This document is published in:

Neurocomputing, (2013), 109 (3), pp. 49-55.

DOI: http://dx.doi.org/10.1016/j.neucom.2012.03.023

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*

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.

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

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).

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, move-ment 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 up to take into account the following features of this technology [26]:

- Biometric data are unique and permanent. One of the major problems currently posed by biometrics is that an item of biometric data cannot be revoked when it is compromised. On this ground, legislators must make provision for cases in which biometric data are usurped, establishing appeal or remedial mechanisms for victims.
- Biometrics is based on probability. This is the reason for applying a false-rejection rate and a false-acceptance rate. The legal system should include effective appeal procedures for victims of erroneous rejection.

In addition, the regulatory model should neutralize the risks of personalization with respect to potential breaches of fundamental rights (inter alia, nondiscrimination, due legal process). In Europe, this problem has been analyzed case by case [27] in the light of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The legal solution to this problem was found to be based on the following principles:

- Special protection for particular categories of data. Data capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his/her explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms (Recitals 33 and 34 of the Directive).
- Automated individual decisions. The data subject shall have the right not to be subjected to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct, unless the decision is expressly authorized pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor. In either case, measures to safeguard the data subject's legitimate interests, such as arrangements allowing him or her to put his or her point of view, must be taken (Article 19 of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data).
- Accountability, where a responsible organization should be able to demonstrate compliance with its data protection obligations. This would stimulate the use of privacy impact assessments and privacy audits.

3. Privacy by design in a face recognition system

The inclusion of biometric technology has legal implications because it has the potential to reveal much more about a person than just their identity. For instance, retina scans, and other methods, can reveal medical conditions. Thus biometric technology can be a potential threat to privacy [28]. European and American judges [23,29] have categorized privacy as taking four distinct forms. These include [24]: (a) physical privacy or freedom from contact with other people; (b) decisional privacy or the freedom of individuals to make private choices about the personal and intimate matters that affect them without undue government interference, (c) informational privacy or freedom of individuals to limit access to certain personal information about themselves, and (d) easy transmission of information. Obviously, biometric technology is related to issues (a) and (c). Biometric identification is, of course, not a new technology. Introduced more than a century ago, fingerprint technology is perhaps the most common biometric identification technique. Thus the social risk [31] associated with this technology is not new. However, technological advances and other factors [30,32] have increased the social risk associated with the technique because: (a) they have reduced the social tendency to reject its use; (b) they have enabled its widespread use [33], and (c) they have provided access to more sensitive information on the subject.

Ontario's Privacy Commissioner, Dr. Ann Cavoukian, addressed the ever-growing and systemic effects of information and communication technologies in the 1990s, creating a new concept of privacy by design [34]. The idea is that privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. In ubiquitous computation, the initial concept extends to systems, business practices, and physical design and infrastructure. Privacy by design principles should be applied with special emphasis on sensitive information such as biometric information and particularly medical information. The objectives of privacy by design are to ensure privacy and personal control over one's information. Privacy by design is based on the following foundational principles: proactive not reactive; preventative not remedial; privacy as the default; privacy embedded into design; full functionality; end-to-end lifecycle protection; visibility and transparency; and respect for user privacy. These principles should help the development of some applications in some scenarios, but they need strong foundations to be applied in any situation. Specified rules allow faster developments in specific domains and general principles define these specific rules.

Some late 2009 results of public consultation by the European Commission on how the current legal framework for data protection could best deal with the challenges of globalization and technological change suggest that "privacy by design" will probably be introduced as a new principle—not only relevant for responsible controllers, but also for vendors and developers. Specific areas such as RFID, social networking sites or cloud computing, broaden the scope for "privacy by default" settings.

