Copy-Move Forgery Detection in Digital Images Using DWT, SIFT, and RANSAC Algorithms (Multimedia Security)

Samoua Alsamoua, No:422705

Software Engineering Department, Karadeniz Teknik University, Trabzon, Turkey.

Email: samoua.alsamoua@gmail.com

Abstract: As copy-move forgery is one of the most popular image forgery so importance of forgery detection techniques is increasing day by day. Various image forgery detection techniques are proposed by researchers to withstand against several post processing operations applied over forged region but there is lot of scope in this field to search for methods which are robust to challenges like geometric transformations (scaling, rotation). Time complexity is major issue with forgery detection algorithms. Frequency-based techniques discussed in this paper are very efficient in forgery detection. These techniques can detect forgery even if blurring, noise addition and JPEG compression is used over image. Some methods are also robust to geometrical transformation.

Keywords: *Copy-move forgery, JPEG compression, image Forgery, Digital image fogey, DWT, SIFT, Key points.*

INTRODUCTION:

Digital photo Forgery is not a stranger for human, but this is a very old problem. First, it was limited to art and literature, although it did not affect ordinary people. Today, the fastest development of the internet, image processing software and the latest editing tools make this work very easy and can easily edit or modified images. In addition, it is almost impossible for human visual system to recognize whether the picture is solid or solid with a naked eye.

The digital making has improved rapidly on mainstream media and internet on the social media. By reducing the reputation of digital images, this trend shows intense sensitivity. Therefore, it is important to promote the better algorithm to verify the authenticity of digital photographs, especially considering that photographs can be used as part of medical records, news, and financial documents. Therefore, in detecting photos is one of the main goals of the prime digital image forensics. The classification of image forgery is shown in Figure 1.

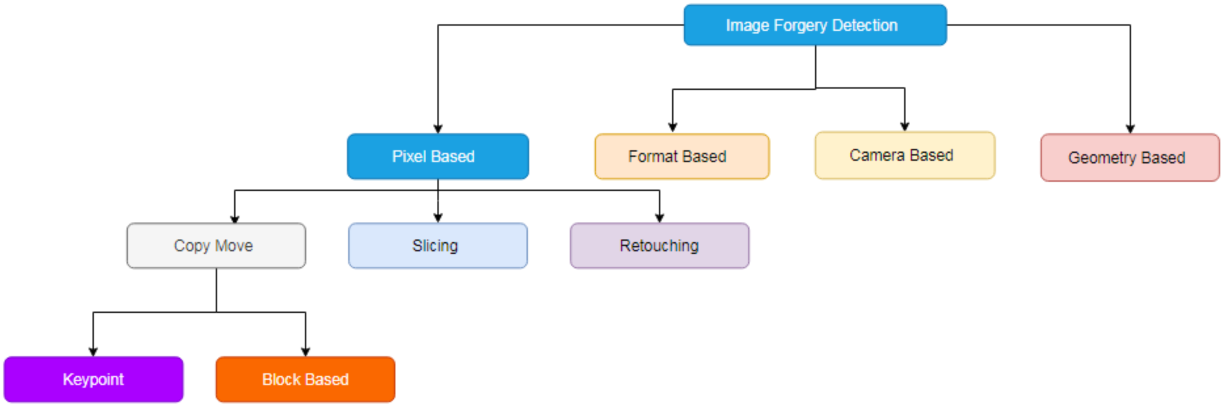


Figure 1: Image forgery detection techniques

1. Pixel-Based Image Forgery Detection:

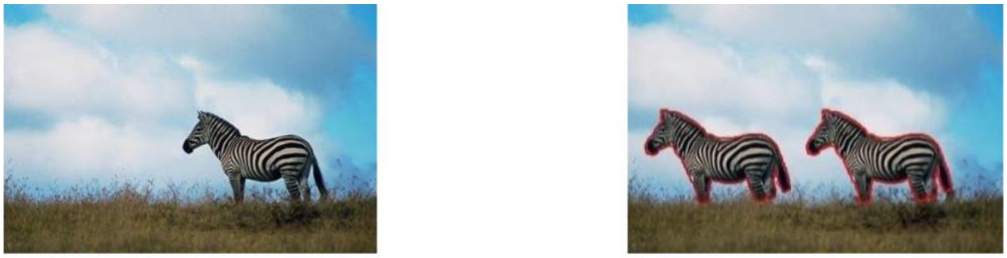
Pixel-based approach emphasis the pixels of the image. Pixel-based approach is also known as passive detection image techniques. In addition, the method is divided into four types. In this work, the photo copying image of our attention is going to forget. The figure shows the ranking of image forgery modes. Pixel-based approach emphasis the pixels of the image. Pixel-based approach is also known as teaser detection of passive image. In addition, the method is divided into four types.

