Enhancing the Performance of Multimodal Automated Border Control Systems

Abhinav Anand, Ruggero Donida Labati, Angelo Genovese,
Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, Gianluca Sforza
Department of Computer Science, Università degli Studi di Milano, Italy.
firstname.lastname@unimi.it

***Abstract*—Biometric recognition in Automated Border Control (ABC) systems is performed in response to an increased worldwide traffic, by automatically verifying the identity of the passenger during border crossing. Currently, ABC systems seldom use methods for multimodal biometric fusion, which have been proved to increase the recognition accuracy, due to technological and privacy limitations. This paper proposes a framework for the biometric fusion in ABC systems, with the features of being technology-neutral and privacy-compliant, by performing an analysis of the most suitable biometric fusion techniques for ABC systems and considering the current technical and legal limitations.**

I. Introduction

Automated Border Control (ABC) systems have emerged as a satisfactory solution that can reduce the border crossing time and the costs of border controls, while increasing throughput and security, by exploiting biometric technologies for comparing a live biometric sample acquired during the border crossing (fresh image) with the data stored in an electronic document, like the e-Passport (stored image) [1]. In this way, border guards can get discharged from tedious controls and focus on different tasks [2].

An important problem of ABC systems is that the biometric accuracy can be reduced by human factors such as: inexperience of the travelers; stress due to long travels; uncomfortable acquisitions due to the luggage; dirty biometric traits; dirty acquisition sensors; lack of feedback; lack of supervision by an operator [3]. In this context, multimodal biometric systems can perform more accurate and reliable biometric verifications by taking advantage of the increase in information [4]. For this reason, multimodal approaches are gaining acceptance in ABC scenarios, with deployments in Spain, Italy, China, and Japan [1].

Nonetheless, current multimodal ABC solutions are still not standard, and generally use simple fusion strategies, such as cascaded decision level processes that combine face and fingerprint [5]. In fact, technological limitations reduce their applicability since hardware and software modules in ABCs can be produced by different providers, thus presenting differences in the captured images and biometric data. Moreover, privacy limitations do not allow to disclose biometric data captured in ABC systems for training advanced biometric fusion models [6].

This work was supported in part by: the EC within the 7FP under grant agreement 312797 (ABC4EU); the EC within the H2020 program under grant agreement 644597 (ESCUDO-CLOUD).

To deal with these problems, this paper proposes a framework for the biometric fusion in ABC systems, with the features of being technology-neutral and privacy-compliant. By performing an analysis of the multimodal fusion techniques that can improve the recognition accuracy in ABC systems, the most suitable techniques for ABC systems are determined based on security, technological, and privacy requirements. Currently, no public biometric database captured using ABCs is available. To simulate real application scenarios, we collected databases resembling the different conditions arising in ABC scenarios, and we used commercial biometric recognition software employed in ABC installations.

The paper is organized as follows. Section II analyzes the suitability of the most commonly used multimodal fusion techniques for ABC scenarios. Section III presents the performed experiments and obtained results. Section IV concludes the work.

II. Multimodal biometric fusion in ABC systems

A. Challenges in ABC scenarios

The main objective of the application of multimodal fusion to ABC systems is to increase the border security while facilitating the clearance process to the traveler. For this reason, it is important to rely on well-established and robust fusion techniques.

Privacy protection represents another important challenge for the development of viable fusion methods for ABC systems. In some countries, the legal framework denies the possibility to store and disseminate biometric data obtained from government systems [6], resulting in a design problem from two perspectives. First, many advanced fusion techniques, such as classifier-based techniques [4], require a preliminary training to tune some of the parameters. In these cases, the larger the amount of data similar to the data that can be found in the operational environment, the more accurate the obtained model will be. However, it is difficult to obtain large quantities of biometric samples due to privacy limitations. Hence, the obtained models could not perform as expected, and it would be preferable to use techniques that only require simple training or that can be trained using public datasets. Second, the operational evaluation of the ABC system is

more complex than the procedure used in other application scenarios, and the computation of typical figures of merit, such as FAR, FRR or ROC curves is also more difficult. It is therefore necessary to rely on evaluations carried out using public datasets or with internal testing procedures [7]. An alternative is to perform the analysis using a subset of the transactions carried out by the ABC system that guarantees privacy protection [6].