In the case of face recognition systems, privacy by design rules could be defined as follows [35]:

1. The recognition system should be designed to comply with the principles of purpose (images should be collected and processed for specified and explicit purposes and their subsequent use may only be authorized in accordance with very strict conditions) and proportionality (the processing of images is authorized only to the extent necessary and insofar as no other means involving a lesser breach of privacy is as effective).
2. The source of biometric data (images, in this case) and the way they will be collected must comply with the legal requirements. Data controllers are responsible for compliance with data protection rules; they are especially responsible for compliance with the strict distinction between images collected and stored for public purposes on the basis of legal obligations and for contractual purposes on the basis of consent.
3. The use of biometrics for identification (comparison of one to many) is critical because the results of this process are less accurate than the use for authentication or control

(one-to-one comparison). Biometric identification should not therefore be the only means of identification.

4. Readily available fallback procedures shall be implemented in order to respect the dignity of people who could have been wrongly identified and to avoid transferring onto them the burden of system faults.

These principles should be considered in the software development analysis and design phases of biometric applications to include legal requirements, and, at the same time, national and international regulations should consider the new technological capabilities applied in this kind of systems. The identification procedures could be modified to obtain results that preserve user anonymity. Our proposal uses face recognition as biometric identification. The developed identification system is able to work with low bit rate images, following the architecture presented in [36]. This system has been tested on several AAL developments com-pleted in our laboratory. For a full description of the AAL domain in which the identification system has been used, see [37–39] describ-ing the AAL system and giving some illustrative examples. Our aim was to build an identification system into these applications, and we conducted a legal analysis of requirements [40]. The legal analysis governed by privacy-by-design rules led to the development of an identification system capable of identifying user membership of a pre-defined class but avoiding personal identification.

4. Biometric identification system for AmI following privacy by design rules

In [36], we developed a detailed tuning of a face recognition system based on SVM classifiers and Gabor filters for use in a non-critical application where the input images have low and highly variable quality—making it possible to use a wide range of capturing devices, even webcams. The proposed face recognition system con-forms to the simple architecture shown in Fig. 1. The purpose of this research is to adjust each part to obtain the best results. Input images receive several pre-processing operations—resizing, face detection, histogram equalization—, and are then filtered with the bank of Gabor wavelets just before being used to feed the SVM classifier.

The features resulting from applying a bank of Gabor filters to a single image are usually reported to have a huge dimensionality and thus represent an unmanageable load for subsequent steps. Some efforts have been made to decrease the amount of information to be processed, either by downsampling (scaling) the resulting features, by applying a dimensionality reduction technique such as PCA [41] or by selecting the most interesting features as in [42].

We have chosen downsampling, as the size is not a limiting factor in our system: we will show that the information loss only has negative effects when using images below 8 × 8 pixels.

The second step of dimensionality is to combine on a per-pixel basis the features output using filters of similar frequency with a different orientation (Fig. 2). There is more than one way to make this combination. We have used the L2 norm, where the squared values of the convolution results for the orientation in question is added together pixel-wise and followed by a pixel-wise square root computation to produce the combined result. This way we are not just reducing dimensionality by a factor of 8, but the resulting image will also offer improved robustness against minor changes like small deformations and/or rotations.

No other technique is necessary even with ten thousand dimensions per sample, a SVM classifier can be trained with 300 images of 17 individuals within a minute on a medium-end modern computer. Classification can be performed at a pace of several tens of samples per second. All the experiments and results reported in this paper were obtained using a custom-modified version of LIBSVM [43] library for SVMs.

In [36], results were obtained by forcing the classifier to guess the identity of the person provided as input, irrespective of whether or not it actually knows the person. Nevertheless, the AmI application classifier has to be configured so that it correctly detects an input image to represent an unknown person.

This scenario can be modeled by introducing a new dataset containing the faces of people not presented during the training phase. We used the database offered by Dr. Libor Spacek because the quality and appearance of the images it contains is quite similar to the self-made dataset.

The output of a SVM is a set of numbers whose meaning is the probability of the input sample belonging to each class known by the classifier. This way, the class with the highest probability is always the best candidate for classifying the sample. Depending on how high this probability is, however, we can form an idea of how confident the classifier is about its own verdict.

