Enhancing Image Copy-Move Forgery Detection Efficiency through Key Point Clustering and Similar Neighborhood Algorithm

Salkapuram Chaitanya

Department of Computer Science Sri Venkateswara University, Tirupati

Abstract— *We propose a fast and effective method for detecting copy-move forgery in images. By adjusting the contrast threshold and resizing the input image, we ensure that key points are generated even in small or smooth regions. Our hierarchical matching approach addresses key point matching challenges, while an iterative localization technique reduces false alarms and accurately identifies tampered regions. Extensive experiments validate the efficiency and accuracy of our method.*

I. INTRODUCTION

The rise of image editing software has made digital image forgery inexpensive and common. Copy-move forgery, where parts of an image are duplicated within the same image, is a prevalent manipulation. Detecting such forgeries, especially in cases involving small or smooth regions, or severe attacks like scaling and rotation, is challenging. Existing methods fall into two categories: dense-field and sparse-field approaches. Dense-field methods are accurate but complex, while sparse-field methods are less accurate. Our work focuses on key point-based algorithms, aiming to improve accuracy in detecting copy-move forgeries involving small or smooth regions as shown in Fig. 1. The main drawbacks of the existing key point-based copy-move forgery detection methods can be summarized as follows:

1) They fail to generate a sufficient number of key points (hence matched pairs) in those small or smooth copy move regions, causing detection failure;
2) It is very difficult (even impossible) to find a *universally good* clustering/segmentation algorithm and associated parameters applicable for all images. This is because the copy-move regions can be of any sizes, and can be highly diverse from the textures. In addition, the number of copy-move regions is typically unknown; properly performing the clustering in this case is difficult;
3) The existing key point-based methods lack of reliable affine matrix validation and inliers selection, in the sense that some outliers could be treated as inliers by the existing holography estimation techniques (e.g., RANSAC), causing a high false alarm rate. In this paper, we propose an efficient and accurate key point-based method for image copy-move forgery detection and localization, achieving consistently good performance even if the copy-move forgery only involves smooth or small regions, or the forged images have been processed by some. severe attacks (e.g., large-scale resizing and heavy noise addition presents the framework of our proposed image forgery detection scheme, which follows the classic workflow, namely, 1) feature extraction; 2) feature matching; and 3) forgery localization. Our main contribution lies in designing novel and sophisticated solutions for *all* these three steps. At the first stage, we design a simple yet effective way to extract a sufficient number of SIFT key points, even in smooth and small regions, by lowering the *contrast threshold* and rescaling the input image. At the second stage, a novel hierarchical point matching strategy is proposed to solve the *key point matching problems* over a massive number of key points. At the third stage, a novel iterative holography estimation and a copy-move localization technique are suggested, without involving any clustering and segmentation procedures. By fully exploiting the robustness properties (including the dominant orientation and the scale information) and the color information of each key point, our proposed method achieves very accurate detection results at considerably lowered computational cost. Extensive experimental results demonstrate that our proposed scheme leads to a higher True Positive Rate (TPR) and a lower False Positive Rate (FPR) simultaneously in most of the cases, compared with both the existing dense-field and key point-based approaches. *Difference from the Conference Version:* Portions of the work presented in this paper have previously appeared in as a conference version. We have substantially refined the paper in terms of both technical and experimental parts. The primary improvements can be summarized as follows. First of all, we carefully present the strategy to select inliers.

II. PROPOSED WORK

We developed a quick and efficient key point-based forgery detection method. By adjusting the SIFT algorithm, we showed it can detect enough key points even in smooth or small regions by tweaking contrast and resizing. We measured detection performance at both image and pixel levels, focusing on accuracy in recognizing forgeries and localizing them

Advantages:

- The matching procedure is of very low computational and effective to alleviate the critical matching problems.
- A large number of matches are found by resorting to the scale clustering strategy, showing its effectiveness to migrate the key point matching problem.
- It can be readily figured out that the computational cost is significantly reduced by the overlapped gray level clustering
- The relatively low computational cost of running individual.

III. METHODOLOGY

3.1 Input image

Import two images' files one is normal image another one is tempered image of that original image.

3.2 Pre-processing

In pre-processing we firstly resize the original image then we enhanced that image towards contrast and remove noise using Gaussian filter.

3.3 Feature matching using sift

The SIFT algorithm can be roughly divided into four phases:

i) candidate keypoint identification through the scale space extrema detection;

ii) key points refinement according to the contrast and edge thresholds;

iii) dominant orientation assignment of each keypoint; and

iv) feature descriptor generation.

