Fingerprint Biometrics:
Address Privacy Before Deployment

November 2008

Information and Privacy
Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner

The Commissioner gratefully acknowledges IPC staff members Alex Stoianov, Ph.D., Biometrics Specialist, and Vance Lockton, Technical Policy Analyst, for their contributions to this publication.

This document is a companion to our prior publication "Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy," and is intended to aid those organizations that are undertaking the laudable task of fully analyzing the usage of biometrics prior to deployment.

Information and Privacy
Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Fingerprint Biometrics: Address Privacy Before Deployment

A follow-up to "Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy"

While there are many biometric systems on the market, we will consider one of the most typical: a fingerprint-based identification (i.e. one-to-many) system for access control. The following information attempts to dispel some misunderstandings about fingerprint technologies and their privacy impact, and presents a number of important privacy issues that organizations must consider before implementing a fingerprint biometric system. It should be noted that most of the findings or advice contained in this document are also applicable to a fingerprint verification (i.e. one-to-one) system with central template storage, where a person first claims his or her identity (e.g. by swiping a card) and then verifies it by placing his or her finger on the sensor.

1. Typical fingerprint identification system for access control

At a high level, a fingerprint-based identification system works in the following manner:

Enrollment

Users are not required to carry any cards. On enrollment, a user places his or her finger on the scanner, which captures a fingerprint image. The image is sent to a PC ("client"). If the image quality is acceptable, fingerprint minutiae information is extracted, and the image is then discarded. The minutiae information is sent via a secure line to the biometric server, usually located in a secure room. This information is stored in a database on the biometric server. The system may enroll one or up to all ten fingers. Modern one-to-many systems are capable of searching as many as 20,000 templates, even more at times, in real time, within a few seconds.

Identification

To obtain access to a facility, the user places the appropriate finger on the sensor, and the captured fingerprint is sent to the client. The client extracts the minutiae information (with the fingerprint image subsequently discarded) and sends it to the biometric server. Here, the minutiae information is run in a one-to-many mode against the entire database of stored templates. If there is a match with one of the templates, the user is granted access. Alternatively, the system may go to the next level of authentication, for example: the corresponding photo of the user whose template has been matched is retrieved from the database and displayed to the operator. If the photo matches to the individual, the user is granted access.

The system sets a default False Acceptance Rate (FAR), for example, at 0.0001, meaning that there is a one in 10,000 chance that an impostor will be accepted. The system administrator may set a system FAR to a higher (for example, one in 1,000) level in order to lower the False Rejection Rate (FRR), which is the probability that a legitimate user will be rejected.

The system is convenient for the majority of users (no need to carry cards), and prevents the problems that can undermine card systems such as, the sharing of cards with unauthorized persons. The system also tracks an individual's use of the facility, i.e. records the fact that the individual was given access and the time and date of the access.

2. Is the stored biometric information "personal"? How sensitive and unique is it?

In some Canadian jurisdictions, personal information is defined as recorded information about an identifiable individual, other than contact information. Under that broad definition, any biometric information is personal information. However, in this document, we will adopt a narrower concept of "personally identifiable information" (PII). Information is considered personally identifiable if an individual may be uniquely identified either from this information only or in combination with any other information. If it is determined that the information is PII (and not just contact information), it will also be considered "personal information" by other Canadian jurisdictions (including the federal *Personal Information Protection and Electronic Documents Act*).

Some organizations may see the following claims: (i) the stored biometric information is just a meaningless number, and therefore is not personally identifiable information; (ii) biometric templates stored in a database cannot be linked to other databases because a sophisticated proprietary algorithm is used; or (iii) a biometric image cannot be reconstructed from the stored biometric template. In most of these cases, none of these statements is true. If organizations do not have sufficient, state-of-the-art expertise in biometrics, they can easily fall victim to misleading information.

