Copy Move Image Forgery Detection Using CNN

Pandre Nikhitha[1], K M N Kumari[1], Boggarapu Nithin Sai[1], S Kavitha[2]
[1]*Student, Computer Science and Engineering, Institute of Aeronautical Engineering, India*
[2]*Assistant Professor, Computer Science and Engineering, Institute of Aeronautical Engineering, India*
Corresponding Author: kavithachejarla@gmail.com

Abstract— **Digital images are crucial in various fields, and image forgery, a practice where individuals alter images to conceal or present false information, is becoming more prevalent with advanced image processing tools. The proposed system aims to identify and expose copy-move forgery, a common manipulation technique in which a portion of an image is copied and pasted within another picture, copy-move forgery is what the suggested system seeks to detect and reveal. Singular Value and Discrete Cosine Transform (DCT)-based methods are also reliable. Decomposition (SVD) was established in order to improve resilience against standard post-processing procedures. Additionally, better algorithms using Local Binary Histograms of the pattern (LBP) show superior ability to locate and identify copy-move frauds amongst different datasets. These developments demonstrate the continual initiatives to raise the precision and effectiveness of techniques for detecting image fraud.**

***Index Terms*—Image tampering, Key points, Copy Move, Descriptor, CNN (Convolutional Neural Networks), SIFT Detector.**

1. Introduction

For the dissemination of sensitive information, such as trade secrets and national security, digital photographs are necessary. Tasks related to image processing encompass compression, segmentation, enhancement, and zooming. As social media has grown in popularity, photo sharing has also expanded, which has influenced public perception but also caused a large-scale distribution of false photographs. Image forging is the alteration of original images with the intention of presenting misleading information or obtaining financial gain. Because convolutional neural networks (CNNs) can automatically extract information without the need for statistical or mathematical calculations, they are widely used for image fraud detection.

A digital representation of an image or picture is called a digital image. It is a binary numerical representation of a two-dimensional picture.

Manuscript revised November 04, 2024; accepted November 05, 2024. Date of publication November 08, 2024.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.59

A vital tool for information distribution on the Internet, digital images are widely employed in practically every industry. Digital photos may include sensitive information about companies or even national security. The ease of sharing brought forth by internet expansion and multimedia has made picture content security a critical concern for scientists and engineers. A picture can be converted to a digital image by image processing, and from there, it can be altered to retrieve the needed data. Generally speaking, image processing involves manipulating images, photographs, videos, etc. [6]

Results broken down into sentences matched sources Image processing is any type of signal processing in which an image such as a picture or a frame from a video is used as the input and the output is either another image or a set of attributes or features associated with images. Examples of image processing include working with video, segmenting pictures, compressing images, enhancing images, and zooming. Thanks to advancements in image processing and editing techniques, it is becoming increasingly challenging to distinguish between real and fraudulent photographs. This tendency reduces the trustworthiness of digital photographs and reveals significant flaws. It is essential to create a system that can be utilized to confirm the accuracy and integrity of these pictures.

2. Literature Review

In the paper [1], Deep Learning, a well-recognized paradigm in the field of pattern recognition, is used to develop a model. The algorithm it makes use of is the CNN, or convolution neural network. CNN has unique quality utilizing a machine learning type of neural artificial network learning tool and take out key traits based on the information. The photos that were categorized as the model receives input from testing and training. The data set consisted of 2000 images out of which 1200 are original and other 800 are forged. The accuracy of the model was 97.52%.

In paper [2], is based on SIFT feature extraction. Localization of key points is the one of the main steps of feature extraction in SIFT using a threshold. Key points of same threshold are matched together using Brightness Binary Feature (BBF). These key points are sent to Random Sample Consensus

(RANSAC) after forming a 128-dimensional vector. This RANSAC algorithm check the key points in using a threshold. For obtaining best parameters like threshold of BBF and RANSAC an algorithm named Grey Wolf Optimizer (GWO) is used.

In paper [3], the parts of the image that are duplicated and pasted are thought to be the most crucial aspect of image cloning. Thus, the authors of this paper described the inactive algorithms that are helpful in identifying fake section of the picture. algorithm based on blocks and important points consisting algorithm are the two most popular techniques in the method for detecting images. Discrete Cosine Transform (DCT) is used to get features which are the quantized coefficients which are seemed to be blocks that are overlapping. Key-point-based algorithm can be used to know the region of image that is used for forged. Key points of an image are extracted using the algorithm known as Scale invariant feature transform (SIFT).

