Implementing Copy Move Forgery in Photography Web Application for Edit Detection

Alan Varghese
PG Scholar
Department of Computer Applications
Amal Jyothi College of Engineering,
Kanjirappally, India
alanvarghese2023a@mca.ajce.in

Ms. Meera Rose Mathew
Assistant Professor
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
meerarosemathew@amaljyothi.ac.in

Abstract—This paper says about "Photo copy move forgery", a form of digital image manipulation, is copying a section of an image and pasting it onto another location to produce a fictitious image. This method can be used to fabricate images for a number of purposes, such as disseminating false information, producing phony papers, or fabricating evidence. Identifying the source of the modified areas and looking for anomalies in the image are necessary for detecting photo copy move forgeries, which is a difficult task. This technique is briefly described in this abstract, along with any implications it has for digital image forensics.

Keywords— Digital image, forensics, Copy-move forgery, Gray-scaling, Pixel-comparison, Distance calculating, Detection algorithms

I. INTRODUCTION

Photo copy-move forgery is a type of digital image tampering where a component of a picture is copied and pasted onto another portion of the identical image in a practice known as photo copy-move forgery. This method is frequently used to conceal or duplicate an object in a picture or to combine images from several sources to produce a composite image. Copy-move forgery can pose a severe problem for a photography website since it violates the fairness of the judging and the contest's credibility. If contenders are permitted to modify their photos in this way, it may provide those who are willing to cheat an unfair advantage Use effective picture analysis algorithms that can spot such alterations to prevent copy-move forgeries in your photography competition. This can entail utilizing specialist software applications or counting on the knowledge of skilled judges who can spot questionable visual elements. You can make sure that your photography contest is always a fair and open competition that recognizes and rewards the real ability and innovation by taking a proactive approach to image forensics.

The process of changing or manipulating a digital image using software tools is referred to as "digital image manipulation." The necessity for verifying the accuracy of digital photographs has grown as a result of their expanding use in a variety of fields, including journalism, forensics, and entertainment. Digital image alteration, however, can be used maliciously to produce fraudulent images and have serious repercussions, especially in forensic and legal contexts.
The development of digital image alteration techniques has made it challenging to tell modified photos apart from their genuine counterparts. Copy-move forgery, in which a portion of a picture is copied and pasted to another area of the same image, is one of the most popular methods of digital image modification. Objects in the image can be hidden or added using this technique, misleading viewers who rely on the image's veracity.

To create efficient methods for detecting and avoiding image tampering, especially in fields like journalism, forensics, and legal contexts, research on digital image alteration is therefore crucial. Because we use digital images more frequently in our daily lives, it's critical to maintain the authenticity of those images.

CMF is a kind of digital image forgery that entails copying a particular area of an image and pasting it onto another area of the same picture to produce a new image. Objects in the image can be added or removed using this technique, and it can also be used to hide crucial information. To make it seem as though the copied and pasted portion of the image is a part of the original, it can be scaled, rotated, or even blurred.

CMF is a challenging type of image forgery to detect because it involves only a small portion of the original image, and the copied region may be modified to make it look like part of the original image. Therefore, detecting copy-move forgery requires advanced algorithms and techniques that can identify the manipulated region and distinguish it from the original image.

II. LITERATURE REVIEW

Shahad Lateef abdulwahid et al.[1] Copy-move forgery, generally described as cloning, arises because only a single picture is evaluated for the machining operation., is used.is comparable to the second type of the other type image

DOI: 10.5281/zenodo.7955748
ISBN: 978-93-5906-046-0@2023, Dept. of Computer Applications, Amal Jyothi College of Engineering Kanjirappally, Kottayam

splicing in terms of the fact that both approaches alter the specific picture area containing a different photo A single duplicated location is a picture that has been copied and then written onto an area of the same photo.

Jaiswal A. et al. [2] developed a method for detecting copy-move forgeries in grayscale images. They created a feature vector by combining four handmade features (HoG, LTE, DWT, and LBP) and trained it using a logistic regression classification model. Statistical characteristics were then obtained and reduced to simplify similarity measurement. After post-processing, the resulting characteristics were sorted in lexicographical order, and duplicated picture blocks were identified by comparing block combinations.

