Pattern Recognition Letters 57 (2015) 81–87

Contents lists available at ScienceDirect

Pattern Recognition Letters

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

Iris liveness detection for mobile devices based on local descriptors[☆]

Diego Gragnaniello, Carlo Sansone[*], Luisa Verdoliva

DIETI, University Federico II, Via Claudio 21, 80125 Naples, Italy

ARTICLE INFO

Article history:
Received 21 April 2014
Available online 21 November 2014

Keywords:
Iris liveness detection
Local descriptors
Biometric spoofing

ABSTRACT

Iris recognition is well suited to authentication on mobile devices, due to its intrinsic security and non-intrusiveness. However, authentication systems can be easily tricked by attacks based on high-quality printing. A liveness detection module is therefore necessary. Here, we propose a fast and accurate technique to detect printed-iris attacks based on the local binary pattern (LBP) descriptor. In order to improve the discrimination ability of LBP and better explore the image statistics, LBP is performed on a high-pass version of the image with 3 × 3 integer kernel. In addition a simplified interpolation-free descriptor is considered and finally a linear SVM classification scheme is used. The detection performance, measured on standard databases, is extremely promising, despite the resulting very low complexity, which makes possible the implementation for the relatively small CPU processing power of a mobile device.

1. Introduction

Mobile devices, like cellular phones, smartphones and tablets, are becoming increasingly sophisticated and versatile. By now, they are used not only for basic communications, but also as tools to access wireless services, including e-commerce, e-health, and online banking. These applications, however, require extremely high levels of security and privacy protection to prevent fraudulent or unauthorized use. Therefore, it is important that they include a user authentication phase, which must be both reliable and handy. Such attributes are typical of biometric systems. By relying on physical or behavioral traits of the user, e.g., fingerprints, voice, face, iris, gait or signature [34], biometric systems guarantee security and theft prevention with little involvement by part of the user.

Possible scenarios of mobile-phone biometrics are discussed in [36], and some practical systems have also been investigated, based on gait recognition through acceleration sensors [17], and on speaker and face recognition [26]. Fingerprint biometrics has been already adopted by some mobile manufacturers, which have included fingerprint scanners in their phones, such as the old model of Fujitsu F505i and the Motorola Atrix. Also Apple has recently relied on fingerprint-sensing technology with its Touch ID fingerprint scanner for iPhone 5s, and wishes to continue along this path with the upcoming iWatch, which will be likely equipped with a secure user identification mechanism based on biometrics.

Among the many possible alternatives, iris-based recognition systems have been receiving much attention by the scientific community, thanks to their high reliability in both identification and verification tasks. The iris pattern is unique for each individual (even for identical twins). Moreover, being extremely complex and random, characterized by many distinctive features, it is very difficult that two different patterns are so similar to cause a wrong identification. Finally, as an internal component of the eye, the iris is well protected from the environment and stable with age [5]. For all these reasons, iris-based systems have been thoroughly investigated in the literature, e.g. [6,22].

With mobile phones, of course, an important additional constraint on complexity must be considered. To deal with the limited computing power of portable devices, [2], and later [15], introduced some simple and efficient pre-processing for iris localization, while [28] faced also the iris recognition problem. The feasibility of the iris technology on portable computing devices has been thoroughly studied in [20], where a mobile biometric identification system has been implemented, requiring less than 200 ms to perform the iris recognition, with an acceptable performance.

Unfortunately, biometric systems are vulnerable themselves to specific attacks, as shown experimentally already in 2004 in [23]. There are several ways to trick an iris identification system, by means of an artificial eye, but also through much simpler tools, such as photographs or high quality paper prints of the iris. Indeed, in [30] the printed-iris attack (using commercial printers) was shown to achieve a success rate exceeding 50%. Therefore, to raise the security of iris-recognition systems to an acceptable level, some liveness detection tools must be necessarily included.

With reference to the screen and printed-iris attacks, probably the simplest and by far the most common scenarios, we propose a

[☆] This paper has been recommended for acceptance by G. Sanniti di Baja.

[*] Corresponding author. Tel.: +39 081 768 3640; fax: +39 081 253 1726.
E-mail address: carlo.sansone@unina.it, carlo.sansone@gmail.com (C. Sansone).

http://dx.doi.org/10.1016/j.patrec.2014.10.018
0167-8655/© 2014 Elsevier B.V. All rights reserved.

liveness detection technique based on local descriptors. Although a large number of image descriptors have recently appeared in the literature, they are often conceived with little concern for complexity. Our design, instead, takes this issue into account, looking for a suitable trade-off between performance and computational load. In spite of this constraint, the proposed algorithm provides a very good performance on all tested datasets.

The rest of the paper is organized as follows. In Section 2 the current literature on iris liveness detection is reviewed. In Section 3 our approach is described, while the experimental results obtained on two different datasets are reported in Section 4. Eventually, Section 5 draws some conclusions and outlines future directions.

2. Related work

Several approaches have been proposed in the last few years to counter attacks carried out against iris-based recognition systems. Some of them rely on dedicated additional hardware, embedded in the sensor, which detect particular traits related to the vitality of the eye. In [27] the reaction (or lack thereof) of the pupil to light changes is observed together with pupil dynamics and analysis of frequency spectrum, while in [18] four near infra-red illuminators attached on the left and right sides of iris camera are used to acquire the 3D structure of the iris pattern. Hardware-based systems have, typically, a better liveness detection performance, but they are obviously more expensive and less flexible. In a mobile-device context, software-based approaches are clearly more suitable, since they are less intrusive, operate directly on the acquired iris image, and are readily embedded in a system already existing and working, improving its performance.

