

Privacy Issues in Biometric Identification

a report by

**Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi and
Fabio Scotti**

University of Milan, Italy

Biometric technologies have been recently considered as a means to obtain a higher level of security in order to cope with the increasing demand for reliable personal identification systems.

Indeed, biometric systems enable the automatic recognition of a person through the measurement of distinguishing physiological or behavioural traits. For this reason, they are increasingly put forward as solutions to identification problems in both commercial and government applications, such as when concluding a financial transaction or when passing a border control.

Applications for biometrics have been developed in different fields, such as banking, finance and transportation. For example, at Schiphol Airport, Amsterdam, a biometric system is already being used to identify both passengers in transit, in order to speed up border control procedures, and employees accessing restricted areas. Similarly, at London Heathrow airport, UK citizens and some foreign travellers can opt to use a biometric test to skip passport checks. In the future, biometric authentication systems could also be used for online transactions. However, users acceptance of biometric processes may face a number of problems related to possible attacks on their privacy through potential misuse of stored biometric information.

Biometric systems represent a change of direction with respect to traditional authentication schemes. Some traditional approaches are knowledge-based, i.e. they identify each individual on the basis of some secret the person knows e.g. password, PIN. Other systems are token-based, i.e. they recognise a person through possession of a physical object e.g. smart card, magnetic card).

With respect to these systems, biometric authentication has a number of advantages:

- The need to store or remember long and different passwords (one for each authentication domain) is eliminated, since biometric traits are always with the authenticated person.
 - Biometric traits cannot be shared. Consequently, sharing the access to a restricted content is not possible, thus enhancing security.
 - Biometric traits are not transferable and the person must be present at the moment of the authentication. For this reason, biometric systems offer non-repudiability because fake biometric traits cannot be reproduced easily.
- In the literature, many techniques and methods for biometric authentication have been presented by considering different traits, such as face, ear, iris or retinal scan, fingerprints, signature, hand and finger geometry, voice and keystroke dynamics.
- For all of these traits, privacy is a fundamental, critical, sensible issue, since – if their digital representation is lost or stolen – they cannot be replaced or modified in any way. Great care must therefore be given in storing and processing the digital representations of biometric traits, and appropriate measures must be adopted to ensure protection of biometric data.

Operations of a Biometric Authentication System

Basically, the biometric authentication systems can be used in three different ways:

- Identification – the sample produced by the biometric reading is compared with all the samples contained in a database of different identities. If a match is obtained, then the person is associated with the identity corresponding to the one contained in the database. This application is related to the growing use of identification cards, e.g. national ID cards, voter ID cards, and border control.
- Verification – the sample produced by the biometric reading is compared with the one

associated with the claimed identity. The system can accept or deny the claim.

- Screening – the sample produced by the biometric reading is compared with the ones contained in a watch list, in order to determine whether the person belongs to a set of identities to whom the access to restricted areas or content should be forbidden. These applications are often related to access control in restricted areas, such as an airport or other places of public interest.

The main phases of a biometric system are:

- Enrolment – during this phase, a biometric trait is captured and processed to produce a biometric template, i.e. a digital representation of the trait. The template can be stored in a database or in an electronic ID card.
- Identification – each time an individual needs to be authenticated at a point of access, the system executes a new reading of the biometric trait to produce a biometric template. In verification, such a template is then compared with the one stored in the database or in the ID card and associated with the identity of the individual. In identification, the template is compared with all the templates contained in the database to establish the identity of the authenticating person.

Different biometric traits can be combined in a multi-modal system such that the reliability of the whole authentication system can be improved. In this way, the error rates associated with multiple biometric readings can be reduced by combining the matching for the different traits.

Biometric Documents

In the last 10 years, biometrics has played an important role in the definition of the rules for the releases of travel documents. The International Civil Aviation Organization (ICAO) launched a program relying on machine-assisted identity confirmation of persons,¹ both for identification at the time of initial issue of travel documents and verification at border control. The goal is to develop new types of travel documents, in which a citizen's personal data are stored electronically, in order to establish a unique connection between a document and its owner. Biometrics is the core of such program, being the way of uniquely encoding a particular physical characteristic into a biometric template that can be machine-verified to confirm the presenter's identity or that can provide assistance for verification personnel as to whether the person presenting is an impostor.

The Biometrics Deployment Technical Report² provides guidelines for the introduction and deployment of biometrics, in order to produce machine-readable travel documents (MRTDs). From June 2002, for such documents, the use of face recognition has been endorsed as the globally interoperable biometrics for machine-assisted identity confirmation. Fingerprint and/or iris recognition has been selected as additional biometric technologies.

Indeed, in phase two of the European ePassport project, scheduled for 2007, the biometric data of two fingerprints will also be stored in the chip of the ePassport, in addition to personal information and the digitised facial image of the passport holder.