Das et al. [3] suggested using the Analysis of the Principal Components (PCA) to detect copy-move forgeries in photos that have been converted to grayscale. They divided the photo into several pieces and used vectors to represent each part. The individual blocks were classified based on lexicographical order, and the PCA was used to represent the dissimilar blocks. This approach can detect even minor differences caused by distortion or inadequate reduction. It is more effective in identifying copy-move frauds and produces fewer false positives than other methods. However, it is less efficient for large block sizes and poor JPEG quality, and its effectiveness decreases for smaller block sizes. Additionally, this method has a low level of complexity but is significantly discriminatory.

Goel, N et al. [4] created a Dual branch CNN method for copy-move forgery detection (CMFD). The dual-branch CNN method was divided into two stages: pre-processing and image classification. The CNN consisted of two branches that extracted features using kernels of various sizes. These features were combined to obtain the dominant feature for classifying the image. The dual-branch CNN achieved high prediction accuracy and had a lightweight architecture, although it was not evaluated for images with different sizes.

Lyu, Q et al. [5] proposed a copy-move forgery detection (CMFD) method based on double matching, which was carried out in two phases: double matching and region localization. In the double matching phase, a triangle matching model was implemented using Delaunay triangles composed of Local Intensity Order Pattern (LIOP) key points. Key point matching was carried out by considering the threshold. In the region localization phase, key point pairs were classified using Density-Based Spatial Clustering of Applications with Noise (DBSCAN). This method was highly robust against various manipulations and effective in detecting CMF even in small areas. However, it suffered from high complexity and processing time.

Pandey, A. and Mitra, A. [6] used a Deep Learning and image transformation approach for detecting forged regions and predicting the mask. Error Level Analysis (ELA) was used to identify the forged area, and U-Net was used to detect the mask of the forged area in the image. This method effectively identified forgery with high robustness, but it was unable to detect multiple manipulations within the image.

III. METHODOLOGY

The proposed system is an online forgery detection in photography contest. In the context of a photography contest website, the use of copy-move forgery would be considered smart as it helps in finding the altered and the original image which make it easy to the judges and viewers. The purpose of a photography contest is to showcase the originality, creativity, and authenticity of the photographers' work.

Using these techniques, it may be possible to identify images that have been tampered with, including those that have been manipulated using copy-move forgery. Therefore, contest organizers may use such techniques to identify any fraudulent entries and ensure that the contest is fair and transparent.

In the system the photographer can only upload one photo in a contest. The image must remain in its original, unaltered state and should not be subjected to any modifications or color grading. As the photographer uploads the photo the machine learning code will be working.

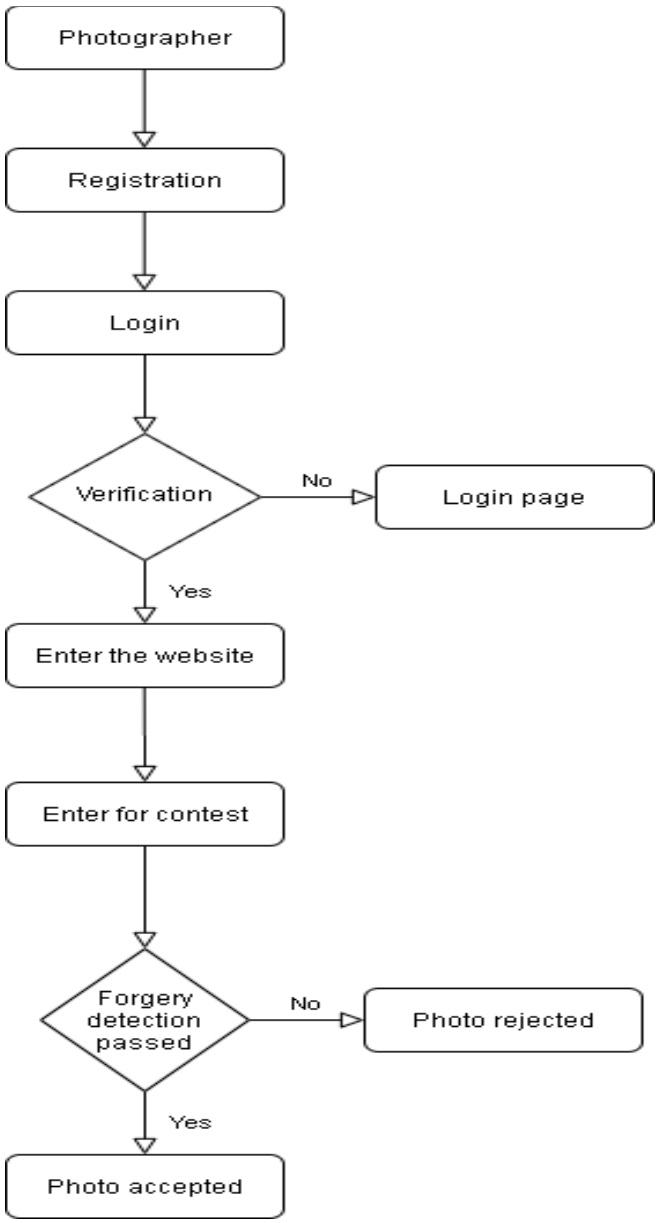
The algorithm takes an image as input and divides it into sub-blocks. For each sub-block, the algorithm computes its feature vector, sorts the feature vectors in lexicographical order and then analyzes the adjacent feature vectors with predefined thresholds. Finally, the algorithm reconstructs the image to generate a marked copy-move attacked image.

