Behavioural biometrics and human identity

Schouten, B.A.M.; Salah, A.A.; van Kranenburgh, R.

Published in:
Second Generation Biometrics: The Ethical, Legal and Social Context

DOI:
10.1007/978-94-007-3892-8_9

Published: 01/01/2012

Chapter 9
Behavioural Biometrics and Human Identity

Ben A.M. Schouten, Albert Ali Salah, and Rob van Kranenburg

Abbreviations

ADABTS	Automatic detection of abnormal behaviour and threats in crowded spaces
GSR	Galvanic skin response
HUMABIO	Human monitoring and authentication using biodynamic indicators and behavioural analysis
ICT	Information and communication technologies
OECD	Organization for economic cooperation and development
PIR	Passive infrared
RFID	Radio frequency identification

9.1 Prelude

Biometrics is a key fundamental security mechanism, which links the identity of an individual to a physical characteristic or action of that individual, using methods that focus upon the individual variations between members of a given population. Currently mainstream biometrics that are being exploited in commercial systems include fingerprint and face recognition, speech verification, dynamic signature

B.A.M. Schouten (✉) • R. van Kranenburg
Fontys University of Applied Sciences, Rachelsmolen 1, R1 5612 MA Eindhoven,
The Netherlands
e-mail: ben.schouten@fontys.nl; r.vankranenburg@fontys.nl

A.A. Salah
Computer Engineering Department, Bogazici University, 34342 Bebek, Istanbul, Turkey
e-mail: salah@boun.edu.tr

E. Mordini and D. Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, The International Library of Ethics, Law and Technology 11,
DOI 10.1007/978-94-007-3892-8_9, © Springer Science+Business Media B.V. 2012

Fig. 9.1 Some commercially available sensors to detect vibration, rotation and humidity (from *left to right*); see www.phidgets.com

recognition, iris and retinal scanning, hand geometry and keystroke dynamics. In general, there are two types of biometrics: behavioural and physical. Behavioural biometrics focuses on how a human characteristics evolves over time (handwriting, gait, etc.), while physical and more traditional biometrics can be seen as an imprint of a certain physical property (face, iris, etc). Combinations are also possible when different biometrics are fused (so called *multi biometrics*).

The interest in behavioural biometrics is rapidly growing. New advanced sensor technologies enable different bodily behavioural characteristics (heart beat, electrical skin conductance, etc.) to be analyzed for authentication, and the robustness of these techniques is rapidly improving. Moreover, new and networked sensors have been introduced in smart environments, capable to detect physical properties (like pressure, temperature, etc.), motion and motion-based properties, contact properties, and presence (e.g. radio frequency identification (RFID), passive infrared (PIR) sensors etc.), and come commercially available, see Fig. 9.1. An overview of these is given in (Cook and Das 2005). The fusion of these characteristics over time and place are very promising for biometrical authentication (Li et al. 2009).

With the availability and advances of this new sensor technology and the improved network capabilities, there is a growing interest in intelligent distributed sensor networks. Such proliferation of technology has immediate implications on biometrics technology, which requires this kind of infrastructure to extend the capabilities offered by the biometric system, particularly in terms of increased accuracy and decreased intrusiveness (Tistarelli et al. 2009). Taken together with the multiplicity of digital identities most people in modern societies maintain, the future lifestyle in a digitally enhanced environment will obviously require more and more biometric technology to protect information and to ease access to personal resources. The ISTAG report published in July 2009 stresses this point aptly: "*Citizens need to be assured of the security of the complex systems that they do not control and on which they depend. The information society is becoming more fragile with respect to the threats of a totally networked world*" (ISTAG). In this chapter we discuss the implications of these trends.

9.2 Introduction: Identity and Body

In our networked society one of the most crucial questions in many transactions or engagements is the identity of the entity (person) with whom the transaction is being conducted. Historically our acquaintances are very much local: personal relationships, face-to-face contract signings, notaries, and third party counsels are used to help establish trust in our communications. There are currently two mainstream trends in identity management: a technology-driven approach and a sociology-driven approach, respectively. In the definition of Goffman (1959) identity is based on interaction; a fluid, active process, depending on context of actions (gender, class, ethnicity etc.). It consists of independent and partial sub-identities, which are to be constructed anew in everyday life. In this way information and communication technologies (ICT) can be seen as tools to support these actions. Facebook and Second Life are examples of this. Lamb and Davidson (2002) state that individuals build and maintain social networks through which they "negotiate" their identities.

In a second definition of identity, Hayles posits information over the material itself, and erases the traditional boundaries of body and personality (Hayles 1999). As the breathing medium of information, communication becomes the defining characteristic of the human. This definition of identity is perhaps inevitable, as (historically) the information processing paradigm dominated cognitive sciences and reduced the human mind into a black box that processes data and produces information for a while. The metaphor prevailed in shaping the notion of identity, and the actual body became almost an afterthought. However, in the light of accumulating research evidence, the body had to be re-introduced through theories of embodied cognition, thereby reasserting the dynamic nature of the human organism that creates itself historically in constant feedback loops within its physical and social setting (Varela et al. 1992).

In the more biometrical or technology-driven practice (or equivalently, in more conventional practice), identity is seen as a relatively stable set of personal data, occasionally divided into subsets (partial identities), but mostly constituted of sensitive personal data, which, as such, needs protection, privacy and control. This approach treats the body as a source of multimodal patterns that can be predicted and verified. In all cases, given the direction of development, two types of digital data are being communicated: bodily data and non-bodily data, respectively. Both can be used for authentication; however, biometrics focuses on the first category.

With the advance of biometrics, medical science and other disciplines, the cardinality of data related to the body is ever growing, allowing us not only to measure the health and functionality of our body, but also its appearance. Moreover, with the influence of the advertisement sector and TV commercials, the bodily appearance becomes a playground, and subject to constant change with programs like Adobe Photoshop or other visual manipulation tools. The status of body in terms of its information content and the implications of its digitalization with respect to biometrics are the two topics under study in this chapter.

The remaining part of the chapter is structured as follows. In Sect. 9.3, we discuss the new trends in biometrical research, focusing on behavioural biometrics, remote biometrics and multibiometrics. Section 9.4 elaborates on disembodied, ephemeral scenarios and use-cases and the impact of these new technologies for engineering the body, as well as identity management and bodily aspects. In Sect. 9.5 we discuss the use of biometrics for an ambient lifestyle and we conclude in Sect. 9.6.

