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