Chapter 12
Salient Region Detection for Biometric Watermarking

Bin Ma
Beihang University, China

Chun-lei Li
Beihang University, China & Zhongyuan Institute of Technology, China

Yun-hong Wang
Beihang University, China

Xiao Bai
Beihang University, China

ABSTRACT

Visual saliency, namely the perceptual significance to human vision system (HVS), is a quality that differentiates an object from its neighbors. Detection of salient regions which contain prominent features and represent main contents of the visual scene, has obtained wide utilization among computer vision based applications, such as object tracking and classification, region-of-interest (ROI) based image compression, etc. Specially, as for biometric authentication system, whose objective is to distinguish the identification of people through biometric data (e.g. fingerprint, iris, face etc.), the most important metric is distinguishability. Consequently, in biometric watermarking fields, there has been a great need of good metrics for feature prominency. In this chapter, we present two salient-region-detection based biometric watermarking scenarios, in which robust annotation and fragile authentication watermark are respectively applied to biometric systems. Saliency map plays an important role of perceptual mask that adaptively select watermarking strength and position, therefore controls the distortion introduced by watermark and preserves the identification accuracy of biometric images.

DOI: 10.4018/978-1-4666-3994-2.ch012
INTRODUCTION

Nowadays, while the rapid development of multimedia and network technology greatly facilitates the creation and distribution of digital media contents, it also provides convenience for unauthorized manipulation and duplication of digital work, thus poses new challenges to multimedia security.

Cryptography is a traditional tool to address security issues. It encrypts original content into incomprehensible cipher text, and only allows legitimate customers to decrypt them with provided secret keys. However, such strategy has two critical shortcomings. Firstly, the encrypted messages are conspicuous; the exposed cipher text could be examined by attackers and therefore poses a risk to the secret communication. Secondly, once intercepted and decrypted, the content will no longer have any protection.

Digital watermarking could be regarded as a complement to cryptography. It is one technique that embeds secret message named watermark into digital media by making non-perceptible slight change to the original host content. It is generally accepted that, digital watermarking was firstly described in (Van, 1994), and has received constant attention ever since (Cox, 1997; Bender, 1996; Miller, 2001). Embedded in digital media as secret information, the watermark can provide further protection even after decryption, and consequently be regarded as the last defensive line of multimedia security.

Existing digital watermarking methods can be classified into two categories: robust watermarking and fragile watermarking. The former can be applied to protect the copyright of digital multimedia (Pereira, 2000; Mohammad, 2008; Bi, 2007; Wang, 2004; Prayoth, 2005). And the latter is used to identify the integrity of media contents. It can be further separated into two classes: fragile watermarking and semi-fragile watermarking (Maeno, 2006; Yuan, 2006; Zhang, 2007; Li, 2007; Yu, 2006; Chang, 2006; Zhu, 2007; Thiemert, 2006). Fragile watermarking can detect any changes on the contents, and semi-fragile watermarking is used as detecting malicious manipulations performing on the contents while robust to natural operation, such as filtering, cropping, rotation and so on.

Digital watermarking is different from other techniques in some aspects. Firstly, watermarks are inseparable from the host contents in which they are embedded. Any attacks trying to remove the watermark, will destroy the contents as well. Secondly, watermarks are invisible, thus will not detract from the aesthetic of digital media. Furthermore, when transmitted over the Internet, such transparency makes the watermark inconspicuous to malicious attackers. In the end, watermarks can undergo the same transformations as the contents. The performance of watermarking technology can be evaluated on three features: robustness, fidelity, and embedding capacity. As a novel technology, digital watermarking has been applied in many fields, such as broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control and legacy enhancements (Cox, 2007).

Salient region detection plays an important role in many computer vision tasks, especially matching problems, such as tracking, object classification, and so forth. The detection result is a saliency map which represents the importance of the object in the scene that is projected into the visual field at that position. In a similar manner, saliency maps are useful in computer vision as they provide an efficient means of processing complex scenes by locating likely areas of interest for directing analysis (Rosin, 2009). Thus it has wide applicability: object extraction, content aware resizing, region-of-interest based compression, and so forth. Moreover, the characteristic of salient region can be applied into watermarking system. Firstly, the features of salient region have good invariance to geometric and some signal processing operations, they are already used by robust watermarking schemes to resist RST