3.4 Scale Space Extrema Detection

At phase i), the candidate key points are identified at different scales. Given an input image **I**, successive Gaussian-blurred images are generated by repeatedly convolving **I** with Gaussian filters at multiple scales. Then, the candidate SIFT key points are selected as local extrema. At phase ii), all the candidate key points are further refined according to a contrast threshold and an edge threshold. This procedure plays a key role for rejecting unstable extrema in the SIFT algorithm.

At phase iii), a dominant orientation is assigned to each survived keypoint to achieve rotation invariance. An orientation histogram is then constructed by gathering the gradient orientation information of points in a local window centered at the SIFT keypoint. The peak in the orientation histogram corresponds to the dominant orientation. At phase iv), a 128-dimensional descriptor is calculated by encoding the surrounding information in a local area centered at the SIFT keypoint.

3.5 SIFT Feature Matching

To find a reliable match (may not exist though) of the keypoint **k**, simply evaluating the distances with the other (n −1) key points against a global threshold does not perform well in the high dimensional feature space. The

Widely used matching algorithm was suggested in the original SIFT, where the matching procedure is conducted by evaluating the ratio of the closest distance to the second closest one. The rationale behind is that for those false matches, there will very likely be several other false matches with similar distances. This is because the distances are computed.

3.6 Key point Descriptor

Now keypoint descriptor is created. A 16x16 neighbourhood around the keypoint is taken. It is divided into 16 sub-blocks of 4x4 sizes. For each sub-block, 8 bin orientation histogram is created. So a total of 128 bin values are available. It is represented

as a vector to form keypoint descriptor. In addition to this, several measures are taken to achieve robustness against illumination changes, rotation etc

3.7 Keypoint Matching

Key points between two images are matched by identifying their nearest neighbours. But in some cases, the second closest-match may be very near to the first. It may happen due to noise or some other reasons. In that case, ratio of closest-distance to second-closest distance is taken.

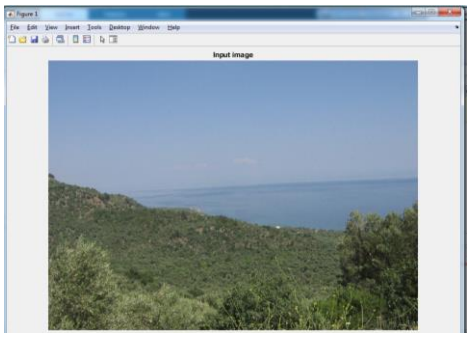
3.8 Copy detection

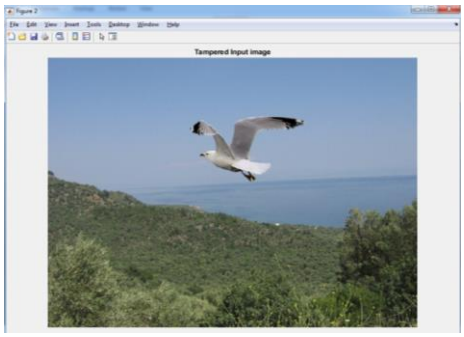
Our method effectively detects extremely smooth copy-move forgeries, even when the variance of the copied region is as low as 1. We continuously smooth the regions using Gaussian filters and achieve high localization accuracy, as demonstrated by pixel-level F1 curves

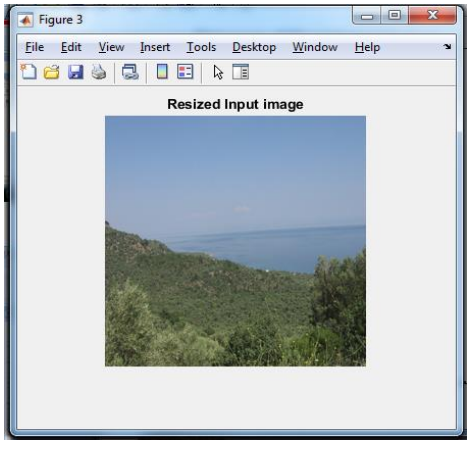
3.9 Localization

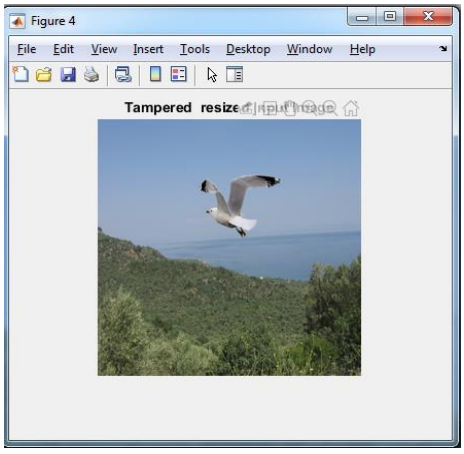
We propose a novel forgery localization algorithm for dense fields that avoids clustering or segmentation. It consists of two phases: 1) constructing suspicious regions based on scale information, and 2) refining these regions by validating color consistency."