As such, great caution must be taken when stored biometric information is referred to as a "meaningless number." It will be shown below that this is not necessarily true; in fact, a skilled (but not necessarily malicious) individual, with the proper knowledge, may be able to not only derive personally identifiable information from the stored "number," but also to reconstruct a replica fingerprint from template data. What follows in this section is a discussion of the validity, or lack thereof, of the notion that the stored biometric information is a "meaningless number." In particular, the following questions will be addressed:

- Does calling a biometric template a "number" reduce its sensitivity as personal information?
- Which biometric information is, in fact, collected?
- Is it possible to identify an individual based on the collected information?

- Is it possible to link the collected information with other fingerprint databases?
- Can a fingerprint image be reconstructed from the collected information?

3. Does calling a Biometric Template a "number" reduce its sensitivity as personal information? – No.

It is true that a fingerprint template, which is unique to an individual, typically appears as a string of numbers. However, although the template may appear to be "just a string of numbers," it cannot be said to be "of no use to anyone." It is important to recognize that any information, whether it be numbers or alphanumerics, is rendered PII when linked to personal identifiers. One only needs to consider other examples of seemingly arbitrary but unique numbers (i.e. credit cards, passports, social security numbers, etc.), where misuse and theft have resulted in considerable anguish for the victims, to understand the harm that can result when this information is not secured. Fingerprint biometric systems function on the basis that templates can be linked to the identity of a person; without this data linkage, the biometric system is rendered useless. Therefore, the templates that are generated, regardless of whether they appear in the form of numbers or not, serve as a surrogate of a person's identity and are sensitive PII by virtue of the fact that they are permanently and uniquely linked to an identifiable individual.

In academic publications [1, 2, 3], documents from biometric industry associations [4, 5], or in international standards [6], biometric information is not called a "number" but a template as defined:

> "Template: A digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Templates are used during biometric authentication as the basis for comparison."[4]

Some biometric vendors, system integrators and consultants may refer to the template as a "number" or even a "meaningless number" to imply that the information is not personal or sensitive in nature. For example, the fingerprint template has been called a "number" by school boards that have tried to deploy fingerprint technology at schools in the U.K. and also in some U.S. jurisdictions (see, for example, [7, 8, 9]). These are situations where fingerprinting has taken place without parental consent and has faced strong public opposition. Referring to the template as only a "number" in these situations may be viewed as an attempt, whether intentional or not, to mislead the public, especially when fingerprinting young children in schools.

It is, of course, true that in a fingerprint application each biometric template can be assigned a *reference number*. The reference number is returned if, for example, a match is obtained. Those reference numbers may be stored separately from the templates; however, the reference numbers do not replace the templates. The fingerprint templates still continue to be stored somewhere, and are deterministically linked to the reference numbers.

Sometimes it is claimed that the template information is a *hash* and, therefore, cannot be reverse engineered or reconstructed into an image of the fingerprint. The validity of this claim is very doubtful. It is well known that hash functions do not tolerate a single bit error. However, due to the natural variability of biometrics, any new sample taken from the same user will be different (at least slightly) from the sample taken previously. Therefore, a hash of such information will be completely different for each sample and useless for the biometric system. In other words, hashing biometric information would completely destroy the system tolerance to the natural variability of the biometric samples.

Some systems may derive a hash from the enrolled biometric template *upon* successful verification and use this hash as a reference number. However, in this case, fingerprint templates are still stored.

It should be mentioned that there is a group of emerging, privacy-enhancing technologies called "Biometric Encryption (BE)," also known as "Biometric Cryptosystem," "Fuzzy Extractor," "Secure Sketch," "Biometric Locking," "Biometric Key Generation," etc. [10, 11, 12]. These technologies securely bind a digital key to a biometric, or generate a digital key from the biometric, so that no biometric image or template is stored. What is stored is the BE data, otherwise known as a "biometrically-encrypted key" or "helper data." As a result, neither the digital key nor the biometric can be retrieved from the stored BE data. With BE, the digital key is recreated only if the correct biometric sample is presented on verification.

