J. Vis. Commun. Image R. 29 (2015) 16–32

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes ☆

Ewerton Silva, Tiago Carvalho *, Anselmo Ferreira, Anderson Rocha

RECOD Lab., Institute of Computing, University of Campinas, Av. Albert Einstein, 1251, Cidade Universitária "Zeferino Vaz", Campinas, SP 13083-852, Brazil

A R T I C L E I N F O

Article history:
Received 5 November 2013
Accepted 22 January 2015
Available online 7 February 2015

Keywords:
Copy-move forgery detection
Interest points
Speed-up Robust Features
Keypoints clustering
Multi-scale analysis
Scale-space
Voting processes
Realistic dataset

A B S T R A C T

This work presents a new approach toward copy-move forgery detection based on multi-scale analysis and voting processes of a digital image. Given a suspicious image, we extract interest points robust to scale and rotation finding possible correspondences among them. We cluster correspondent points into regions based on geometric constraints. Thereafter, we construct a multi-scale image representation and for each scale, we examine the generated groups using a descriptor strongly robust to rotation, scaling and partially robust to compression, which decreases the search space of duplicated regions and yields a detection map. The final decision is based on a voting process among all detection maps. We validate the method using various datasets comprising original and realistic image clonings. We compare the proposed method to 15 others from the literature and report promising results.

1. Introduction

In 2004, a research team from Seoul National University led by professor Woo-Suk Hwang became famous publishing in the academic journal *Science* [1], papers showing strong advances in stem cells research. Some months later, however, investigations revealed that some images, which depicted important results of the research, have very likely been tampered with. The scandal and the pressure of the scientific community resulted in paper retractions by *Science* in 2006, and in the professor's dismissal in that same year [2–4].

The above event has direct connection to the technological improvements that our society have been observing. Advanced technology and software have provided users with an active role in the image handling process, from simple naïve adjustments to realistic image manipulations produced with criminal intents.

Copy-move forgery, also known as cloning, is one of the easiest, yet powerful, ways to create fake images. It consists of copying segments of an image and pasting them elsewhere in the same image [5]. The objectives of this tampering are hiding, duplicating or moving elements depicted in the image. Fig. 1, shows a copy-move forgery example.

As only copying and pasting are usually not enough to produce realistic clonings, several additional operations are employed to fill this requirement. For example, if one intends to conceal an element by overlapping it with a texture-like segment (e.g., foliage, sand, etc.), it might be necessary to match the segment with its new neighborhood. That could be accomplished by rotating, resizing, flipping or blurring the copied patch before pasting it. Such transformations also reduce visual traces of tampering. Furthermore, as the cloning is finished, the author could add Gaussian noise or save the image in a lossy compression format like JPEG. This would make the cloning detection even harder to be achieved visually and by computer methods as the copied information is well matched to the background and the compression artifacts make it harder to separate natural telltales resulting from the cloning from the ones resulting from the compression.

Several methods from the literature deal only with simple copy-move forgery scenarios, while other approaches present relevant contributions toward the detection of sophisticated clonings, but still having major limitations. In this sense, we propose a new approach to detect copy-move forgeries in digital images that is focused mainly on investigating and spotting out traces of copy-move forgeries aided by complex operations, such as rotations, resizings and combinations of them. We tackle this problem by using a strategy based on a multi-scale analysis and a voting process. Given a suspicious image, we extract representative interest points robust to scale and rotation transformations from it. Next, we cluster the correspondent points into regions considering

☆ This paper has been recommended for acceptance by Yehoshua Zeevi.

* Corresponding author.

E-mail addresses: ewerton.silva@students.ic.unicamp.br (E. Silva), tjose@ic.unicamp.br (T. Carvalho), anselmoferreira@ic.unicamp.br (A. Ferreira), anderson.rocha@ic.unicamp.br (A. Rocha).

http://dx.doi.org/10.1016/j.jvcir.2015.01.016

the following geometric constraints: (i) the spatial distance between interest points; (ii) the inclination of the line that links such points relative to the *x*-axis. We also construct a multi-scale pyramid to represent the image scale-space. Each region (cluster) from each scale is examined as a cloning candidate using a descriptor robust to rotation, scaling and compression. This process decreases the search domain and yields a detection map. The final decision is provided by a voting step among all detection maps, in which a pixel is considered as tampered as long as it is marked so in the majority of the pyramid scales.

To validate the proposed method, we have built a dataset comprising 216 realistic cloning images. Using such dataset, we show qualitative and quantitative experiments and we compare our proposed approach to 15 other methods in the literature. Such dataset is publicly available and was used in the *1st IEEE Intl. Image Forensics Challenge (IFC)*.[1] We also validated the methods on a number of freely available datasets proposed by [6]. All validations considered scenarios divided by operations (simple copy-paste, resizing, rotation, compression) and also combined scenarios with different combinations of operations.

