Facial Recognition with Biometric Encryption in Match-on-Card Architecture for Gaming and Other Computer Applications (Feasibility Study)

June 30, 2014

Information and Privacy Commissioner, Ontario, Canada

Ontario Lottery and Gaming Corporation, Canada

Morpho (Safran), France

Authors:

Ann Cavoukian, Ph.D.
Michelle Chibba, M.A.
Alex Stoianov, Ph.D.
Office of the Information and Privacy Commissioner of Ontario, Canada

Tom Marinelli, P.Eng.
Klaus Peltsch, M.Sc., M.B.A.
Ontario Lottery and Gaming Corporation

Hervé Chabanne, Ph.D.
Olivier Beiler, M.Sc.
Julien Bringer, Ph.D.
Vincent Despiegel, Ph.D.
Morpho (Safran)

Acknowledgements

The authors would like to express their gratitude to Jean-Christophe Fondeur for helpful discussions and for continuous support of this work.

Information and Privacy Commissioner
Ontario, Canada

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

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

Facial Recognition with Biometric Encryption in Match-on-Card Architecture for Gaming and Other Computer Applications

(Feasibility Study)

Table of Contents

I. Introduction

Last year, as part of improvements in the Responsible Gambling program, the Ontario Lottery and Gaming Corporation (OLG) completed the implementation of facial recognition technology utilizing Biometric Encryption techniques in most of its casino facilities [1, 2]. Biometric Encryption or BE (a.k.a. biometric template protection, biometric cryptosystem, fuzzy extractor, etc.) is a process that binds a digital key to, or generates a key from, a biometric so that no biometric image or template is stored. This work was a result of a partnership with the University of Toronto, Ontario's Information and Privacy Commissioner (IPC) and OLG. The process employed *Privacy by Design* (*PbD*) techniques to ensure the privacy of the public and self-excluded players, while at the same time improving the overall detection rate of self-excluded patrons.

While the facial recognition with BE has delivered the best practice solutions for authentication, responsible gambling, player protection and privacy, there is an opportunity to determine if it is feasible to apply biometric authentication for other contexts. Some examples include authentication for online gaming, strengthening the lottery retail sales security (i.e. making sure that the person logged into the retail terminal is actually being verified for conducting each sales transaction), etc. Outside of the gaming industry, there are a countless number of applications where strong remote or local authentication is required, such as accessing electronic health records or other government-held personal records, online banking, etc.

The Office of the Information and Privacy Commissioner of Ontario, Canada, has approached OLG and Morpho, a world leader in biometrics, in order to conduct a research/feasibility study of privacy-protective biometric techniques. These techniques could improve the authentication, security and protection of users by setting a new 'gold standard' using persons' own facial biometric in Morpho's Match-on-Card architecture. OLG, from their side, contributed to this study by supplying the facial images of volunteers – taken at the OLG lab, thus capitalizing on the OLG's expertise in facial acquisition. In this joint paper, we present the preliminary results of this study.

The paper is organized as follows:

Section II introduces the context of the study and then outlines the *Privacy by Design* approach to biometrics; that is, privacy protection relies not only on regulatory or policy measures but is embedded into the system on a technological level. A brief overview of the objectives, including the key areas of research for this study, is presented in Section III. Section IV provides a high-level description of the proposed system, which is essentially a Biometric Encryption running in a Match-on-Card architecture. The results of our experiments with the OLG database of facial images are presented in Section V.

II. Background

Among authentication scenarios, the online authentication is by far the most challenging in the sense of making sure that the right individual is accessing the service. In the case of online gaming, the following are examples of requirements that may need to be met to verify the identity of an online customer:

- the individual must meet the legal minimum age requirement;
- where programs exist, the system should detect an individual who is a problem gambler, such as one who has self-excluded;
- identity theft should be thwarted, i.e. nobody else should obtain access to the user's account;
- the system should not be abused for illegal activities, such as money laundering;
- a user's privacy should be respected.

In other words, the system must ensure in a privacy-protective way that the right user is registered, and then, while accessing the service for gaming or other purposes, is correctly authenticated. Therefore, the online authentication includes two main steps: a) registration; b) authentication during gaming. The present industry standard is the following.

At registration (which can be either on-site or online), the user presents to a service provider (SP) a proof of his/her identity, such as a driver's license, a third-party verification (e.g., from a major bank where the user has an account). The SP would verify the user's information through its database(s) and work with the casino to ensure that the user is not self-excluded and meets other registration requirements (e.g., minimum age). At the end of the registration, an online gaming account is opened and the username and password are created. The SP may also provide a secure hardware token to the user.

