Neurocomputing 109 (2013) 49–55

Contents lists available at SciVerse ScienceDirect

Neurocomputing

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

Privacy-by-design rules in face recognition system

J. Pedraza [a], Miguel A. Patricio [b], A. de Asís [a], J.M. Molina [b,*]

[a] University Carlos III de Madrid, Public Law Department, Avda. Universidad Carlos III, 22, 28270, Colmenarejo, Madrid, Spain
[b] University Carlos III de Madrid, Computer Science Department, Avda. Universidad Carlos III, 22, 28270, Colmenarejo, Madrid, Spain

ARTICLE INFO

Available online 8 October 2012

Keywords:
Biometric identification
Ambient intelligence
Privacy-by-design
European law
Human rights

ABSTRACT

In this paper, we develop a face recognition system based on softcomputing techniques, which complies with privacy-by-design rules and defines a set of principles that are context-aware applications (including biometric sensors) and should contain to conform to European and US law. This paper deals with the necessity to consider legal issues concerning privacy or human rights in the development of biometric identification in ambient intelligence systems. Clearly, context-based services and ambient intelligence (and the most promising research area in Europe, namely ambient assisted living, ALL) call for a major research effort on new identification procedures.

© 2012 Elsevier B.V. All rights reserved.

1. Introduction

Many current developments apply soft computing models in environmental applications [1]. These models are capable of improving classification techniques [2], system analysis [3] or visualization tools [4] in human-centered applications. In Europe, particularly, the concept of ambient intelligent (AmI) covers developments including contextual information and expands this concept to the ambient surrounding the people. So, the electronic or digital part of the ambience (devices) will often need to act intelligently on behalf of people. It is also associated with a society based on unobtrusive, often invisible interactions among people and computer-based services taking place in a global computing environment. Context and context-awareness are central issues to ambient intelligence [5]. AmI has also been recognized as a promising approach for tackling problems in the assisted living domain [6].

Ambient assisted living (AAL) came into being as a European Union initiative stressing the importance of addressing the needs of the ageing European population, which is growing every year [7]. The program intends to extend the time that the elderly can live in their home environment by increasing people's autonomy and helping them to carry out their daily activities. Several prototypes encompass the above functionalities. Rentto et al. [8] developed a prototype of a smart home as part of the Wireless Wellness Monitor project. The prototype integrates context information from health monitoring devices and information from the home appliances. Becker et al. [9] describe the amiCa project, which provides support for monitoring daily liquid and food intakes, location tracking and fall detection. The PAUL (Personal Assistant Unit for Living) system from the University of Kaiserslautern [10] collects signals from motion detectors, wall switches or body signals, which it interprets to assist users in their daily life but also to monitor their health and provide safeguards. The data is interpreted using fuzzy logic, automata, pattern recognition and neural networks. It is a good example of the application of artificial intelligence to create proactive assistive environments.

Many of these approaches do not include personal identification functionalities because they are based on home devices. But there are also several approaches, like AMADE [11], that integrate an alert management system as well as automated identification, location and movement control systems. The inclusion of personal identification could boost the development of promising applications from an engineering point of view, but it does not account for legal issues. Clearly, an important point is the legal issue of system user identification. With the inclusion of biometric sensors, identity and location are major privacy concerns in context applications.

These privacy problems have been addressed in the literature from two different viewpoints. The first focuses on the development of frameworks [12,13] and the second on searching for some degree of user anonymity [14–16]. In [16], Beresford and Stajano combine these two ideas in a framework with anonymity levels. They focus on the privacy aspects of using location information in pervasive computing applications. User location tracking generates a lot of sensitive information. They consider the privacy of location information as controlling access to this information. The approach is a privacy-protecting framework based on frequently changing pseudonyms. This prevents users from being identified by the locations they visit. Agre [17] advocated an institutional approach that casts privacy as an issue not simply of individual needs and

* Corresponding author.
E-mail addresses: jpedraza@der-pu.uc3m.es (J. Pedraza), mpatrici@inf.uc3m.es (M.A. Patricio), aeasis@der-pu.uc3m.es (A. de Asís), molina@ia.uc3m.es (J.M. Molina).

0925-2312/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.neucom.2012.03.023

Table 1
Comparison of several biometric identification procedures.

Biometric technique	Verify	Identify	False positive	False negative	Intrusiveness	Cost
Face recognition (2D)	Yes	No	Hard	Easy	Very low	Low
Fingerprint	Yes	Yes	Very hard	Very hard	Medium	Low
Hand geometry	Yes	No	Very hard	Medium	Low	Medium
Iris scanning	Yes	Yes	Very hard	Very hard	Medium	High
Retinal scanning	Yes	Yes	Very hard	Very hard	High	High
Voice recognition	Some	No	Medium	Easy	Very low	Low
Signature	Some	No	Medium	Easy	Low	Medium

specific technologies, but as a matter arising out of recurrent patterns of social roles and relationships.