Moreover, ABC systems in many cases depend on hardware and software modules implemented by different producers, and may also need to include legacy systems. For this reason, it is necessary to design technology-neutral techniques that do not affect existing and proprietary biometric systems.

B. Analysis of state of the art techniques

Multimodal systems can mitigate important problems of monomodal approaches, such as non-universality and high intra-class variability [4], and are more robust against non-ideal environments and spoofing attempts [8]. Traditionally, multimodal systems have been divided in four levels, depending on the step of the biometric process at which the data are fused: sensor level, feature level, score level, and decision level [4]. This section analyzes which fusion techniques can be easily adapted to current ABC scenarios to improve the recognition performance, and which fusion methods are less suitable.

Sensor level methods operate by concatenating the data acquired using different sensors, which makes them technology-dependent, less commonly used and, hence, they are considered not robust enough for ABCs. Feature level fusion methods, which combine the templates from each trait, represent a more promising research line. However, their dependence on the access to biometric templates, which in ABC scenarios are generally not accessible to border operators, makes their current application more difficult. Decision level techniques are simpler and easier to implement. Nonetheless, their capability to improve recognition performance is limited compared with more advanced techniques.

For all the above reasons we have decided to focus on score level techniques, which combine the matching scores obtained from different matching methods. In an ABC context, these fusion methods offer a technology-neutral approach, which can favor the integration of the different modules of the biometric recognition process. Score level methods have been used, for instance, in the Spanish ABC systems to combine face and fingerprint in a hierarchical way [5]. In the literature, many score level methods have been proposed, however not all of them are suitable for ABC scenarios. In particular, the application of learning-based methods that require the training of fusion models [9] is limited by privacy issues, since it is not possible to use biometric data captured in ABCs for training the models.

Nonetheless, there are techniques that can be easily applied to ABCs and that, to the best of our knowledge, have not been previously tested. These techniques include the well-known methods such as sum, product, maximum score, minimum score, and weighted sum. Several works have demonstrated that the rule of the sum always helps in increasing the recognition accuracy [10].

Usually, the works proposing classifier-based methods require a training phase, use the same database to train and validate the technique, and only in some cases the tests are performed using techniques such as cross validation, which allows to avoid over-fitting and obtain realistic error estimations. However, this kind of approach is not directly applicable to ABC scenarios, because the possibility to store data needed by this operation is not common in real ABCs. The likelihood ratio technique [9] offers a good alternative in this sense, since it is a mature technique that relies on a robust simple model, Gaussian Mixture Models. In addition, it also permits to exploit quality scores. For these reasons, we have decided to use it in this work. Moreover, we designed a privacy-compliant training procedure, by using different datasets for training and test (including public datasets).

III. Experimental results

A. Used datasets

To the best of our knowledge, no biometric database captured using ABC systems is publicly available. Moreover, not all public databases "as it is" allow to correctly predict the performance of biometric systems in ABCs. For these reasons, we collected different datasets by considering biometric samples extracted from public biometric databases, simulating different conditions that can arise in ABC systems. We considered face and fingerprint databases since they are the most common biometric modalities used in ABC systems [1]. All the images have been captured using acquisition devices similar to the ones used in e-Gates, and in controlled environments. In the case of face databases, we considered both ICAO compliant (good quality) images and non-ICAO compliant (medium-low quality) samples, to obtain a trade-off between the quality of images stored in e-Passports and the quality of live images captured at the e-Gate. In particular, we considered the following databases:

- FEI Face Database [11], containing face images captured using a color camera with a uniform background. We selected 100 individuals, with 8 samples for each individual captured in the same session, for a total of 800 images. A subset of the images is ICAO compliant [12], thus allowing to simulate e-Passport's images, while the rest of the images are more challenging. In particular, these images present challenging aspects that may appear in an ABC scenario, such as variations in the lighting or changes in pose and expression, which can simulate the possibility of a live acquisition at the e-Gate where the person is not correctly following the acquisition protocol [13]. Also, even if a uniform background is not always present in real ABC systems, methods for face detection and segmentation have been proved to work also with unconstrained backgrounds in ABC scenarios [14], [15].
- AR Face Database [16], containing face images captured using a color camera with a uniform background. We se-

lected 100 individuals, with 8 samples for each individual captured in two sessions taken 14 days apart, for a total of 800 images. Part of the database is ICAO compliant [12], as images stored in e-Passports should be, whereas other images present some challenges. In particular, this database allows us to simulate other conditions of an e-Gate, such as when the biometric samples stored in the passport have been captured before the passage through the e-Gate and differences in make-up or hairstyle can be present during the border crossing.

- FVC (Fingerprint Verification Database) 2002 DB1 [17], containing fingerprint samples captured using a medium-quality, legacy optical sensor with a 13.2×25 mm sensing area and with 500 ppi resolution. The database is composed by 100 individuals, with 8 samples for each individual, for a total of 800 images. This database permits to simulate passports with samples captured with old equipment.
- FVC (Fingerprint Verification Database) 2006 DB2 [18], containing fingerprint samples captured using a more recent medium-quality optical fingerprint acquisition sensor, with 17.8×25mm sensing area and 500ppi resolution. We selected 100 individuals, with 8 samples for each individual, for a total of 800 images. Differently from the FVC 2002 DB1 database, the volunteers included also manual workers and elderly people. Moreover, the acquisition procedure did not consider any constraint used for increasing the quality of the captured samples. This database allows to simulate people with all kinds of ages, jobs, and familiarity with technology. Moreover, the fingerprint images captured in non-ideal situations simulate the possibility of people passing through the e-Gate with fingers swollen, dirty, or greasy from the travel [3].

Then, using the four databases, we created two scenarios: *Scenario 1*, using FEI for face and FVC 2002 DB1 for fingerprint; *Scenario 2*, using AR for face and FVC 2006 DB2 for fingerprint. Moreover, in order to recreate the operational conditions of ABC systems, we applied the compression techniques described by the ICAO for storing biometric samples in e-Passports [12]. In particular, we used the WSQ compression to produce fingerprint samples with $\approx$ 10 kB file size, and the JPG compression to produce face images with ≈ 90 pixels between the eyes and $\approx 15 - 20$ kB file size.

B. Experimental procedure

We used the biometric recognition softwares Cognitec FaceVACS v9.1.1.0 and Dermalog Fingercode3 v1.2.1613.13 to compute and match the templates from face and fingerprint images, respectively. In both scenarios, we performed a scenario evaluation [19] for all the fingerprint and face databases, separately. For each database, the evaluation included 5600 genuine comparisons and 633600 impostor comparisons. We considered as error metrics the EER and the FMR_{1000} (the lowest FNMR for FMR $\leq 0.1\%$). Then, for each scenario, we performed the score-level fusion using the sum, product, max, min, weighted sum using Fisher's rule [20], NCW rule [21], MEW rule [22], OLD rule [22], likelihood ratio, and quality-based likelihood ratio [9]. The training of the likelihood ratio methods was performed on a random subset containing 50% of genuine scores and 50% of the impostor scores, and tested on the remaining scores. The procedure was repeated 10 times, then the average FMR and FNMR were used to compute the error metrics [9]. We tested the privacy-compliant biometric fusion technique that can be applied in ABC systems by performing the training and the test using two different datasets. Moreover, a technology-neutral evaluation was performed by considering biometric recognition algorithms produced by different vendors.

C. Results of score-level fusion

The results for the Scenario 1 and Scenario 2 are reported in Table I. In both scenarios, it is possible to observe that learning-based methods using the likelihood ratio obtained the best results in terms of EER and the FMR_{1000}, independently from the used normalization technique. Moreover, Table I shows that the sum rule allowed to obtain high accuracy in terms EER and FMR_{1000}, similar to the one obtained using learning-based methods, but required a preliminary Z-Score normalization to obtain the best results.