During authentication, the user presents his/her username and password and, perhaps, the token. This would make a two-factor authentication, i.e. "what you know" and "what you have" pieces.

This general approach has a potential downside that both the user's token and password could be lost, stolen, borrowed, or shared. To do more to ensure that the right user is authenticated, a third piece of authentication, biometrics ("who you are") could be added. However, this would present privacy implications that are well documented in the literature [3]. A *Privacy by Design (PbD)* approach stipulates that privacy should not be sacrificed for the system security or functionality. They are all achievable by applying *PbD* principles that have become an international standard for privacy [4].

2.1. *PbD* approach to biometrics

As biometric uses and databases grow, so do concerns that the personal data collected will not be used in reasonable and accountable ways, especially given the recent revelations about the state surveillance programs [5]. The threat to privacy arises not from the positive authentication that biometrics provide best, but from the issues related to informational privacy rights that include potential data misuse, function

creep, linkage of databases via biometric templates, that make surveillance, profiling and discrimination without the knowledge of the individual, all possible. Biometric data transmitted across networks and stored in various databases by others can also be stolen, copied, or otherwise misused in ways that can materially affect the individual involved such as identity theft or fraud. Moreover, unlike passwords, biometric data are unique, permanent and therefore, irrevocable.

There have been a number of technological solutions proposed to address privacy issues in biometrics, such as Cancellable Biometrics, Biometric Encryption, Homomorphic Encryption, Weak Links, Biometric Setbase, and Match-on-Card. For the online applications such as gaming, Biometric Encryption in a Match-on-Card architecture seems to be the most feasible.

Biometric Encryption (a.k.a biometric template protection, biometric cryptosystems, fuzzy extractor, secure sketch, etc.) was proposed as a viable *PbD* approach to meeting the intent of conventional (mostly 1:1) biometric systems while at the same time addressing the privacy issues. BE is a group of technologies that securely bind a digital key to a biometric or generate a key from the biometric, so that no biometric image or template is stored. It must be computationally difficult to retrieve the key or the biometric from the stored BE data. The key (which we call Biometric Key, BK) can be recreated only if a genuine biometric sample is presented on verification. The output of the BE authentication is either a key (correct or incorrect) or a failure message. See surveys [6, 7, 8] for more details on BE.

Over the last few years, there has been substantial progress in developing BE technologies [9]. However, for some BE schemes there still exist accuracy and security problems. Consequently, a lot of work has been undertaken to attempt to integrate BE into cryptographic protocols (such as homomorphic encryption) to improve BE security [10, 11, 12, 13, 14]. One preferred solution, for the reasons described in the next sections, is to run BE in a Match-on-Card (MOC) architecture [15, 16].

III. Objectives and Overview of the Study

The objective of this study is to determine the feasibility of using facial recognition with Biometric Encryption (BE) in Match-On-Card (MOC) architecture utilizing a database of test images developed by OLG. The results will be used to assess the viability of such an approach in the online environment, such as gaming, to improve the authentication, security and protection of online users. In the OLG context, this could also be extended to the retail lottery environment to strengthen the security of retail sales.

The critical success factors important to the OLG applications are:

- Reliability of the facial recognition and Biometric Encryption technology to meet state of the art performance;
- Solutions identified to mitigate interference with customer experience; and
- Cost-effectiveness of the approach.

The technologies involved include video capabilities of mobile devices, facial recognition, Biometric Encryption and portable storage. The study areas need to explore the maturity of the technologies and their acceptable use.

The Match-on-Card (MOC) technology allows the secure storage and processing of biometric data within a tamper-resistant secure module (SM) of a device which is in the user's possession (e.g. smart cards, some USB flash drives, certain types of smartphones, etc.). This technology also allows the comparison of the new acquired biometric trait to the stored one directly on the card to avoid security leakage. It should be noted that MOC does not necessarily require a laptop or PC with a smart card reader; in fact, a variety of MOC products (see, for example, [17]) require nothing more than a USB port. Moreover, some smartphones already contain SM that can be used instead of a smart card.

A classic use-case scenario of the MOC (Fig. 1) could be described as follows:

a. The cardholder presents his/her card to a smart card reader.
b. The cardholder presents his/her biometric trait to a biometric sensor.
c. The host (a PC or a terminal connected to the smart card reader and the biometric sensor) establishes a secure session with the card.
d. The host prepares an encrypted template containing the features extracted from the biometric trait and transmits it to the card.
e The card decrypts the template and compares it with the reference template stored on the card.
f. The card returns result (Yes/No) to the host.