9.3 Second Generation Biometric Modalities

9.3.1 Behavioural Biometrics and Applications

With increased availability of cheap and innovative sensors, is has become possible to derive correlations from many sensors and construct prototypical patterns of behaviour, which can be employed to authenticate a person, as well as to derive a host of associations and inferences about a person. We will call this *behavioural biometrics*. What is learned from such behavioural patterns usually pertains specifically to a particular sensor setup, and thus it is difficult to generalize or ‘hijack’ this kind of information, although analysis can be carried out to learn many more things than ordinarily indicated by the sensor readings. The type of personal and interaction information collected this way is a rich source for mining all kinds of social signals, and opens new vistas in marketing and business intelligence (Pentland 2008). Pattern recognition methods are adapted to find spatio-temporal patterns in multiple streams of sensor data for automatic analysis of human behaviours and habits in these settings. These methods include search for recurrent event patterns (Magnusson 2000; Tavenard et al. 2007), clustering time series generated by low-resolution sensors using Markov models (Wren et al. 2006), using compression algorithms for extracting patterns (Cook 2005), and eigen-analysis of behaviours (Eagle and Pentland 2006).

The modern mobile phone is already equipped with many such sensors. In a revealing study, Eagle and Pentland have equipped a large number of students with smart phones, and collected simple behaviour data for over a year (Eagle and Pentland 2006). The data included information about when the phone is turned on, or whether a conversation is carried out, location information, and other simple sensor reading. A correlation analysis of behaviour patterns proved to be sufficient to determine for instance with good accuracy, to which group (e.g. management vs. engineering students, junior vs. senior) a particular student belonged. It is thus possible to create a behaviour template of the user of a system, and authenticate the user with this, or at least reject a large number of attempts to use the system based on deviations from the user’s normal behaviour.

Another good platform is the sensor network setting, for instance an ambient intelligence environment like a smart home or a smart car (Cook 2005). It is possible to perform biometric authentication by correlating many simpler sensors rather than collecting data directly revealing the identity. The benefits of this setup are multiple; it becomes possible to authenticate groups of users (for instance to prevent access of children to potentially dangerous areas) and the perceived intrusiveness of simple sensors is much lower than for instance cameras observing the environment. Comparing data streams emanating from a sensor network will uncover meaningful associations, which might have a significant practical value in contributing to the robustness of identification process via traditional biometric modalities.

The recent FP7 research project ACTIBIO explores the possibility of continuously determining and verifying the identity of a user in typical and non-obtrusive scenarios, for instance during activities observed in a working environment (Ananthakrishnan et al. 2008). Possible novel biometric modalities include grasping patterns, facial actions, hand and body movement patterns, and keyboard typing behaviour. Its precursor project HUMABIO (Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis) has proposed a posture analysis authentication mechanism for preventing the hijacking of heavy goods vehicles (Damousis et al. 2008). For digital environments, it is possible to define biometrics that do not require additional sensors. For instance mouse movements (Ahmed and Traore 2007) and keystroke dynamics (Monrose and Rubin 2000) are behavioural cues that can lead to identification. However, these modalities contain a high variance, and thus are rarely usable as stand-alone modalities.

9.3.2 Patterns of the Body and New Modalities

Traditional biometric modalities are the ones that people use for identifying other people. Computers have access to sensors that go beyond these modalities, making novel biometric applications a possibility. For instance brain patterns, which are distinctive to individuals, can be a potential modality for authentication (Marcel and Millan 2007). The American company Emotive Communications, Inc sells headsets that can be used to navigate through a game by simple imagination (www.Emotive.com).

A new biometric modality that has come into consideration is the gait of a person (Boyd and Little 2005; Sarkar et al. 2005). The gait has been analyzed before to determine the activity type of a person (running, walking, etc.), but its use for biometric purposes requires more advanced techniques, resistant to variations due to shoe type, clothes, walking surface type, and view point. According to the extensive HumanID evaluation, shoe type has a small but statistically significant effect, followed by camera view point changes and carrying a briefcase. Matching over different time periods and surface type have also been shown to affect the authentication rates greatly (Sarkar et al. 2005).

Some novel biometric modalities are derived from research originally started for other purposes. For instance tongue diagnosis is an important method in Traditional Chinese Medicine, which makes automatic tongue image analysis an interesting application (Zuo et al. 2004). Once the analysis techniques are developed, it becomes possible to ask the question of whether or not it is possible to authenticate a person by his or her tongue image.

In a recent and excellent review of novel biometric modalities (Goudelis 2008) enlists over 20 different non-traditional approaches to person authentication. Most of these new modalities do not enjoy the extensive testing traditional modalities like face recognition received, but they certainly point out to different possibilities for different application requirements, as each of them has distinct advantages and disadvantages. For instance thermal images of the face are robust to surface modifications like make-up and possibly aging, and it can be operated in darkness (Socolinsky et al. 2003). Near-infrared imaging, on the other hand, is illumination resistant, and ideal for controlled indoor scenarios (Buddharaju et al. 2007).

Usability is of great importance for a biometric modality. Subsequently, many systems rely on biometrics that can be easily acquired or natural for a person to present. Biometrics based on palm print, finger vein patterns, nail texture, skin spectroscopy, hand or finger texture all rest on the idea that presenting the hand is natural and fast. Acquisition convenience and accuracy needs to be balanced for a given scenario. For instance dental images may be highly accurate in identifying persons (Chen and Jain 2005), but the acquisition of the image is difficult. X-ray imaging is not an option for everyday usage, because of the radiation exposure. On the other hand, ear images are easier to acquire, but the discriminativeness of the ear is not as high, and their uniqueness is contested (Chang et al. 2003). Biometrics that rely on patterns of DNA, ECG and EEG do require special equipment, and their use remains restricted to specific scenarios.

There are already a plethora of biometric possibilities, and we can very well expect new modalities to be considered in the future. The choices are further tailored to application scenarios by taking combinations of modalities.

9.3.3 Multi Biometrics and Soft Biometrics

The future of biometrics involves adapting biometrics to ever more challenging situations. For this purpose, several extensions to conventional biometric systems are relevant. In this section we look briefly at recent research in multi-biometric fusion and soft biometrics.

Multi-biometrics, i.e. consolidating the evidence by multiple biometric sources, is a primary way of adjusting the security-convenience trade-off in a biometrics system. It can be implemented by authenticating a user on a number of multiple modalities at the same time (parallel scheme), or in a cascade (serial scheme), where a user only has to submit a second (and subsequent) biometric signal in the case of doubt (Ross et al. 2006). In parallel architectures the security is increased by reducing the false accept. Disadvantages are higher financial costs and larger user involvement, as the evidence acquired from multiple sources is simultaneously processed in order to authenticate an identity (Maltoni et al. 2003).