The Box class is a simple container for the feature vectors. It has a method to append a new feature vector to the container, another method to get the length of the container, and another method to sort the feature vectors by their features.

The CM_Detection class is the main class that implements the copy-move forgery detection algorithm. It has a constructor that initializes several parameters and variables such as thresholds, image path, image width and height, and the size of the sub-blocks. The class has a run method that calls several other methods of the class in a specific order to implement the copy-move forgery detection algorithm. The compute_CFeatures method computes the characteristic features for all the sub-blocks in the input image, the sort_features method sorts the feature vectors in lexicographical order, and the analyze method analyzes the adjacent feature vectors with predefined thresholds.

Finally, the reconstruct method generates a marked copy-move attacked image and outputs the path of the marked image. As it creates the attacked image it is proved that the image is edited so it is rejected and not uploaded for the contest.

DOI: 10.5281/zenodo.7955748
ISBN: 978-93-5906-046-0@2023, Dept. of Computer Applications, Amal Jyothi College of Engineering Kanjirappally, Kottayam



The script first divides the input image into overlapping blocks of size 32x32 pixels. Then, it extracts a set of features from each block using arithmetic operations and principal component analysis (PCA). The arithmetic operations can be, for example, mean, median, standard deviation, or a combination of these. The PCA features are obtained by projecting the original features onto the eigenvectors of the covariance matrix.

Next, the script sorts the resulting feature arrays in lexicographical order and locates similar arrays, which correspond to blocks that have been copied and pasted in the image. To determine the distance between these blocks in the original image, the script calculates the Euclidean distance between their centroids.

Finally, the script plots the detected copied blocks as white squares on the output image. This is the implementation on a python script which detects copy-move forgery on images.

Here overlapping blocks of 32*32 and then extract 7 features that we use to analyse our image. These seven features are-

Feature 1: Average of all the red pixel values

Feature 2: Average of all the blue pixel values

Feature 3: Average of all the green pixel values

Function C takes the pixel values of an image and sums up all the pixel values of the upper half of the block and divides this by the sum of all pixel values of the block.

Y= 0.299R+0.587G+0.114B where R, G and B are red, blue and green pixel values respectively.