The paper [4] particularly focused SIFT-CNN frame work where CNN model takes an image as input and its output is based on the classification of the input image. Any image has a large number of pixels and for every pixel a descriptor is formed using Scale Invariant Feature Transform (SIFT). These descriptors are fed to CNN model. The CNN model that was built is using ResNet which is especially used for image classification. The accuracy was around 89% for the cases of with transfer learning and without transfer learning.

The paper [5] is about how recompression of a JPEG is helpful for detecting whether the image is forged or not. When a tampered or forged JPEG image is recompressed i.e. compression after compression and again saved in the same JPEG format, the compression features or artifacts in the final saved image will be different from that of the images that are compressed for a single time. These compression feature or artifact changes or abnormalities, can be used to detect recompression in JPEG using spatial domain or frequency domain.

3. Methodology

Convolutional Neural Networks (CNNs) are extensively utilized in picture recognition and processing applications due to their remarkable capacity to learn visual information. These applications include the identification of photo fraud. A typical CNN design has several input and output layers, layers that are fully linked and convolutional. An ordered data flow is used in forgery detection to evaluate an correctness of the input image. In the start of the procedure, Scale-Feature Extractor is used to extract features from the input image. The SIFT algorithm is an invariant feature transform. Regions that match across photos can be found using key points, which are distinct, scale-invariant features that SIFT detects in the image. Moreover, SIFT generates descriptors, which are unique vectors that represent the immediate neighbourhood surrounding every key point.[7]

Regions that match across photos can be found using key points, which are distinct, scale-invariant features that SIFT detects in the image. Together with key points, SIFT also computes descriptors, which are unique vectors that represent the immediate neighbourhood surrounding each key point. These descriptions are crucial for aligning focal points across several images. The next step is to compare the descriptors to identify any forgeries. If the system finds matching descriptors in a particular location, it flags that location for further investigation. This method, which starts with the input image and proceeds to feature extraction using key points and descriptors, comparison, and detection, is the basis of image forgery detection systems.[8]

SIFT is a rather complex algorithm. The SIFT algorithm consists of four major phases. We'll examine each one separately. Scale-space peak selection, key point localization, orientation assignment, key point descriptor, and key point matching are crucial elements in the feature recognition and description process, particularly when taking the SIFT (Scale-Invariant Feature Transform) algorithm into account. The task of scale-space peak selection involves identifying potential locations for features at different image scales. This is achieved by applying Gaussian filters to blur the image at various scales, resulting in a scale-space representation. By analysing the differences between different scales, local extrema are found in the scale-space, which aids in the identification of potential important spots that do not change as a function of scale.

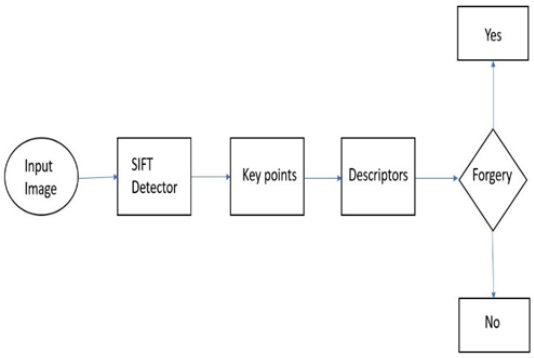

Fig.1. Data Flow Diagram

A. Input Image:

This is the initial stage where an image is provided to the system for analysis.

B. SIFT Detector:

The Scale-Invariant Feature Transform (SIFT) detector is employed to identify key points within the image. SIFT is a robust feature detection algorithm that locates distinctive features in images. These features will never change to scale, rotation, and partially invariant to changes in illumination and 3D viewpoint, making SIFT particularly useful for various image analysis tasks.[9]

C. *Key Points:*

Key points, also known as interest points, are distinctive locations in the image identified by the SIFT algorithm. These points usually correspond to edges, corners, or blobs (high-contrast regions) in the image. The key points serve as anchors for further analysis and matching between images.

D. *Descriptors:*

For each key point detected, a descriptor is computed. Descriptors are vectors that describe the local image patch around each key point. They capture the appearance and structure of the region, providing a unique signature for the key point that can be used for matching purposes.

E. *Forgery Detection:*

The descriptors from the input image are analysed to determine if there are any inconsistencies or anomalies that suggest forgery. This analysis could involve comparing the descriptors with those from other images or assessing the spatial relationships and consistency of the key points and descriptors within the same image.[11]

F. *Decision:*

Based on the analysis, the system makes a decision:

i) Yes: If the analysis indicates that the image has been tampered with, the decision is "Yes," signaling that forgery is detected.

ii) No: If the analysis does not find any signs of tampering, the decision is "No," indicating that the image is not forged.