IV. IMPLEMENTATION









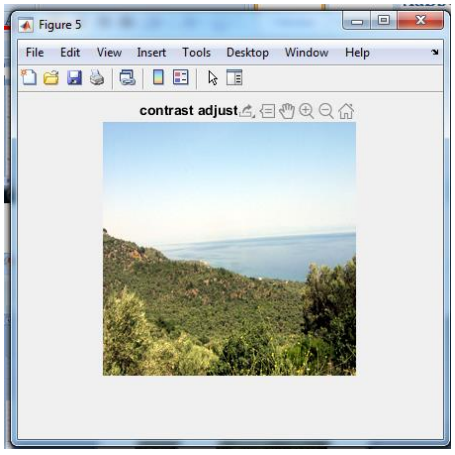


Figure 5
File Edit View Insert Tools Desktop Window Help
contrast adjust

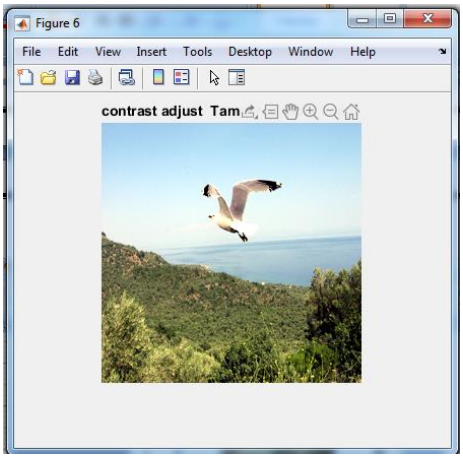


Figure 6
File Edit View Insert Tools Desktop Window Help
contrast adjust Tam

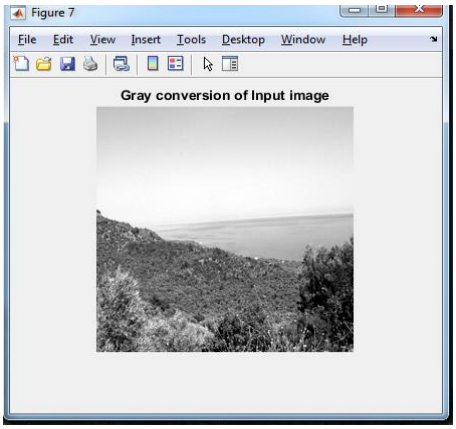


Figure 7
File Edit View Insert Tools Desktop Window Help
Gray conversion of Input image

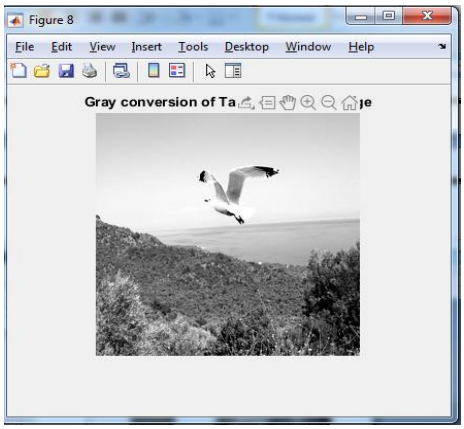


Figure 8
File Edit View Insert Tools Desktop Window Help
Gray conversion of Ta je