In order to adjust the confidence threshold of the classification result, we proceed to calculate the rejection threshold. Having set a rate of “false positives”, the goal is to avoid having to calculate the SVM threshold value output to comply with the rate of “false positives”. Obviously, the higher the rate of “false positives”, the lower the hit rate and the higher the rate of rejection (rejection means inability to identify an individual).

Starting from a classifier trained with a known dataset, we get two probability distributions with the SVM output values depending on whether or not they successfully identify individuals. From these two probability distributions, we can calculate the rejection

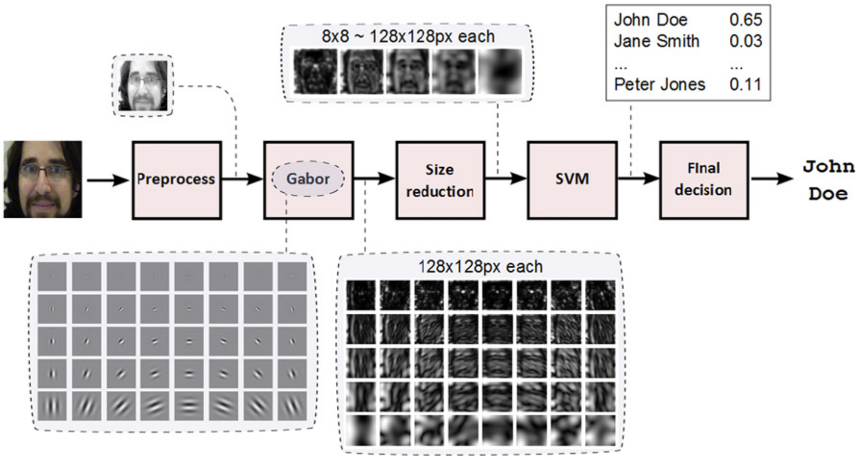

Fig. 1. Face recognition system architecture.

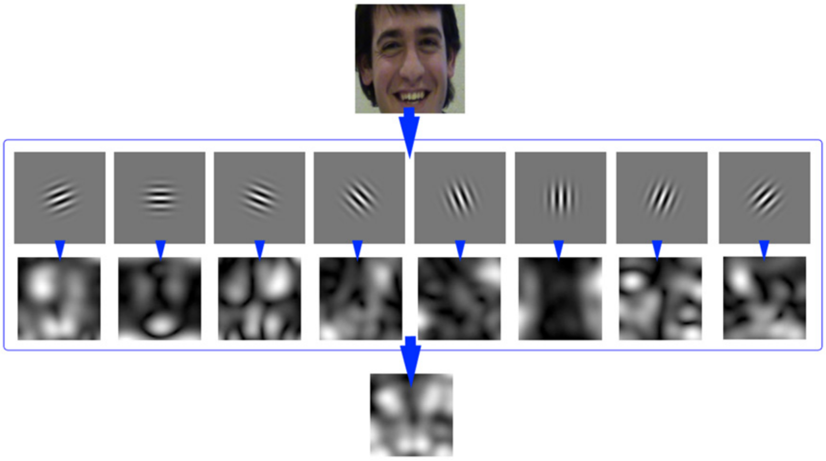

Fig. 2. Gabor features combined using L2 norm.

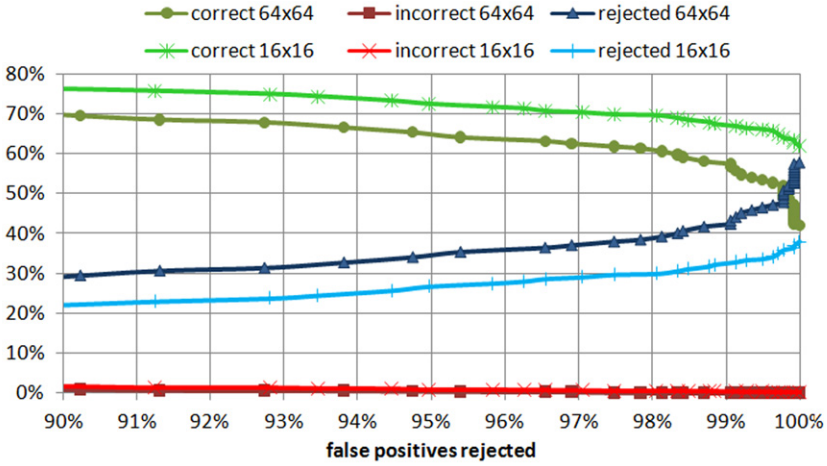

Fig. 3. Results of face recognition system.

threshold, which complies with the established rate of "false positives".

