Journal of Network and Computer Applications 34 (2011) 1557–1565

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A passive image authentication scheme for detecting region-duplication forgery with rotation

Guangjie Liu [a,*], Junwen Wang [a], Shiguo Lian [b], Zhiquan Wang [a]

[a] School of Automation, Nanjing University of Science & Technology, Nanjing 210094, China
[b] France Telecom R&D (Orange Labs) Beijing, Beijing 100080, China

ARTICLE INFO

Article history:
Received 6 March 2010
Received in revised form
9 August 2010
Accepted 1 September 2010
Available online 7 September 2010

Keywords:
Region duplication
Image forensics
Passive authentication
Hu moment
Rotation
Robustness

ABSTRACT

Region-duplication forgery is one of most common tampering artifices. Several methods have been developed to detect and locate the tampered region, while most methods do fail when the copied region is rotated before being pasted because of the de-synchronization in the searching procedure. To solve the problem, the paper proposes an efficient and robust passive authentication method that uses the circle block and the Hu moments to detect and locate the duplicate regions with rotation. Experimental results show that our method is robust not only to noise contamination, blurring and JPEG compression, but also to the rotation. Meanwhile, the proposed method has better time performance compared with exiting methods because of the lower feature dimension.

1. Introduction

It is a very sophisticated skill to tamper images in the past film time, which usually requires the forger to have professional dark-room equipments such as the special developer, the photographic paper, and so on. With the wide application of powerful digital image processing software, such as Photoshop, it has become easier and easier to create digital forgeries from one or multiple images. The tampered image might cause some great threats. For example, in 2007, the event of South China tiger's photograph misled many people to believe the existence of wild South China tiger, while finally, the photograph was proved to be a "paper" tiger (Lian and Zhang, 2010). In 2008, Iran published a picture of missile test, which contains 4 missiles in rocketing. It is doubted that one of the missile is copied from another one (Lian and Zhang, 2010).

Through the above examples, we can find that the multimedia forgery will bring many troubles. In the photo contest, some journalists make the forgery photos, which disobey the principle of fair play. In the news reports, the forgery pictures will distort the truth and mislead public opinions. And, someone may change the person's face in a photo with another person's, and put the forged image over Internet, which also destroys the person's privacy or reputation. A faked image also may be used in the academic paper to indicate a better experimental result. Furthermore, the important object may be wiped off from an evidence image, which causes the miscarriage of the court. Thus, it is important and critical to tell "When is seeing believing?" According to the above analysis, a multimedia forensics system (MFS) is urgently needed for identification of the authenticity of a multimedia object as illustrated in Fig. 1.

Here, we just discuss the forensics of digital image. There are two kinds of techniques, the active authentication and the passive one (Lian et al., 2009). The active methods can be divided into two classes. The first class is based on digital watermarking that embeds a watermark into the image at the acquirement end and extracts it at the authentication end to check whether the image is tampered. The second class is based on the digital signature. It generates a signature at the acquirement end and regenerates another one using the same method at the authentication end. Through comparison, the authenticity of the image can be identified. The passive authentication, also called digital forensic, is the method to make authentication without any help of the additional information. The typical applications include media source identification (Ng and Tsui, 2009a,b), forgery detection (Wang et al., 2009a,b), etc. Taking image forgery detection for example, it makes use of images' distinct properties to detect unnatural operations and identify the tampered regions (Zhang and Kong, 2009; Cao et al., 2009).

* Corresponding author.
E-mail addresses: gjieliu@gmail.com (G. Liu), junwen_wang@yahoo.com.cn (J. Wang), shiguo.lian@orange-ftgroup.com (S. Lian), wangzqwhz@yahoo.com.cn (Z. Wang).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.09.001

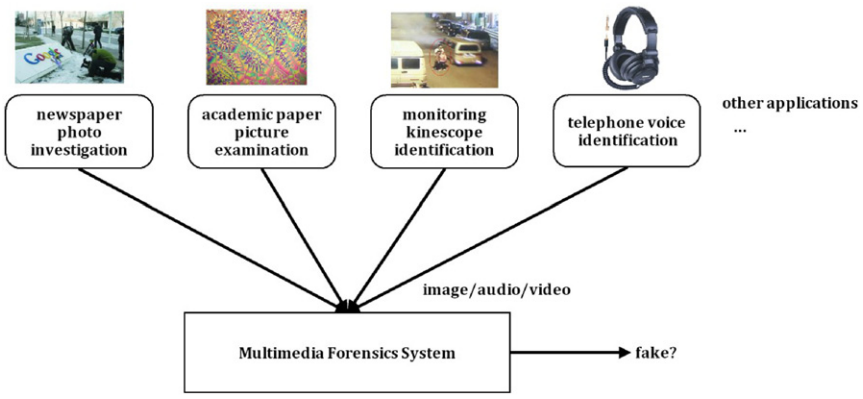

Fig. 1. Application scenarios of multimedia forensics system.