Requirements of a good detection algorithm are:

- The algorithm must detect an approximate match between small image patches
- It must not be computationally complex and must detect a forged image correctly as forged and an authentic image correctly as authentic (i.e., it should have high values of sensitivity and specificity).

2. Copy-Move (Cloning):

Copy-move is widely used as well as trivial method use one of the common ways, as well known as cloning. In this type of forgery, the image or image of this image is copied and then it is shifted to one place within the image. Figure.3 presents the original picture with its doctor. The original image has a copy of six balloons and nine balloons.



(a) The original image. **(b) The forged image.**

Figure 2: Example of Copy-Move Forgery

3. Resampling (Resize, Stretch, Rotation):

For combine two items or people, it can perform different actions, such as we have to do something or other things to match with other people. In addition, during this process, we must re-sample the original image into a new sampling lattice.

4. Splicing:

This is a different variety of and widely used photo fake technology. In this way, two or more photos are converted into a composite image. Assume that we have two pictures, as shown in Figure 4. We collect both of them in one picture. If so careful, limitations between to identify visually.

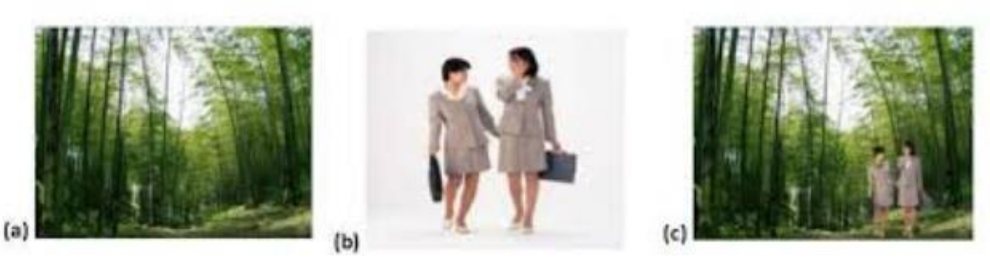


Figure 3: Spliced image forgery

❖ Proposed Method:

That primary advantage in using DWT is reduction in dimension (a smaller number of features) and the primary advantage in using SIFT is its robustness. The proposed method combines the two algorithms to give an optimal solution. The method can detect an image as forged even if the copied part is rotated or scaled and then pasted. First the test image is converted into grayscale format if it is in RGB format. DWT is applied on the image. The image gets divided in to 4 sub bands- LL, HH, LH and HL. We apply SIFT to the LL part only. We now perform a searching to search for occurrence of same features at different locations in the image. Image blocks that return similar SIFT features from all four images are marked as forged regions. The process block diagram is shown in figure 4.

The proposed approach to detect copy-move forgery in an image is based on the Scale Invariant Feature Transformation (SIFT) algorithm. The SIFT algorithm is used because it helps extract robust features from the image to detect if a part of an image was copy–moved. Generally, the copied region of the original image has an almost identical appearance to the region it was copied from besides any scaling or rotation transformation applied on it. Hence, the descriptor of key points extracted from the original region will be quite similar to the descriptor of the key points extracted from the forged region regardless of any transformations applied due to the use of the SIFT algorithm. Hence, with this concept, the general idea to detect if an image has been forged by applying copy-move attack is to match each of the SIFT features extracted from the image by finding key points that share almost similar characteristics which can be assessed based on its respective descriptor