Fig. 3 shows the percentage of samples from the general dataset that were correctly classified, incorrectly classified and rejected as not known (plot curves, percentage shown on vertical axis) depending on the value of the rejection threshold. Instead of explicitly stating the threshold, the horizontal axis shows the fraction of rejected samples from the unknown dataset (horizontal axis). The region of interest for a real scenario is where over 99% of false positives are rejected, where the classifier using 16 × 16 Gabor features achieves a 67% recognition rate and an error rate of barely 35% against 57.5% and 0.06% for the 64 × 64 version.

The different configurations for the Gabor wavelet bank explored in the previous section are revisited here to confirm the results. Fig. 3 analyzes the accuracy of the system depending on the final size of the Gabor features for a bank covering five frequencies (only 16 × 16 × 5 and 64 × 64 × 5 are shown for clarity's sake). The 32 × 32 × 5 version returns a result more or less midway between the two, and the two extremes, 8 × 8 and 128 × 128, achieve the poorest results.

Clearly, the version with a size of 16 × 16 features is almost 10% more accurate than the 64 × 64 version at the cost; however, of more errors. In both cases the amount of errors is practically zero—the erroneous predictions are usually discarded as unknown persons due to low confidence. Thanks to this, the more downsampled version appears to be the most robust for an access control system.

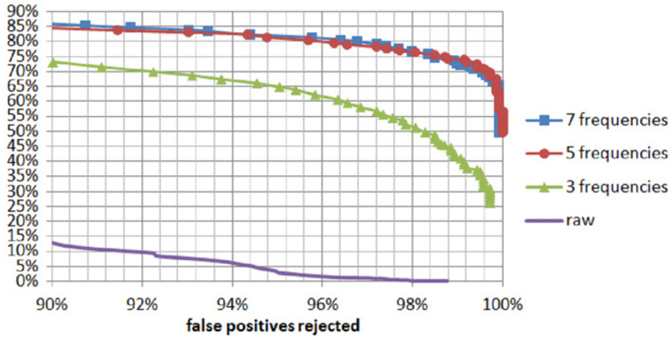

Fig. 4. Classification accuracy using Gabor wavelet banks that cover different numbers of frequencies, varying with the rejection threshold.

Fig. 4 illustrates what happens when the number of frequencies are varied. Here there is no difference between versions with five and seven frequencies, supporting the theory that the highest of the seven frequencies are maybe producing aliased Gabor feature vectors (although it is slightly more robust against failure). Accuracy using three frequencies is significantly lower, and the use of raw images instead of Gabor features is shown to be a completely useless option.

Using the Extended Yale Face Database B we were able to reproduce the experiments in [44]. We used two randomly

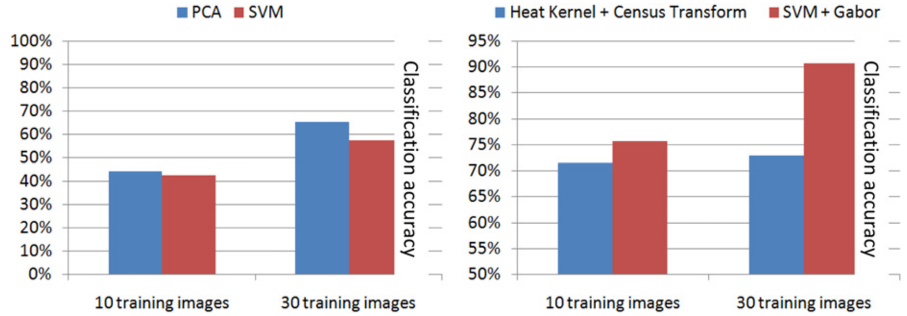

Fig. 5. Comparison of our results (red) against outcomes reported by Whittier and Xiaojun [44] (blue). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

chosen training datasets: the first uses 10 out of the 65 sample images per individual, and the second increases the number to 30. The whole database is taken as a validation set.