The first signal-processing method for fake iris detection dates back to 1999, when Daugman [4] suggested to analyze the image in the Fourier domain to reveal some printing artifacts, in particular the periodic dot pattern. More in general, it seems reasonable to expect some significant differences in the quality of real and fake images, like, for example, the degree of sharpness, color and luminance levels, local artifacts and structural distortions. Indeed, the methods proposed in [10,11,13] rely on this consideration. In particular, in [13] 4 features are considered, related to image mean, variance, contrast and angular second moment. In [11] the quality of iris images has been assessed by measuring properties related to motion, occlusion and focus features. Differently in [10], the authors propose 25 quality measures which, being independent of either the specific biometric modality or attack, can be used also for fingerprint and face recognition.

Recently, local image descriptors have gained much popularity for a large number of applications in which a compact and discriminative description of images is necessary. Security-related applications, in particular, have been among the first to exploit the potential of these tools. Local descriptors have been used extensively for texture classification and recognition [19] and, as a special case, for face recognition [1]. Local descriptors are intrinsically well fit to tackle the iris liveness detection problem. In fact, they describe the fine-scale statistical behavior observed locally in small patches of the image, relying on texture-like information. Indeed, the iris, with its complex structure, provides abundant textural information that, once captured, can enable reliable recognition and classification. On the other hand, such detailed information can be easily disrupted by spoofing attacks.

Fine-scale information was already considered in [21] for the iris recognition task, where a local analysis through a bank of spatial filters was carried out. A similar approach is followed in [37], inspired by the work of Varma and Zisserman [35] on texture classification, for the detection of printed color contact lenses. Iris-texton features are extracted using a Gabor filter bank and coded through k-means clustering. Their histogram is then used as feature vector representative of the iris. A further improvement of this technique is proposed in [33] for the more general task of iris classification. A novel texture representation method, called Hierarchical Visual Codebook (HVC), is used to encode the texture primitives of iris images, and dense SIFT descriptors are used to codify the gradient information of the local iris region, which has to be previously segmented and normalized.

In these sequences of papers, the tendency is toward more and more complex methods, hardly portable on mobile platforms. However, some of the most successful local descriptors are characterized by very low complexity, which is certainly the case for the local binary pattern (LBP) [25]. This descriptor explores the variations observed in circularly symmetric neighbor sets and is able to detect microstructures whose underlying distribution is estimated by histograms collected over the ensemble of all patches. They are extremely simple to compute and have been also used for the task of contact lens detection in [14]. In this work, the iris is first divided into six-subregions, which are reshaped into rectangular blocks, then the LBP patterns are extracted at different scales, and finally the Adaboost algorithm is used to learn the most discriminative regional LBP features. A still effective version of this algorithm has been proposed recently in [39], where the iris image is divided into three regions: pupil, iris and sclera, and multiple-scale features are extracted from them. Finally, the LBP has been modified in [42] where SIFT descriptor is extracted at each pixel of the image and used to rank the LBP elementary features (two-pixel differences) in order of importance.

3. Proposed method

3.1. Local binary patterns

In order to build a very-low complexity iris liveness detector, suitable for implementation on a mobile device, we rely on the LBP descriptor. LBP encodes the information on the variations of intensity occurring between the image pixels and their neighbors. In more details, for each target pixel, x, P neighbors are sampled uniformly on a circle of radius R centered on x. These neighbors are then compared with x, taking only the sign of the difference, and forming thus a vector of P binary values, which is eventually converted to an integer. In formulas,

$$\mathrm{LBP}_{P,R}(x) = \sum_{i=0}^{P-1} \mathrm{u}(x_i - x)\, 2^i$$

where x_i is the ith neighbor of x, and $\mathrm{u}(t) = 1$ when $t \geq 0$ and 0 otherwise. The resulting feature provides information on the level of activity in the target-pixel area. By scanning the whole image, a field of integers is obtained, which is then summarized by a histogram, accounting for the frequency of occurrence of each feature. The parameter P controls the quantization of the angular space, while the radius R determines the spatial resolution of the operator. With $R = 1$, considering $P = 4$ and $P = 8$, we obtain the first two configurations shown in Fig. 1. Note that, since the neighbors are located on a circle surrounding the target, they do not always correspond to actual pixel values (see the diagonal neighbors in the central configuration of Fig. 1), in which case they must be computed by interpolation.

When P is large (fine angular resolution) the resulting feature vector has a considerable length. Besides the increased complexity, this fact implies that many patterns occur very rarely in the image, and their frequency of occurrence is an unreliable feature. Therefore, to improve performance, some more compact versions of LBP have been proposed. The circular symmetry allows for the definition of a rotation invariant version of the descriptor [25], recalled by the superscript *ri*

$$\mathrm{LBP}^{ri}_{P,R}(x) = \min_{n\in\{0,\ldots,P-1\}} \sum_{i=0}^{P-1} \mathrm{u}(x_i - x)\, 2^{[(i+n)\mathrm{mod}P]}$$