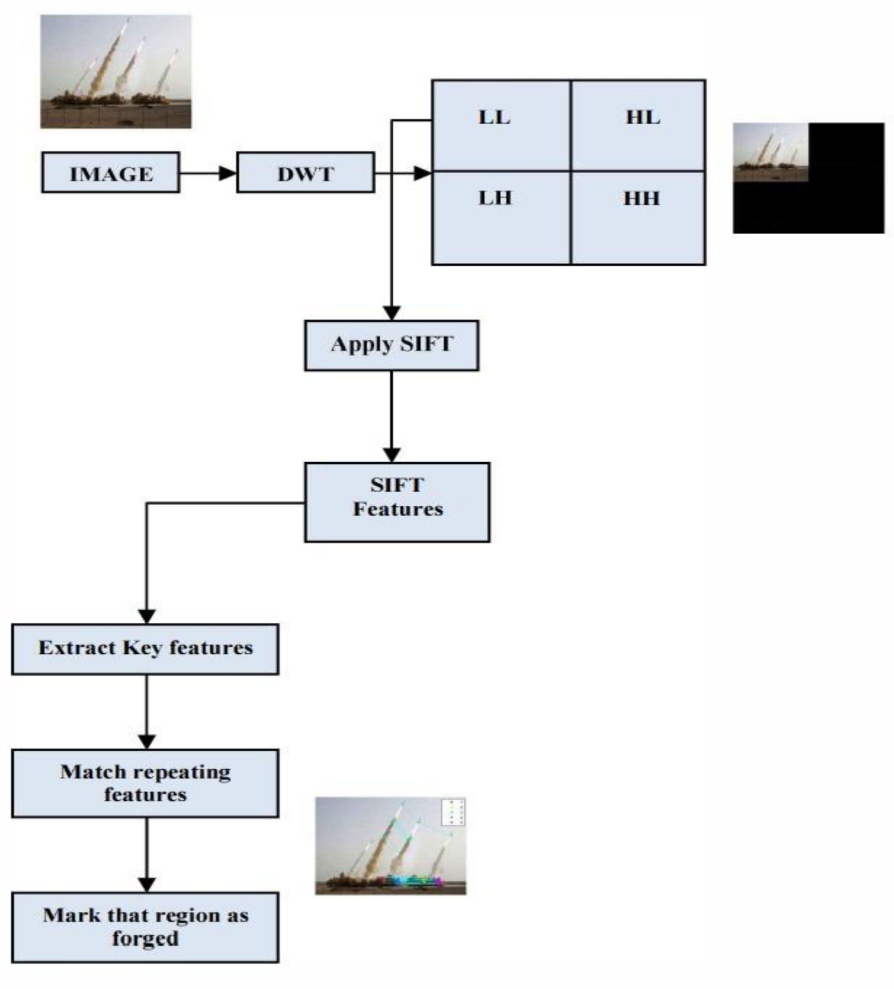


Figure 4: Block Diagram of the proposed method

❖ Scale Invariant Feature Transform (SIFT):

In any image there are a lot of points of interest which can be extracted to provide feature description of the image. The SIFT algorithm can be used to locate a particular object in an image which contains many different objects. SIFT algorithm provides a set of features which do not get modified even by scaling or rotation. Another distinct advantage is that the SIFT is very resilient to noise in the image. A four-stage filtering approach is used in the SIFT algorithm [1].

And we can use any another algorithm like SURF(Speeded-Up Robust Features) or AKAZE that use to feature detection and description.

❖ Matching the features by applying RANSAC (Random Sample Consensus) and False Matches Removal :

The RANSAC algorithm returns with the affine transformations that lead to the largest number of matched key points and the smallest error. Some mismatched key points can be discarded by RANSAC. But when there are lots of mismatched key points, the inaccurate affine transformation will be obtained by RANSAC.

This algorithm is used to remove false positive matches. RANSAC is used as the mismatched points or outliers can obstruct the estimated homography. In the RANSAC algorithm, a set of matched points are randomly selected and then the homography is estimated. After that other remaining matched points are transformed and then compared in terms of distance with their respective matches. A threshold value is set. If this distance is less than threshold value, it is marked as inliers and if it is above the threshold is catalogued as outliers.