D. Privacy-compliant fusion for ABC systems

In order to test the accuracy of the privacy-compliant score-level fusion, the scores obtained in Scenario 1 were used to train the likelihood ratio fusion model, which was then tested on the scores obtained in Scenario 2, and vice versa. A preliminary Z-Score normalization was used. The results are reported in Table II, showing that the recognition accuracy was not significantly affected when the fusion model is trained on different datasets, thus demonstrating that it is possible to perform an off-line training of the fusion model in ABC even with data captured in a different context (e.g. public datasets).

E. Technology-neutral evaluation

In this section we provide a technology-neutral evaluation of the score-level fusion performance, by using the different combinations of recognition algorithms from different vendors, and analyzing the improvement in the EER and FMR_{1000} with respect to using only the most accurate biometric trait (the fingerprint). In particular, we used the software Dermalog Fingercode3, Cognitec FaceVACS, Neurotechnology VeriFinger, and Neurotechnology VeriLook. No previous normalizations were performed, and the sum rule was used as fusion method since it does not require any learning process. In all cases, it increased the accuracy of the recognition [10]. For each combination, we evaluated the differences ΔEER and ΔFMR_{1000} obtained by using the sum fusion strategy with respect to using the fingerprint, which were computed as follows:

$$\begin{aligned} \Delta\text{EER} &= \text{EER}_{\text{sum}} - \text{EER}_{\text{finger}} \ ; \\ \Delta\text{FMR}_{1000} &= \text{FMR}_{1000\,\text{sum}} - \text{FMR}_{1000\,\text{finger}} \ . \end{aligned} \tag{1}$$

TABLE I
SCORE-LEVEL FUSION RESULTS

Ref.	Fusion	Scenario 1 Normalization method: No norm. EER (%)	No norm. FMR 1000 (%)	Min-max EER (%)	Min-max FMR 1000 (%)	Z-Score EER (%)	Z-Score FMR 1000 (%)	Scenario 2 Normalization method: No norm. EER (%)	No norm. FMR 1000 (%)	Min-max EER (%)	Min-max FMR 1000 (%)	Z-Score EER (%)	Z-Score FMR 1000 (%)
-	Face	1.55	6.78	1.55	6.78	1.55	6.78	4.42	17.53	4.42	17.53	4.42	17.53
-	Fingerprint	1.14	1.71	1.14	1.71	1.14	1.71	0.82	1.07	0.82	1.07	0.82	1.07
-	Sum	1.00	1.60	0.17	0.42	0.09	0.07	0.64	1.07	0.28	0.60	0.21	0.21
-	Product	0.32	0.64	0.28	0.53	0.47	0.64	1.25	2.42	1.10	2.10	0.21	0.21
-	Max	1.14	1.71	0.45	6.75	0.21	0.39	0.82	1.07	0.57	1.46	0.37	0.75
-	Min	1.55	6.78	0.99	4.60	1.00	1.75	4.42	17.53	2.35	4.35	2.21	4.75
	Weighted sum												
[20]	Fisher	0.10	0.10 [a]	0.10	0.10 [b]	0.10	0.10 [c]	0.17	0.21 [d]	0.17	0.21 [e]	0.17	0.21 [f]
[21]	NCW	0.10	0.10 [g]	0.10	0.10 [h]	0.10	0.10 [i]	0.17	0.21 [j]	0.17	0.21 [k]	0.17	0.21 [l]
[22]	MEW	0.10	0.10 [m]	0.10	0.10 [n]	0.10	0.10 [o]	0.21	0.21 [p]	0.21	0.21 [q]	0.21	0.21 [r]
[22]	OLD	0.42	0.60 [s]	0.42	0.60 [t]	0.42	0.60 [u]	0.57	0.89 [x]	0.56	0.89 [y]	0.56	0.89 [z]
[9]	Likelihood ratio	0.09	0.08	0.07	0.07	0.09	0.09	0.17	0.19	0.21	0.22	0.19	0.20
[9]	Quality-based likelihood ratio	0.07	0.07	0.07	0.07	0.07	0.07	0.13	0.14	0.11	0.12	0.10	0.10