Information fusion in biometrics is useful for two main purposes. Firstly, it may be the case that the design specification of the biometric system requires a range of operational beyond the technological provisions of a single biometric modality, either in terms of security, or user convenience. Through multiple biometrics, it becomes possible to design systems that fit more demanding requirements. In terms of user-convenience, we should also mention that multiple biometrics may be essential to prevent discrimination of users. Some biometric modalities (like fingerprints) are not applicable to for a small percentage of the population (Newham 1995), and consequently, the introduction of these modalities will discriminate these users. It is easily conceivable that a company, instead of implementing a costly backup strategy for these cases, just replaces the employees that do not conform to the requirements of the biometrics system used in the company. Multi-biometric fusion offers a way out by providing alternative authentication paths, at the cost of making the security of the system equal to the security of the weakest modality. As a compromise, it is possible to allow a small number of known users through a single modality, whereas 'normal' users will be authenticated through multiple biometrics in parallel.

Biometric information can be fused at different levels, including fusing the raw data, features, match scores, or decisions of individual matchers. Dynamic Bayesian networks are popular for probabilistic fusion of biometric evidence, allowing to cope with uncertainties in the input (Maurer and Baker 2007). An important issue is the evaluation of the statistical correlation of the input to such fusion systems (COGNIRON; Salah et al. 2008). Another dimension of fusion is the architecture, which can be serial or parallel. In (Gökberk et al. 2005), a serial (hierarchical) fusion scheme is considered for 3D face recognition in which the large number of possible classes is first reduced by a preliminary classifier that ranks the most plausible classes, followed by a second and more specialized tier of classifiers. This scheme is contrasted with a parallel fusion scheme in which all classifiers outputs are evaluated and fused at decision level. The parallel approach has increased real-time operation cost, but its accuracy is superior to that of the serial, and both fusion approaches excel in comparison to individual classifiers.

The quality of biometric samples used by multi-modal biometric experts to produce matching scores has a significant impact on their fusion. The quality depends on many factors like noise, lighting conditions, background, and distance to sensor (Tabassi et al. 2004; MIKR 2005). In Poh et al. (2009), 22 multi-biometric systems are assessed for the inclusion of quality information, as well as the cost of using additional modalities. The comparative evaluation suggests that using all the available biometric sensors will definitely increase the performance. The consequences however are increases costs in terms of acquisition time, computation time, the physical cost of hardware and its maintenance cost. These costs are alleviated to a certain extent in serial fusion schemes, where a fusion algorithm sequentially uses match scores until a desired confidence is reached, or until all the match scores are exhausted, before outputting the final combined score. In practice, the scenario may correspond to two settings; one in which multiple biometrics are acquired at the same time (at no additional cost in terms of user convenience) and the benefit is in processing time, and one in which the user is repeatedly queried until authentication occurs (or fails).

A second enhancement to ordinary biometrics is the inclusion of *soft biometrics* (Jain et al. 2004), which are easily measurable personal characteristics, such as weight and fat percentage, which can improve the performance of biometrics in verification type applications. Studies show that such simple physiological measurements can be used to support biometric recognition. Furthermore, most soft biometric traits are unobtrusive, posing no risk of identity theft, and they can be obtained via cheap sensors and simple methods. Their simplicity and weak link to identity are positive aspects with respect to usual negative connotations of biometrics, which make them especially adequate in applications where convenience is more important than security. A typical example is a weight-sensing car seat that can differentiate between two typical users of a car and allows customization based on this simple information. This seat may also prevent the child of the family from starting the car. In certain environments with a small number of subjects, like a smart car or a smart home environment, these features are robust enough to perform authentication or at least capable of determining partial identity classifications like gender, age group and such, thereby enhancing forms of anonymous identity management.

9.3.4 Biometrics from a Distance and Transparent Biometrics

The vast progress in sensor technology and computer vision enables the capture of biometrical traits from a distance for certain modalities like face recognition and iris recognition. The use of CCTV camera networks for security is an example of advanced face recognition at a distance using distributed sensor networks. Such sensor systems can be used to explore the correlations of biometric traits over time and place (spatio-temporal correlations). The processing methods depend on the configuration of sensors; for instance methods for tracking and authentication people from camera input are different for the case of a single-camera and the case of multi-camera (Fleuret et al. 2008). With present technology, it is possible to track people by using simple background-foreground separation in combination with colour features when the scene is not crowded (Kang et al. 2004; Mittal and Davis 2003). In more crowded environments, several methods are developed for segmentation and movement filtering to deal with occlusions (Haritaoğlu et al. 2000; Black et al. 2002). Tracked subjects can be authenticated remotely with face and gait recognition approaches.

What these techniques have in common is the fact that no explicit action is required from the user during the authentication (in contrast to for instance presenting a finger during the crossing of a border). We will call this *transparent biometrics* (Tangelder and Schouten 2006). In general, biometric recognition techniques at a distance are less robust as a consequence of uncontrolled occlusions, movements of objects and subjects, lighting variations, acquisition noise, or simply because smaller templates due to distance. To enable authentication in these more difficult conditions, it becomes necessary to consult more modalities, through fusion and cross correlations in time and space to improve the performance of such systems, in addition to using more powerful (and expensive) sensor sets. Many machine learning methods are used to improve offline template construction, to adapt the algorithms to operation conditions, and to integrate spatio-temporal information probabilistically see (Salah 2009) for a review of machine learning methods as applied in biometrics research).

9.4 The Impact of Behavioural Biometrics on Society

As should be obvious from our survey in the previous section, new technological developments, especially those focusing on behavioural biometrics, soft biometrics and transparent biometrics, open up many possibilities of gathering and storing physical information about individuals. In this section we will elaborate on the impact of new behavioural biometrics on our society.

The first and foremost implication of this proliferation of biometric modalities is the possibility of using gathered information for classifying a subject into arbitrary subclasses. These classes can include gender, age, economic or sociological status (Eagle and Pentland 2006), as well as spontaneous evaluation of behaviours, including the analysis of (potential dangerous) behaviour. These classifications must follow pre-defined models, or pre-selected sets of samples that are manually classified into subgroups. The central question is who defines these models and on which assumptions they are based. Such models are employed for instance in a recent European research project (FP7) *Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces* (ADABTS). ADABTS aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime, and riots. In another project called *Samurai* (short for "suspicious and abnormal behaviour monitoring using a network of cameras and sensors for situation awareness enhancement"), a surveillance system is developed for monitoring people and traffic at critical infrastructures (Samurai Project).