❖ RESULTS AND DISCUSSIONS:

Digital image forgery detection is a technology that is used to detect whether an image is manipulated or not. There are various ways to manipulate an image e.g., copy-move forgery, image splicing, image retouching etc. Therefore, the task of detecting a forged image is very complex. Hence, the approach to handle and detect different types of forgery is different. Among the various types of image tampering approach, copy-move is widely and commonly used. In copy-move image forgery a part of image is copied and then it is pasted in the same image having an intention to make a false image or hide some important object within the image. There are a number of copy-move image forgery detection algorithms but most of them are not robust and efficient in terms of computational expanse and affine or geometric transformation. The goal of this proposed method is to detect forgery irrespective of all the ways of copy-move tampering including the tampering with geometric transformation with giving importance on the reduction issue of time complexity.

We can show the results in the next figures.

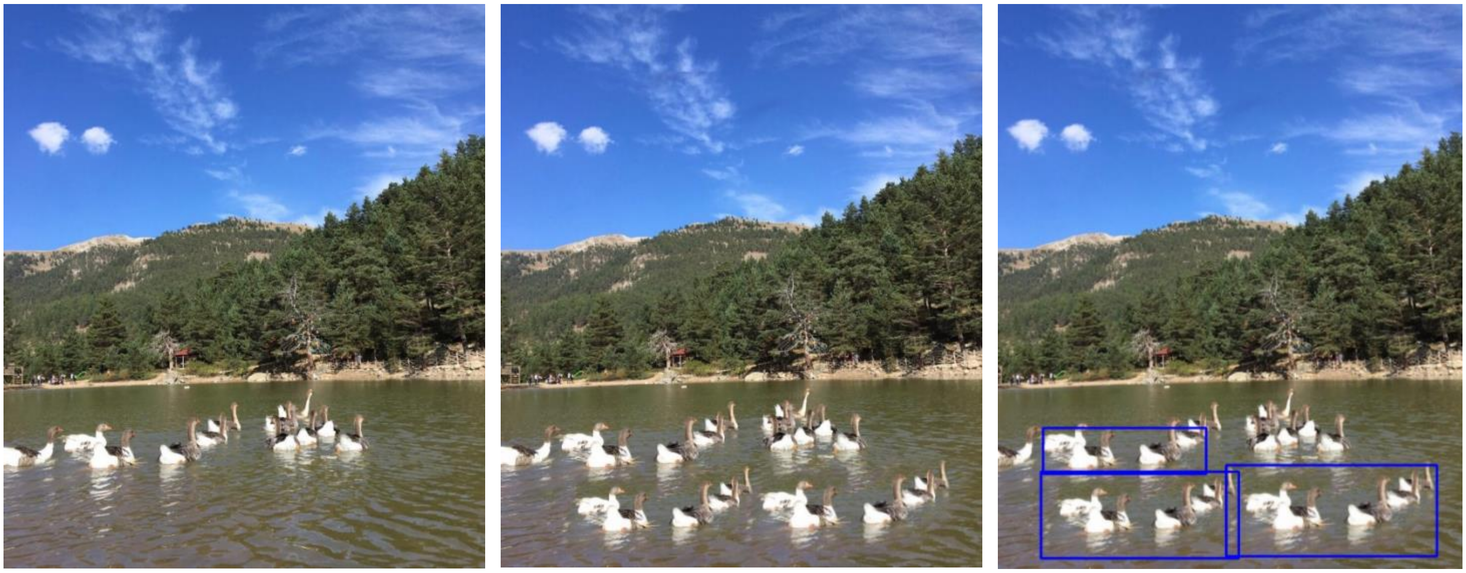


Figure 5: (a) Original image (b) Forged image (c) Forged part detected after SIFT