In this paper, we develop a face recognition system for ambient intelligence applications. From the technical point of view, we try to reduce the computational cost by using Gabor filters and SVMs, and, from the legal point of view, we modify the classical classification method to preserve user privacy.

We describe a face recognition system that is a very suitable biometric approach for avoiding intrusiveness. But non-intrusiveness usually means that the resolution and quality of the available face images will generally be low (lack of definition, color fidelity and others), a problem analyzed in [18]. Face recognition in AmI has a major drawback: the computational power required to make it work—even by means of wearable devices such as mobile phones [19]—. Under these constraints, we apply a simpler approach that performs satisfactorily at a reduced computational cost. In this paper we will tackle the practical task of configuring a 2D face recognition system (based on a SVM classifier and a bank of Gabor filters) under partially controlled conditions when the image quality is degraded and resolution is low-face image sizes around 100×100 pixels and a wide variety of image artifacts due to light configuration, movement and compression. The configuration parameters will be exhaustively analyzed in order to determine how they affect the result and realize the system's full potential. The decision to use a SVM as a classifier was based on its performance on this type of problems reported in several pieces of research [20,21].

The deployed face recognition system uses a set of faces without individual identification and recognizes users as members of a set. This algorithm could be a good way to preserve privacy in AmI using the recognition system as a black-box that gives access to the AmI system without breaking user anonymity and safeguarding their privacy.

2. Legal Issues in biometric identification

Nowadays, the development of reliable procedures enabling secure access to new services, and univocal user identification, a key functionality in ambient intelligence and access control scenarios is increasingly important. The level of security provided by traditional techniques based on object (card) or information (personal number) holdership are surpassed by new techniques that work with measurable anatomic (fingerprints, iris, etc.) and behavioral (gait, key-stroking, etc.) personal traits. At present, many research efforts focus on developing new algorithms and techniques for implementing multi-biometric systems that combine different biometric traits for a more secure and reliable identification.

Identification and personalization are key features of context-based services [22]. The development of efficient, non-vulnerable and non-intrusive biometric recognition techniques is still an open issue in the biometrics field (where; however, enormous scientific progress has been made over the last decade) [23]. Contextual systems should also be able to provide a satisfactory user experience.

Reliable biometric systems have long been an attractive goal. Prof. John Daugmann of the University of Cambridge describes the reliability of biometric systems as a pattern recognition problem, where the key issue is the relation between interclass and intraclass variability; objects can be reliably classified only if the variation between different instances of a given class is less than the variation between different classes. In face recognition; for example, difficulties arise from the fact that the face is a changeable social organ displaying a variety of expressions, as well as being an active three-dimensional (3D) object whose image varies with viewing angle, pose, illumination, accoutrements, and age. It has been shown that for images taken at least 1 year apart, even today's best algorithms can have error rates of 43% to 50%. Interclass variation is limited compared with this intraclass (same face) variation, because different faces possess the same basic set of features in the same canonical geometry.

Biometric identification must be robust, efficient and quick to process in order to comply with the strict security requirements in networked society [24]. Biometrics aims to recognize a person through physiological or behavioral attributes [25], such as iris, retina, fingerprints, DNA and so on. The security sector and possible applications in many fields, such as video-surveillance or access control, is the main drive behind this growth in research fields. Table 1 summarizes identification procedures, where the classical concepts of verification, identification, false positive, false negative, intrusiveness and cost are compared across several classical biometric techniques.

The new proposals aim to come up with an innovative approach to biometric recognition, providing technological solutions that overcome their current limitations and integrating biometrics recognition into context inference and fusion activities. They will integrate human body images acquisition technology using radiation in non-visible ranges (from the S to the millimeter wave band and beyond). The contextual framework will exploit biometric schemes with the following features:

- Multi-biometrics: combining several sources of biometric information (traits, sensors, etc.) with the aim of mitigating the inherent limitations of each source and assuring a more reliable and accurate system.
- High transparency, high acceptance, and non-intrusiveness, using biometric traits that can be acquired even without any cooperation from the user (e.g., face, voice) and that are socially well accepted (like the handwritten signature).
- Capability of inferring human activity and analyzing user emotions, therefore significantly focused on services customization.

These requirements directly affect many legal issues that should be considered before developing industrial applications to be used in the private or public sectors.

Any legal system geared towards the protection of fundamental rights in the use of biometric techniques should be drawn

Download English Version:

https://daneshyari.com/en/article/407092

Download Persian Version:

https://daneshyari.com/article/407092

Daneshyari.com