It is important to state that behavioural biometrics in this context is fundamentally different from traditional biometrics, which are based on the actual imprint of physical characteristics. If dissociated from the identity, the imprint cannot be used for authenticating the subject. Conversely, one behaviour alone is rarely enough for establishing identity. This is especially important when we take into account the possibility of adjusting and changing of behaviours with the purpose of conforming to a biometric setting. This possibility harbours a certain degree of danger to personal freedom of individuals.

9.4.1 Reality-Changing Implications

The extreme empowerment of the control-state, which is a generic argument against any conceivable technology in the use of power holders and policy makers, is often heard in the context of biometrics. These concerns include *big brother* scenarios (the feeling of control and less freedom), privacy and security aspects like the storage of personal data in (central) databases, and a host of other issues.

Privacy concerns are not new to the biometric community. In particular, Marek Rejman-Greene (2005) defined several criteria, which we summarize under three headings: (1) the authentication process should be accurate and data should not be kept longer then necessary, (2) the biometric (and identity) data should not be processed further than for a specific and lawful purpose (Purpose Principle) and (3) the use of biometrics should be proportional, adequate and relevant. Unfortunately, these principles are often only taken into consideration for evaluating existing applications and find limited use in the design of new applications.

In light of the latest technical development in biometrics we can predict a stronger tension between public interest and individual privacy, especially in the case of distance-based biometrics, where the user is non-obtrusively observed and authenticated over a distance (Tistarelli et al. 2009). As a consequence of these technologies, a user can be tracked and traced 24 h a day, 7 days a week. The growing resentment for hundreds of public cameras installed on the streets of London is but a small example of what could be in store. Through the violation of the purpose principle, the existence of the dense surveillance structure creates a situation where citizens are held accountable over their actions, regardless of any private aspects of their activities. Imagine an ordinary city life where each citizen commits little crimes and trespasses every now and then, ranging from littering the streets to crossing an empty street on a red light. When the state is given the power to selectively punish a citizen for all such crimes, the oppressive nature of all-around surveillance is revealed.

Moreover, with the new behavioural biometric technology, function creep becomes more likely in general. As an example, take CCTV cameras which are installed to serve public interest. The same data can be used for abnormal behaviour analyses, as in some of the currently running EU-funded research projects. Unless proper legislation is in place in accordance with the EU directive on Data Protection (or other frameworks like the Use Limitation Principle of the Organization for Economic Cooperation and Development (1980)), these applications will not be accepted by the informed citizens.

9.4.1.1 The Human Aspect

In the modern notion of technology, the end user has a crucial role, especially with regards to the environment and to sustainability. Before going any further, let us make a distinction between the **user** and the **end-user**. In a typical biometric application the user of the system is the one who deploys the system (for instance the airport authority), while the end-user is controlled by the system (for instance the passenger) (Schouten and Salah 2008). This distinction is relevant in elucidating the objectives of systems and for issues of decision control. Much of the concern for technology originates from the lack of meaning associated with applications on the side of end-users. According to Mordini (2007), present technology is developing without a sound cultural framework that could give technology a sense beyond mere utilitarian considerations.

An even more important realization is that the immersive and surrounding technologies we create around us do not remain passive objects of action and manipulation (van Oortmerssen 2009). They become a part of the everyday existence, subtly infusing our reality with their basic assumptions and the logic that dictated their creation and operation. For any technology put into operation, including the biometric technology, it is erroneous to think of an external reality mildly accepting a new concept into its bosom; instead, we conceive of the new technology with its imposed and implied behaviour patterns as establishing a new equilibrium with the existing culture, changing it (hopefully) in relatively small ways. Yet, there is always the possibility that one small change is one too many, and it is well conceivable that a cascade of consequences follows from the small kernel of discomfort introduced through the novel technology.

The extreme empowerment of the control-state is not as scary as the reality-shift scenario, as the latter implies a wholesale and invisible reconstruction of meaning. This, in itself, may be seen as natural, since there is an inevitable momentum and slow but continuous morphing of the culture, as new cultural artefacts are generated and absorbed into the public consciousness. Some of these changes are necessarily detrimental to the existing set of values, a snapshot of which is a static picture of the culture. Yet, once absorbed, these changes are seen from a different and more favourable perspective. The development of camera, for instance, is the primary enabler of most surveillance technologies, although this was not a foreseen result at the time of its conception. Once accepted, it has changed the culture fundamentally.

As the new technology gets more transparent, and vanishes into the backdrop of the existing cultural behavioural codes, the changes it calls for (from its users and end-users) are reduced, perhaps to non-existence. This transparency does not necessarily mean that the reality-shift introduced by this technology is minor. Quite on the contrary, a transparent biometric technology converts all ordinary existence into existence under surveillance. It is not the *actualization* of the technology, but the *implications of its possibility* that are damaging in this case. The data that are generated from surveillance can be discarded immediately, but this is completely irrelevant. For instance, the tools for analyzing surveillance data from thousands of cameras in London are not developed yet, but the presence of the cameras is enough to instil a feeling of paranoia in the collective subconscious of the population. The removal of visible cues that indicate surveillance may even be more damaging, as it leaves open a possibility of their existence at any given location.

Moreover, there is another consequence of making the biometric technology ubiquitous. If understood as a challenge, the surveillance technology can prompt misbehaviour. The cameras that are visibly observing people imply reaction for punishable actions. In the absence of consequent reaction, the camera becomes an empty taunt. This is also true for other biometric scenarios, where the collected biometric is not immediately linked to a clear and unchallenged purpose. Even access control scenarios are not immune to this danger, particularly for situations in which the collected biometric is excessive with respect to the perceived security requirements. This is one risk that the designers of multi-biometric systems need to take into account.

We would like to mention one last aspect of biometrics, particularly pertaining to behavioural biometrics. Irma van der Ploeg speaks of another reality shifting scenario in "*The Machine Readable Body*": the *informatization of the body,* or the digitalization of physical and behavioural attributes of a citizen and the distribution of these attributes across information networks (van der Ploeg 2005). With improved biometrical technologies, the amount of bodily data will grow exponentially, but more importantly, it will become more and more feasible to use these data in other settings. In our technological history we have seen earlier examples, where digital information of natural processes was used to influence these processes and their objects. Genetically manipulated crops or cattle are the first such examples that come to mind, of the many that exist.