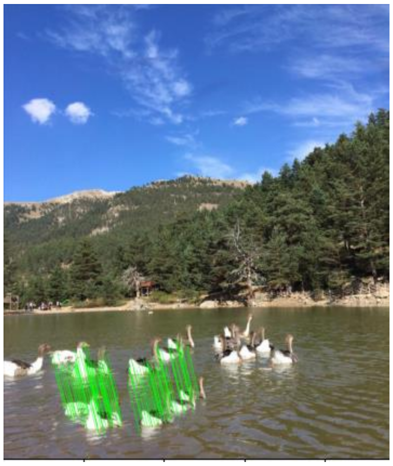


Figure 6: Matching of similar features

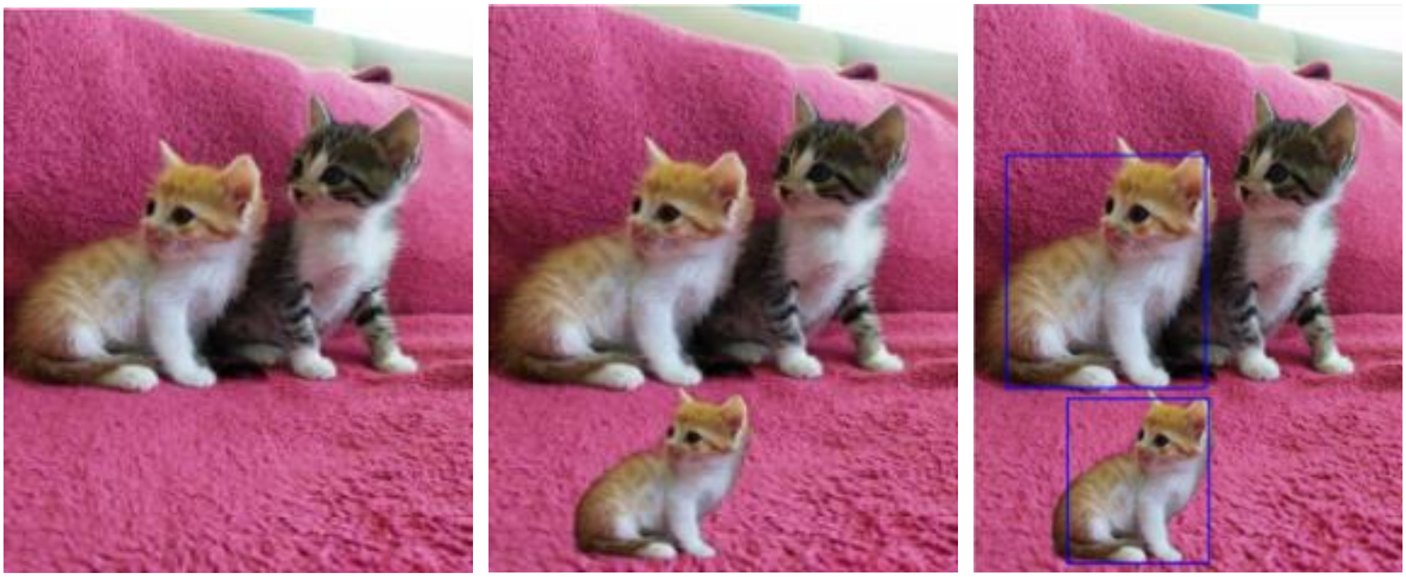


Figure 7: (a) Original image (b) Forged image (c) Forged part detected after SIFT

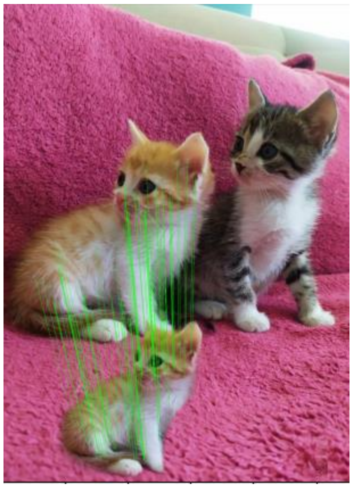


Figure 8: Matching of similar features

Figure 9: show the result with rotate:

