Pseudo Identities based on Fingerprint Characteristics

Nicolas Delvaux, Hervé Chabanne
Julien Bringer, Bruno Kindarji
Sagem Sécurité, France

Patrik Lindeberg, Johannes Midgren
Precise Biometrics AB, Sweden

Jeroen Breebaart, Ton Akkermans,
M. van der Veen, R. Veldhuis
Philips Research, UTW, Netherlands

Els Kindt, Koen Simoens
K. U. Leuven , Belgium

Christoph Busch, Patrick Bours,
Davrondzhon Gafurov, Bian Yang
Gjøvik University College, Norway

Julien Stern
Cryptolog International, France

Carsten Rust
Sagem Orga Gmbh, Germany

Bruno Cucinelli
ARTTIC, France

Dimitrios Skepastianos
3d - GAA S.A. , Greece

Abstract

This paper presents the integrated project TURBINE which is funded under the EU 7th research framework programme. This research is a multi-disciplinary effort on privacy enhancing technology, combining innovative developments in cryptography and fingerprint recognition. The objective of this project is to provide a breakthrough in electronic authentication for various applications in the physical world and on the Internet. On the one hand it will provide secure identity verification thanks to fingerprint recognition. On the other hand it will reliably protect the biometric data through advanced cryptography technology. In concrete terms, it will provide the assurance that i) the data used for the authentication, generated from the fingerprint, cannot be used to restore the original fingerprint sample, ii) the individual will be able to create different "pseudo-identities" for different applications with the same fingerprint, whilst ensuring that these different identities (and hence the related personal data) cannot be linked to each other, and iii) the individual is enabled to revoke an biometric identifier (pseudo-identity) for a given application in case it should not be used anymore.

1. Introduction

A pressing issue in European jurisdictions is, how to protect biometric data in eGovernment-, eHealth-, eFinance-Applications. The key concern here is how to ensure that high security and data protection needs can be simultaneously satisfied while also ensuring ease of use and flexibility. Moreover the fingerprint as a biometric characteristic is widely associated with forensic applications. These concerns become obvious once we investigate the following typical application scenarios for biometric fingerprint recognition:

1. *Registered Customer Application (RCA)*

   The individual is interested to participate in - and benefit from - an eCommerce or eFinance application. The operator of the application is considered as service provider. The individual generates for each application a unique biometric identifier (the "pseudo identity"), such that each application the client is associated with a different pseudo-identity. The client verifies his pseudo-identity prior to each transaction or consumption of the offered service. Each transaction will be charged to the individuals account subsequent to the transaction.

   However a concerned individual may have limited trust to the service provider and does neither want the service provider to store his fingerprint images (nor derived features such as minutiae data) at enrolment, nor does the individual want to provide fingerprint images with each transaction.

2. *eGovernment Customer Application (GCA)*

   The individual is interested to participate in and benefit from an eGovernment application. The operator

represents a public administration (municipality, state etc.). The individual (the client) is citizen of the municipality / state and verifies his pseudo-identity prior to each transaction or consumption of the offered service. Each transaction is linked to his real identity (citizen number) and some transactions may be charged to the individuals account subsequent to the transaction.

Requirements and concerns for this scenario are equivalent with the previous RCA-scenario with the following exception that establishing a link to a payment scheme might be obsolete, if the municipality / state decides to offer the service free of charge. Furthermore issuing a token might be obsolete, if a valid governmental token can be used instead (eID-Card, eHealth-Card, European Citizen Card derivate, etc.)