Protecting Users' Privacy

Biometric templates are uniquely associated with each user and thus represent the strongest form of personally identifiable information. If on the one hand, this strengthens the authentication process, on the other the possibility that a biometric template could be stolen or exchanged raises concerns on its possible uses and abuses.

One concern seems to be the possibility that a government agency or a company that maintains personal data can monitor and track the actions and the behaviour of each individual. This may augment the enormous amount of information that both public and private organizations can already collect by tracking, for example, credit card or mobile phone use.

Another fundamental concern regards the loss of anonymity when biometrics is used in a pervasive way. The control on the release of personal information should always be kept with its owner, so that they can maintain the capability of denying other parties from knowing who they are and so avoid 'Big Brother' scenarios and identity misuses.

In order to improve user acceptance, biometric systems should be designed to protect personal data and not to monitor them. To this aim, there have been several proposals combining cryptography and biometrics to ensure the security both of the biometric templates and the cryptographic keys associated with them. When biometric templates are stored in the database of an identification system, a critical issue is data protection. A strict control of accesses to the database containing personal identification information is certainly a mandatory requirement.

Another general technique consists of restricting the

access to biometric templates by encrypting them by means of one of the encryption/decryption algorithms available in the literature.

The use of one-way hash functions has been proposed to protect the sensitive user template.³ Instead of storing the template T (or the corresponding binary code, or the key C directly), the hash of the template $H(C)$ is computed and then stored. There is no security requirement imposed on the hash function or the error correcting codes. During verification the acquired biometric code C_0 is reduced to the canonical representation C by using the user specific error-correcting code. The user is authenticated if the signature and the generated hash are identical.

A scheme (known as fuzzy commitment) was proposed⁴ that binds a biometric trait to a cryptographic key in an error-tolerant way by using an error correcting code. In this way neither the key nor the biometric template itself is stored in the database. A codeword c is randomly chosen and an offset $\delta = c + x$ is computed, where x represents the biometric template ($x \in \{0, 1\}^n$). The commitment consists of the public pair $(\delta, h(c))$, where $h(c)$ is the one way hash function of the key c . To de-commit the key using another sufficiently close biometric template x' , the system computes $c_0 = \delta + x_0$. The user is authenticated if $h(c_0) = h(c)$.

Another scheme (known as fuzzy vault)⁵ allows for securely storing secret data that can be retrieved by using sufficiently similar keys, even though they may not be identical.

Personal Identification System

Building on the fuzzy commitment scheme, we recently developed and patented a novel solution.⁶ In our authentication scheme, the personal verification of the identity is obtained after different biometric traits (at least two) are combined in an original way.

Our method relies on two basic modules: the enrolment and the verification modules. The enrolment module creates a non-reversible ID, starting from the biometric samples/features provided by the individual. The verification module compares the ID with the string obtained from the biometric sample/features given by the person to be identified.

The identification module has two inputs: the string x' obtained by a classical biometric system and a non-reversible ID. If the provided string x' is not compatible with respect to the owner of the ID, the procedure is stopped. Otherwise, the proposed

identification method produces a string which can be a readable biometric trait or a set of biometric features. This output can be used as reference input to the subsequent biometric authentication. This biometric matching module compares the reference biometric sample/feature obtained by the proposed method with respect to the biometric sample/feature provided in realtime by the person to be identified.

A number of advantages are provided by our technique. First of all, privacy of the users is ensured, since only the non-reversible ID (i.e. a string computed starting from biometric traits) is stored in the ID card. With this approach, different IDs can be computed and associated with each individual.

In case of a stolen ID card, the biometric traits cannot be easily reconstructed. To protect the ID, no encryption algorithm is required: this implies that no public key infrastructure is required.

It is worth to noting that, unlike the fuzzy commitment scheme, the final step of our authentication process is performed by a classical biometric matching system; in this way it is possible to deploy any reliable matching algorithm or modularly replace it with a more reliable system when needed.

The system is intrinsically multi-modal, since the authentication process works using at least two different biometric traits, for example the iris scan and the fingerprint. According to the security level requested, more than two biometric readings can be combined and processed during the verification phase, so that the resulting authentication scheme is a composition of different modules combined in a parallel or hierarchical way.

Conclusions

According to several market overviews, the biometrics market is in rapid expansion, with different commercial companies active in developing applications based on biometric technologies and biometric authentication systems. However, to increase user acceptance, the benefits that a biometric system offers to consumers should outweigh the threats caused by the release of sensitive information such as biometric data to the system maintainers.

Privacy and the protection of biometric templates, therefore, is a critical, significant aspect for the diffusion of biometric authentication systems. Several techniques have been proposed in the literature to address the privacy issues, among which there is our innovative technique which offers several advantages and highly respects the users' privacy. ■