[a] $w = (0.98, 0.02)$; [b] $w = (0.36, 0.64)$; [c] $w = (0.49, 0.51)$; [d] $w = (0.95, 0.05)$; [e] $w = (0.25, 0.75)$; [f] $w = (0.31, 0.69)$
[g] $w = (0.28, 0.01)$; [h] $w = (0.08, 0.21)$; [i] $w = (0.11, 0.17)$; [j] $w = (0.27, 0.01)$; [k] $w = (0.07, 0.18)$; [l] $w = (0.09, 0.16)$
[m] $w = (0.28, 0.01)$; [n] $w = (0.09, 0.19)$; [o] $w = (0.13, 0.15)$; [p] $w = (0.28, 0.01)$; [q] $w = (0.11, 0.16)$; [r] $w = (0.14, 0.14)$
[s] $w = (0.26, 0.02)$; [t] $w = (0.03, 0.26)$; [u] $w = (0.04, 0.24)$; [x] $w = (0.20, 0.08)$; [y] $w = (0.01, 0.27)$; [z] $w = (0.01, 0.26)$

TABLE II
PRIVACY-COMPLIANT SCORE-LEVEL FUSION RESULTS USING THE QUALITY-BASED LIKELIHOOD RATIO

Train scenario	Test scenario: Scenario 1 EER (%)	Scenario 1 FMR_{1000} (%)	Scenario 2 EER (%)	Scenario 2 FMR_{1000} (%)
Scenario 1	0.07	0.07	0.16	0.18
Scenario 2	0.26	0.30	0.10	0.10

The results are summarized in Table III for both Scenario 1 and Scenario 2, showing that in all cases the fusion allowed to obtain lesser or equal EER and FMR_{1000} with respect to using only the most accurate biometric trait, independently of the used recognition algorithm in the ABC context we simulated.

IV. CONCLUSION

In this paper we proposed an analysis of multimodal biometric fusion techniques for enhancing the recognition accuracy in ABC scenarios. In particular, we selected two sets of biometric databases with characteristics similar to the ones that can be found in biometric samples captured in ABC gates, or stored in e-Passports. After analyzing the challenges and limitations present in ABC systems, we performed a technology evaluation of the most commonly used score level fusion techniques, showing that recent learning-based methods such as the likelihood ratio obtain the best accuracy. Moreover, we evaluated the performance of a privacy-compliant score-level fusion using the likelihood ratio, demonstrating that fusion methods can be used to enhance the performance of ABC systems, even when actual data collected using ABC systems is not available. Lastly, a technology-neutral evaluation proved that it is always possible to use score-level fusion to increase the recognition accuracy in multimodal ABC systems, independently of the used recognition algorithm. Future works will consider new technological specifications for e-Passports that may eventually be published, biometric databases captured during the pilot testing of new ABC systems, and the fusion of face and fingerprint with iris samples. Moreover, privacy-compliant and technology-neutral aspects will be further analyzed.

REFERENCES

[1] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric recognition in Automated Border Control: a survey," *ACM Comp. Surv.*, vol. 49, no. 2, pp. 24:1–24:39, 2016.

[2] Frontex, *Best practice technical guidelines for Automated Border Control (ABC) systems*, 2016.

[3] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Automatic classification of acquisition problems affecting fingerprint images in Automated Border Controls," in *Proc. of CIBIM*, 2015.

[4] A. Ross, K. Nandakumar, and A. Jain, *Handbook of multibiometrics*. Springer, 2006, vol. 6.

[5] D. Cuesta Cantarero, D. A. Pérez Herrero, and F. Martín Méndez, "A multi-modal biometric fusion implementation for ABC systems," in *Proc. of EISIC*, 2013, pp. 277–280.

[6] I. Iglezakis, "EU data protection legislation and case-law with regard to biometric applications," *Social Science Research Network*, 2013.

[7] V. MacLeod and B. McLindin, "Methodology for the evaluation of an international airport Automated Border Control processing system," in *Innovations in Defence Support Systems -2*. Springer, 2011, vol. 338, pp. 115–145.