These application scenarios outline the need for protected biometric identifiers as dedicated form of a secure Privacy-Enhancing Technology (PET) beyond symmetric or asymmetric encryption of the biometric reference record. In order to achieve biometric PET, this paper outlines a concept that will be researched in the project TURBINE which is funded under the EU 7th research framework programme. The goal of this research is to provide significant advances over currently used ID management techniques. This can be reached with the following principal objectives:

- As opposed to current biometrics based identity management solutions, no trade-offs between high security and respect of privacy shall be required; TURBINE technology will simultaneously deliver both. It enables high security for the operators/the authorities and uncompromised levels of personal privacy for the individual.
- Biometric templates of enrolled subjects are not stored. Individual retain complete control of their biometric data.
- Multiple identities, including pseudo-identities can be generated from a single biometric characteristic without any risk that these can be linked together; and any of these identities can be cancelled and replaced by a new one. The project will research the practical impact of what happens when a biometric identity or a pseudo-identity is breached and thus needs to be revoked. This will include the case where some or all of the identities/pseudo-identities are stored on the user's tokens and may require continued validity for some transitional period, which would depend on the actual role/use of the identities. The ideal system will be flexible and give several options to each of these scenarios.
- Higher security, because more complex identifiers with inherent resistance to most of the known attacks (substitution, tampering, Trojan horse, masquerade, etc.,) can be used.
- Interoperability: The capability to analyze biometric references from multiple vendors (multi-source) will be fostered regarding the protection mechanism, without losing verification performance.
- The research will aim to develop the mechanisms that are required to effectively operate the trusted pseudo-identities built on protected fingerprint templates. In line with the performance objectives of the template protection processes, efficiency and ease of use will be targeted to make the designed architecture a viable privacy-enhanced user-centric solution with a high level of trust.

Figure 1 illustrates the basic concept of pseudo identities. Sensitive information such as biometric samples or biometric templates are processed such that the generated biometric reference is a non-invertible yet unique identifier.

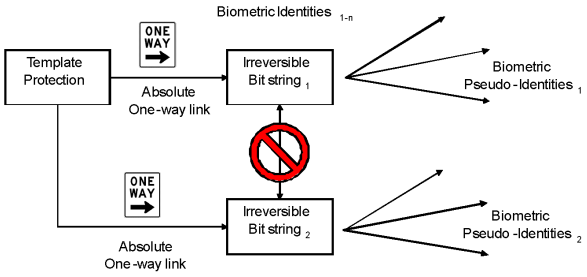

Figure 1. Pseudo identities derived from biometric samples.

To achieve this level of innovation in the domain of identity management, TURBINE will carry out innovative research and technology development work focused on the underlying core technologies of both biometrics and cryptography.

2 Related Work

Biometric template protection techniques provide technological means to protect the privacy of biometric reference information stored in biometric systems. These methods stand in sharp contrast to approaches where biometric information is protected only by legislation and unreliable procedures around storage facilities. Template protection guarantees the protection of biometric information without

the assumption that individuals must be trusted or procedures are properly implemented. Template protection techniques transform classical representations of biometric references (e.g. the image of an iris, a feature vector derived from a face, etc.) into a so-called secure template. These secure templates are constructed such that it is very hard to retrieve information regarding the original biometric sample. Furthermore, comparison is done directly on the secure templates. Lastly, in many implementations of template protection it is possible to derive several distinct secure templates from a single biometric characteristic. Template protection brings huge benefits for biometric systems[12].

A centralised database can be constructed in compliance with privacy laws. Distinct templates from the same biometric characteristic can also be generated for different applications, in order to reduce/eliminate possibility of cross matching. Revocation and reissue is feasible in case of such template compromise. Risks of spoofing attack using stored or transmitted template can also be prevented. One of the first concepts for biometric template protection was pioneered in 1994 by George Tomko[27]. Since then, about 50 universities and commercial companies have reported on similar types of technologies in scientific papers and patents.

Key academic institutions and industry leaders are Michigan State University, University of Bologna and IBM, RSA, Sagem Sécurité and Philips, respectively[1]. Over time, different approaches to template protection mechanisms have been presented and the following ones seem promising:

1. *Biometric salting* - Concatenated hash of biometric templates with a high entropy ”password”.

2. *Non-invertible transforms* - Original biometric samples cannot be extracted from the protected templates[23], [24].