We know that in the process of a skilled forgery, besides changing the important region about the image content, there are lots of post-processing manners that can be used to remove the artificial trace. The post-processing will not make the forensic work, so how to deal with various post-processing and improve the robustness of forensic methods has become a very important subject. In this paper, we propose a method to deal with a complex region-duplication forgery including region-rotation and other kinds of post-processing.

The rest of the paper is organized as follows. In Section 2, the related work about the passive authentication and the region-duplication forgery model are introduced. The mechanism of feature extraction and the detection method are presented in detail in Section 3. In Section 4, some experimental results are given and the corresponding analysis is presented. Finally, some conclusions are drawn in Section 5.

2. Related work

In recent years, many researchers have started to develop passive techniques for detecting various forms of image forgeries. Farid et al. developed several statistical methods for detecting forgeries based on region duplication (Popescu and Farid, 2004), color filter interpolation (Popescu and Farid, 2005a,b), re-sampling (Popescu and Farid, 2005a,b) and lamp direction (Johnson and Farid, 2005). Fridrich et al. (2003) presented methods for detecting the copy-move forgery and performed the forgery detection based on the pattern noise of digital cameras' sensor (Lukas et al., 2006). Ng and Chang (2004) and Ng et al. (2005) proposed an image spicing model to detect photomontage and physics-based models to distinguish computer graphics from natural photographs. Luo et al. (2007) developed a method to detect cropped and recompressed image blocks. They also presented a new method for detecting the region-duplication forgery (Luo et al., 2006). Zhou et al. (2007) and Kirchner (2008) proposed some methods to detect re-sampling and blur. Here we mainly pay our attention to region-duplication forgery.

2.1. Model of region-duplication forgery

Luo et al. (2006) gave a model of region-duplication forgery. This model describes four basic constraints of region-duplication forgery, including the region connectivity, two regions unintersection, translation vector constraint and the duplicate region area threshold. It assumes that the largest copied region must be holeless and be pasted away from its original location without intersecting with its primer location. However, this model cannot describe the forgery when one copy region is pasted onto two places, and the copy region is rotated before being pasted.

A more comprehensive region-duplication forgery model was given by Wang et al. (2009a, b). Assuming that the translation vector threshold is $\mathbf{V}_T=[V_{tx},V_{ty}]$, and the copy-region area threshold (defined as the ratio of the copy region's area and the whole image's) is A_T, we say an image $\mathbf{I}$ is tampered to $\mathbf{I}'$ via region-duplication means, if

i) The copy region C_i, $i\in\{1,2,\ldots,n\}$ is connective and has no hole inside, and its area is larger than $A_T a(\mathbf{I})$, where $a(\mathbf{I})$ denotes the area of the image $\mathbf{I}$.

ii) Suppose the duplication of the copy region C_i is M_i, there might be many region-duplication pairs $\{C_1||M_1,C_2||M_2,\ldots,C_n||M_n\}$, $C_i,M_i\subset\mathbf{I}'$, which satisfy $C_i\neq C_j,\forall i\neq j,\ i,j\in\{1,2,\ldots,n\}$ and $C_i\cap M_i=\emptyset$. For any pair $C_i||M_i$, defining the origin of the reference frame as the rotation center, the duplication forgery can be considered as shifting after rotating, described by

$$\begin{aligned}&\forall(x,y)\in C_i,\quad f(x,y)=f'(x',y')\\&x'=x\cos\theta-y\sin\theta+\Delta_x\\&y'=x\sin\theta+y\cos\theta+\Delta_y\\&\sqrt{\Delta_x^2+\Delta_y^2}\geq|\mathbf{V}_T|\\&a(C_i)>A_T\cdot a(\mathbf{I})\end{aligned}\tag{1}$$

Here, f denotes the pixel at the position (x,y), Δ_x,Δ_y is the shift distance along x and y axis, respectively, and θ is the rotation angle.

It should be noted that in an intact forgery process, the image tampered by region-duplication artifice is often processed by other operations to eliminate the imprint caused by the forgery. The common means are lossy compressing, noise contamination, filtering and so on. Therefore the two duplicate regions are not equal exactly, and how to make the duplication detection with the inferences of post-processing has become an important issue.

2.2. Current region-duplication forgery detection methods

According to the forgery process, the similar regions have large size is more possible to be faked. Therefore the detection focuses on how to find the similar regions with as short time as possible. For improving the robustness and decreasing the computational complexity, Fridrich et al. (2003) analyzed the DCT coefficients of each block and proposed the method based on fuzzy matching. The method just worked well under the JPEG compression attack. Popescu and Farid (2004) proposed to capture the main feature of image blocks by principal component analysis (PCA), and complete