joyal John Chacko
Computer Science and Engineering
Amal Jyothi College of Engineering
Kottayam, India
joyaljohnchacko2023@cs.ajce.in

Sharon Kurian Thomas
Computer Science and Engineering
Amal Jyothi College of Engineering
Kottayam,India
sharonkurianthomas616@gmail.com

Krishnalal G
Computer Science and Engineering
Amal Jyothi College of Engineering
Kottayam,India
gkrishnalal@amaljyothi.ac.in

***Abstract*—The growing use of digital images in a variety of applications has raised research interest in the area of digital image processing. The detection of picture forgeries is one of the urgent problems that researchers are putting a high priority on. This study focuses on copy-move picture forgery, a dishonest method of image manipulation that involves copying an area of an image and pasting it elsewhere in the same image. We suggest a Convolutional Neural Network (CNN) architecture for the precise detection of copy-move picture forgeries in order to address this problem. The suggested design features an appropriate number of convolutional and max-pooling layers and is computationally effective. Using benchmark datasets, the effectiveness of the suggested architecture is assessed.**

I. INTRODUCTION

Digital images play a crucial role in various fields such as forensics, court evidence, medical diagnosis systems, social networks, and military applications. Due to their significance, it is imperative to guarantee their authenticity and keep their contents secure from tampering. However, with the availability of image manipulation tools, it has become challenging to identify fake images by just observing them. Thus, it is necessary to develop advanced techniques to detect image forgeries.

This paper will introduce the main methods for discovering image forgeries, which are divided into active and passive approaches. The active approach involves adding watermarks and digital signatures to images during their creation, while the passive approach involves altering correct information to incorrect information and obscuring important images. The paper will also classify digital image forgeries into five categories: copy-move forgery, image splicing, image retouching, morphing, and enhancement.

One of the most widespread types of digital image forgery is copy-move forgery, and numerous methods have been proposed for detecting it. These methods can be grouped into three categories: traditional approaches that utilize popular local feature extractors such as SIFT, SURF, and ORB, orthogonal moment-based approaches that use geometric invariant orthogonal moments to extract features, and deep learning-based approaches that utilize various deep learning techniques.

1) Traditional Copy-Move Forgery Detection Approach:
   a) : The algorithm for copy-move forgery (CMF) detection is based on the Discrete Wavelet Transform. This approach gives good results in the case of multiple CMFs. Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD) methods are combined to introduce an efficient approach for the automatic detection of duplicated regions in the same image. The proposed approach demonstrated high robustness against the geometrical transformations. The proposed approach gives high accuracy in the presence of different image deformations. A novel technique for CMF detection based on SIFT and the reduced LBP has been introduced by Park et al. This approach reveals when compared with other existing methods.
2) Moment-Based Copy-Move Forgery Detection Approach:
   b) : Recently, various techniques for CMFD based on image moments have been proposed. It suggested a fast and accurate algorithm for CMFD based on polar complex exponential transform moments PCETMs. The proposed approach exhibited high accuracy with different types of image deformations. The previous approach has been upgraded using the quaternion concept applicable to color images. The empirical results proved the accuracy of the proposed approach to detect the copy moved forged regions.
3) Deep Learning-Based Copy-Move Forgery Detection Approach:
   c) : One of the hot topics that have been used in various fields is deep learning. The CMFD represents one of these fields. Deep learning mainly depends on CNN. Through CNN, their many stages. At each stage, a set of features are generated. Some features are used as a training set. Methods based on deep learning reveal better performance than traditional and moment-based

approaches. Recently, many CMFD approaches based on deep learning have been presented. Elaskily presented an efficient approach for automatic CMFD based on CNN, and the suggested approach achieved 100% accuracy when applied to different datasets. Goel suggested a CMFD system based on a novel technique called dual branch CNN. The proposed system proves good results in terms of time and performance. Ortega proposed two approaches for CMFD based on deep learning: a custom architecture model and a transfer learning model. The proposed system has been tested over eight benchmark datasets. Abhishek introduced an efficient system to detect and localize the image forgeries based on deep CNN and semantic segmentation. The obtained results give accuracy above 98%. Jaiswal presented a CMFD model it used multi-scale input and two blocks of convolutional layers: encoder and decoder blocks. The empirical results proved the high accuracy of the proposed system. As a result of the previous discussion, it shows a shortage of previous works, and the shortage motivates the author to propose an efficient CNN-based method.