Currently videos can be found on YouTube that demonstrate how to "graphically enhance" ordinary females, using Photoshop, to look like a photo model. This practice is initially only limited to the digital domain and/or used in plastic surgery. In the future we might foresee a situation where biometrical data can directly be used to analyze the body and change it according to the desired values of bodily appearance.

9.4.2 Identity: Accountability and Control

Digital technology has changed our notion of identity. Current biometric practice favours governmental applications and reinforces a centrally controlled identity. John Torpey (1999) argues that modern states, and the international state system of which they are a part, have expropriated from individuals and private entities the legitimate means of movement. In contrast and in a more fluid process we currently see within virtual communities (e.g. Facebook) identity being established and negotiated. The striking difference between biometrical identity and this *social* identity is the role of the end-user. Thomas Erickson and Wendy Kellog (2000), in their article "*Social Translucency: An Approach to Designing Systems that Mesh with Social Processes*," introduce three core aspects: Transparency, Awareness and Accountability, respectively, as essential properties of systems for the collaboration and communication of large groups. We would like to propose another quality, namely Control. In this case control is (or should be) given to the end user for applications related to identity management.

Accountability is a concept in ethics with several meanings. It is often used synonymously with such concepts as responsibility, answerability, enforcement, blameworthiness, liability, and other terms associated with the expectation of account-giving. As an aspect of governance, it has been central to discussions related to problems in both the public and private domains.

Accountability is defined as "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer punishment in the case of eventual misconduct" (Schedler 1999).

In his definition of **control**, the American Psychologist James Averill distinguishes three types of control (Averill 1973): (1) Informational control, to be informed about (the functionality of) a system, (2) Behavioural control, the user has influence on the behaviour of the system and (3) Decision control to have different options and the ability to choose among them.

It is important to see how accountability and control are assigned to the different stakeholders in biometrics and the difference in objectives between them. For end-users, convenience and privacy might be the reasons to use an application, whereas for the user or authority of the system, throughput or security might be the main arguments. Although (identity) data are private information in many countries, the interpretation of these data, and the consequences it has in the process of authentication are defined by the user (authority). The end-user has no other options apart from being held accountable over his or her actions. As there is little communication and/or interaction in the process of authentication, mistakes in both biometric recognition as well as the storage of identity data, are hard to prevent or correct. More importantly, as long as accountability and control are not (partially) assigned to the end-user, there will always be a fundamental difference in the objectives between the different stakeholders, for instance in cases where private data is exposed in the public domain (Fig. 9.2).

The following pictures show an abandoned police station. These are documentary images that are part of the project *Special Attention* by the artist Jimini Hignett. This police station is located in the wider Detroit area, in the United States of America. Fingerprints, mug shots, personal information of real individuals are scattered on the floor. In analogy, digital biometric data stored in databases can pass into disuse. Central databases are vulnerable to being hacked from outside, but they are also vulnerable from an operator point of view, who has control but is not accountable for misuse (or disuse).

A potential solution is empowering the end-user in selecting, banning and controlling biometrics that would be used in a particular scenario, although at this moment, second generation biometric technologies are not matured enough to offer a great choice, nor an integrated control over the process (see next section) itself.

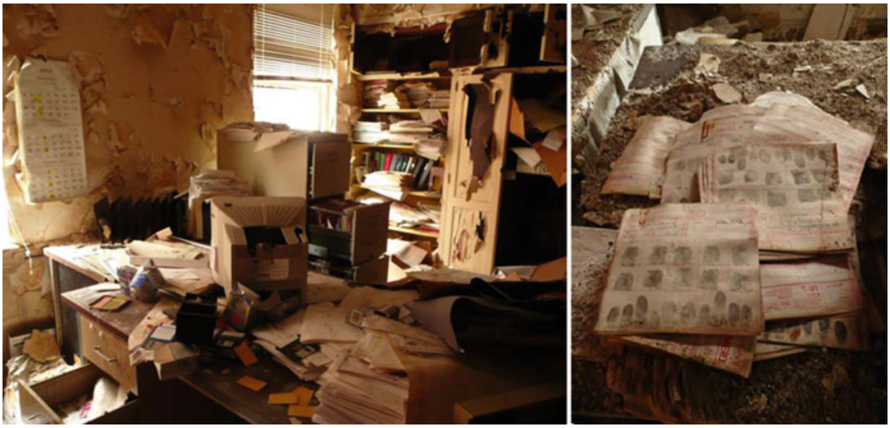


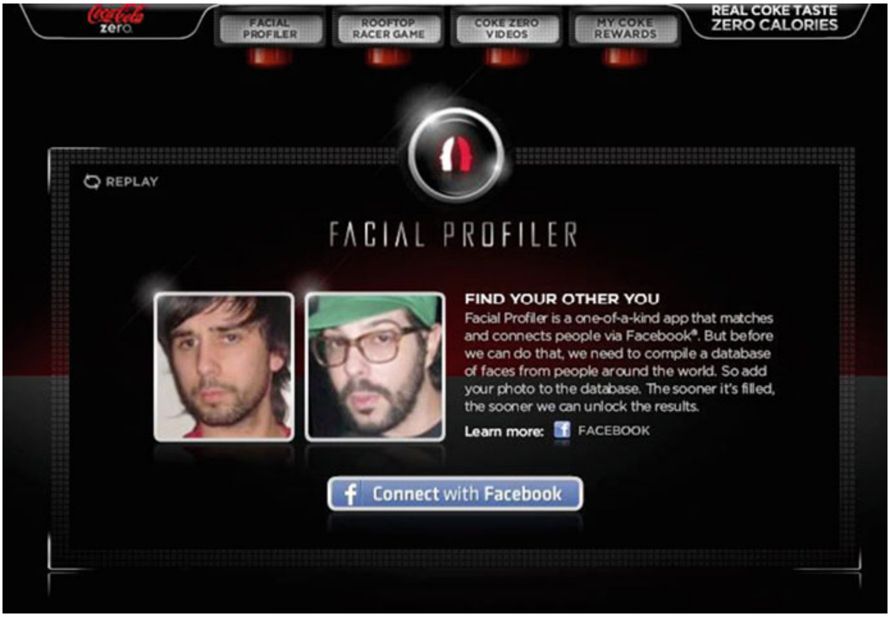
Fig. 9.2 Pictures of an abandoned police station in the Detroit Area (USA), showing fingerprints and other personal data scattered on the floor

But, difficulties aside, involving the end-user in the process itself has a big advantage over existing scenarios (Schouten and Salah 2008). It allows the rules to be questioned, or even challenged, by removing their a-priori status. The challenge is in preventing the spoon-fed cues of suppression and authority in a world that slowly loses its freedoms and diversity.