Feature 4: Function C for greyscale or Y pixel values

Feature 5: Function C for red pixel values

Feature 6: Function C for blue pixel values

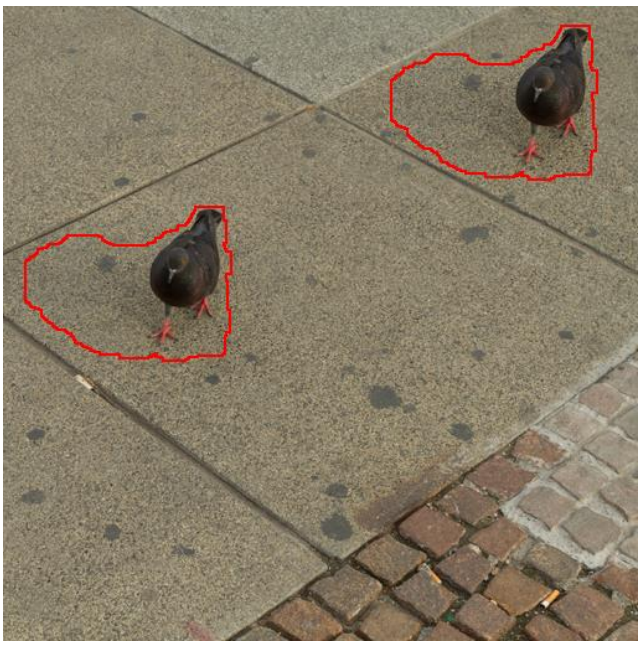
Feature 7: Function C for green pixel values

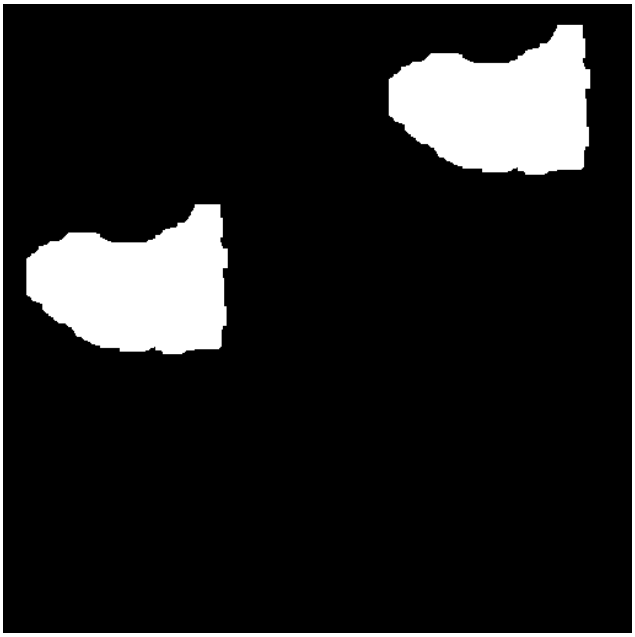
IV. RESULT

The input given by the user

The output generated by the algorithm

DOI: 10.5281/zenodo.7955748
ISBN: 978-93-5906-046-0@2023, Dept. of Computer Applications, Amal Jyothi College of Engineering Kanjirappally, Kottayam





V. CONCLUSION

An online forgery detection in the website is a good solution for admin in order to select the best photograph without any tampering or colour grading in the picture. It will provide equal right to the photographers and the one with experience and talent will win the contest.

Detecting copy-move forgery in a photography contest website can be a challenging task, but forgery detection methods can help identify potential forgeries. In addition, checking the metadata of an image and conducting a reverse image search can provide valuable information about the authenticity of the image and can be considered as future scope for the project. Furthermore, with the increasing use of artificial intelligence to generate images, detecting forgeries created using AI algorithms will become an important task in the future.

As we know that we can't assure 100% of correctness in forgery detection in the picture so we can only maintain the code with new technologies and algorithms.

REFERENCES

[1] Shahad Lateef abdulwahid, The detection of copy move forgery image methodologies, 18 Jan 2021

[2] A.K. Jaiswal, R. Srivastava A technique for image splicing detection using hybrid feature set, 08 Jan 2020

[3] T. Das, R. Hasan, M.R. Azam, J. Uddin
A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform, February 2018

[4] Goel N., Kaur S., Bala R.Dual branch convolutional neural network for copy move forgery detection
IET Image Process, 15 Mar 2021

[5] Lyu Q., Luo J., Liu K., Yin X., Liu J., Lu W.
Copy Move Forgery Detection based on double matching, 2021

[6] Pandey A., Mitra A.Detecting and localizing copy-move and image-splicing forgery, 2022

DOI: 10.5281/zenodo.7955748
ISBN: 978-93-5906-046-0@2023, Dept. of Computer Applications, Amal Jyothi College of Engineering Kanjirappally, Kottayam