The outcomes of these experiments reproduced using our system are summarized in Fig. 5. Note that PCA is superior to SVM classifiers using the basic version of the algorithms, i.e., using the proposed classifiers without pre-processing input data. Apart from possible discussions regarding this particular result, this again shows that the real power of our system depends more on the Gabor wavelet filtering than on the SVM classifier.

In fact, when it is applied, accuracy is better than attributed to the heat kernel+modified census transform combination. This is especially true when a large training dataset is used. With 30 training images, the classification accuracy of our best configured system is 91%, compared with 72.6% for [44].

5. Conclusions

In this paper, we discuss the need to consider legal issues, related to privacy or human rights, in the development of the emerging context-based services. New identification procedures introduced in context-based services should be non-intrusive and non-cooperative for users to be immersed in an intelligent environment that knows who they are, where they are and their preferences. The inclusion of new biometric identification techniques pose new user privacy-related problems related to user privacy. These problems should be addressed according to privacy by design principles. We analyze and apply these principles to a face recognition system for ambient assisted living; AAL, one of the most promising fields of research in Europe related to ambient intelligence. The proposed face recognition system identifies users and conforms to legislation, safeguarding users' legal rights as citizens.

Acknowledgments

This work was supported in part by Projects CICYT TIN2011-28620-C02-01, CICYT TEC2011-28626-C02-02, CAM CONTEXTS (S2009/TIC-1485) and DPS2008-07029-C02-02.