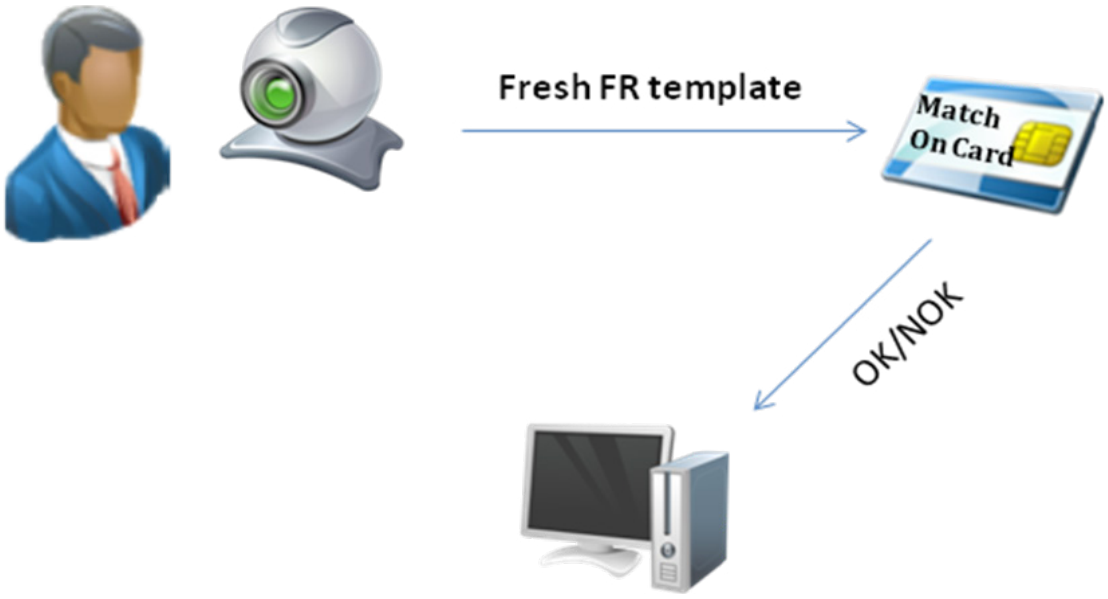

Fig. 1. Match-on-Card with facial recognition in a classic scenario.

As all image processing algorithms and the feature extraction process are performed on the host, only the comparison algorithms have to be implemented on the card or other storage device. This is made possible because these comparison algorithms, that classically run on a PC, have been optimized according to the hardware constraints of the smart cards.

The key areas of research for this study include:

a. Evaluation of the quality of the images captured by various hardwares, such as webcams, digital cameras, smartphone cameras, tablet computer cameras, and in various conditions (e.g., illumination);
b. Determining if Biometric Encryption in Match-on-Card architecture works with the images captured by those cameras;
c. Obtaining accuracy numbers and estimating the overall speed of the system by running simulations over the databases of images;
d. Specifying cryptographic protocols for secure and privacy-protective integration of all components of the system.

IV. Proposed System Approach

As shown in Fig. 2, the system uses facial recognition with Biometric Encryption in Match-on-Card architecture. The card is equipped with a tamper-resistant secure module (SM). Biometric data are stored and compared only locally, i.e. on the card, which is at all times in the user's possession. The server stores only a biometric key (BK) that is generated from the user's biometric by a one-way transform (e.g., hashing), i.e. the biometric cannot be reverse engineered from BK.

