Chapter 18
Efficient Image Matching Using Local Invariant Features for Copy Detection

H. R. Chennamma
University of Mysore, India

Lalitha Rangarajan
University of Mysore, India

M. S. Rao
Indian Academy of Forensic Sciences, India

ABSTRACT

Retrieval based approach has recently emerged as an attractive option for image copy detection. The Content Based Copy Detection (CBCD) can be treated as a restricted case of near duplicate image detection. Near duplicate images can be: (i) perceptually identical images (e.g. allowing for change in color balance, change in brightness, compression artifacts, contrast adjustment, rotation, cropping, filtering, scaling etc.), (ii) images of the same 3D scene (from different viewpoints). As we are searching for copies which are altered versions of the original image, the images with slight viewpoint variations of the same scene should not be retrieved. In this chapter, we focus on image matching strategy based on local invariant features that will assist in the detection of forged (copy-paste forgery) images. So far, no specific robust homography estimation method exists for this application. The state of the art methodologies tend to generate many false positives. In this chapter, we have introduced a novel strategy for pattern matching of key point distributions for copy detection. Typical experiments conducted on real case images demonstrate the success in near duplicate image retrieval for the application of digital image forensics. Efficiency of the proposed method is corroborated by comparison, with contemporary methods.

INTRODUCTION

Forensic experts believe that no criminal can do his activities without leaving evidence at the scene of crime. However, it is very difficult to trace out evidences especially in case of digital image forgeries. Nowadays, image content manipulation is a well known serious issue in digital image forensics. Such content pirating creates several near duplicate images. Usually, such near duplicate

DOI: 10.4018/978-1-60960-515-5.ch018

images are altered copies of the original image. These unauthorized copies can be detected by retrieving similar images. Thus the concept of Content Based Copy Detection (CBCD) has recently emerged as an alternative means of identifying illegal image copies. The idea is that, instead of hiding additional information (watermark) in the image to enable image tampering detection, the image as such can be used to detect tampering. A content based copy detection system works as follows: given an image registered by the owner, the system can determine whether near replicas of the image are available on the internet or given an image suspected to be a copy, the system can determine whether the original image which was used in the creation of this query image is available in the database of copyrighted images.

Although, the frameworks of CBCD are considered to be similar to those of Content Based Image Retrieval (CBIR), there are some differences between CBCD and CBIR. An image copy detector searches for near replicas of an image, whereas CBIR not only retrieves image replicas, but also images that share same or similar semantics. Figure 1 and Figure 2 shows an example of a tampered image and a similar (but not a copy) image respectively. According to the definition in literature (Joly et al., 2007), a copy can be seen as a duplicate for which the capturing conditions can not differ (such as camera view angle, scene lighting conditions, camera parameters, etc.).

Figure 1. Example of a copy image (Image 2 is created using Image 1)

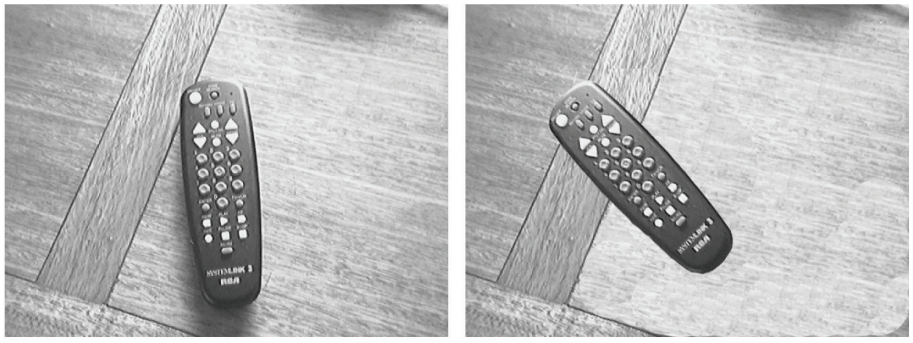

Image 1 Image 2

Figure 2. Two different views of the same scene that are not copies

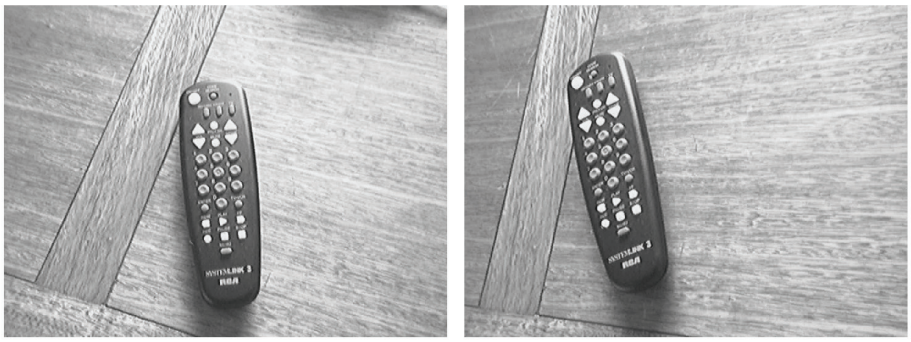

Image 1 Image 2