Key point localization is the next step, which involves pinpointing these potential feature key points. A complete model is fitted to establish the precise location and scale of the essential points identified from the scale-space. At this stage, only the most stable and distinct key points are retained, thus low contrast or poorly localized edges are removed. The orientation assignment phase comes next, when the local image gradient directions dictate each key point's orientation. This ensures that as the image rotates, the important details stay the same. A key point's orientation is dictated by the dominant gradient direction around it, making the resulting descriptor rotation-invariant.[10]

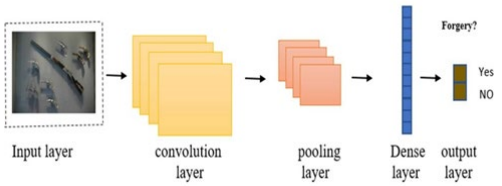

Fig.2. CNN layers

4. Implementation

To detect forgery images, we need to provide input images and they should be stored in datasets or device. Connect your drive with the Google Colab. We need to import all necessary modules like NumPy, matplotlib, cv2, etc.. Then we use plot_image function to create a new figure and it converts an OpenCV image from BGR to RGB. And then displays the image with correct colour representation using Matplotlib.

There are four steps to identify forgery they are Initialization, feature detection, Forgery Detection and Visualization. We read and store image in initialization. Key points and descriptors are identified by using SIFT. This is featuring detection. And we apply DBSCAN to cluster descriptors and detect copied regions this is the step where forgery is detected. And visualization is in which we draw lines between duplicated features, indicating potential forgery.

The image is taken as input as path to determine whether it is fake or not. We use two parameters' eps, min_samples along with Matplotlib to read and display input image. 'eps' is the maximum distance between two samples for one to be considered as in the neighbourhood of the other in DBSCAN. 'min_samples' is the minimal number of samples in a neighbourhood for a point to be considered a core point. The image will be displayed in an output cell or plotting window.

After reading the image from given path and extracting key points and descriptors we use eps, min-samples to identify clusters of duplicated features. We draw green lines connecting these clusters on the image, highlighting possible manipulated regions. Finally, the result will be an image with lines indicating suspected forgery regions.

The image will initially go through scale spacing that spans several octaves. For each pixel, we obtain a separate blurred image by using several Gaussian values. The blurred photographs are stacked together to generate what appears to be a massive collection of images. The difference between the Gaussian, which is an image, and the successful images will be generated. Each DoG has its own set of focal points. The following process has these Key points. [12]

A pixel is regarded as a potential key point if it is surrounded by 8 pixels of the same DoG, 9 pixels of the previous DoG, and 9 pixels of the next DoG. By producing an 8-bin orientation histogram, these key points are transformed into 128 high dimensional vectors. DBSCAN, which stands for Density Based Spatial Clustering of Applications with Noise, is given these descriptors in order to identify related key points and establish a connection between them. Since similar portions of the photos will share common key points, analyzing the fabricated portion of the image will be aided.

A. *Overview*

This system is designed to detect copy-move forgery in images using a Convolutional Neural Network (CNN) model along with the Scale-Invariant Feature Transform (SIFT) algorithm for feature extraction. The system operates in three stages: preprocessing, feature extraction, and classification. Additionally, it highlights the forged areas in the image.

B. System Architecture

1) Preprocessing Stage:

Resize the input image to a standard size (e.g., 256x256 pixels) without cropping any parts.

Convert the image to grayscale to simplify processing.[13]

2) Feature Extraction Stage:

Convolution Layers: To extract feature maps, use a number of convolution layers.

Convolution Layer 1: Filters are applied to identify low-level characteristics, such as corners and edges.

Max-Pooling Layer 1: Diminish the number of dimensions among the feature maps.

Convolution Layer 2: Detect higher-level features.

Max-Pooling Layer 2: Reduce the amount even more dimensionality.

Convolution Layer 3: Identify intricate patterns as well as textures. Fully Connected Layer: Condense the last feature and join them to a thick layer to assemble every characteristic that was extracted.

3) Classification Stage:

Use the dense layer output to classify the image into forged or original categories. If classified as forged, use additional logic to identify and highlight the forged areas using the SIFT algorithm.

The algorithm shows how manipulations are identified in given input. We need to follow every step to identify the manipulations of original image.