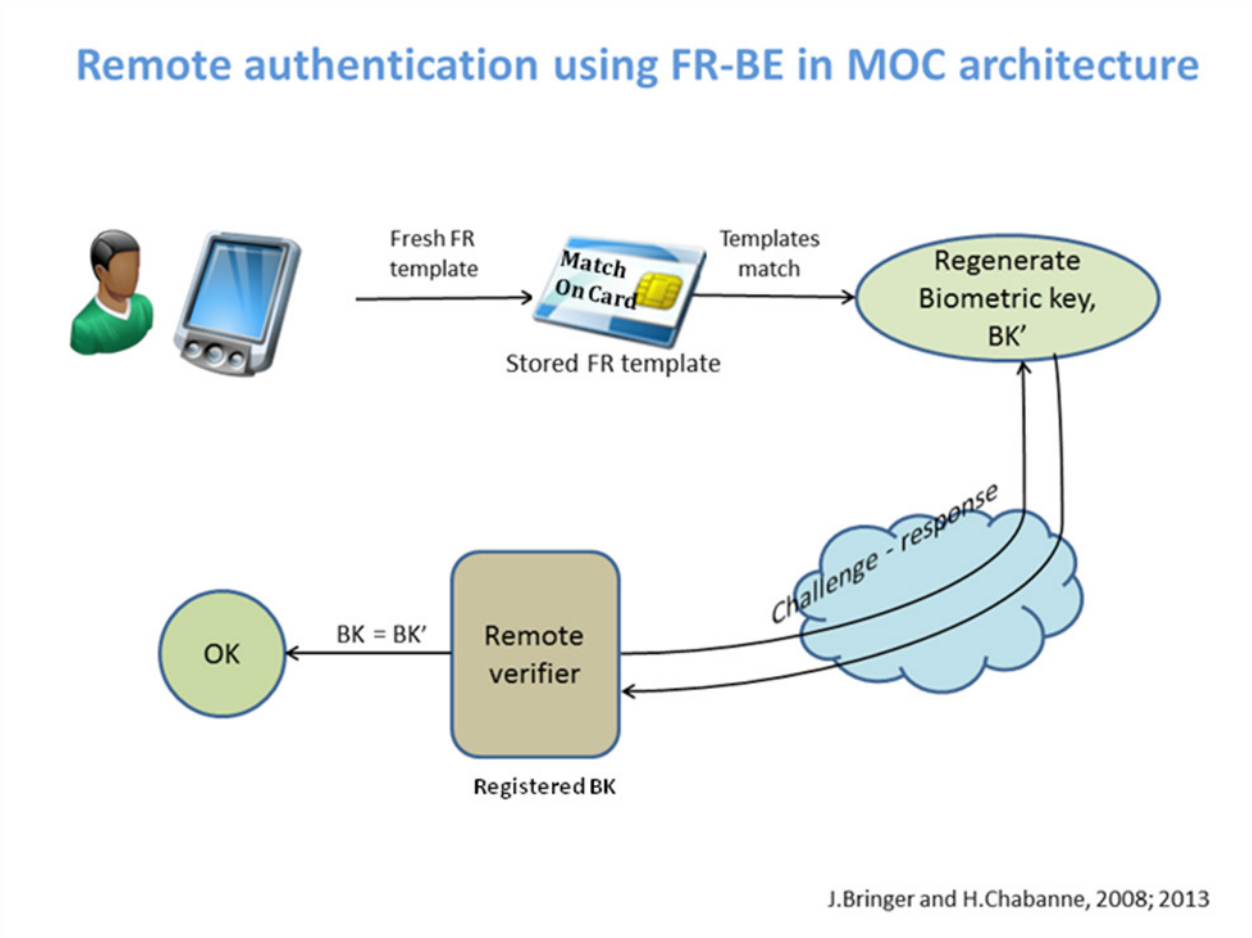

Fig. 2.

On enrollment/registration, the user's facial image is captured by a camera. A biometric reference template is created and stored in the SM of the card. A BK is generated from the reference template and is sent to the server where it is stored (in an encrypted or hashed representation). At the end of enrollment, all biometric information (i.e. image, template) outside of SM is deleted.

During authentication, a user's facial image is captured. A challenge/response cryptographic authentication protocol is established between the card, a local processor, and the server. This protocol does not require the user's anonymity. Upon positive liveness detection, a new biometric template (or a feature vector) is created from the image. It is matched within the card against the reference template stored in SM. In case of positive matching, the BK is regenerated and will play the role of a cryptographic key under the

challenge/response cryptographic authentication protocol. If the BK is the same as was generated on enrollment, the user will be authenticated by the server. Upon authentication, the biometric information outside of SM is deleted.

4.1 Choice of a biometric

The proposed system, with a possible exception of a one-to-many check during the registration, is essentially a one-to-one system. The user's identity is claimed as soon as the smart card is inserted into the reader. Also, the user in most cases has to enter a username and a password. Unlike the self-exclusion facial recognition project [1], in a one-to-one scenario other biometric modalities, e.g. fingerprints or irises, can be used. However, we believe that the face biometric remains a natural choice here, too, as:

- it is more acceptable to the public;
- it can provide real-time authentication without a significant effort from the user (e.g., the user does not have to put his/her finger on a fingerprint reader all the time – compare with the recently released iPhone 5S [18]);
- it could supposedly be made compatible with the existing self-exclusion facial database;
- OLG and the gaming industry as a whole have experience in dealing with face biometrics;
- the accuracy of face recognition has shown a dramatic improvement over the past 10 years.