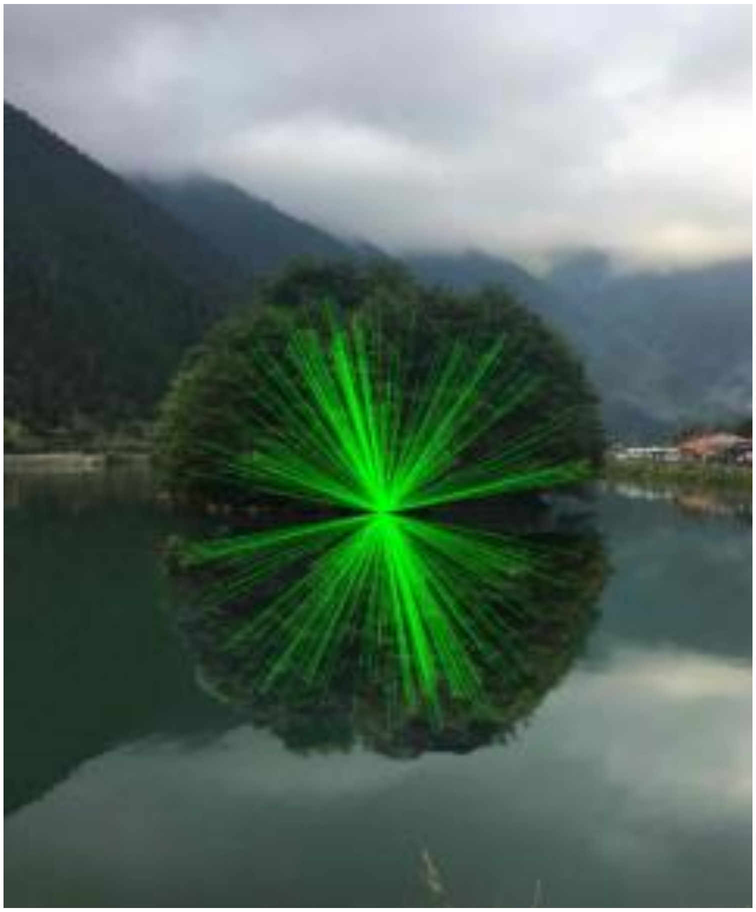
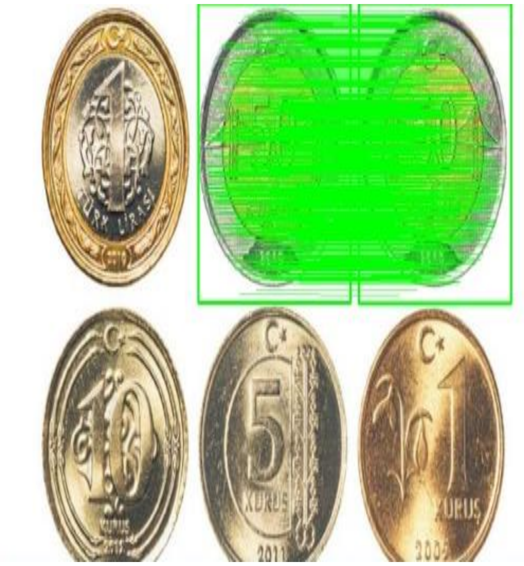
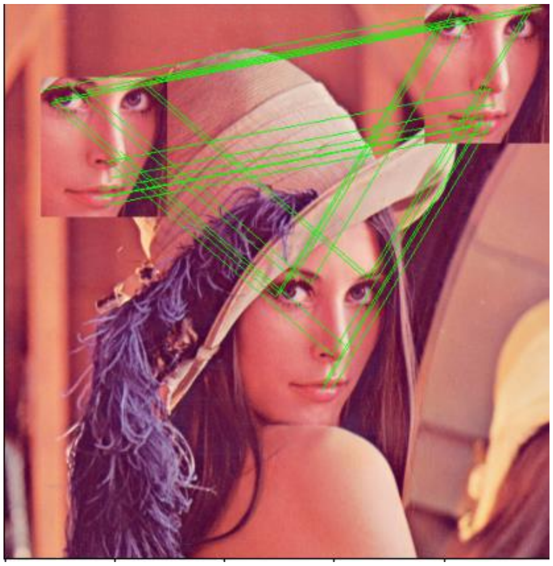


Figure 9: Show the result with rotate:





❖ CONCLUSION:

In the proposed work, a SIFT algorithm is implemented to detect the copy move forgery in digital images. Proposed algorithm is tested on various images of standard dataset. simulation results show that the forged region is detected accurately by using the SIFT algorithm. Robustness is also checked by applying the geometric transform to the copied region of an image. the accuracy rate has been found higher than the existing algorithm. It is concluded that the proposed system shows considerably high improvement than the existing systems. Average time is calculated as 45 seconds to process the input by the proposed system which is again less than that of existing systems. In proposed work, clusters and their mean values are used to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that contain forgery with geometric transformations.