9.5 The Use of Biometrics in an Ambient Lifestyle

The ambient lifestyle pertains to a vision of end-user empowerment through technology, in all aspects of everyday existence. To empower the end-user in ID management systems in particular, their meaning and mechanisms must be communicated to the user. One way of leaving control in the hand of individuals is to introduce negotiation into the authentication process. These actualities would make a strong case for decentralized protocol, strong local grounding and an effective use of sensor and actuator technologies, which are emerging in ambient, pervasive, and ubiquitous computing that can be collected under the rubric of the Internet of Things (see www.theinternetofthings.eu). We foresee a future situation where people will carry certain identity tokens (e.g. in a handheld phone, an identity card, or possibly an implanted chip) constituting partial identities by which they would present themselves, enabling them to communicate with their environment through different applications. A very similar representation is valid for digital identities, which are currently in use by millions of people.

The creation of different identities with different levels of security and channels of communication, which do not need to be centralized and organized, is not only a challenging, but also deeply necessary idea. To be accepted, the same technology should come available for local initiatives or certified organizations that can handle different identities, as well as for (local) initiatives where user and end-user are



FIND YOUR OTHER YOU

Facial Profiler is a one-of-a-kind app that matches and connects people via Facebook®. But before we can do that, we need to compile a database of faces from people around the world. So add your photo to the database. The sooner it's filled, the sooner we can unlock the results.

Learn more: FACEBOOK

Fig. 9.3 Coke Zero Facial Profiler "…will let you use the same facial recognition software that governments and international security agencies use. But instead of finding criminals or identity thieves, you'll be able to find a person that looks just like you"

the same entity as in the case of Facebook. Biometrics will only be accepted by the public if more commercial and user centred applications will become available (see Fig. 9.3).

There is some interest in the arts community to realize biometric applications. An example is the Bio-Mapping project (see http://www.biomapping.net), which had more than 1,500 participants in 4 years. In this project, participants are equipped with a device which records the participant's Galvanic Skin Response (GSR), which can be used as an indicator of the emotional arousal. This value is linked to the geographical location of the acquired sensor readings. Subsequently, a map is created to visualize emotional arousal levels topographically. Through interpretation and annotation, the community can derive a communal emotion map from its collected biometrics, and visualize one aspect of the social space of the community.

Such examples of constructive use of biometrics are rare, but illustrative. Mordini and Massari (2008) claim in *Body, Biometrics, and Identity*, that "biometric identification technologies may offer a way for individuals to cooperate in the construction of their public identities in a more democratic and polytechnic fashion, and may perhaps eventually replace the current centralized and bureaucratic forms of identification (birth certificates, passports, drivers' licenses, and the like)." In a bold and important step, they offer a turnaround of today's view of biometrics as a tool of control and a system of binaries by stating: "biometric technologies also promise to liberate citizens from the 'tyranny' of nation states and create a new global decentralized, rhyzomatic scheme for personal recognition."

The first step of the authors towards this possible view of a more decentralized yet global system is to ascertain the primary issue of accountability, as there would be "no right, no liberty, without certified personal identities. One can claim her rights, included the right to be left alone, and the right to refuse to be identified, only if she is an identifiable subject, if she has a public identity. …there would be no liberty and no private sphere if there were no public identity" (Mordini and Massari 2008). The crucial issue is however, whether these identities need to be public, or can be private and as they put it, "*the way in which we ascertain public identities*."[1]

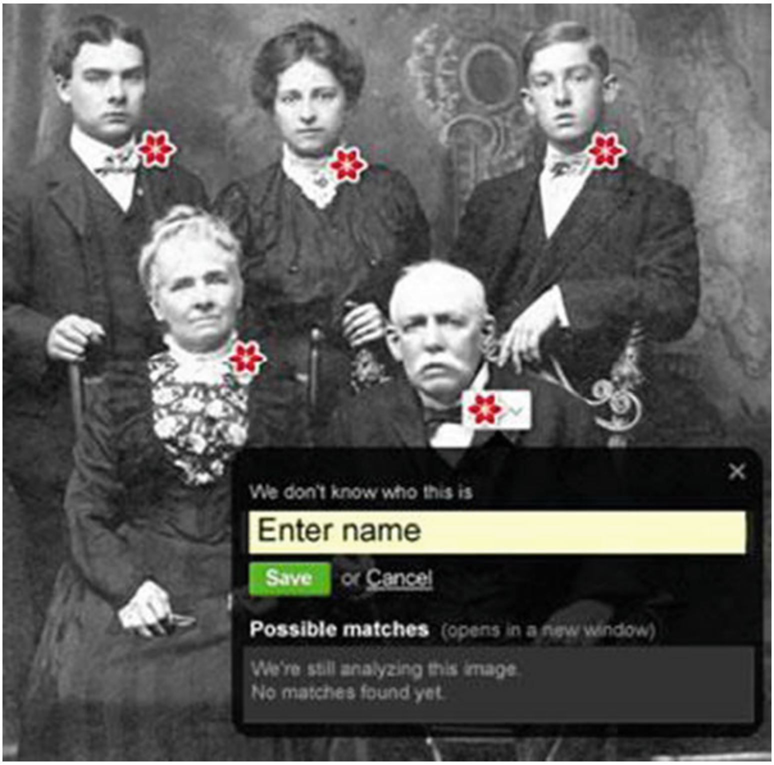
In the current situation, "states hold the power to establish national identities, to fix genders, names, surnames and parental relationships, and to assign rights and obligations to individual subjects according to the names written on their identity documents." All aspects of this identity are contested by the state, regardless of their conformity to the core principles upon which the state is established. To give an example, the Turkish state is constitutionally secular, yet the national identity card includes a field declaring the religion of the citizen, (paradoxically) to ascertain that its religious minorities are treated within the secular framework. In the case of a newborn child born to parents of different religions, father's religion is given to the child by default. To leave this field empty, both parents need to sign a written petition, and personally deliver it to the authorities. The state can thus complicate the procedures that challenge its influence over personal information arbitrarily.