Having said that, it should be noted that the state-of-the-art performance of face recognition in an uncontrolled environment similar to the proposed system may lead to a False Rejection Rate (FRR) of 2-4 percent (or even higher) at a False Acceptance Rate (FAR) of 0.1 percent. This means that 2-4 percent of the online gamers would encounter difficulty in authenticating themselves. There are other solutions that could improve the customers' experience and grant them the access to the online gaming in case of a failure of the biometrics. For example, a customer may contact a call center and provide security answers, etc. Such measures are outside of the scope of this study.

One of the concerns with face biometrics is its proliferation into social networks. There are more than a hundred billion online photos accumulated. It was demonstrated that a facial biometric template can be easily generated from these photos using off-the-shelf software [19]. As a result, a person can potentially be identified from a snapshot. Therefore, the proposed system must ensure that no biometrics is linked or leaked to the social networks or any other site. This is what makes MOC architecture with BE absolutely necessary to prevent this threat.

Also, the availability of face images makes spoofing attacks against the system possible (i.e. when an impostor presents a still photo to the camera instead of live image). The main countermeasure against spoofing includes liveness detection, such as the ability to estimate the 3-D shape of the face and reject all the spoofing attempts using planar attacks (photos). Some of these algorithms have been developed by Morpho. The liveness detection is challenging and necessary for any future deployment, but this topic is outside of the scope of this study.

4.2. Biometric Encryption (BE) in MOC architecture

The MOC system with BE was proposed in [15]. The registered biometric template is stored in SM of the card. A biometric key (BK) is generated from the reference template using, e.g., hashing, and registered on the server (e.g. via an encrypted or hashed representation). This BK plays a double role. Firstly, it is used as a biometric-related reference to which fresh captures have to be matched against by the MOC. Secondly, it plays the role of a cryptographic key under a challenge/response cryptographic authentication protocol. It was suggested to use the Boneh and Shacham group signature scheme, which allows the user to preserve his/her anonymity while being authenticated to the server. Since the proposed OLG system does not require the users' anonymity, other (simpler and more efficient) cryptographic protocols can be considered.

The way of processing enforces the user's privacy in the overall system while keeping its performance/accuracy at a good level. It is interesting to note that the very use of BK in this scheme relies on the fact that there is a lot of noise between different captures of a biometric data which makes its guessing by an adversary hard (even if one bit is changed for the new capture, its hash and BK will be completely different). Contrast this to conventional biometrics, where the variability of biometric samples is always considered the greatest challenge to overcome.

Since the biometric reference is actually stored in SM of the card, this system is not exactly BE as defined in Section II. However, it possesses all other properties of BE (plus, supposedly, a better accuracy), is compliant with the ISO/IEC 24745 standard [20] and, thus, can be called "BE-lite".

4.3 Advantages of the proposed system

- The proposed system provides two integrated pieces of authentication ("what you have" and "who you are") and, as such, enhances the accuracy of authentication and the overall security of the system;
- It is resilient against the substitution attack since the BK is generated from the user's biometric: an attacker cannot substitute it with his/her own biometric, even if he or she manages to read the data from the SM of the smart card and/or to clone the card;
- It protects the user's privacy by limiting the diffusion of biometric data to a local or remote environment as both the storage and the matching are performed on the card under the control of the user;
- The tamper-resistance of the smart card ensures that the reference biometric template is well-protected;
- The smart card cannot be loaned to another user, so that minors, self–excluded people and known cheaters are prevented from gaming;

- The server stores BK that is generated from biometric but cannot be reverse engineered. This further ensures the privacy protection, since the server's database cannot be linked with other biometric databases, including social networks. Moreover, it cannot be linked with other databases that store BKs since a BK generated for the same user, but from a different capture, will be completely different;
- The system is expected to preserve the accuracy of the state-of-the-art facial recognition.

V. Experiment

The objective of the test is to simulate the use of laptops, digital cameras, smartphone and tablet cameras for remote biometric enrollment and authentication. The test was not exhaustive and, therefore, the results should be treated as preliminary.

5.1 Database information

The OLG database of facial images consists of several acquisitions of faces for 79 people (in 3 sessions) with different types of acquisitions devices (digital camera, smartphones, laptops, etc.). There were also acquisitions with the cameras used at OLG for the self-exclusion program. Those acquisitions served controlled purposes and were not included in this test. The list of devices is shown in Table 1.