C. Algorithm

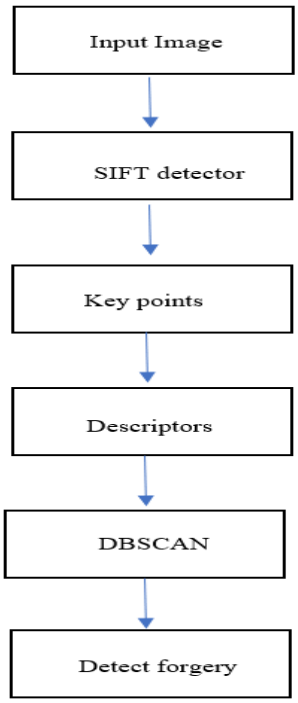

Fig.3. Flowchart

5. Results And Discussion

It can be quite difficult to tell whether a photograph is fake or not, and even if it is, it can be hard to tell which exact area of the picture is fake. If the image was altered, the green line will indicate which part of the output was altered. It shows that if there is no formation of the image, the result will display "Image is Not Forged".

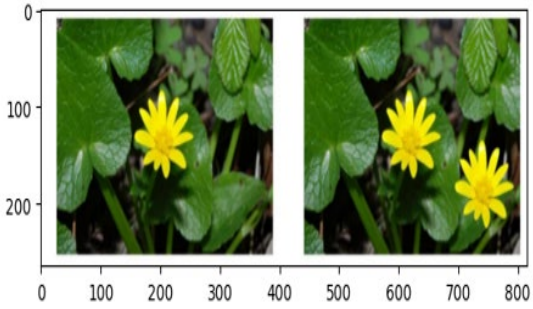

Fig.4. Input1 image

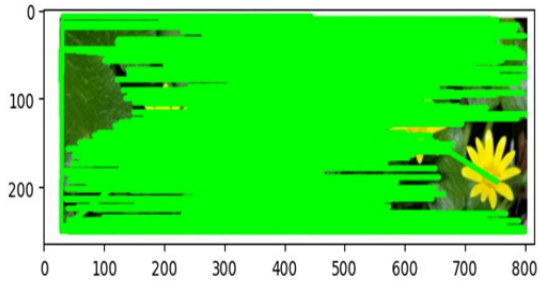

Fig.5. Output1 image

Fig.4. is the Input Image which have two almost identical flower and leaf halves. As duplicate elements are frequently copied and pasted inside of images to change or create content, this symmetry can be a prevalent indicator of manipulation. Fig.5. are the output image where Certain portions of it are covered in a series of green patches. An algorithm may have recognized these green patches as suspected forgeries since they probably correspond to the duplicated or altered sections that were found.[14]

Fig.6. Input2 image

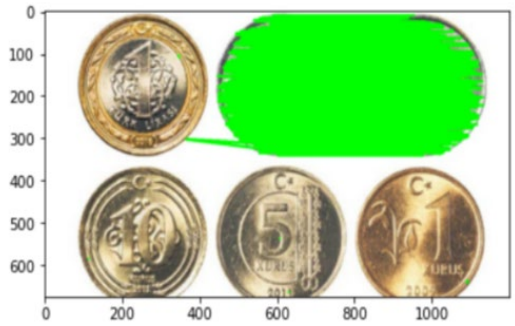

Fig.7. Output2 Image

A variety of post-processing techniques, including additive Gaussian noise, Gaussian blurring, JPEG compression, and mixed operations, are used since forgers typically go to great lengths to produce an undetectable manipulated image. We test the suggested method's robustness through a number of experiments. [15]

Metric		Method		Efficiency gain = proposed – compared
		The Proposed method	M.A. Elaskily et al. [25]	
25 epochs	Accuracy	97.6	95.1	2.5
	log less%	2.4	4.99	-2.59
	TT (sec)	40.2	46.56	-6.36
35 epochs	Accuracy	100	98	2
	log less%	zero	2	-2
	TT (sec)	47.78	52.31	-4.53

The forgery detection algorithm successfully located the duplicated parts in the input image, as seen by the green overlay in the output image. We can have the proof of Manipulation as the left and right portions of the input image are identical, proving that image manipulation was used to create this duplicate rather than a spontaneous occurrence.

The system has been tested on the Google Collaborator server using a Google Compute Engine backend with GPU RAM of 2.5GB/12GB. It runs locally and doesn't require network connectivity. TensorFlow with Keras as the backend and Python 3.0 for development are used in the implementation. Using the MICC-F2000 dataset, the system's performance was assessed, and the outcomes were contrasted with those of newly released methods. It was simple to classify the photos into original and fake classes in the results tables, the original class was labeled as positive and the fake class as negative.

