Available online at www.sciencedirect.com
ScienceDirect
Forensic Science International 171 (2007) 180–189
Forensic Science International
www.elsevier.com/locate/forsciint

Detection of copy–move forgery using a method based on blur moment invariants

Babak Mahdian *, Stanislav Saic

Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod vodárenskou věží 4, 182 08 Prague 8, Czech Republic

Received 5 June 2006; received in revised form 9 October 2006; accepted 7 November 2006
Available online 11 December 2006

Abstract

In our society digital images are a powerful and widely used communication medium. They have an important impact on our life. In recent years, due to the advent of high-performance commodity hardware and improved human–computer interfaces, it has become relatively easy to create fake images. Modern, easy to use image processing software enables forgeries that are undetectable by the naked eye. In this work we propose a method to automatically detect and localize duplicated regions in digital images. The presence of duplicated regions in an image may signify a common type of forgery called copy–move forgery. The method is based on blur moment invariants, which allows successful detection of copy–move forgery, even when blur degradation, additional noise, or arbitrary contrast changes are present in the duplicated regions. These modifications are commonly used techniques to conceal traces of copy–move forgery. Our method works equally well for lossy format such as JPEG. We demonstrate our method on several images affected by copy–move forgery.

Keywords: Authentication; Image forensics; Image tampering; Duplicated image regions; Copy–move forgery; Image moments

1. Introduction

In our society digital images are a powerful and widely used medium of communication, containing a huge amount of information. They are a compact and easy way in which to represent the world that surrounds us. The question is, how much can we trust a photograph which is not obtained from a secure source.

Nowadays, images have an important impact on our society and play a crucial role in most people's lives. Without a doubt, image authenticity is significant in many social areas. For instance, the trustworthiness of photographs has an essential role in courtrooms, where they are used as evidence. Every day newspapers and magazines depend on digital images. In the medical field physicians make critical decisions based on digital images. As a consequence, we should pay a special attention to the field of image authenticity.

As pointed out in [1], photograph tampering has a long history. In today's digital age, due to the advent of low-cost, high-performance computers, more friendly human–computer interface, and the availability of many powerful and easy to control image processing and editing software packages, digital images have become easy to manipulate and edit even for non-professional users. It is possible to change the information represented by an image and create forgeries, which are indistinguishable by naked eye from authentic photographs. This introduces a need for a reliable tamper detection system for digital images. Such a system can determine whether an image has been tampered with. A reliable forgery detection system will be useful in many areas, including: forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, medical imaging, and journalism. Such a system can evaluate the authenticity of digital image.

Existing digital forgery detection methods are divided into active [2–6], and passive (blind) [7–10] approaches. Active approaches could be further divided mainly into digital watermarks and signatures. The passive (blind) approach is regarded as the new direction. In contrast to active approaches,

* Corresponding author. Tel.: +420 266052211; fax: +420 284680730.
E-mail addresses: mahdian@utia.cas.cz (B. Mahdian), ssaic@utia.cas.cz (S. Saic).

0379-0738/$ – see front matter © 2006 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.forsciint.2006.11.002

Fig. 1. An example of a copy–move forgery. The photograph of crime scene (from [11]) is altered by the copy–move forgery. The original (left) and forged version (right).

passive approaches do not need any explicit priori information about the image. Therefore, it does not require watermarks or signatures.

It is obvious that there are many ways to manipulate and alter digital images. An attempt of categorization has been proposed by Farid [1]. As mentioned, passive methods are regarded as a new approach and have not yet been thoroughly researched by many. Different methods for identifying each type of forgery must be developed. Then, by fusing the results from each analysis, a decisive conclusion may be drawn.

In this work we focus on detecting a common type of digital image forgery, called copy–move forgery. In copy–move forgery, a part of the image is copied and pasted into another part of the same image, with the intention to hide an object or a region of the image. Fig. 1 shows an example. We can determine whether an image contains this type of forgery by detection of duplicated regions. Duplicated regions may not always match exactly. For example, this could be caused by a lossy compression algorithm, such as JPEG, or by possible use of the retouch tool.

The importance of digital images in forensic science creates a significant need for reliable detection of copy–move forgery. Due to the possibilities of today's standard image processing software, the creation of a high quality copy–move forgery has became particularly easy. Therefore, we can expect that this type of tampering will become more common. For example, with infringement of copyright, blackmail, insurance fraud and other schemes based on digital forgery. However, note that when creating high quality and consistent forgeries, several types of tampering techniques are employed simultaneously. For example, image splicing in combination with copy–move forgery and localized image retouching techniques. Thus, when we consider copy–move forgery, we often assume this tampering technique has been used simultaneously with others. Therefore, by having a reliable technique to detect the copy–move forgery, we will be able to detect forgeries that contain among others this type of tampering.

Fig. 1 shows an example of the use of copy–move forgery in a forensic investigation. Here the photograph of a crime scene is tampered with using the copy–move technique with; intention is to hide some important objects in the photograph. We believe that a reliable tamper detection system will useful in forensic applications, where making decisions are based or affected by imaging.

As pointed out in [7], ideal regions for using copy–move forgery are textured areas with irregular patterns, such as grass. Because the copied areas will likely blend with the background it will be very difficult for the human eye to detect any suspicious artifacts. Another fact which complicates the detection of this type of tampering is that the copied regions come from the same image. They therefore have similar properties, such as the noise component or color palette. It makes the use of statistical measures to find irregularities in different parts of the image impossible.

1.1. State of the art

As mentioned, despite of the strong need for a reliable detection of digital forgeries in the absence of watermarks and signatures, this area has an unexplored character. The field of copy–move forgery detection is even smaller: only two publications concerned with this topic have been found.

The first one has been proposed by Fridrich et al. [7]. This method tiles the image by overlapping blocks. The detection of duplicated regions is based on matching the quantizied lexicographically sorted discrete cosine transform (DCT) coefficients of overlapping image blocks. The lexicographically sorting of DCT coefficients is carried out mainly to reduce the computational complexity of the matching step. The second method has been proposed by Popescu and Farid [8] and is similar to [7]. This method differs from [7] mainly in the representation of overlapping image blocks. Here, the principal component transform (PCT) has been employed in place of DCT. The representation of blocks by this method has better discriminating features.

2. Detection of duplicated regions

To detect the copy–move forgery we focus our aim on detection of duplicated regions in the image. Since duplicated