References

[1] A. Abraham, Editorial—hybrid soft computing and applications, Int. J. Comput. Intell. Appl. 8 (1) (2009).
[2] T. Wilk, M. Wozniak, Soft computing methods applied to combination of one-class classifiers, Neurocomputing 75 (1) (2012) 185–193.
[3] J. Sedano, L. Curiel, E. Corchado, E. de la Cal, J.R. Villar, A soft computing based method for detecting lifetime building thermal insulation failures. Integrated Comput. Aided Eng. 17(2) (2010) 103–115, IOS Press.
[4] E. Corchado, B. Baruque, WeVoS–ViSOM: an ensemble summarization algorithm for enhanced data visualization, Neurocomputing 75 (1) (2012) 171–184.
[5] A. Schmidt, Interactive context-aware systems interacting with ambient intelligence, IOS Press, Amsterdam, 2005.
[6] P. Emiliani, C. Stephanidis, Universal access to ambient intelligence environments: opportunities and challenges for people with disabilities, IBM Syst. J. 44 (3) (2005) 605–619.
[7] World Population Prospects: The 2006 Revision and World Urbanization Prospects: The Revision. Technical Report, Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat (last access: Saturday, February 28, 2009 12:01:46 AM).
[8] K. Rentto, I. Korhonen, A. Vaatanen, L. Pekkarinen, T. Tuomisto, L. Cluitmans, R. Lappalainen Users preferences for ubiquitous computing applications at home. in: Proceedings of the First European Symposium on Ambient Intelligence, Veldhoven, The Netherlands 2003.
[9] M. Becker, E. Werkman, M. Anastasopoulos, T. Kleinberger, Approaching ambient intelligent home care system. in: Proceddings of the Pervasive Health Conference and Workshops, 2006 pp. 1–10.
[10] Floeck, M., Litz, L., Integration of home automation technology into an assisted living concept. in: Proceedings of the Assisted Living Systems-Models, Architectures and Engineering Approaches 2007.
[11] J. Fraile, J. Bajo, J. Corchado, Amade: Developing a multi-agent architecture for home care environments. in: Proceedings of the 7th Ibero–American Workshop in Multi-Agent Systems 2008.
[12] I-An Hong Jason, An Architecture for Privacy-Sensitive Ubiquitous Computing. Ph.D. Thesis, University of California, Berkeley, 2005.
[13] M. Weiser, R. Gold, J.S. Brown, The origins of ubiquitous computing research at PARC in the late 1980s, IBM Syst. J. 38 (4) (1999) 693–696.
[14] Lederer Scott, Mankoff Jennifer, K. Dey Anind, Who wants to know what when? privacy preference determinants in ubiquitous computing. in: Proceedings of the Conference on Human Factors in Computing Systems. Extended Abstracts on Human factors in Computing Systems 2003 pp. 724–725.
[15] Palen Leysia, Dourish Paul, Unpacking "privacy" for a networked world. in: Proceedings of the Conference on Human Factors in Computing Systems, Florida, USA, 2003 pp. 129–136.
[16] A.R. Beresford, F. Stajano, Location privacy in pervasive computing, IEEE Pervasive Comput. 2 (1) (2003) 46–55.
[17] P. Agre, Changing places: contexts of awareness in computing, Human Comput. Interaction 16 (2–4) (2001) 177–192.
[18] Hazim Kemal Ekenel, Mika Fischer, Rainer Stiefelhagen, Face recognition in smart rooms. lecture notes in computer science. s.l, Vol. 4892/2008, Springer, Berlin/Heidelberg, http://dx.doi.org/10.1007/978-3-540-78155-4_11, pp. 120–131.
[19] Alex Pentland, Tanzeem Choudhury, Face recognition for smart environments, Computer 33 (2) (2000) 50–55, http://dx.doi.org/10.1109/2.820039.
[20] Bernd Heisele, Purdy Ho, Tomaso Poggio, Face recognition with support vector machines: global vs. component-based approach. in: Proceedings of the International Conference on Computer Vision 2001 pp. 688–694.
[21] P.J. Phillips, Support vector machines applied to face recognition, Adv. Neural Inf. Process. Syst. (1999).
[22] H. Jongyi, S. Euiho, K. Sung-Jin, Context-aware systems: a literature review and classification, Expert Syst. Appl. 36 (4) (2009) 8509–8522.
[23] A. Ross, A. Jain, Information fusion in biometrics, Pattern Recognition Lett. 24 (13) (2003) 2115–2125.
[24] A.K. Jain, R.M. Bolle, S. Pankanti, Biometrics: Personal Identification in a Networked Society, Kluwer, Norwell, 1999.
[25] J. Daugman, Biometric Decision Landscape. Technique Report no. TR482, University of Cambridge Computer Laboratory 1999.
[26] Hustinx Peter, European Data Protection Supervisor. Third Joint Parliamentary Meeting on Security: Which Technologies and for What Security? The New Instruments of Internal and Civil Security. Maison de la Chimie, Paris, 23 March 2010.
[27] EDPS Video-Surveillance Guidelines, 17 March 2010, Guidelines Concerning the Processing of Health Data in the Workplace by Community Institutions and Bodies, 28 September 2009.
[28] That Right is Enshrined in Article 12 of Universal Declaration of Human Rights, Article 7 the Charter of Fundamental Rights of the European Union and Implicitly in Fourth Amendment (2000/C 364/01), 2000.

[29] European Court of Human Rights, López Ostra v. Spain-16798/90 (1994) ECHR 46 (9 December 1994). Katz v. United States, 389 US 347 (1967) Skinner v. Railway Labor Executives Ass'n, 489 US 602 (1989). To See Differences Between Legal Systems: Kirtley: Is Implementing the EU Data Protection Directive in the United States Irreconcilable With the First Amendment?. In: Government Information Quarterly, vol. 16(2) 2001 pp. 87–91.

[30] John Woodward, Biometric Scanning, Law and Policy: Identifying the Concerns-Drafting the Bio-metric Blueprint. In: U. Pitt. L. Rev no. 59 1997–1998 pp. 97–155.