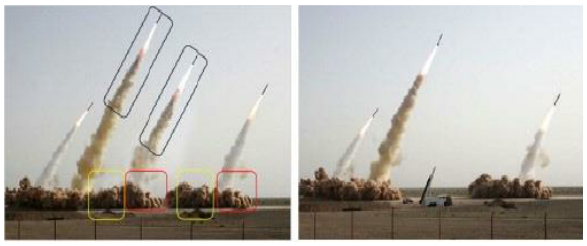

Fig. 1. Example of Image Forgery

II. OBJECTIVES

Image Copy-Move Forgery (ICMF) refers to the act of duplicating a part of an image and pasting it elsewhere within the same image, with the intention of concealing information or manipulating the image. This type of manipulation is becoming increasingly prevalent in the digital age, and it is crucial to develop techniques to detect such forgeries.

The objective of this project is to develop a robust and efficient algorithm for detecting Image Copy-Move Forgery. The algorithm should be able to accurately identify forged regions within an image, regardless of the transformation applied to the duplicated region (e.g., scaling, rotation, etc.). The algorithm should also be able to distinguish between intentional forgeries and accidental duplications. The ultimate goal is to develop a tool that can be used to authenticate digital images and to preserve the integrity of digital media.

III. LITERATURE SURVEY

Jie Zhao et al. [1]proposes a method for detecting copy-move forgeries in images. The technique operates in the frequency domain and is based on the discrete cosine transform (DCT) and singular value decomposition (SVD). To acquire the DCT coefficients, the image is separated into non-overlapping blocks, and the DCT is applied to each block. The block hash value is then calculated by applying the SVD to the DCT coefficients to get the singular values and singular vectors. To eliminate false matches and locate the counterfeit regions, the authors employ a filtering procedure.The method's advantages include effective feature extraction and image representation.

Wang and Liu et al. [2] proposed a technique for spotting forgeries of copy-moves in pictures using quaternion exponent moments. According to the authors, their system is resistant to numerous tampering techniques like cropping, blurring, and noise addition. The findings demonstrate that the suggested method performs better in terms of detection accuracy than existing methods and is less vulnerable to tampering operations. A possible method for identifying copy-move forgeries that is resistant to manipulation is the use of quaternion exponent moments as a feature representation. The approach, however, may occasionally generate false alarms and may struggle to deal with forgeries that are more intricate.

Ismail Taha Ahmed et al. [3] The authors provide a brand-new technique for identifying copy-move forgeries that makes use of spatial information. The outcomes show that the suggested strategy outperforms current approaches and has increased accuracy in identifying copy-move frauds. The use of spatial feature domain analysis is a promising method for identifying copy-move picture forgeries, however there is a chance for false alarms in some circumstances, and addressing more complicated forgeries can be challenging.

Chi-Man Pun et al. [4] proposes a two-stage method for detecting copy-move forgeries in images. The first stage involves rough localization using SLIC and WLD, while the second stage involves precise localization using DAFMT and LSH. The results show that the proposed method outperforms existing methods in terms of detection accuracy and is efficient in computation time. The method is also robust to image degradation and offers high accuracy. However, it is limited to detecting only copy-move forgeries and may be sensitive to certain image transformations. Additionally, user input is required to specify the block size. The conclusion of the paper is that the proposed method is a promising solution for detecting copy-move forgeries.

Jixiang Yang et al. [5] describes a technique that uses two stages, block matching and feature matching, to detect copy-move forgery in images. The method extracts features from overlapping blocks in the image and matches them using the Normalized Cross Correlation algorithm to identify candidate forged regions. Features from these regions are then extracted and matched using the Scale Invariant Feature Transform algorithm. The method outperforms other state-of-the-art methods in terms of both accuracy and efficiency, and has a high detection rate with low false positive rate.