6. Conclusion

In conclusion, this project introduced a robust Copy-Move Forgery Detection methodology utilising deep neural networks. The system effectively classifies images as forged or original, leveraging feature extraction and classification techniques. Tested on benchmark datasets with different inputs and the proposed model achieved 100% accuracy at 35 epochs and demonstrated superior performance in terms of accuracy and training time (TT). By locating the portions of the image that were replicated, the analysis was able to successfully identify the duplicates. The input image was modified using an easy duplication technique, indicated by the green patches in the output image that precisely show where the image was duplicated and pasted. For future work, the system can be enhanced by integrating additional forgery detection techniques and improving the model's efficiency with more extensive datasets. In digital forensics, this type of forgery detection is crucial to confirming the authenticity and lack of alteration of photographs. The incorporation of advanced machine learning algorithms and real-time processing capabilities could further bolster its utility in various forensic and security domains.

References

[1]. G. R. S. Murthy, R. S. Jadon. (2009). A Review of Vision Based Hand Gestures Recognition, International Journal of Information Technology and Knowledge Management, vol. 2(2), pp. 405- 410.

[2]. P. Garg, N. Aggarwal and S. Sofat. (2009). Vision Based Hand Gesture Recognition, World Academy of Science, Engineering and Technology, Vol. 49, pp. 972-977.

[3]. FakhreddineKarray, MiladAlemzadeh, Jamil AbouSaleh, Mo Nours Arab, (2008). Human Computer Interaction: Overview on State of the Art, International Journal on Smart Sensing and Intelligent Systems, Vol. 11).

[4]. Mokhtar M. Hasan, Pramoud K. Misra, (2011). Brightness Factor Matching for Gesture Recognition System Using Scaled Normalization, International Journal of Computer Science &Information Technology (IJCSIT), Vol. 3(2).

[5]. Xingyan Li. (2003). Gesture Recognition Based on Fuzzy C-Means Clustering Algorithm, Department of Computer Science. The University of Tennessee Knoxville.

[6]. S. Mitra, and T. Acharya. (2007). Gesture Recognition: A Survey IEEE Transactions on systems,Man and Cybernetics, Part C: Applications and reviews, vol. 37 (3), pp. 311- 324, doi:10.1109/TSMCC.2007.893280.

[7]. Simei G. Wysoski, Marcus V. Lamar, Susumu Kuroyanagi, Akira Iwata, (2002). A Rotation Invariant Approach On Static-Gesture Recognition Using Boundary Histograms And Neural International.

[8]. J. Bunk, J. H. Bappy, T. M. Mohammed, L. Nataraj, A. Flenner, B. Manjunath, S. Chandrasekaran, A. K. Roy-Chowdhury, and L. Peterson, "Detection and localization of image forgeries using resampling features and deep learning." IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 1881-1889, 2017.

[9]. D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient dense-field copy–move forgery detection,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2284-2297, 2015.

[10]. X. Bi, and C.-M. Pun, “Fast reflective offset-guided searching method for copy-move forgery detection,” Information Sciences, vol. 418, pp. 531-545, 2017.

[11]. X. Bi, and C.-M. Pun, “Fast copy-move forgery detection using local bidirectional coherency error refinement,” Pattern Recognition, vol. 81, pp. 161-175, 2018.

[12]. Y. Rao, and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images." in Proceedings of IEEE International Workshop on

Information Forensics and Security, pp. 1-6, 2016.

[13]. Ardizzone, E.; Bruno, A.; Mazzola, G. Copy–move forgery detection by matching triangles of keypoints. IEEE Trans. Inf. Forensics Secur. 2015, 10, 2084–2094.

[14]. Wen, B.; Zhu, Y.; Subramanian, R.; Ng, T.T.; Shen, X.; Winkler, S. COVERAGE—A novel database for copy-move forgery detection. In Proceedings of the 2016 IEEE International Conference on Image Processing (ICIP), Phoenix, AZ, USA, 25–28 September 2016; pp. 161–165. 25. Castro, M.; Ballesteros, D.M.; Renza, D. A dataset of 1050-tampered color and grayscale images (CG-1050). Data Brief 2020, 28, 104864.

[15]. Castro, M.; Ballesteros, D.M.; Renza, D. CG-1050 v2: Original and Tampered Images. 2019. Available online: https://data. mendeley.com/datasets/28xhc4kyfp/1 (accessed on 17 December 2020). 27. Amerini, I.; Ballan, L.; Caldelli, R.; Del Bimbo, A.; Serra, G. A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. 2011, 6, 1099–1110.