If a BE technology were deployed, then the biometrically-encrypted key could indeed be called a sequence of meaningless numbers. The major technological challenge is to consistently recreate the digital key, given the natural variability of biometric samples. These privacy-enhancing technologies have matured to the point that they could currently be deployed in small-scale applications [13]. However, we are unaware of any BE installations in Canada (with the exception of those being developed in Ontario.) Also, there is no known BE system that could work in a one-to-many mode doing a large number (~10,000 or more) of comparisons. We would like to encourage organizations to take a serious look at BE as a privacy-enhancing alternative. The most promising potential applications are one-to-one, or small-scale one-to-many, biometric systems. See Ref. [12] or contact the Office of the Information and Privacy Commissioner of Ontario for more information.

At this point in time, we will refer to stored biometric information as a "template", which is in line with the biometric industry and academic practices.

3.1 Which Biometric Information is Collected?

There are two main groups of fingerprint algorithms: minutiae-based and non-minutiae, or pattern-based [1, 2]. The vast majority of systems use minutiae-based algorithms. However, this does not preclude the use of some non-minutiae information as an auxiliary means to improve system performance.

There are several types of fingerprint minutiae [1 - 3]. The most common are the following two types: fingerprint ridge endings and bifurcations. Each fingerprint may contain a few to a few dozen minutiae (30 – 40 on average); this number is a biological characteristic of an individual's finger. As specified by the standards [14, 15] and commonly referenced in scientific literature [1 - 3], each minutia is defined by at least the following basic information: position x, position y, and minutia direction (i.e. angle). Having this information for all minutiae, one can create a 2D minutiae map, which is, again, a biological characteristic of an individual's finger. The standards also allow storing other optional minutiae information: type (ending, bifurcation, or "other"), and minutiae quality. Further, the standards allow the storage of "extended data," such as ridge count data, fingerprint core and delta data, zonal quality data, or any other vendor's proprietary information. This additional minutiae and non-minutiae information can be used to improve the performance of a matching algorithm.

In one-to-many matching applications, it is very likely that optional and/or extended data will be used, given the challenges of such an identification system. However, we will here make a conservative assumption that only the *basic* minutiae information is collected in a particular application. In other words, the fingerprint template stored contains at least the number of minutiae per finger, the minutiae positions x, positions y, and directions. This information is not a "meaningless number" but a biological characteristic of an individual's finger and is, therefore, highly sensitive personal information. Unlike many other forms of personal information, this biometric information cannot be changed, cancelled, or revoked.

It must be understood that in order to obtain this information from the stored template, it is not necessary to be familiar with the particular proprietary algorithm in use. It is also of no consequence how sophisticated the algorithm is. What is needed is only the format in which the information is stored. Also, templates can generally be made compatible with the existing minutiae standards. Even if this functionality is not directly built into the deployed system, anyone ordinarily skilled in biometrics can make the template compatible with the standards, provided that the template storage format is known.

3.2 Is it possible to identify an individual based on the collected information?

The answer to the question of whether an individual may be identified based on the biometric information collected by a particular fingerprint application depends on what other information is stored with, or referenced by, the fingerprint template. In a typical case where a user record (containing, for instance, a name, photograph, etc.) is associated with a set of fingerprint minutiae, all that is needed to identify an individual is the submission of a digital image of his or her fingerprint into the system. The image does not necessarily have to be captured by the deployed application sensor. It may be captured elsewhere and/or retrieved from another biometric database. For example, the FBI IAFIS and RCMP fingerprint databases store the images of all ten fingerprints of many individuals. Therefore, the physical presence at the deployment site and/or the consent of the individual are not necessarily needed to perform the matching.

This identification scenario would work even if the claims about the storage of a "meaningless number" were correct.

The accuracy of such identification can be estimated from the false acceptance numbers claimed by a vendor. For example, if the FAR is set to 0.0001 (i.e. less than 1 in 10,000) for a database of 15,000 records, an impostor would have a chance of only 1 in 10,000 to be accepted. (Note that the vendors' accuracy claims may turn out to be unrealistic in a real-life scenario, but this issue is beyond the scope of our publication).