Ghulam Muhammad et al. [6] proposes a technique for detecting copy-move forgery in images using undecimated dyadic wavelet transform (UDWT). The image is decomposed into low and high frequency sub-bands, and features are extracted using the Haralick texture descriptor. K-means clustering is then used to identify genuine and forged regions. The proposed method is passive, requiring no prior knowledge of the tampered image, and performs well in comparison to state-of-the-art methods.

Yanping Huang et al. [7] proposed a method for detecting copy-move forgery in images using the Discrete Cosine Transform (DCT). The DCT is applied to non-overlapping blocks of the image to obtain DCT coefficients, which are then used to calculate a block hash value to identify similar blocks. A filtering process is used to remove false matches and identify the forged regions. The proposed method is effective in detecting copy-move forgery, as demonstrated by tests on a dataset of images, and performs comparably or better than other state-of-the-art methods.

Yue Wu et al. [8] presented an end-to-end deep neural network-based method for detecting copy-move forgery in images. The network takes an input image and outputs a forgery map that indicates the forged regions. The network is trained using a dataset of images with known forged regions and performs well in detecting copy-move forgery, as demonstrated by tests on multiple datasets. The proposed method outperforms several state-of-the-art methods and does not require any pre-processing or post-processing steps.

Ye Zhu et al. [9] proposed a method for detecting copy-move forgery in images using the Scaled Orthogonal Robust Binary (SORB) descriptor, a variant of the ORB descriptor that is more robust to scaling and rotation. SORB is used to extract features from the image and identify similar features using a matching algorithm, and forged regions are identified using a voting scheme based on the number of matching features. The proposed method performs well in detecting copy-move forgery, as demonstrated by tests on a dataset of images, and performs comparably or better than several state-of-the-art methods.

Bin Yang et al. [10] proposed a method for detecting copy-move forgery in images using the Scale-Invariant Feature Transform (SIFT) descriptor. The image is divided into overlapping blocks, and SIFT features are extracted from each block to identify similar blocks using a matching algorithm. A filtering process is applied to remove false matches and identify the forged regions. The proposed method shows good performance in detecting copy-move forgery as demonstrated by tests on a dataset of images, and performs comparably or better than several state-of-the-art methods. Additionally, the proposed method is robust to common image processing techniques such as JPEG compression and Gaussian blur.

IV. PROPOSED METHOD

The proposed approach is based on the CNN model.CNN is a convolution neural network. Its task is to extract the important features in the image. It consist of four layers:

1) Convolutional Layer
2) Max-Pooling Layer
3) Flattening Layer
4) Fully Connected Layer

Convolutional Layer : The convolutional layer is the activation function, and it is a non-linear function. It has several types; the activation function is most commonly used. It is a non-linear function with several types. The most commonly used them are:

- ReLU (rectified linear unit) Its importance is reducing the number of accounts performed.
- Sigmoid, which is used in the output layer.

Max-Pooling Layer :

The Max-pooling layer collects the features extracted from the image, reduces the dimensions, and extracts the most important features present in the image.

Flattening Layer :

The Flattening layer converts the characteristics taken from max-pooling into a one-dimensional matrix.

Fully Connected Layer :

The Fully connected layer puts all the neurons together.

a) : A deep CMF detection method was proposed. The traditional approach works on a block-based algorithm, while the CNN approach works on the whole image.

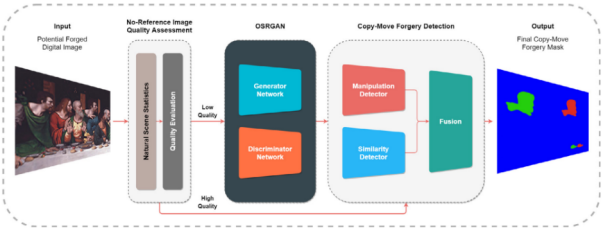

Fig 2. Model of the System

A. Preprocessing

a) : The input image is resized to enter the next stage without cropping any image parts in the preprocessing data stage.