3. *Fuzzy schemes* - These methods are based on a fuzzy commitment scheme[19], fuzzy extractors[13] and helper-data schemes[21] (see also[16],[29]). Examples of practical implementation of fuzzy schemes are given in[30], [28], [32], [17], [14], [33], [6], [9].

4. *Fuzzy vault schemes* - A particular family of fuzzy schemes proposed by Juels and Sudan[18] based on chaffing and winnowing. Example of implementations for minutiae are[31], [22].

5. *Secured comparison* - Utilization of enhanced cryptographic mechanisms to achieve comparison bit by bit of data while still encrypted[4], [15], [26], [10], [8].

[1]Recent research projects include the french ANR RNRT project BACH and the European FP6 project 3D-Face.

6. Or combination of several techniques, e.g.[7], [20],[9], [11], [5].

Although there is a decade of history in biometric template protection technology developments, to date, commercial systems are not yet deployed. There are two main reasons for this: (i) the technical difficulty in applying cryptographic protection techniques on noisy biometric data and (ii) the lack of awareness of these privacy enhancing technologies by the political decision makers. Also biometric protection techniques are difficult to apply to traditional minutiae based fingerprint systems.

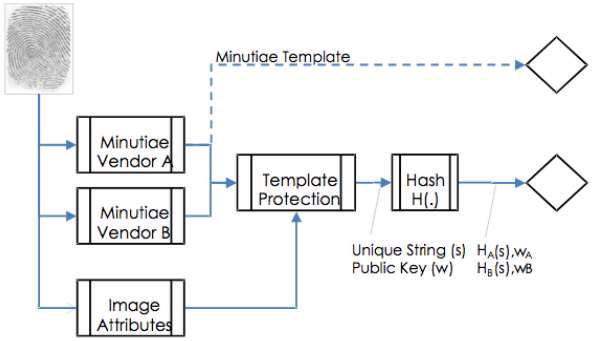

Figure 2. Template protection and hashing

The system presented by Ratha, Connell and Bolle is proposing a solution for minutiae fingerprint [23]. The main drawbacks of this approach are that it is not based on cryptographic techniques and hence security cannot easily be proved. Security of practical constructions have recently been investigated by Scheirer [25]. The approach of using fuzzy schemes combines cryptographic techniques with error correction coding so that off-the-shelf hashing tools can be deployed. However, TURBINE will not confine itself to off-the-shelf hashing tools. The error-correction makes sure that stable feature vectors can be derived from the noisy biometric input data. Practical implementations of these systems for different biometric modalities like face, pattern fingerprint and iris are successfully reported [30], [28],[32],[17], [6],[9]. Although these systems are suited for these modalities, current state-of-the-art does not allow usage on minutiae-based fingerprint systems. In the TURBINE project we focus on adapting this approach to minutiae fingerprints.

This requires the processing of an unordered set of ”noisy” minutiae features (i.e. locations, ridge directions etc). The goal of TURBINE is to find effective transforms that translate these unordered feature sets to an ordered float features vector, such that we obtain comparable matching performance while introducing privacy protection.

Figure 2 shows the overall structure of such a system. The first 3 blocks perform the feature extraction and subse-

quent blocks the template protection and hashing. In general, applying template protection may result in some performance loss in terms of FAR and FRR of biometric systems. TURBINE will also address this problem and aims to minimize the performance loss such that it becomes negligible with respect to the current state of the EER art which today is in the order of 10^{-2}.

3 Project Objectives

TURBINE aims to explore and help to establish an innovative use of cancellable fingerprint based identity management for applications in the real and the virtual world that will provide trust for service operators and end-users. The project addresses the full-scale verification of identity.

In keeping with its intended use as a Privacy Enhancing Tool, and for instance in order to eliminate the need for databases holding information on the protected templates, TURBINE will allow an individual to hold a personal secured token, to manage his identities (legal and pseudo), such as a legal identity for central eGovernment or local town hall services, and also various pseudo-identities, e.g. for Internet services, loyalty cards etc. The identities are consolidated from the same individual using a "protected" biometric template that can be cancelled and re-issued.