9.6 Conclusions

The future of biometrics involves adapting biometrics to ever more challenging situations. The two main streams in identity management we have previously mentioned (i.e. the technologically driven approach and the sociologically driven approach, in which individuals build and maintain social networks through which they "negotiate" their identities) are in need of a new iteration that brings them together in a different way that bridges the current gap between authorities and end-users. This should naturally favour a trend towards a more liberated and diverse identification bazaar, with munificent commercial implications. Its focus should be long term: educating citizens into socially innovative and inclusive uses of the new technologies that are ever more rapidly being offered to them. Every technology faces the problem of creating its able user groups; biometrics is not an exception in this respect. However, the presence of state edicts necessitates a very wide education in their usage.

[1] "Of course one could argue that this would be a tragedy, and that an ID management solution controlled and operated by governments is absolutely essential in order for government agencies to provide the services citizens expect to receive and to guarantee the survival of the same notion of state. Discussing this question is well beyond the scope of this paper, but there is no doubt that this is one of the main ethical and political challenges raised by biometric technologies." quoted from Mordini and Massari (2008), p. 497.

Some recommendations for further development of ambient biometrics would be, to make biometric generally accepted and part of our culture, to have more user applications and localized (commercial) initiatives, including open-source software in biometrics available for larger user groups (see Fig. 9.4 for example). Artistic projects that are focusing on identity management and democratizing data visualization such as Christian Nold's Bio-Mapping – can open up a public debate.



We don't know who this is

Possible matches (opens in a new window)

We're still analyzing this image.
No matches found yet.

Fig. 9.4 'Polar Rose', a publicly available identity management system capable of recognising faces in a photobook (Copyright Univ. Lund & Univ. Malmö)

A spin-off company from the Universities of Lund and Malmö proposes simple and straight-forward identity management. Polar Rose is a publicly available application where you can find the identity of person in any photo on any site. The Polar Rose plug-in helps build a local database of identified people by aggregating user input. There is an optional feature to receive a message when someone names the user in a photograph, see http://www.polarrose.com.

With respect to the identity data, it may be argued that data aggregation should be made public; the alternative we would propose is to allow the public to make data. Last but not least, we should have a more fluid notion of identity for which the end-user is empowered to select and control the biometrics to be used in a certain scenario.

We like to end with a quote from Jan Yoors (2004). In his autobiographical story of his life with gypsies, Yoors writes how hard it was for him to be outside in the open for weeks on end. At times he longs for a door and to be able to lock it. The gypsies understand him, but for them privacy is a state of mind: "…privacy was first of all a courtesy extended and a restraint from the desire to pry or interfere in other people's lives. However, privacy must not be the result of indifference to others, but rather a mark of respect for them and of real compassion…."

References

ADABTS, Automatic detection of abnormal behaviour and threats in crowded spaces. http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&RCN=91158.

Ahmed, A.E., and I. Traore. 2007. A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable Secure Computing* 4(3): 165–179.

Ananthakrishnan, G., H. Dibeklioğlu, M. Lojka, A. Lopez, S. Perdikis, U. Saeed, A.A. Salah, D. Tzovaras, and A. Vogiannou. 2008. Activity-related biometric authentication. In *Proceedings of the 4th eNTERFACE Workshop*, 56–72. Orsay.

Averill, J.R. 1973. Personal control over aversive stimuli and its relationship to stress. *Psychological Bulletin* 80: 286–303.

Black, J., T. Ellis, and P. Rosin. 2002. Multi-view image surveillance and tracking. In *Proceeding of the IEEE Workshop on Motion and Video Computing*. Orlando.

Boyd, J.E., and J.J. Little. 2005. Biometric gait recognition. In *Lecture notes in computer science*, vol. 3161, 19–42. Berlin: Springer.

Buddharaju, P., I.T. Pavlidis, P. Tsiamyrtzis, and M. Bazakos. 2007. Physiology-based face recognition in the thermal infrared spectrum. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(4): 613–626.

Chang, K.I., K.W. Bowyer, S. Sarkar, and B. Victor. 2003. Comparison and combination of ear and face images in appearance-based biometrics. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 25: 1160–1165.

Chen, H., and A.K. Jain. 2005. Dental biometrics: Alignment and matching of dental radiographs. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 27: 1319–1326.

COGNIRON: The Cognitive Robot Companion. [Online] Available: http://www.cogniron.org/Home.php.

Cook, D.J. 2005. Prediction algorithms for smart environments. In *Smart environments: Technologies, protocols, and applications*, Wiley series on parallel and distributed computing, ed. D.J. Cook and S.K. Das, 175–192. Hoboken: Wiley.

Cook, D.J., and S.K. Das. 2005. *Smart environments: Technology, protocols and applications*. Hoboke: Wiley-Interscience.

Damousis, I.G., D. Tzovaras, and E. Bekiaris. 2008. Unobtrusive multimodal biometric authentication – The HUMABIO project concept. *EURASIP Journal on Advances in Signal Processing*. doi:10.1155/2008/265767.

Eagle, N., and A. Pentland. 2006. Eigenbehaviors: Identifying structure in routine. In *Proceedings of Ubicomp'06*. Orange county.

Erickson, T., and W. Kellogg. 2000. Social translucence: An approach to designing systems that Mesh with social processes. In *Transactions on computer-human interaction* (New York: ACM Press) 7(1): 59–83.

Fleuret, F., J. Berclaz, R. Lengagne, and P. Fua. 2008. Multi-camera people tracking with a probabilistic occupancy map. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 30(2): 267–282.

Goffman, E. 1959. *The presentation of self in everyday life*. New York: Anchor Books.

Gökberk, B., A.A. Salah, and L. Akarun. 2005. Rank-based decision fusion for 3D shape-based face recognition. In *Proceedings of the International Conference on Audio- and Video-based Biometric Person Authentication, LNCS 3546*, 1019–1028. Hong-Kong.

Goudelis, G. 2008. Emerging biometric modalities: A survey. *Journal on Multimodal User Interfaces* 2: 217–235. doi:10.1007/s12193-009-0020-x.

Haritaoğlu, S., D. Harwood, and L. Davis. 2000. W4: Real-time surveillance of people and their activities. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 22(8): 809–830.

Hayles, N.K. 1999. *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. Chicago: University of Chicago Press.

ISTAG, European Challenges and Flagships 2020 and beyond. 2009. Report of the ICT Advisory Group (ISTAG). ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/fet-proactive/press-17_en.pdf

Jain, A.K., S.C. Dass, and K. Nandakumar. 2004. Soft biometric traits for personal recognition systems. In *Proceedings of the International Conference on Biometric Authentication*. Hong-Kong.