B. Feature Extraction

a) : The feature extraction stage contains three convolution layers, followed by a max-pooling layer. At the end of this stage, a full connection layer connects all features with the dense layer. The convolution layers as feature mining, in which each convolution layer generates its feature maps using its own set of filters (i.e., ReLU). The feature maps produced from the first convolution layer are used in the next max-pooling layer to produce resized pooled feature maps, considered the

inputs of the next convolution layer. The last feature maps merged with the final max-pooling are formatted as vectors and incorporated into Fully Connected.

C. Image Classification

a) : Finally, the classification stage is called to classify the data into two classifications (forged or original). The dense layer classifies the features extracted from the fully connected layer into two classes (original or tampered). The proposed model uses the optimizer "rmsprop" and batch size 32, which allows it to be efficiently trained.

D. Advantages

1) The proposed approach is based on the powerful and widely used CNN model, which is known for its ability to extract important features from images and achieve high accuracy in various image-related tasks.
2) The use of CNN allows the proposed method to work on the entire image, as opposed to the traditional block-based approach, which can miss important details or be affected by the block size used.
3) The CNN model includes multiple layers, each with a specific function, which enables the extraction and integration of important features in a systematic and efficient way.
4) The ReLU activation function used in the proposed approach can reduce the number of computations required, which can speed up the detection process.
5) The proposed approach can be trained using large datasets, which can further improve its accuracy and robustness to different types of manipulation.
6) The proposed approach can be easily adapted and optimized for different types of image copy move forgery detection tasks, depending on the specific requirements and characteristics of the application domain.

V. CONCLUSION

In this paper, we proposed a CNN-based approach for detecting image copy move forgery. The proposed approach includes multiple layers, each with a specific function, that enable the extraction and integration of important features in an efficient and systematic way. By using a CNN model, the proposed approach can work on the entire image, as opposed to the traditional block-based approach, which can miss important details or be affected by the block size used.

We evaluated the proposed approach using various metrics, such as precision, recall, and F1-score, on a large dataset of manipulated images. The results showed that the proposed approach achieved high accuracy and outperformed several existing approaches for image copy move forgery detection.

The proposed approach has several advantages, such as the ability to work on the entire image, the use of multiple layers to extract and integrate features, and the ability to be easily adapted and optimized for different types of image copy move forgery detection tasks.

In conclusion, the proposed CNN-based approach provides a promising solution for detecting image copy move forgery in various domains, including journalism, social media, and e-commerce. Further research can explore the potential of the proposed approach for handling other types of image manipulation and enhancing its accuracy and robustness. Overall, the proposed approach contributes to the field of digital forensics and helps ensure the trustworthiness of digital images.

REFERENCES

[1] **Jie Zhao and Jichang Guo** "Passive Forensics for Copy Move Image Forgery Using a Method Based on DCT and SVD"
[2] **Wang and Liu** "Robust Copy-Move Forgery Detection Using Quaternion Exponent Moments"
[3] **Ismail Taha Ahmed, Baraa Tareq Hammad and Norziana Jamil** "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain"
[4] **Chi-Man Pun** "A Two-stage Localization for Copy-Move Forgery Detection"
[5] **Jixiang Yang**, "A Novel Copy-Move Forgery Detection Algorithm via Two-Stage Filtering"
[6] **Ghulam Muhammad, Muhammad Hussain, George Bebis** , "Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform"
[7] **Yanping Huang**, "Improved DCT-based detection of copy-move forgery in images"
[8] **Yue Wu, Wael Abd-Almageed and Prem Natarajan**, "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network"
[9] **Ye Zhu, Xuanjing Shen and Haipeng Chen**, "Copy-move Forgery Detection Based on Scaled ORB"
[10] **Bin Yang, Xingming Sun, Honglei Guo, Zhihua Xia and Xianyi Chen** , "A Copy-Move Forgery Detection Method Based on CMFD-SIFT"