[31] Ulrich Beck, La sociedad del riesgo: hacia una nueva modernidad 1998.

[32] Liou Lin, Wu: opportunities and challenges created by terrorism, Technol. Forecast. Soc. Change 74 (2) (2007) 148–164, p. 158.

[33] Gwen Kennedy, Thumbs up for Biometric authentication, Comput. Law Rev. Tech. 8 (2003–2004) 379–407.

[34] Peter Hustinx (European Data Protection Supervisor) Privacy by Design: The Definitive Workshop Madrid, 2 November 2009, 〈http://www.privacybydesign.ca/〉.

[35] European Commission and Institute for Prospective Technological Studies. Biometrics at the Frontiers: Assessing the Impact on Society for the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), 2005. European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Draft Council Regulation (EC) Laying Down the Form of the Laissez–Passer to be Issued to Members and Servants of the Institutions (2006/C 313/13).

[36] E.D. Martí, M.A. Patricio, J.M. Molina, A practical case study: face recognition on low quality images using gabor wavelet and support vector machines, J. Intell. Rob. Syst. (2011), http://dx.doi.org/10.1007/s10846-011-9548-6.

[37] R. Cilla, M.A. Patricio, A. Berlanga, J. García, J.M. Molina, Non-supervised Discovering of User Activities in Visual Sensor Networks for Ambient Intelligence applications. Special session Challenges in Ubiquitous Personal Healthcare and Ambient Assisted Living, ISABEL 2009.

[38] N. Sánchez, J.M. Molina, A Smart Solution for Elders in Ambient Assisted Living. Methods and Models in Artificial and Natural Computation, (Ed.) J. Mira et al, Lecture Notes in Computer Science 5602, pp. 95–103 (part II), Springer–Verlag, 2009, in: Proceedings of the Third International Work-Conference on the Interplay Between Natural and Artificial Computation, Special session. The Role of Knowledge Based System on Supporting Elderly Care at Home, IWINAC 2009. Santiago, Spain, June 23–26, 2009.

[39] N. Sánchez, J.M. Molina, A Centralized Approach to an Ambient Assisted Living Application: An Intelligent Home. Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing and Ambient Assisted Living, (Ed.) S. Omatu et al, Lecture Notes in Computer Science 5518, pp. 706–709, Springer–Verlag, 2009. In: Proceedings of International Workshop on Ambient Assisted Living (IWAAL) 2009.

[40] J. Pedraza, Miguel A. Patricio A. de Asís, Jose M. Molina, Regulatory Model for AAL. Soft Computing Models in Industrial and Environmental Applications, (Ed.) E. Corchado et al., Advances in Intelligent and Soft Computing, 87, pp. 183–192, Springer–Verlag, 2011. in: Proceedings of the International Conference, SOCO 2011.

[41] Y. Liang, et al., Gabor Features-Based Classification Using SVM for Face Recognition. in: Proceedings of the 2nd China International Symposium on Neural Networks, Advances in Neural Networks–ISNN, vol. 2, 2005 pp. 118–123.

[42] Linlin Shen, et al., Gabor Feature Selection for Face Recognition Using Improved AdaBoost Learning. Advances in Biometric Person Authentication. s.l, Vol. 3781/2005, Springer, Berlin/Heidelberg, 2005, pp. 39–49.

[43] Hsu Chih-Wei, , Chang Chih-Chung, Lin Chih-Jen, A Practical Guide to Support Vector Classification. [Online] July 2007 [Cited: 8 April 2009] 〈http://www.csie.ntu.edu.tw/∼cjlin/papers/guide/guide.pdf〉.

[44] Crystal Whittier, Qi Xiaojun, Supervised Heat Kernel LPP Method for Face Recognition. Computer Science Department. Utah State University, [Online] 2006 〈http://www.cs.usu.edu/∼xqi/Teaching/REU06/Website/Crystal/CrystalFinalPaper.pdf〉.