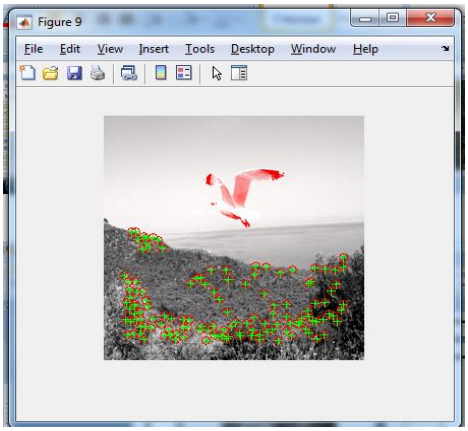


Figure 9
File Edit View Insert Tools Desktop Window Help

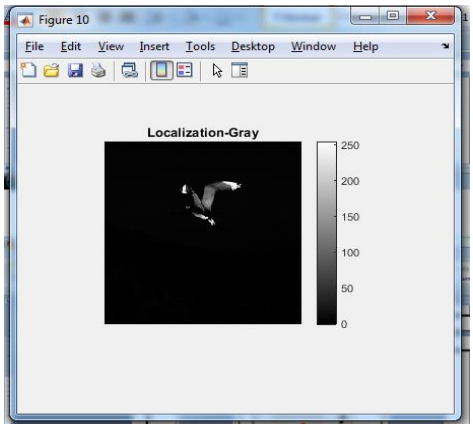
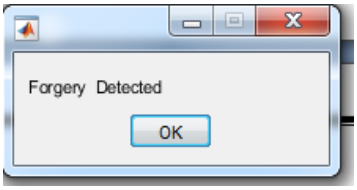


Figure 10
File Edit View Insert Tools Desktop Window Help
Localization-Gray
250
200
150
100
50
0


Forgery Detected
OK

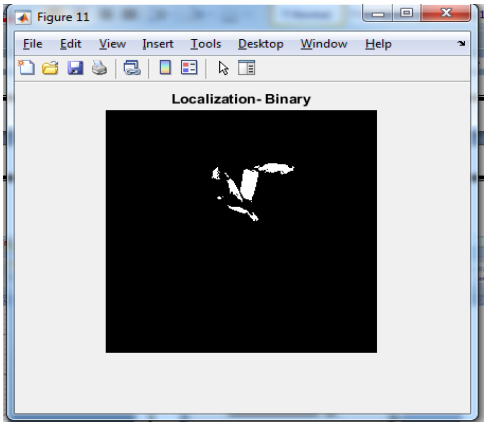
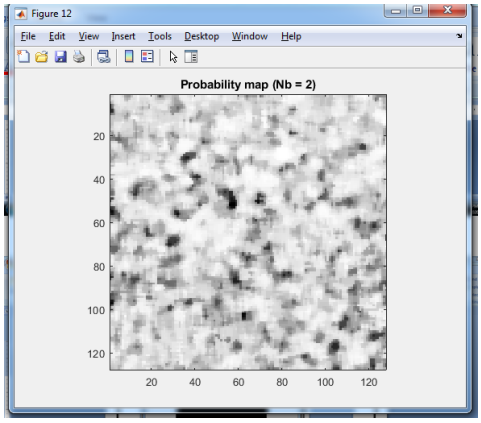
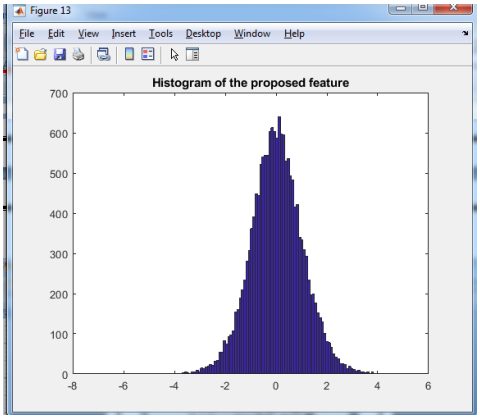


Figure 11
File Edit View Insert Tools Desktop Window Help
Localization- Binary





V. CONCLUSION

We introduced a quick and effective key point-based forgery detection method. By tweaking the SIFT algorithm, we showed it can detect enough key points even in smooth or small regions. We also proposed a new matching strategy and an iterative localization scheme to improve accuracy without clustering or segmentation. Our approach leverages SIFT's robustness and color information for high detection accuracy, as shown in extensive experiments.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, 2003, pp. 10.

[2] G. Muhammada, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digit.Invest., vol. 9, no. 1, pp. 49–57, 2012.

[3] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[4] Y. Li, J. Zhou, A. Cheng, X. Liu, and Y. Y. Tang, "SIFT keypoint Removal and injection via convex relaxation," IEEE Trans. Inf. Forensics Security, vol. 11, no. 8, pp. 1722–1735, Aug. 2016.

[5] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy move forgery detection scheme," IEEE Trans. Inf. Forensics Security,vol. 10, no. 3, pp. 507–518, Mar. 2015.

[6] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[7] Y. Li, J. Zhou, and A. Cheng, "SIFT keypoint removal via directed graph construction for color images," IEEE Trans. Inf. Forensics Security,vol. 12, no. 12, pp. 2971–2985, Dec. 2017.

[8] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, NH, USA,Tech. Rep. TR2004-515, 2004.

[9] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Sci. Int., vol. 233, nos. 1–3, pp. 158–166, 2013.

[10] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., Apr. 2009, pp. 1053–1056.