COPY-MOVE IMAGE FORGERY DETECTION USING SIFT DESCRIPTORS

K. Parkavi and A. Ramanan
Department of Computer Science, Faculty of Science, University of Jaffna
parkavi113@gmail.com

Introduction

Image manipulation and editing is very common in this multimedia era. Forgery images are known as manipulated images if the semantics of the original image is changed. This study is developed to detect copy-move image forgery detection under keypoint-based approach using SIFT descriptors since block-based techniques have high computational complexity.

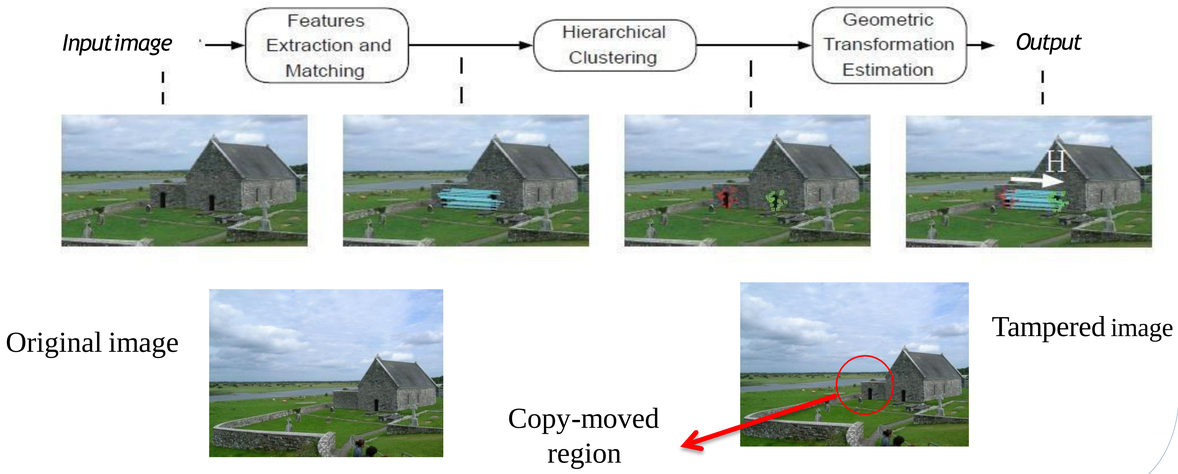
Background

There are two main approaches for image forgery detection: Active and passive approaches [1]. Copy-move falls under passive approach. Image manipulation can be achieved through image enhancing, image retouching, image splicing, image morphing and copy-move. Certain region(s) can be copied and pasted in another region of the same image so as to hide or misinterpret a particular image. This manipulation technique is known as copy-move forgery. To detect copy-move images there are two main approaches: Keypoint feature extraction and block-based features. In keypoint-based detection, keypoints are extracted using either scale invariant feature transform (SIFT) or speeded up robust features (SURF), and in block-based detection a given image is subdivided into blocks using various block-based techniques. Even though block based detection gives better performance, it has high computational complexity.

Methodology

- Given test image is first preprocessed. Preprocessing includes changing the RGB image into grayscale image. This step is optional if the image is already a grayscale image.
- For the preprocessed image, a set of keypoints and corresponding SIFT descriptors are extracted. Matching operation is performed in the SIFT space among the descriptors in order to identify local patches that are similar. The best candidate match for each keypoint is found by identifying its nearest neighbor from all the rest of the keypoints of the image, which is the keypoint with the minimum Euclidean distance in the SIFT space. To identify among multiple copied regions, g2NN-ratios [2] between the adjacent pairs of distances are found. g2NN ratio is the ratio between two adjacent distances.
- The ratios that are greater than a predefined threshold value are chosen for the next step clustering. An agglomerative hierarchical clustering is performed on spatial locations of the matched keypoints to identify possible cloned areas. Based on the adopted linkage method, a specific tree structure is obtained. An appropriate cut-off value is chosen and number of matching keypoints is determined.
- Forgery is detected through previously obtained number of clusters and number of keypoints in each cluster. If there are at least two clusters and in each cluster if there are at least three pairs of matching keypoints, then such image is detected as a forged image. If an image has copy-moved region, there should be at least one similar cluster and to detect forgery there should be at least three pairs of matching keypoints. Therefore this limitation is achieved.

Methodology…



Objective

To improve the overall performance in detecting the copy-move forgery images using SIFT features.

Experimental Setup

The experiment has been carried out in such a way training data is 70% of the dataset and testing is 30% of the dataset.

Dataset:

MICC-F220 dataset [2]

There are 220 images with 110 tampered and 110 original images with the resolution varies from 722 × 480 pixels to 800 × 600 pixels and on average, 1.2% size of the whole image is covered by forged region.

The dataset is divided into two classes namely "Original" and "Tampered" where all the non-tampered images were grouped into the first category and the tampered images were grouped into the other.

Testing Results

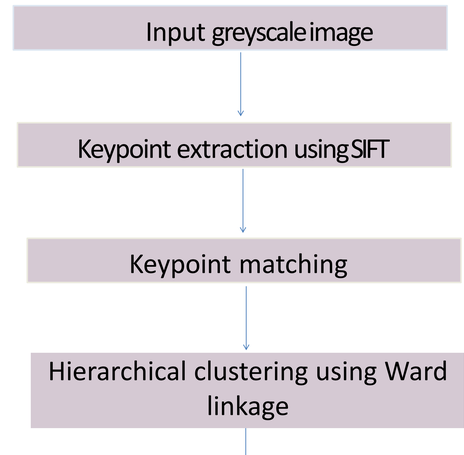
Performance in detecting the forged image using, 'Ward linkage' hierarchical clustering and one-versus-one SVMs.
An image is considered as a copy-move attacked image if the method detects two or more clusters with at least three pairs of matching keypoints.
The performance indicates the True Positive Rate (TPR) which correctly classifies the tampered images in the dataset.
The table shows that choosing cut-off threshold of 2.2 in hierarchical clustering gives better performance in detecting copy-moved images. The cut-off threshold here is referred to the point at which the obtained dendrogram is cut to determine the number of clusters in a particular image.

Cut-off threshold	Performance
2.2	38%
2.5	51%
2.8	42%
3.2	35%

Conclusion

- This method shows a good performance in detecting copy-moved forgery images even though the performance can be further improved.
- The performance can be further improved by iterating the method for various linkage methods and estimate the best cut-off threshold.
- This method falsely detect an original image as tampered when there are two identical regions or objects placed in a particular image.

Methodology…



References

1. V. Christlein and J. Jordan, "An Evaluation of Popular Copy-move Forgery Detection Approaches," IEEE Transactions on information forensics and security, pp. 1-26, 2012.
2. I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, Sep.2011.
3. S.Kumar, J.Desai., and S.Mukherjee , "A Fast Keypoint Based Hybrid Method for Copy Move Forgery Detection," International Journal Computing Digital System, 4(2), 2015.
4. B. Yang, X.Sun, H. Guo, Z. Xia and X.Chen, "A copy-move forgery detection method based on cmfd-sift," Multimedia Tools and Applications pp. 1–19, 2017.
5. J.Zhao and W. Zha, "Passive forensics for region duplication image forgery based on Harris feature points and Local Binary Patterns," in Mathematical Problems in Engineering, pp. 1–12, 2013.