AN IMAGE FORENSICS TOOL FOR COPY-MOVE DETECTION AND LOCALIZATION

Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, Giuseppe Serra

Media Integration and Communication Center (MICC), University of Florence, Italy

ABSTRACT

We demonstrate a novel image forensics tool for copy-move detection and localization. The proposed method can determine if such tampering has occurred and which image patches are involved, and it also recovers which geometric transformation was used to perform cloning.

Index Terms— Image tampering, image forensics, copy-move attack, authenticity verification.

1. INTRODUCTION

One of the principal problem in image forensics is determining if a particular image is authentic or not [1], which could be a crucial task when images are presented as basic evidence to influence judgment (e.g. in a court of law). Special attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to make a duplication or to cancel something that was awkward (*copy-move* attack). Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on Scale Invariant Features Transform (SIFT) is demonstrated. Such a method allows both to understand if a copy-move attack has occurred and, furthermore, to recover which has been the geometric transformation happened to perform cloning. Our technique is able to precisely individuate the feigned area and, in addition, to estimate the geometric transformation parameters with high reliability. Our method, in contrast to other related approaches, also deals with multiple cloning (an example is given in Fig. 1). For more detail, see [2].

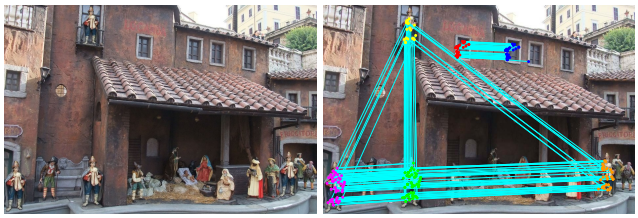

Fig. 1. An example of image tampering with multiple cloning. Original image (left) and tampered image (right).

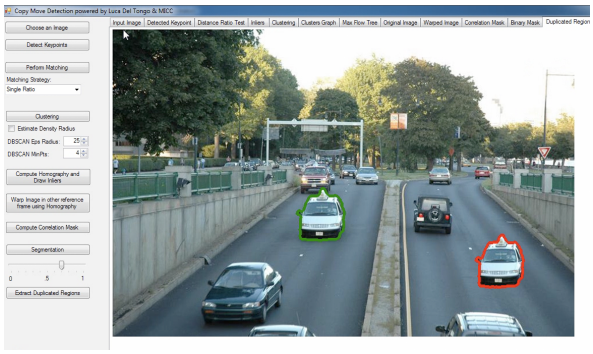

Fig. 2. A screenshot of the interface of our system.

2. THE METHOD

The proposed approach is based on the SIFT algorithm to extract robust features which can allow to discover if a part of an image was copy-moved. In fact, the copied part has basically the same appearance of the original one, thus keypoints extracted in the forged region will be quite similar to the originals. The first step consists of SIFT features extraction and keypoint matching, the second step is devoted to cluster such keypoints and assess forgeries detection, while the third one is in charge to estimate the occurred geometric transformation, if a tampering has been individuated. Finally the tampered area is localized by applying the estimated geometric transformation and calculating correlation masks between the original and the transformed image.

3. DEMONSTRATION

We will show a live demo in which users can try out the tool with a large set of tampered images. We will show the robustness of the proposed approach against several different forgeries in a realistic scenario.

4. REFERENCES

[1] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: a booklet for beginners," in *Multimedia Tools and Applications*, 2011, vol. 51, pp. 133–162.

[2] 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 Transactions on Information Forensics and Security*, vol. in press, 2011.