TURBINE research work will address the fundamental challenges of fingerprint biometric cryptography and also aim at establishing the large deployment capability of this technology. It aims to eliminate the current perception that increased security and privacy is a zero sum game, by demonstrating that both are possible simultaneously and that the authentication security needs of the operator and the trust requirements (security and privacy) for the individual can be consistently met in a convenient and application specific manner.

The underlying scientific/technical challenges and objectives required to deliver a revocable protected biometrics based identification include a range of specific functionalities, distortion tolerance performance and other capabilities. The relevant project objectives are briefly outlined and summarised under the following headings:

1. *Revocable protected biometrics references*

   Evaluate extent to which a practical protected fingerprint biometric reference can be consistently generated from the fingerprint image shape and minutiae associated with the chosen transformations. Ensure that the "protected" biometric information cannot be used to derive the original biometric data (image or minutiae). Ensure that the "protected" biometric information can be cancelled and a new replacement can be readily and securely generated. Ensure that a protected biometric sample can be processed to generate different application specific results and that such capabilities are supported in the replacement biometric reference in the event of cancellation for whatever reasons.

2. *Distortion Tolerance Performance*

   Evaluate and ensure, possibly for example via a normalisation and vector threshold scheme, that the association of transformation and a captured fingerprint can be used in instances where only a subset of the fingerprint minutiae can be matched.

3. *Evaluation at High Confidence Level*

   Evaluate and ensure targeted accuracy, reliability and convenience in 1:1 verification implementations using available and independently compose fingerprint databases. The primary scalability objective will be to assess the applicability for very large population verification systems and compile accurate performance data confirming the success and providing important contextual information about such implementation (performance, accuracy and exception processing).

4. *Biometric Template Protection and Multi-source Interoperability*

   A specific objective will be to ensure that the protection deployed on the biometric sample has the lowest possible impact on biometric verification performance. The protection mechanisms must also be designed to allow vendor independence via interoperable solutions i.e. the protection mechanisms and transformation deployed must ensure and allow that the Enrolment Algorithm and Query Algorithm for key generation process are well matched and separately usable by different system vendors. (see next sub-section).

5. *Interoperable ID management and standardisation*

   Any identity management scheme must be designed to last for several years and be rolled out and adopted by at least a significant number of the targeted population. Standardisation of specific interchangeable elements, and interoperability of identity management systems are therefore essential. The key issue for TURBINE in this respect is the capability to encourage and adopt interoperable software and hardware components developed by different vendors. Ensuring adequate knowledge and support for existing deployed solutions is essential while ensuring sufficient flexibility and scope to accommodate emerging standards and future evolutions. Thus TURBINE will pay particular attention to the process for developing and releasing the specifications that vendors must use to ensure the needed interoperability. Contributions will be made by the consortium to ISO/IEC JTC1 standardisation in SC37 and

SC27 where WD ISO 24745 is relevant to the project work.

6. *Use of Smaller Fingerprint Templates*

   TURBINE will investigate the use of very small fingerprint templates. The compact size of the template is not the main goal. The objective is based on the data protection principle of proportionality and ensuring that the TURBINE solution can be tailored to mix security and privacy according to the needs of specific applications. From the "minimal data" perspective it is envisaged that the size of the fingerprint template could be correlated with the level of security required for particular applications. Thus research will be conducted on varying the size of the template and determining how this may be used to meet levels of security in different identity verification scenarios. In addition, this research will be used to position image size in relation to boundary conditions in the entropy requirements for biometric template protection.

7. *Multi-application usage and Pseudo-identities*

   TURBINE will design and test a process and technology that allows the embedding of the interoperable "protected" biometric information into a secure token. The use and resilience of multi-application specific information based on the same biometric sample will also be evaluated. In this respect TURBINE will propose and evaluate mechanisms for the management of secure tokens and multiple identities for a same person, where each identity can be trusted based on a protected biometric mechanism. This approach must support provision of different pseudo-identities for the same individual that are all protected and consolidated on the same secure token. These pseudo-identities will also, where required, be compatible with a "legal" identity. This pseudo-identity requirement is in line with the recommendations from previous RTD projects like PRIME and INSPIRED (INtegrated Secure Platform for Interactive tRusted pErsonal Devices) which have consistently shown that people also need identities with a subset of information related to the context of specific applications [3],[2].