Device	Name
Lenovo LapTop – T510	Laptop
BlackBerry 9810	BlackBerry
iPhone 4	iPhone
iPad 2	iPad
Asus Transformer	Asus
Samsung Infuse	Samsung
Canon PowerShot SD1200 IS	Canon

Table 1 : List of devices

A specific data set has been chosen for the test:

- A set of gallery images taken with Canon and consisting of 110 images of 79 people (48 people with one image and 31 people with two images, with or without glasses)
- A set of probe images, consisting in 553 images of 80 people taken with the rest of the devices. The precise repartition for each device is summed up in Table 2.

Device	Number of images / persons
Asus	95 / 67
BlackBerry	105 / 76
iPad	36 /27
iPhone	111 / 80
Laptop	103 / 80
Samsung	103 / 75

Table 2: Details of acquisitions for each device

5.2 Test results

A 1:1 matching has been done between the gallery set and the probe set with Morpho face recognition algorithm F2.2.2-MOC (Match-on-Card). Performances have been computed for all the acquisition devices together and also separately. The numbers of genuine and impostor attempts are shown for each experiment in Table 3.

Device	Number of genuine attempts	Number of impostor attempts
All	850	59980
Asus	149	10301
BlackBerry	162	11388
iPad	54	3906
iPhone	171	12039
Laptop	155	11175
Samsung	159	11171

Table 3: Number of tests for each experiment

The Receiver Operating Characteristic (ROC) curves are presented on Fig. 3 and the FRR for a FAR of 1 percent are reported in Table 4.

Device	FRR @ FAR=1%
All	2.9%
Asus	2%
BlackBerry	1.9%
iPad	0%
iPhone	0%
Laptop	11.6%
Samsung	0.6%

Table 4: Performances for each device

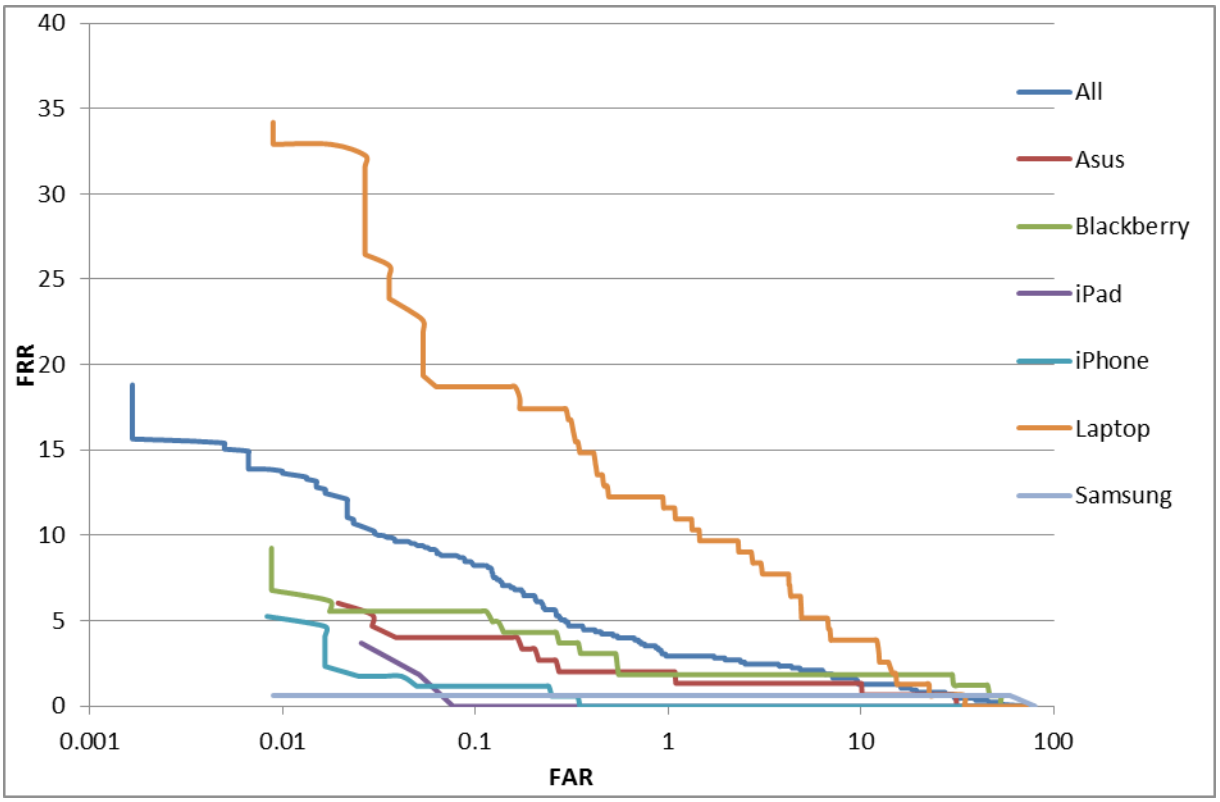

Fig. 3: ROC curves

Performances are good on all devices except laptops. A quick analysis of high impostor scores and low genuine scores helps us to make the following observations:

The main reasons for low genuine scores on laptops are difficult conditions of acquisition: uncontrolled illumination with shadows cast on the face, perspective distortions due to people too close to the camera, lower resolution between eyes compared to other devices. For other devices, the issues are glasses reflections, which disturb eye detections, and noisy acquisitions (for BlackBerry).

5.3 Limitations of the experiment

This experiment has limitations compared to a real-life scenario, which could be explored in a future work:

- The number of tests is a little low for being statistically representative. A trial or study with more individuals could be considered.
- The time difference between gallery and probe acquisitions is quite short. It might be useful to evaluate the performance with at least a week between acquisitions.
- Images have been acquired by an operator. It would be interesting to evaluate the issues when a person does an auto-enrolment.
- Having several acquisitions by device (preferably with different illumination conditions) would help to better evaluate each device.

Even though the simulation results of those experiments were obtained on PC, the actual MOC was used to evaluate the speed of the processing and to make sure that the numbers produced by PC simulations are in line with MOC.

One may ask the question of how a good accuracy of the facial recognition shown in the above experiments would allow generating a biometric key (BK) of sufficient strength. The answer is that, despite good performance of the facial recognition algorithm, the facial templates remain quite different from each other when compared bit by bit. This high variability between different captures of the same user is the property that enables generation of a BK, for instance, by hashing a specific biometric reference using cryptographic hash functions, e.g. SHA-2, SHA-3, etc. Even with the knowledge of another template from the same user, the inherent variability of biometric samples ensures that it is not possible to guess the BK obtained from the reference.

VI. Conclusion

This study brought very satisfactory results for facial recognition with Biometric Encryption in the Match-on-Card architecture. These experiments confirm its feasibility on different platforms. Moreover, one could say that the proposed system is quite in the zeitgeist as it fits the spirit of the Universal Authentication Framework protocol pushed forward by the FIDO Alliance [21]: a local biometric authentication is followed, when applicable, by a classic cryptographic challenge/response between the user device and the relying party. The biometric data are continuously kept under the user's control. This study has demonstrated that the proposed solution is a triple-win for security, privacy, and accuracy – hallmarks of the *Privacy by Design* approach.

References

1 Ann Cavoukian, Tom Marinelli, Alex Stoianov, Karl Martin, Konstantinos N. Plataniotis, Michelle Chibba, Les DeSouza, Soren Frederiksen, "Biometric Encryption: Creating a Privacy-Preserving 'Watch-List' Facial Recognition System". In: Security and Privacy in Biometrics, Patrizio Campisi (ed.), Ch. 9, pp. 215-238. Springer-Verlag London, 2013.

2 Cavoukian, A., & Marinelli, T. (2010). Privacy-protective facial recognition: Biometric encryption proof of concept. Toronto: Office of the Information and Privacy Commissioner of Ontario.

3 Ratha NK, Connell JH, Bolle RM (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3):614–634

4 Privacy by Design Resolution (2010). 32nd international conference of data protection and privacy commissioners, Jerusalem, Israel, 27–29 October 2010

5 Laura Poitras, Glenn Greenwald. (2013, June 9). "NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sorts of things' – video." *The Guardian*. Retrieved from http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

6 Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. EURASIP Journal on Advances in Signal Processing 2008:1–17. Article ID 579416

7 Cavoukian A, Stoianov A (2009). Biometric encryption: the new breed of untraceable biometrics. In: Boulgouris NV, Plataniotis KN, Micheli-Tzanakou E (eds). Biometrics: Fundamentals, Theory, and Systems. Wiley/IEEE Press, New York, pp 655–718. Chapter 26

8 Rathgeb C, Uhl A (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011:3–25. http://jis.eurasipjournals.com/content/2011/1/3

9 Ann Cavoukian, Michelle Chibba, and Alex Stoianov, "Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment". Review of Policy Research, V. 29, Issue 1, pp. 37-61 (2012).

10 Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., & Zimmer, S. (2007). An application of the Goldwasser-Micali cryptosystem to biometric authentication. LNCS, 4586, 96–106.