For comparison, if a birth date was used for identification instead of fingerprints, the chance of a false acceptance would be close to 1 (more exactly, 0.6321 if all the birth dates were equiprobable) in a database of about 36,600 records (we assume a 100 year lifespan and 366 days per calendar year for this example). Therefore, the fingerprint system may have at least 3 orders of magnitude lower chance of misidentification. Note that birth dates are considered personal information (or PII) in all jurisdictions. The other important difference is that birth dates are usually verified based on paper records while fingerprints are inherent biological characteristics of individuals.

Our further analysis will deal with the question of whether the minutiae template alone (i.e. without a fingerprint image) can be used for identification; in short, the answer to this question is "yes." This problem was analyzed in the literature using theoretical modeling and running the actual tests.

The theoretical modeling approach was considered by several scientific groups [16, 17, 18] for the purposes of assessing fingerprints individuality. They calculated a probability of randomly matching a number of minutiae (not necessarily all) in two fingerprint samples. Only the basic minutiae information (i.e. positions x, positions y, and directions) was taken into account. For a fingerprint containing 36 minutiae, Pankanti et al [16] estimated a probability that two fingerprints will falsely match on all 36 minutiae as 5.5×10^{-59}, and on 12 out of 36 minutiae as 6.1×10^{-8}. Both probabilities are very low and show that the basic minutiae information can uniquely identify an individual.

The actual tests were performed by the U.S. National Institute of Standards (NIST) in Minutiae Interoperability Exchange Test, MINEX'04 [19]. The minutiae templates generated by fourteen biometric vendors were matched against each other. A template generated by one vendor was compared to a template generated by a second vendor using a fingerprint matcher from a third vendor. They tested both standard ANSI-INSITS 378 (i.e. containing minutiae positions x, positions y, directions, and types in some cases) and proprietary (i.e. with extended data) templates. The test showed that the standard templates (i.e. with the basic minutiae information only) provide sufficient accuracy for both verification (i.e. one-to-one) and identification (i.e. one-to-many), even though the proprietary templates can provide better accuracy. Moreover, the standard templates generated by one vendor can be matched to the templates generated by another vendor using an algorithm from a third vendor. Some accuracy degradation observed in the interoperability test was still acceptable for the top performing algorithms. The accuracy significantly improves if the templates are generated from two or more fingers per individual.

Thus, the MINEX'04 tests confirm that basic minutiae information is sufficient to identify an individual.

3.3 Is it possible to link the fingerprint template with other fingerprint databases?

The answer to this question is "yes," based on the above-noted results from the MINEX'04 test. Collected minutiae templates can be submitted to any other minutiae-based database. The template can easily be made compatible with the format used by another database, be it a format specified by the ISO or other standards body, or any other format, as long as the basic minutiae information is stored.

In particular, templates can be run against the FBI IAFIS or RCMP fingerprint databases. Even though these databases normally require a fingerprint image as an input, they can accept minutiae templates as well. This is usually done for criminal investigations: a fingerprint expert manually extracts minutiae from a poor quality fingerprint image (collected, for example, at a crime scene) and submits the extracted minutiae to the system. By the same token, the minutiae obtained from a template can be also submitted to these databases.

3.4 Can a fingerprint image be reconstructed from the template?

Since we have already established that minutiae information is personal and sufficient to identify an individual, and interoperable among different databases, this question becomes less important. However, since many proponents of biometric systems make a claim that a fingerprint image cannot be reconstructed from a minutiae template, we will address this issue.

Until recently, the view of non-reconstruction was dominant in the biometrics community. However, over the last few years, several scientific works were published that showed that a fingerprint can, in fact, be reconstructed from a minutiae template. The most advanced work was published in 2007 by Cappelli et al [20]. The authors analyzed templates compatible with the ISO/IEC 19794-2 minutiae standard. In one test, they used basic minutiae information only (i.e. positions x, positions y, and directions). In another test, they also used optional information: minutiae types, Core and Delta data, and proprietary data (the ridge orientation field in this case). In all the tests, the authors were able to reconstruct a fingerprint image from the minutiae template. Very often, the reconstructed image had a striking resemblance with the original image. Even though this reconstruction was only approximate, the reconstructed image was sufficient to obtain a positive match in more than 90% of cases for most minutiae matchers.

The potential repercussions of this work for the security and privacy of fingerprint minutiae systems are as follows:

- The fingerprint image reconstructed from the minutiae template, known as a "masquerade" image since it is not an exact copy of the original image, will likely fool the system if it is submitted.

- A masquerade image can be submitted to the system by injecting it in a digital form after the fingerprint sensor.
- A malicious agent could also create a fake fingerprint and physically submit it to the sensor. The techniques of creating a fake fingerprint are inexpensive and well-known from the literature.
- The ability to create a masquerade image will increase the level of interoperability for the minutiae template. The masquerade image can be submitted to any other fingerprint system that requires an image (rather than a minutiae template) as an input. No format conversion of the minutiae template would be required. Moreover, the minutiae template can be made compatible even with a non-minutiae fingerprint system (these systems are rare, however).

4. Necessity Test

Beyond understanding the technical issues surrounding fingerprint biometric systems, deployers must also be able to provide sufficient evidence of the necessity of the technology. Convenience should not be considered a sufficient reason for implementation of such a system. Instead, organizations should be able to provide a full and comprehensive explanation of the purpose and benefits (or necessity) of the system, the drawbacks (or inappropriateness) of alternative measures, and the reasons why it was decided that the privacy issues associated with biometrics were outweighed by the necessity of the system.

When making these determinations, context plays a very important role. For instance, if we consider a general use for fingerprint identification systems – the accurate and efficient identification of individuals – the purpose of such an identification will determine its appropriateness. If the purpose is to control access to a safety-sensitive site such as a nuclear facility, for example, it is much more likely that a biometric system would be deemed to be "necessary" than if the same system were deployed for use at a health club.

This is not to say that deployment at a health club is necessarily inappropriate; rather, it should be understood that such a use will require significant justification. Questions that should be addressed might include: What is the "problem" being solved by such a system? Have other alternatives been considered? Would alternatives be more or less privacy invasive? Would such a system be voluntary, or mandatory? Do other, similar institutions face similar problems? If so, what solutions have been deployed? Are biometrics common in this situation? … and so forth.

Increasing the accuracy of identification also does not provide a *de facto* acceptable reason for "necessity," as the biometric method has its own accuracy problems. The following error measures of a biometric system are known [1]:

- Failure To Enroll (FTE): a legitimate user cannot get enrolled, mostly because the quality of fingerprints is poor;
- False Rejection Rate (FRR): a legitimate user is rejected by the system.
- False Acceptance Rate (FAR): an impostor is accepted by the system.

Some authors [21] also differentiate False Identification Rate (FIR) from FAR, which is important for a one-to-many access control system: a legitimate user is accepted but falsely identified as another legitimate user.

The literature indicates that the percentage of FTE and FRR cases may vary from a few percent to as high as 20 per cent. To mitigate FTE or FRR problems, several measures may be taken. For example, pre-scan pads, lotions, etc. can be used to enhance the quality of fingerprints. Another measure would be lowering the system threshold to reduce FRR at the cost of higher FAR and FIR. However, lowering the system threshold may boost FAR and FIR from, for example, 1 in 10,000 to 1 in 1,000. This would mean that there would be one misidentification per 1,000 visits. Such a misidentification may have a significant impact on a legitimate user. For example, if a security incident or a crime happened, the user could be wrongly accused based on his attendance record; or, in a financial example, money could be withdrawn from the wrong account. It would be very hard for a legitimate user to challenge the validity of a biometric record. In general, the challenges of rectifying the errors of a biometric system often fall disproportionately on the users.

While it is true that the fingerprint identification system may be more convenient for a majority of users (as the need to carry a card and to remember a PIN is removed), the users having FTE or FRR problems are greatly inconvenienced.

With respect to the view that biometric systems have a deterrent effect on unlawful activities, or that the attendance records they generate are useful investigative tools, it is clear that a card-and-PIN system, for example, would have virtually the same effect. It should also be noted that evidence based on fingerprint templates would not be accepted by the courts (actual fingerprint images are required).

The issues raised in this section highlight the importance of thoroughly investigating the necessity of introducing a biometric identification system prior to deployment.

5. Privacy protection and security safeguards

When deploying fingerprint biometric identification systems, privacy protections and security safeguards should be tailored to the needs of the application. One of the drawbacks of adopting the flawed view of the biometric template as a "meaningless number" is that the "number" is not treated as sensitive information. As a result, it is possible that no privacy protective measures, specific to the biometric information, are put into place. In particular, biometric-specific Privacy Impact Assessments (PIA), Threats and Risk Assessments (TRA) or vulnerability tests may not be conducted, and the principles of data minimization and user control over data may be ignored.

The security vulnerabilities of biometric systems were identified in Ref. [17] (see also Ref. [12]). They include:

Spoofing; *replay attacks*; *substitution attacks*; *tampering*; *masquerade attacks*; *Trojan horse attacks*; and *overriding Yes/No response*.

In particular, when examining the security of a fingerprint biometric system for access control, the following potential vulnerabilities should be assessed:

- The possibility that fake fingerprints could be used successfully (this is also called spoofing). Some vendors, for instance, use "liveness detection" to mitigate this threat.
- The degree to which an outside or inside "attacker" can extract fingerprint templates from the database, and substitute the templates or tamper with them.
- The effort required for an outside or inside "attacker" to extract the minutiae information from the templates.
- The effort required for an outside or inside "attacker" to inject a malicious program into the system for the purposes of launching replay attacks, Trojan horse attacks, or overriding Yes/No response.
- Whether fingerprint images are stored temporarily while being processed.
- Whether an employee could capture the image, if shown onscreen, using the Print Screen button or with a camera, or whether a malicious program could capture the image.
- If minutiae information extracted from a fingerprint resides at a temporary location during processing, whether this information could be obtained by an outside or inside "attacker."

6. Conclusions and Recommendations

Although biometric technologies present a number of benefits, ranging from stronger user authentication, greater convenience for a majority of users, to improved security and operational efficiencies, they also present a number of risks to informational privacy. Any perceived or real threat to privacy could result in a serious loss of public faith and support. Consequently, organizations must carefully assess, prior to deployment, whether their needs can be met using alternative non-biometric means, and whether the privacy risks are outweighed by the necessity of installing a biometric system.

The key considerations for organizations contemplating the usage of biometric systems are summarized as follows:

- Stored fingerprint information should not be called a "number". It is, in fact, sensitive personal information. Rather than "numbers," this information should be referred to as "fingerprint templates."

- Organizations should consider the feasibility of using emerging privacy-enhancing technologies called "Biometric Encryption" that irreversibly bind a cryptographic key to a biometric. The most promising potential applications are one-to-one or small-scale one-to-many biometric systems.

- A fingerprint minutiae template contains at least the basic minutiae information, which is the number of minutiae per finger, the minutiae positions x, positions y, and directions.

- Minutiae information is a biological characteristic of an individual's finger and is, therefore, highly sensitive personal information. This information cannot be changed, cancelled, or revoked.

- To obtain the minutiae information from a stored template, it is not necessary to be familiar with a sophisticated proprietary algorithm. Only the knowledge of the storage format is needed.

- Proprietary minutiae templates in their basic parts can be made compatible with existing minutiae standards (ANSI-INSITS 378 and ISO/IEC 19794-2).

- Basic minutiae information can identify an individual with high accuracy.

- Minutiae templates can be made interoperable between different databases and different vendors.

- Minutiae templates can be linked to other fingerprint databases, including the FBI IAFIS or RCMP fingerprint databases.

- A fingerprint image may be reconstructed from a minutiae template.

- Fingerprint systems are subject to accuracy problems, such as Failure To Enroll, False Rejection, False Acceptance, or False Identification, that may disproportionately fall upon users.

- Among other considerations, biometric-specific Privacy Impact Assessments, Threats and Risks Assessments, and (if possible) vulnerability tests should be conducted prior to the deployment of a biometric system.

- Security safeguards should be adequate in terms of general IT management, and address biometric-specific threats and risks.

If an organization decides that the use of a fingerprint biometric identification system is warranted, it is important to mitigate the privacy risks. Some approaches include:

- Providing alternative means of identification, such as a card-and-PIN. Fingerprinting (or other biometric solution) should be completely voluntary, whenever possible.

- Developing and implementing comprehensive privacy and security policies that treat biometric templates as PII.

- Conducting thorough biometric-specific PIAs, TRAs, and vulnerability tests, on a regular basis.

- Storing templates in servers only in encrypted form.

- Not displaying a fingerprint image during authentication, and preventing any other possibility of capturing the image by unauthorized persons.

- Consulting the Office of the Information and Privacy Commissioner prior to deployment.

References

[1] *Biometric Systems: Technology, Design and Performance Evaluation*. by J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. Springer, 2004.

[2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, New York, 2003.

[3] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A.W. Senior. *Guide to Biometrics*. Springer, 2003.

[4] *Biometrics Glossary*: **http://www.biometricscatalog.org/biometrics/GlossaryDec2005.pdf**

[5] **http://www.findbiometrics.com/Pages/glossary.html**

[6] *Harmonized biometric vocabulary*. JTC 1/SC 37/WG 1

[7] *Nifty gadget or something more sinister?* The Guardian, January 11, 2005. **http://education.guardian.co.uk/elearning/story/0,10577,1387226,00.html**

[8] W. M. Grossman. *Is school fingerprinting out of bounds?* The Guardian, March 30, 2006. **http://www.guardian.co.uk/technology/2006/mar/30/schools.guardianweeklytechnologysection**

[9] N. Rosenkrans. *Meal ID system gets personal*. Winona Daily News, April 17, 2008. **http://www.winonadailynews.com/articles/2008/04/17/news/00lead.txt**

[10] P. Tuyls, B. Škorić, and T. Kevenaar, eds. *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*. Springer-Verlag, London, 2007.

[11] A K. Jain, K. Nandakumar, and A. Nagar. *Biometric Template Security*. EURASIP Journal on Advances in Signal Processing, v. 2008, Article ID 579416, pp. 1-17, 2008.

[12] A. Cavoukian and A. Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, March 2006. **http://www.ipc.on.ca/index.asp?navid=46&fid1=608**

[13] Philips technology called priv-ID^{TM}. **http://www.research.philips.com/initiatives/priv-id/index.html**

[14] ANSI-INCITS 378-2004, *Information Technology—Finger Minutiae. Format for Data Interchange*, 2004.

[15] ISO/IEC 19794-2:2005, *Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data*, 2005.

[16] S. Pankanti, S. Prabhakar, and A. Jain, *On the individuality of fingerprints*. IEEE Transactions on Pattern Analysis And Machine Intelligence, v. 24 , No. 8, pp. 1010-1025, 2002.

[17] N. K. Ratha, J. H. Connell, and R. M. Bolle. *Enhancing security and privacy in biometrics-based authentication systems*. IBM Systems Journal, v. 40, No. 3, pp. 614–634, 2001.

[18] Y. Zhu, S. C. Dass, and A. K. Jain, *Statistical Models for Assessing the Individuality of Fingerprints*. IEEE Transactions on Information Forensics and Security, v. 2, No. 3 (Part 1), pp. 391-401, Sept. 2007. also **http://www.cse.msu.edu/cgi-user/web/tech/reports?Year=2006**.

[19] MINEX'04. *Performance and Interoperability of the INCITS 378 Fingerprint Template*. NISTIR 7296, National Institute of Standards and Technology, March 21, 2006. **http://fingerprint.nist.gov/minex04/minex_report.pdf**

[20] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, *Fingerprint Image Reconstruction from Standard Templates*. IEEE Transactions On Pattern Analysis And Machine Intelligence, v. 29, No. 9, pp. 1489 - 1503, 2007.

[21] **http://www.bromba.com/faq/biofaqe.htm**