8. *Privacy protection / legal framework*

   The projects PRIME and BITE have confirmed that identity information is considered as sensitive information by the European citizen: there is an expectation of adequate privacy protection and also for evidence of a strong trusted authentication mechanism which minimises possibility of identity theft [3], [1]. A consequence of citizen expectations in the context of new emerging technologies is a new set of legal requirements and issues in the protection of private data. One of the key objectives of the RTD work will be to ensure that the developments of TURBINE efficiently address privacy protection requirements according to the EU and member state regulations and laws. It will study and evaluate attack resistance and in particular provide mechanisms to assess the level of trust inherent in such solutions, and progress any recommendation provided by the project regarding the current legal framework.

One of the challenges to achieve theses objectives is to enhance the stability of existing fingerprint templates: Limit the noise and variations of extracted minutiae and to explore the mixing with additional fingerprint attributes to obtain good foundations for the template protection mechanisms.

4 Conclusion

The multi-disciplinary project TURBINE presented in this paper aims at producing a privacy enhancing technology, combining innovative developments in cryptography and fingerprint biometrics. It aims at providing highly reliable biometric 1:1 verifications, multi-vendor interoperability, and system security, while solving major issues related to privacy concerns associated to the use of biometrics for ID management.

TURBINE will remove the current barriers in the use of biometric solutions for user identification: for the first time, no trade-off will need to be made between the level of security provided to the service supplier/merchant in terms of secure authentication, and the level of security provided to the individual in terms of protection of personal data. The technology developed in TURBINE could be implemented in a large variety of applications in the real and the virtual world. To ensure that the developments meet the needs of the various potential market segments and the European and national regulations regarding privacy, the consortium will benefit from the advice of experts in data protection from different European institutions and from representative market sectors, such as banking, eHealth, eGovernment, and airport security.

Acknowledgment

This work is supported by funding under the Seventh Research Framework Programme of the European Union, Project TURBINE (ICT-2007-216339). This document has been created in the context of the TURBINE project. All information is provided *as is* and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The European Commission has no liability in respect of this document, which is merely representing the authors' view.

References

[1] Biometric identification technology ethics - bite. http://www.biteproject.org/, February 2008.

[2] Inspired, the future of smart card. http://www.inspiredproject.com, February 2008.

[3] Privacy and identity management for europe - prime. https://www.prime-project.eu/, February 2008.

[4] M. J. Atallah, K. B. Frikken, M. T. Goodrich, and R. Tamassia. Secure biometric authentication for weak computational devices. In *Financial Cryptography*, pages 357–371, 2005.

[5] J. Bringer and H. Chabanne. An authentication protocol with encrypted biometric data. To appear in *AfricaCrypt*, 2008.

[6] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. In *IEEE Conference on Biometrics: Transactions, Applications and Systems -BTAS'07*. IEEE Press, 2007.

[7] J. Bringer, H. Chabanne, and Q. D. Do. A fuzzy sketch with trapdoor. *IEEE Transactions on Information Theory*, 52(5):2266–2269, 2006.

[8] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, and S. Zimmer. An application of the Goldwasser-Micali cryptosystem to biometric authentication. In *ACISP*, pages 96–106, 2007.

[9] J. Bringer, H. Chabanne, and B. Kindarji. The best of both worlds: Applying secure sketches to cancelable biometrics. *Science of Computer Programming*, 2008. To appear. Presented at WISSec'07.

[10] J. Bringer, H. Chabanne, D. Pointcheval, and Q. Tang. Extended private information retrieval and its application in biometrics authentications. In *CANS*, 2007.

[11] J. Bringer, H. Chabanne, D. Pointcheval, and Q. Tang. A formal study of the privacy concerns in biometric-based remote authentication schemes. To appear in *ISPEC*, 2008.

[12] A. Cavoukian and A. Stoianov. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacyp. Technical report, Information and Privacy Commissioner / Ontario, March 2007.

[13] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extrators: How to generate strong secret keys from biometrics and other noisy data. In L. 3027, editor, *In Advances in cryptology - Eurocrypt'04*, pages 523–540. Springer, 2004.

[14] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia. Using distributed source coding to secure fingerprint biometrics. Technical Report TR 2007-005, Mitsubishi Electrical Research Laboratories, Jan. 2007.

[15] J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. J. Strauss, and R. N. Wright. Secure multiparty computation of approximations. *ACM Transactions on Algorithms*, 2(3):435–472, 2006.

[16] J. Goseling and P. Tuyls. Information - theoretic approach to privacy protection of biometric templates manuscripts. In *IEEE international symposium on information theory (ISIT2004)*, page 172, 2004.

[17] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. *IEEE Computer*, 55:1081–1088, 2006.

[18] A. Juels and M.Sudan. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory*, page 408, http://biometrics.cse.msu.edu/uludag-jain-fuzzy-fp.pdf, June 2002.

[19] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *6th ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[20] A. N. K. Nandakumar and A. Jain. Hardening fingerprint fuzzy vault using password. In *ICB*, 2007.

[21] J. P. Linnartz and P. Tuyls. New shiedling functions to enhance privacy and prevent misuse of biometric templates. In *4th international conference on audio- and video-based biometric person authentication*, 2003.

[22] K. Nandakumar, A. Jain, and S. Pankati. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2008.

[23] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy of biometric-based authentication systems. *IBM Systems Journal*, 40, 2001.

[24] N. Ratha, S.Chikkerur, J. Connell, and R. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, April 2007.

[25] W. J. Scheirer and T. E. Boult. Cracking fuzzy vault and biometric encryption. In *Biometric Symposium*, pages 1–6. IEEE Press, September 2007.

[26] B. Schoenmakers and P. Tuyls. Efficient binary conversion for Paillier encrypted values. In *EUROCRYPT*, pages 522–537, 2006.

[27] G. Tomko, C. Soutar, and J. Schmidt. Fingerprint controlled public key cryptographics system. US Patent 5541994A, September 1994.

[28] P. Tuyls, A. M. Akkermans, T. Kevenaar, G.J.Schrijen, A.M.Bazen, and R.N.J.Veldhuis. Practical biometric authentication with template protection. In *Audio- and Video-Based Biometric Person Authentication*, volume 3546 of *Lecture Notes in Computer Science*, pages 436–446. Springer Belin / Heidelberg, June 2005.

[29] P. Tuyls and J. Goseling. Capacity and examples of template protecting biometric authentication systems. In LNCS, editor, *Biometric authentication workshop (BioAW 2004)*, volume 3087, pages 158–170, Prague, 2004.

[30] P. Tuyls, E. Verbitskiy, T. Ignatenko, D. Schobben, and T. H. Akkermans. Privacy protected biometric templates: ear identification. In *Proceeding of SPIE*, volume 5404, pages 176–182, April 2004.

[31] U. Uludag and A. Jain. Securing fingerprint template: Fuzzy vault with helper data. In *IEEE Workshop on Privacy Research in Vision -PRIV*. IEEE Press, 2006.

[32] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. Akkermans, and F. Zuo. Face biometrics with renewable templates. In *Proceedings of SPIE*, volume 6072. SPIE, 2006.

[33] X. Zhou, T. Kevenaar, E. Kelkboom, C. Busch, M. van der Veen, and A. Nouak. Privacy enhancing technology for a 3d-face recognition system. In *BIOSIG 2007: Biometrics and Electronic Signatures*, volume P-108 of *Lecture Notes in Informatics*, pages 3–14. GI-Edition, July 2007.