[8] M. Kosmerlj, T. Fladsrud, E. Hjelmas, and E. Snekkenes, "Face recognition issues in a border control environment," in *Advances in Biometrics*. Springer, 2005, vol. 3832, pp. 33–39.

[9] K. Nandakumar, Yi Chen, S. Dass, and A. Jain, "Likelihood ratio-based biometric score fusion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 2, pp. 342–347, 2008.

[10] A. Ross and A. Jain, "Information fusion in biometrics," *Patt. Recogn. Lett.*, vol. 24, no. 13, pp. 2115–2125, 2003.

TABLE III

IMPROVEMENT OF EER AND FMR_{1000} USING THE SUM FUSION, WITH RESPECT TO USING ONLY THE MOST ACCURATE BIOMETRIC TRAIT, IN A TECHNOLOGY-NEUTRAL ENVIRONMENT, FOR DIFFERENT COMBINATIONS OF RECOGNITION ALGORITHMS. NEGATIVE VALUES CORRESPOND TO INCREASE IN ACCURACY

Algorithm		Scenario 1		Scenario 2	
Face	Fingerprint	ΔEER (%)	ΔFMR_{1000} (%)	ΔEER (%)	ΔFMR_{1000} (%)
Cognitec FaceVACS v9.1.1.0	Dermalog Fingercode3 v1.2.1613.13	-0.14	-0.11	-0.18	-0.00
Cognitec FaceVACS v9.1.1.0	Neurotechnology VeriFinger v6.0	-0.00	-0.00	-0.00 *	-0.00 *
Neurotechnology VeriLook v6.0	Dermalog Fingercode3 v1.2.1613.13	-0.75	-1.07	-0.70	-0.90
Neurotechnology VeriLook v6.0	Neurotechnology VeriFinger v6.0	-0.24	-0.26	-0.00 *	-0.00 *

* EER and FMR_{1000} were already equal to 0 using only the most accurate biometric trait

[11] E. Carlos and A. Gilson, "A new ranking method for principal components analysis and its application to face image analysis," *Image Vis. Comput.*, vol. 28, no. 6, pp. 902–913, 2010.

[12] ICAO, "Doc 9303 - Machine Readable Travel Documents - Part 9," 2015.

[13] J. Sanchez del Rio, C. Conde, A. Tsitiridis, J. Raul Gomez, I. Martin de Diego, and E. Cabello, "Face-based recognition systems in the ABC e-gates," in *Proc. of SysCon*, 2015, pp. 340–346.

[14] R. Raghavendra, K. Raja, B. Yang, and C. Busch, "Automatic face quality assessment from video using gray level co-occurrence matrix: an empirical study on Automatic Border Control system," in *Proc. of ICPR*, 2014, pp. 438–443.

[15] R. Raghavendra and C. Busch, "Improved face recognition by combining information from multiple cameras in Automatic Border Control system," in *Proc. of AVSS*, 2015, pp. 1–6.

[16] A. Martinez and R. Benavente, "The AR face database," The Ohio State University, Tech. Rep. CVC Technical Report 24, 1998.

[17] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, 2nd ed. Springer Publishing Company, Incorporated, 2009.

[18] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today*, vol. 15, no. 7-8, pp. 7–9, 2007.

[19] J. Jang and H. Kim, "Performance measures," in *Encyclopedia of Biometrics*. Springer US, 2009, pp. 1062–1068.

[20] S. Mika, G. Rätsch, J. Weston, B. Schölkopf, and K.-R. Müller, "Fisher discriminant analysis with kernels," in *Proc. of NNSP*, 1999, pp. 41–48.

[21] C. Chia, N. Sherkat, and L. Nolle, "Towards a best linear combination for multimodal biometric fusion," in *Proc. of ICPR*, 2010, pp. 1176–1179.

[22] N. Damer, A. Opel, and A. Nouak, "Biometric source weighting in multi-biometric fusion: towards a generalized and robust solution," in *Proc. of EUSIPCO*, 2014, pp. 1382–1386.