Enhancing Fingerprint Biometrics in Automated Border Control with Adaptive Cohorts

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.
{abhinav.anand, ruggero.donida, angelo.genovese, enrique.munoz, vincenzo.piuri, fabio.scotti, gianluca.sforza}@unimi.it

***Abstract*—Automated Border Control (ABC) systems are being increasingly used to perform a fast, accurate, and reliable verification of the travelers' identity. These systems use biometric technologies to verify the identity of the person crossing the border. In this context, fingerprint verification systems are widely adopted due to their high accuracy and user acceptance. Matching score normalization methods can improve the performance of fingerprint recognition in ABC systems and mitigate the effect of non-idealities typical of this scenario without modifying the existing biometric technologies. However, privacy protection regulations restrict the use of biometric data captured in ABC systems and can compromise the applicability of these techniques. Cohort score normalization methods based only on impostor scores provide a suitable solution, due to their limited use of sensible data and to their promising performance. In this paper, we propose a privacy-compliant and adaptive normalization approach for enhancing fingerprint recognition in ABC systems. The proposed approach computes cohort scores from an external public dataset and uses computational intelligence to learn and improve the matching score distribution. The use of a public dataset permits to apply cohort normalization strategies in contexts in which privacy protection regulations restrict the storage of biometric data. We performed a technological and a scenario evaluation using a commercial matcher currently adopted in real ABC systems and we used data simulating different conditions typical of ABC systems, obtaining encouraging results.**

I. Introduction

Automated Border Control (ABC) systems automatically verify the traveler's identity by using biometric recognition technologies. During the border crossing, the identity of the individual is ascertained by comparing the fresh template computed from live biometric samples acquired at the automated biometric gate (e-Gate) with the enrolled template computed from biometric samples stored in an electronic document, such as the e-Passport [1]–[3]. With respect to traditional border control checks performed by human operators, ABC systems can speed up the identity control, increase the trust level in the recognition process, and increase the user acceptance of the border control procedure.

Currently, ABC systems are deployed in several countries. The majority of these systems are based on the internationally recognized recommendations for e-Passports of the International Civil Aviation Organization (ICAO) [4]. Fingerprint recognition technologies are adopted in numerous ABC installations [5], [6] because they offer a good tradeoff between high recognition accuracy and user acceptance [7]. Face recognition technologies are also widely used in ABC systems [1], [8]–[11]. Some ABC systems use iris recognition technologies [12].

Fingerprint recognition represents one of the most mature and accurate biometric technologies [13]. However, the recognition performance of fingerprint-based technologies can be negatively impacted by non-ideal conditions typical of ABC scenarios, such as: stress caused by the travel, bulky luggage inducing discomfort, dirt on the hands (e.g., after eating) or on the sensor (e.g., after multiple uses) [14], and lack of effective signaling in an unsupervised context [15].

Several methods have been proposed in the literature to increase the recognition performance of fingerprint recognition technologies in already deployed systems, such as using a quality threshold to discard low-quality samples [13], fusing multiple images [16], or using multi-modal biometric systems [17]. However, these methods could decrease the throughput of ABC systems and reduce the user acceptance. Moreover, it is possible to use enhancement methods for low-quality images [18], but they need to be tuned according to the used acquisition sensor and feature extraction method, which are frequently manufactured by different producers.

Techniques based only on processing the matching scores resulting from identity comparisons can increase the recognition accuracy independently from the underlying hardware and software [19], and without requiring the user to be subject to multiple biometric acquisitions. These techniques are usually called score normalization methods and aim to increase the biometric recognition accuracy by better separating the genuine and impostor matching scores. They are based on the analysis of sets of genuine and impostor matching scores and can use statistical or computational intelligence approaches. Cohort normalization methods are score normalization approaches that use the matching scores obtained by comparing an input template with a set of cohort templates. Cohort templates are the templates in a biometric system other than the template of the claimed identity [20]. Cohort normalization has the advantage of making no assumptions on the nature of the biometric or the matcher [21], facilitating its application to different scenarios [22], [23] and sensors [24]–[26].

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).

However, the regulations of some countries pose strong restrictions on the use of biometric data captured for government applications (e.g., border control) [27], limiting the applicability of score normalization techniques. These regulations regard the type of data stored in ABC systems, limit the amount of usable information, and impose the use of well-known cryptographic algorithms (e.g., AES) that differ from template protection methods specifically designed for biometric systems [28]–[30]. In this context, most of the score normalization techniques, which perform multiple genuine identity comparisons, are not suitable because it is not allowed to store additional data with respect to the biometric samples enrolled in the biometric passport. Also cohort normalization methods, which do not consider genuine matching scores, need to be modified by including privacy-compliant procedures [31] in order to be used in ABC systems.

In this paper, we propose a novel adaptive cohort normalization approach for ABC systems. We propose different contributions. First, our approach increased the accuracy of fingerprint recognition in our tests simulating ABC systems. Second, the approach considers privacy requirements imposed by current laws, using a privacy-compliant procedure that selects a limited number of cohorts from a fingerprint database captured in different conditions and containing different individuals (e.g., a public database). Third, we apply for the first time Support Vector Machines (SVM) for the score normalization in ABC systems. Moreover, to the best of our knowledge, it is the first work in the literature that uses external datasets for cohort normalization.

We performed a technological evaluation and a scenario evaluation by using data simulating different conditions common in ABC applications. To simulate real scenarios, we used a commercial software for feature extraction and matching, which is currently adopted in different ABC systems [32]. The obtained results are encouraging and show that the proposed approach increased the accuracy of the fingerprint recognition software in all the evaluated conditions.

The paper is structured as follows: Section II presents a review of cohort-based methods and the challenges posed by ABC systems, while Section III describes the proposed methodology. Then, Section IV presents the experimental results and Section V concludes the work.

II. