Synthesis
International Scientific Conference of IT and Business-Related Research

PRIVACY FRIENDLY BIOMETRICS

BIOMETRIJA PRIVATNOSTI

Milivoj Mrdaković, Saša Adamović
Faculty of Informatics and Computing, Singidunum University, Belgrade, Serbia

Abstract:
A wider use of biometric devices has led to a greater level of privacy loss. Numerous organizations have created centralized databases of individuals, which often go beyond the legal framework. When such data are compromised, it can mean a kind of "digital death" of an individual.
On the other hand, there is an increasing need for true random generated sequences (TRNG) that can serve as a unique crypto key of individuals. This paper incorporates the concept known as "revocable" or "cancellable biometrics" and offers schemes (in this particular case of traffic control) where biometric data become the specific guardian of one's personal identity, under a term "Privacy friendly biometrics".

Key words:
cancellable biometrics, revocable biometrics, security, encryption, authentication.

Apstrakt:
Sve šira upotreba biometrijskih uređaja uslovila je sve veći stepen gubitka privatnosti. Mnoge organizacije stvaraju centralizovane baze podataka o pojedincima, koje često izlaze van zakonskog okvira. Kada se podaci kompromituju, to može značiti svojevrsnu „digitalnu smrt" pojedinca.
Takođe, postoji sve veća potreba za potpuno slučajnim nizovima bita koji mogu poslužiti kao jedinstveni kripto-ključevi pojedinaca. Ovaj rad obuhvata i koncept poznat kao „opoziva" ili „otkaziva biometrija" (*cancellable, revocable)* i nudi šeme (u konkretnom slučaju kontrole saobraćaja), gde biometrijski podaci postaju specifični čuvar ličnog identiteta pojedinca, za koji je korišćen termin „biometrija privatnosti".

Ključne reči:
otkaziva biometrija, opoziva biometrija, bezbednost, šifrovanje, autentifikacija.

1. INTRODUCTION

Ever since 1890., when Samuel Dennis Warren and Louis Brandeis Dembitz published the article "*The Right to Privacy*" in the "*Harvard Law Review*", this topic hasn't lost its importance even though its concept has become increasingly challenged and reduced. After 9/11. and "*Patriot Act*" (2001), there has been a partial replacement of the concept of privacy – to security concept. Many critics of this position, such as a Roger Clark, Ph.D. (Australia), warn that "the issue of privacy is not an issue of secrecy but of control." It is worth noting that the issue of information privacy is not just a matter of protecting data, because data protection represents only part of the protection of privacy (Subotić, 2011).

As regards protection of privacy in the information age, it is necessary to emphasize that it is a very important concept of anonymity. Also, it has become very difficult to determine the required balance between anonymity and unequivocal authentication, so it is often a conflict of interest. While searching for a compromise, experts have developed the concepts of "*cancellable biometrics*", „*Privacy by Design*" (in Canada) *etc.*, which are the starting point of this paper.

All in all, the right to privacy is a fundamental right, which is protected by numerous international documents such as the *Universal Declaration of Human Rights, the International Convenant on Civil and Political Rights, Convention for the Protection of Human Rights and Fundamental Freedoms.*

2. AUTHENTICATION - GENERAL INFORMATION

Authentication (Greek: *αὐθεντικός* authentikos - real, genuine, from *αὐθέντης*, authentes, author) is an act of confirming the truth of an attribute of a single piece of data (datum) or an entity. Unlike identification related to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming such identity (Wikipedia, 2015).

Biometric authentication is the process of authentication, which involves biometric readings. It is generally divided into two phases:

- *enrollment phase* (which means reading the biometric data of an individual, and creating templates for storage (in the case of revocable or cancellable biometrics), and
- *authentication* (or verification), which involves re-reading (re-creation of the template) and comparison with templates located in the database.

Biometric readings are rarely identical. They are dependent on the conditions of reading and technology used (device diversity). The template is an approximate representation of biometric data (transformed by some irreversible algorithm), and performance verification depends on how much was previously enrolled, with reference pattern being similar to the control one (Ang *et al.*, 2005).

Bearing in mind that authentication based on biometrics can provide irrefutable proof of the user's identity, and that during the life of an individual such data do not change, it is important to keep this information.

Authentication is the very beginning of the procedure that state officers do every day in relation to their citizens. In front of the counter officers, police officers, voting committee members (*etc.*) the "evidence that it's really you," includes a kind of identity card, driving licence, social security card, passport, and payment card, provincial or territorial ID card, contact or contactless, with or without radio Radio-frequency identification chip (RFID).

E-mail: milivoj.mrdakovic.12@singimail.rs

DOI: 10.15308/Synthesis-2015-67-70

There is a lot of sensitive data such as medical data, personal property data, bank account data, student index data, penalty points in the driving licence, *etc.*, that could disqualify or jeopardize a person in several life situations. Centralization of databases and profiling represent a direct attack on privacy, and thus, it is important to distribute databases with controlled access authorization. Also, identification documentation could be stolen, lost, or forgotten, but you "bring yourself with you", that is - biometrics, "something that you are".

3. RELATED WORKS

The following idea of privacy protection, and looking for renewable biometric readings, cancellable *or revocable biometrics* was born (Ratha *et al.*, 2007).

Cancellable biometrics means irreversible transformation and storage of biometric data in a "pattern" (or template). If the transformed version in database eventually gets compromised, it will not come to the privacy breach such as identity theft. Transformation is one of the methods that allows the possession of the transformed biometric information which does not reveal information about the actual biometric data.

Cancellable biometrics also provides a higher level of privacy, allowing many different templates from the original biometric data and therefore, the inability to link data stored in different databases (Ang *et al.*, 2005).

A somewhat different approach is the concept of ***Biometric Encryption*** - *(BE),* first introduced in the mid 90's by George J. Tomko, Colin Soutar, and Gregory J. Schmidt. It is a group of technologies (related to cancellable biometrics) that have two approaches:

- *key binding*, when an arbitrary key (*e.g.*, randomly generated) is securely bound to the biometric, and
- *key generation*, when a key is derived from the biometric (Cavoukian & Stoianov, 2009).

The main technological challenge is to have the same digital key again, despite natural variations in the input biometrics. Thus, there are three ways in which we can express the performance of a biometric system: FRR (*False Rejection Rate),* FAR (*False Acceptance Rate),* and GAR *(Genuine Acceptance Rate).*

Ong, Teoh and Connie (2007) have published in their work the information that there are algorithms with an extremely high level of genuine acceptance rate (GAR) accurate with 99, 83% , false acceptance rate (FAR) that weights to zero rate and false rejection rate (FRR) of 0.17%.

4. ASSUMPTIONS FOR THE PROPOSED PRIVACY FRIENDLY BIOMETRIC (PFB) SCHEMES

The necessary preconditions for successful functioning of the scheme are:

- Wireless security between the mobile biometric reader and remote database is completely safe. Data exchange is encrypted using (for example) the IPSEC Internet protocol.
- Physical security of wireless, mobile devices and database is also unquestionable. The device maintains the armed policeman who exceeds the device, and database objects are under the supervision and with limited access.
- Attack by "silicone finger" is impossible because of the presence of the policeman who controls the finger before reading.
- The readout image is "perfect". Reading can be repeated any number of times, in case of rejection of the system.

THE PARTICULAR CIRCUMSTANCES – PROPOSED PFB SCHEME 1 (FIGURE 1)

Traffic police officer has a device that is in a secure wireless connection to the database. In the course of regulation and traffic control, the vehicle stops and starts the authentication process.

After the official greeting, friendly but authoritative, police officer requires that the driver provides information on his/her name and surname (driver does not even need driver's licence), and should position the index finger of his right hand on a mobile biometric reader at a designated place.

Then, the procedure starts by scanning and processing fingerprint, mainly based on the key points of minutiae of a fingertip. This result is binary template data A. It is sent to two addresses. One template copy is sent through transformation and results in changed template data A'. The second, untransformed copy (template) meets the first copy A' in the algorithm for transformation, where they are binding (fingerprint template A and A') and become irreversibly altered. (It can be said that there is a lock operation under the transformed biometric pattern – by non-transformed biometric template.)

After that, the wireless computer system, by tunneling, the ciphertext (A, A') which is actually a biometric key, arrives to a remote computer system that verifies that key, compares it with the deposited biometric keys. If verification process is successful, the system "unlocks" the appropriate minimum file with necessary data and sends them to a networked wireless biometric reader (to the police officer). If verification is negative, the officer receives a systemic message and repeats the process.

It is extremely important to note that after the transformation of both binary results (on a mobile browser), they are deleted from the remote reader memory. Any attacker, who „sniffs", *i.e.*, eavesdrops on traffic, captures completely unintelligible data.

The downside of this scheme would be the possibility of frequent rejection of results, which is naturally caused by variations in readings, but considering the existence of algorithms (which have already been mentioned) with high levels of accuracy, this can be overcome.

THE SECOND SITUATION – PROPOSED PFB SCHEME 2 (FIGURE 2)

The first part of the second situation is identical to the first situation, up to the moment where the two binary results are hashed, instead of their algorithmic transformations. The hash value is sent through tunneling, and instead of biometric keys stored in databases, these hash values are actually "hash keys". They are compared and if the value is incorrect, the system acts as in the previous case.

THE THIRD SITUATION – PROPOSED PFB SCHEME 3 (FIGURE 3)

The third situation is development of Ann Cavoukian and Alex Stoianov idea, and it technically differs from the first two. It implies the existence of a key generator (PRNG) to generate pseudo-random key. After biometric readings and obtaining a biometric template, it binds template through the algorithm of transformation of the biometric encryption (BE)[1] system. Such transformed pattern goes to the remote system where it continues through an algorithm to reconstruct the key. Server reconstructed key is used (and pattern is erased) and unlocks the required information.

[1] More about Biometric encryption. (Cavoukian & Stoianov, 2009)

DOI: 10.15308/Synthesis-2015-67-70

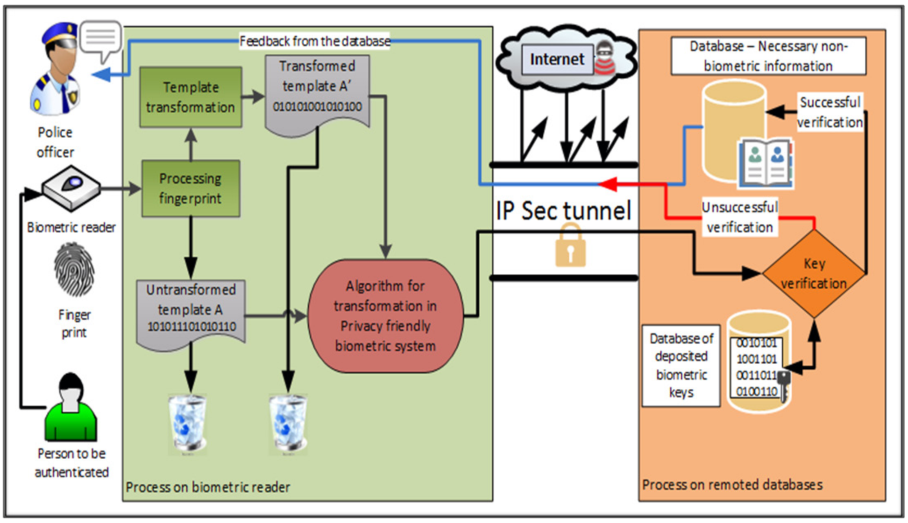
Police officer
Biometric reader
Finger print
Person to be authenticated
Feedback from the database
Template transformation
Transformed template A' 010101001010100
Processing fingerprint
Untransformed template A 101011101010110
Algorithm for transformation in Privacy friendly biometric system
Process on biometric reader
Internet
IP Sec tunnel
Database – Necessary non-biometric information
Successful verification
Unsuccessful verification
Key verification
Database of deposited biometric keys
0010101 1001101 0011011 0100110
Process on remoted databases

Figure 1. The particular circumstances.

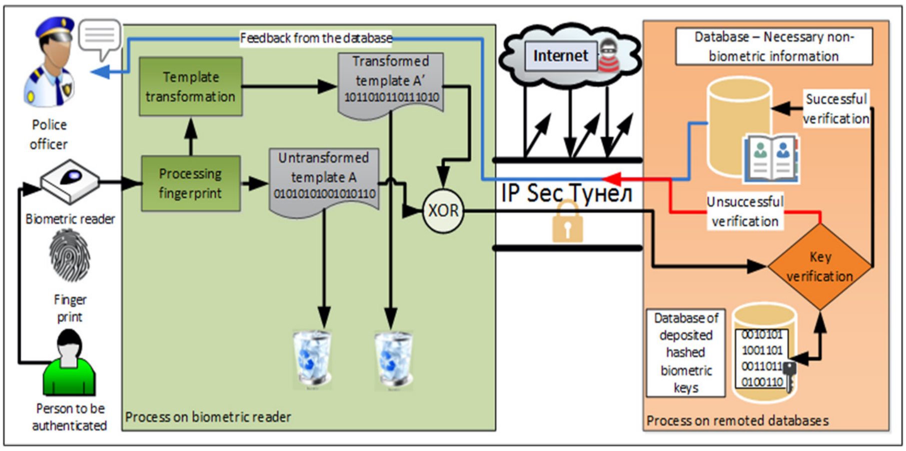
Police officer
Biometric reader
Finger print
Person to be authenticated
Feedback from the database
Template transformation
Transformed template A' 1011010110111010
Processing fingerprint
Untransformed template A 0101010100101010110
XOR
Process on biometric reader
Internet
IP Sec Тунел
Database – Necessary non-biometric information
Successful verification
Unsuccessful verification
Key verification
Database of deposited hashed biometric keys
0010101 1001101 0011011 0100110
Process on remoted databases

Figure 2. The Second Situation.

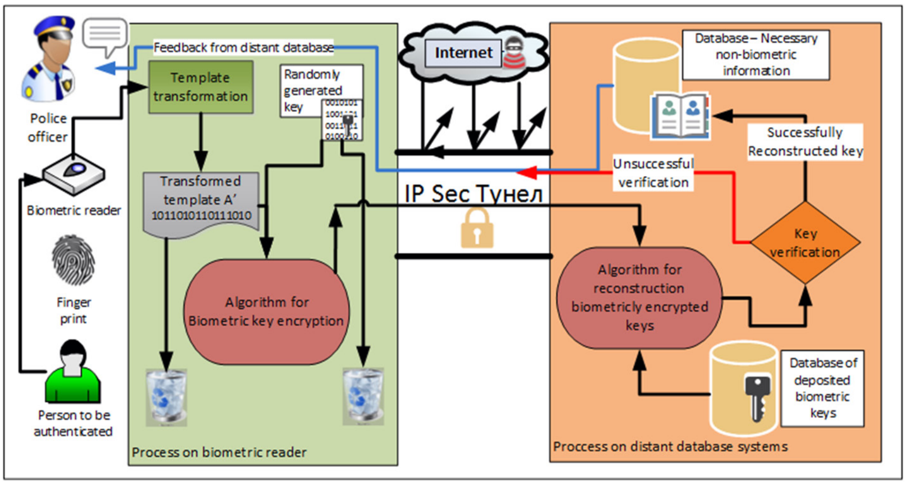
Police officer
Biometric reader
Finger print
Person to be authenticated
Feedback from distant database
Template transformation
Randomly generated key
Transformed template A' 1011010110111010
Algorithm for Biometric key encryption
Process on biometric reader
Internet
IP Sec Тунел
Database – Necessary non-biometric information
Successfully Reconstructed key
Unsuccessful verification
Key verification
Algorithm for reconstruction biometricly encrypted keys
Database of deposited biometric keys
Proccess on distant database systems

Figure 3. The Third Situation.

Such a model can have a potentially high rate of false-accepted keys, but it still depends on the quality of the algorithm. The philosophy of such systems must be fuzzy in order to increase the rate of accuracy and alignment of Hamming distance to the true value can be crucial.

What would certainly be interesting is that a traffic policeman on the ground, would not have access to whole databases on the server (could not " inspect the base") without individual biometrics that can unlock "his" record.

Upon checking, the officer determines whether a person has a driver's license, whether it has been banned or similar. As said at the beginning, a police officer requires the name of the driver, which is a secondary measure of accuracy of biometric data.

Specifically, there is an extremely small probability that the driver and the appearance of a person in the photograph, the name of the driver and the name in data, and biometric readings are similar to those in the database. However, if the system made a mistake in readings and if the folder was inadequate, the officer would have seen the error of the system and repeated enrollment.

5. CONCLUSIONS

The implementation of privacy friendly biometric systems (PFBS) would have undoubtedly great economic, social and political outcomes. Below are listed some of them:

- In the first place, the abolition of the legal obligation of carrying personal documents (in those countries where such legal obligation exists).
- It could be concluded that there is no need for the existence of any personal ID.
- Unambiguous authentication against a civil servant if the improved algorithms achieve the desired 100% accuracy authentication.
- State budgetary savings, and the savings of citizens on the costs related to the identity dosumentation issuance
- The impact on privacy would also be huge. Instead of piling up, centralization of data and profiling of citizens, would initiate opposite trends.
- There would also be some political consequences. A good and honest software solutions could eliminate manipulation around multiple voting on elections. One could vote anywhere in the country, and at any moment, election commission would know the exact number of votes at the polls. Currently, obtaining a mass of data could be useful in social and political analysis.
- Increased comfort, freedom and the sense of happiness due to the lack of obligation to carry documents.
- Danger of chipping and cyborgization of people could be averted and is more discussed. The risk of totalitarian society is always present where data can be centralized and total control established.

Finally, the conclusion can be made that the biometrics certainly cannot be stopped. It should be used for preservation of privacy and promotion of human rights and freedom.

REFERENCES

Arsenin, A. (2012). *Privatnost u 21. veku.* Belgrade: Catena Mundi.

Ang, R., Safavi-Naini, R., & McAven, L.F. (2005). Cancelable key-based fingerprint templates. *Cancelable key-based fingerprint templates. In C. Boyd & J. Gonzalez Nieto (Eds.),* (pp. 242-252). Germany: Springer: Australasian Conference on Information Security and Privacy.

Cavoukian, A., & Stoianov, A. (2009). Biometric Encryption. In A. K. Stan Z. Li, *Encyclopedia of Biometrics* (pp. 1-14). Springer.

Gao, P.Q. (2010). Recent Developments on Applying Biometrics in Cryptography. *Journal of Applied Security Research*, 107-137.

Kenneth R.M., Higgins, P., McCabe, M., Prabhakar, S., & Swann, S. (2004). Automated Fingerprint Identification System - AFIS. U N. I. Justice. In *The Fingerprint Sourcebook* (6th chapter). Washington, DC 20531: U.S. Department of Justice, Office of Justice Programs.

Mankame, R.S. (2013). A Study of Biometric Approach Using Fingerprint Recognition. *Lecture Notes on Software Engineering,* 1(2), 209-213.

Nalini, K.R., Chikkerur, S., Connell, J.H., Bolle, R.M. (2007). Generating Cancelable Fingerprint Templates. *IEEE transactions on pattern analysis and machine intelligence,* 29 (4), 561-572.

Ong Thian Song, Andrew Teoh Beng Jin, Tee Connie. (2007). Personalized biometric key using fingerprint biometrics. *Information Management* & *Computer Security,* 15(4), 313-328.

Ravi Subban, D.P. (2013). A Study of Biometric Approach Using Fingerprint Recognition. *Lecture Notes on Software Engineering,* 1(2), 209-213.

Stanković, O., & Vodinelić, V. (1996). *Uvod u grđansko pravo.* Belgrade: Nomos.

Subotić, O. (2011). *Information Controlled Society (Informaciono kontrolisano društvo - in original).* Belgrade: Bernar.

Wikipedia. (2015). *Authentication.* Retrieved March 14, 2015, from Wikipedia, The Free Encyclopedia.: http://en.wikipedia.org/w/index.php?title=Authentication&oldid=642448085

DOI: 10.15308/Synthesis-2015-67-70