Kang, J., I. Cohen, and G. Medioni. 2004. Tracking people in crowded scenes across multiple cameras. In *Proceedings of the Asian Conference on Computer Vision.* Korea.

Lamb, R., and E. Davidson. 2002. Social scientists: Managing identity in socio-technical networks. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, 99–99. IEEE Computer Soceity.

Li, S.Z., B. Schouten, and M. Tistarelli. 2009. Biometrics at a distance: Issues, challenges and prospects. In *Handbook of remote biometrics, advances in pattern recognition*, 3–21. London: Springer.

Magnusson, M.S. 2000. Discovering hidden time patterns in behavior: T-patterns and their detection. *Behavior Research Methods, Instruments, & Computers* 32(1): 93–110.

Maltoni, D., D. Maio, A.K. Jain, and S. Prabhakar. 2003. *Handbook of fingerprint recognition*. New York: Springer.

Marcel, S., and J.R. Millan. 2007. Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29(4): 743–752.

Maurer, D.E., and J.P. Baker. 2007. Fusing multimodal biometrics with quality estimates via a Bayesian belief network. *Pattern Recognition* 41(3): 821–832.

MIKR, The Ministry of the Interior and Kingdom Relations, the Netherlands. 2005. 2b or not to 2b. http://www.minbzk.nl/contents/pages/43760/evaluatierapport1.pdf.

Mittal, A., and L. Davis. 2003. M2tracker: A multi-view approach to segmenting and tracking people in a cluttered scene. *International Journal of Computer Vision* 51(3): 189–203.

Monrose, F., and A.D. Rubin. 2000. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems* 16(4): 351–359.

Mordini, E. 2007. Technology and fear: Is wonder the key? *Trends in Biotechnology* 25(12).

Mordini, E., and S. Massari. 2008. Biometrics, body and identity. *Bioethics* 22(9): 488–498. ISSN 0269-9702 (print); 1467-8519 (online) doi:10.1111/j.1467-8519.2008.00700.x.

Newham, E. 1995. *The biometrics report*. SJB Services.

OECD, The Eight Privacy Principles of the Organization for Economic Co-operation and Development 1980. Available online: www.oecd.org.

Pentland, A. 2008. *Honest signals: How they shape our world*. Cambridge: MIT Press.

Poh, N., T. Bourlai, J. Kittler, L. Allano, F. Alonso, O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez, H. Ganster, J.-O. Garcia, D. Maurer, A.A. Salah, T. Scheidat, and C. Vielhauer. 2009.

Benchmarking quality-dependent and cost-sensitive multimodal biometric fusion algorithms. *IEEE Transactions on Information Forensics and Security* 4(4): 849–866.

Rejman-Greene, M. 2005. Privacy issues in the application of biometrics: A European perspective in biometric systems. In *Biometric systems*, ed. J. Wayman, A. Jain, D. Maltoni, and D. Maio. London: Springer.

Ross, A.A., K. Nandakumar, and A.K. Jain. 2006. *Handbook of multibiometrics*. New York: Springer Verlag.

Salah, A.A. 2009. Machine learning for biometrics. In *Handbook of research on machine learning applications*, ed. E. Soria, J.D. Martín, R. Magdalena, M. Martínez, and A.J. Serrano. New York: IGI Global Pub.

Salah, A.A., R. Morros, J. Luque, C. Segura, J. Hernando, O. Ambekar, B. Schouten, and E.J. Pauwels. 2008. Multimodal identification and localization of users in a smart environment. *Journal on Multimodal User Interfaces*. doi:10.1007/s12193-008-0008-y.

Samurai project, www.samurai-eu.org.

Sarkar, S., P.J. Phillips, Z. Liu, I.R. Vega, P. Grother, and K.W. Bowyer. 2005. The humanID gait challenge problem: Data sets, performance, and analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 27(2): 162–177.

Schedler, A. 1999. Conceptualizing accountability. In *The self-restraining state: Power and accountability in new democracies*, ed. A. Schedler, L. Diamond, and M.F. Plattner, 13–28. London: Lynne Rienner Publishers. doi:13. ISBN 1-55587-773-7.

Schouten, B., and A.A. Salah. 2008. Empowering the end-user in biometrics. In *Proceedings of the 10th IEEE International Conference on Control, Automation, Robotics and Vision* (ICARCV). Hanoi.

Socolinsky, D.A., A. Selinger, and J.D. Neuheisel. 2003. Face recognition with visible and thermal infrared imagery. *Computer Vision and Image Understanding* 91: 72–114.

Tabassi, E., C. Wilson, and C. Watson. 2004. NIST fingerprint image quality. NIST Res. Rep. NISTIR7151.

Tangelder, J., and B. Schouten. 2006. Transparent face recognition in an unconstrained environment using a sparse representation from multiple still images. In *Proceedings of the ASCI Conference,* Lommel.

Tavenard, R., A.A. Salah, and E.J. Pauwels. 2007. Searching for temporal patterns in AmI sensor data. In *Constructing ambient intelligence: AmI-07 workshops proceedings*, ed. M. Mühlhauser, A. Ferscha, and E. Aitenbichler. Darmstadt: LNCS.

Tistarelli, M.S., Z. Li, and R. Chellappa (eds.). 2009. *Biometrics for surveillance and security*. London: Springer Verlag.

Torpey, J., C. Arup, and M. Chanock. 1999. *The invention of the passport, surveillance, citizenship and the state*. Cambridge: Cambridge University Press.

van der Ploeg, I. 2005. *The machine-readable body. Essays on biometrics and the informatization of the body*. Maastricht: Shaker.

van Oortmerssen, G. 2009. Evolutie van het Internet (Evolution of the Internet). Inaugural Speech, University of Tilburg, September 9, 2009.

Varela, F.J., E. Thompson, and E. Rosch. 1992. *The embodied mind: Cognitive science and human experience*. Cambridge: MIT Press.

Wren, C., D. Minnen, and S. Rao. 2006. Similarity-based analysis for large networks of ultra-low resolution sensors. *Pattern Recognition* 39: 1918–1931.

Yoors, J. 2004. *The heroic present: Life among the gypsies*. New York: Monacelli Publishers.

Zuo, W., K. Wang, D. Zhang, and H. Zhang. 2004. Combination of polar edge detection and active contour model for automated tongue segmentation. In *Proceedings of the Third International Conference on Image and Graphics*, 270–273. IEEE Computer Society.