11 Bringer, J., & Chabanne, H. (2008). An authentication protocol with encrypted biometric data. LNCS, 5023, 109–124.

12 Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., & Toft, T. (2009). Privacy-preserving face recognition. In I. Goldberg & M. J. Atallah (Eds.), PETS '09: Proceedings of the 9th international symposium on privacy enhancing technologies (pp. 235–253). Berlin, Heidelberg: Springer-Verlag.

13 Barni, M., Bianchi, T., Catalano, D., Raimondo, M. D., Labati, R. D., Failla, P., et al. (2010). *Privacy-preserving fingercode authentication. In 12th ACM multimedia and security workshop*. Retrieved from http://www.dmi.unict.it/diraimondo/uploads/papers/fingercodeprotocol-unpublished.pdf

14 Stoianov, A. (2010). Cryptographically secure biometrics. *Proceedings of SPIE, 7667*, 76670C-1–76670C-12.

15 Julien Bringer, Herve Chabanne, David Pointcheval, and Sebastien Zimmer, *Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication,* IWSEC 2008, LNCS 5312, pp. 219–230, 2008

16 Julien Bringer and Herve Chabanne, *Two efficient architectures for handling biometric data while taking care of their privacy*. In: Security and Privacy in Biometrics, Patrizio Campisi (ed.), Ch. 11, pp. 275-295. Springer-Verlag London, 2013.

17 *ypsID SmartCard,* Safran Morpho. http://www.morpho.com/IMG/pdf/morpho_iam_2s_ypsID_smartcard_gb.pdf

18 iPhone 5s: Using Touch ID. http://support.apple.com/kb/HT5883

19 Alessandro Acquisti, Ralph Gross, Fred Stutzman. *Faces of Facebook: Privacy in the Age of Augmented Reality*. Black Hat Webcast Series. http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf

20 ISO/IEC 24745. (2011). *Information technology—Security techniques—Biometric information protection*.

21 FIDO (Fast IDentity Online) Alliance. http://fidoalliance.org/

Glossary

Biometric Setbase:

a system proposed by Adi Shamir consisting of two parts - ID storage and biometric storage. Each part, in turn, consists of drawers filled with about √N (where N is the total number of identities) entries. Only the drawers of both setbases, but not the entries themselves, are linked. To identify a person, both ID and biometrics are needed. Similar to Weak Links.

Cancellable Biometrics:

a template protection technique that does the feature transformation and stores the transformed template. The transform is stored separately, e.g., on a token, or generated from a user's password. On verification, the transformed templates are compared [3]. Also known as feature transformation techniques.

Challenge/response identification:

a cryptographic protocol in which an entity authenticates by submitting a value that is dependent upon both a secret and a variable challenge value.

False Acceptance Rate (FAR):

the percentage of times a system produces a false acceptance, which occurs when a biometric subject is incorrectly matched to another biometric subject's existing biometric sample. A statistic used to measure biometric performance.

False Rejection Rate (FRR):

the percentage of times a system produces a false rejection which occurs when a biometric subject is not matched to his/her own existing biometric sample. A statistic used to measure biometric performance.

Gallery set:

a set of known biometric subjects used for an evaluation experiment. Simulates enrollment data.

Homomorphic Encryption:

an encryption mechanism that preserves certain algebraic structure between the plaintext space and the ciphertext space, thus allowing some (or all) computations to be performed in the encrypted domain.

Liveness detection:

the phase of biometric processing where the system checks whether the biometric data is a fresh capture coming from a real user.

Probe set:

samples submitted to the biometric system to compare against one or more references in the gallery set. Simulates verification data.

Receiver Operating Characteristic (ROC):

compares verification rate vs. FAR (often FRR vs. FAR instead). Measures accuracy performance of a biometric system.

Weak Links:

a system proposed by Bernard Didier consisting of an identity (ID) database and a biometric database. The links between two databases are deliberately weakened. To identify a person, both ID and biometrics are required. Similar to Biometric Setbase.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

Ontario Lottery and Gaming Corporation
4120 Yonge Street, Suite 500
Toronto, Ontario
M2P 2B8
Telephone: (416) 224-1772
Fax: (416) 224-7000
E-mail: olgcontactus@olg.ca

Morpho (Safran)
11 Boulevard Galliéni
92130 Issy-Les-Moulineaux France
Telephone: +33 2 35 64 53 46
Fax: +33 2 35 64 53 97
E-mail: info@morpho.com
Website: www.morpho.com

June 30, 2014

Information and Privacy Commissioner, Ontario, Canada

OLG

SAFRAN Morpho