The main contributions of this paper include:

- the development of a new and effective approach, which combines well-founded literature techniques in a novel way, to detect copy-move forgeries able to deal with rotations, resizings, and compression simultaneously;
- the development of a dataset comprising hundreds of realistic copy-move forgeries[2];
- a comparison of the proposed method to 15 others in the literature on different and complex freely available datasets showing their pros and cons on diverse scenarios.

This paper is organized as follows. First, we provide details about the copy-move forgery detection problem and show related work in Section 2. In Section 3, we introduce the new methodology for identifying copy-move forgeries. We present qualitative and quantitative experiments with our method and compare it to 15 others from the literature in Section 4. In Section 5, we conclude the paper and expose some ideas for future work.

2. Related work

The literature has been concerned with copy-move forgery detection in terms of the additional operations often applied to the falsification. Rotation, resizing, horizontal/vertical flipping, edge blurring and white Gaussian noise insertion are the main transformations used to give realism to manipulated images, thus expanding visual and computing efforts to check the image's authenticity. Still, there is the common JPEG compression procedure, which also changes pixel values. The challenge with such operations relies on the fact that, once they are applied, the correspondences between cloned segments become hard to spot out. For instance, a rotation modifies pixel values and positions compared to the original segment.

To deal with this problem, two different schemes are largely adopted in the literature: a block-based comparison and a keypoint-based comparison.

2.1. Block-based comparison schemes

Most of the approaches are included in this category. The main difference among them is the strategy used to describe the blocks of pixels. Fridrich et al. [7] proposed the *Exact Match*, which can be taken as the basis-algorithm for finding duplicated regions. First, the authors employed a square sliding window to collect image blocks, which were gradually stored in a matrix. After all possible blocks have been collected, the matrix was lexicographically sorted, and two consecutive identical lines were deemed as cloned regions. This approach, however, did not deal with additional manipulations (e.g., JPEG compression). To provide some robustness to that, the authors proposed the *Robust Match*: a second approach in which they used the *Discrete Cosine Transform* (DCT) to characterize each block. Using DCT, the method was able to find some duplicated regions under JPEG compression, but it still failed in Gaussian noise, rotation and resizing scenarios.

Popescu and Farid [8] used *Principal Component Analysis* (PCA) to reduce the dimensionality of the blocks and to produce a new representation of them. This increased the robustness of the method under JPEG compression and Gaussian noise addition. Luo et al. [9] extract seven features based on the average of the pixel intensity in each RGB channel, and on some directional information, from each block. The authors reported high detection accuracy rates for JPEG compression, additive Gaussian noise, Gaussian blurring and mixed operations. However, this approach did not tackle rotations, resizings, and flippings.

Mahdian and Saic [10] calculated 24 Blur moment invariants to generate a feature vector representation of each block of pixels. The final feature vector was 72-dimensional, since the calculation of the invariants were performed in each RGB (*red*, *green*, and *blue*) channel separately. Moreover, to reduce the size of this representation, PCA was also employed. By taking this approach, duplicated regions could be effectively pointed out even in the presence of blurring, additive Gaussian noise and JPEG compression of the image. On the other hand, rotation, resizing, and flipping operations were not considered in the experiments.

Zhang et al. [11] proposed an approach based on the analysis of the image's recursive sub-band by using *Discrete Wavelet Transform* (DWT) and the calculus of phase correlations. The performed experiments showed the method's robustness under JPEG compression and blurring, only. Li et al. [12] also used DWT along with *Singular Value Decomposition* (SVD) to decrease the amount of information examined and to generate a more robust block representation. The approach was mainly effective in the cases of JPEG compression with quality factors greater than 70%.

Kang and Wei [13] used SVD to extract feature vectors from overlapping blocks and detect copy-move regions. According to the authors, SVD provides algebraic/geometric invariance, and insensitiveness to noise which is useful in copy-move detection. However, results using rotated and resized cloned parts were not reported.

Ryu et al. [14] proposed to use Zernike moments, which are invariant to rotations to detect duplicated elements. Such work was overhauled later in [15], with a more reliable block matching procedure that incorporates the phase of Zernike moments into a feature space error-reduction procedure, yielding better accuracies. However, resizing was not treated by this method.

Bravo-Solorio and Nandi [16] took the correlation coefficient of the *Fourier Transform* (FT) as the similarity measure between blocks of pixels in log-polar form. They further analyzed and discarded blocks in which the entropy was lower than a threshold. The experiments showed robustness to deal with flipping and simple copy-move operations, but problems when dealing with resizing and rotation.

Bashar et al. [17] proposed an approach where features can be provided by *Discrete Wavelet Transform* (DWT) or by *Kernel Principal Component Analysis* (KPCA). The detection process uses these features individually to characterize blocks of pixels. Features extracted from blocks are organized into a matrix and

[1] http://ifc.recod.ic.unicamp.br/fc.website/index.py.

[2] Upon acceptance of this paper, the will be freely available from http://dx.doi.org/10.6084/m9.figshare.978736.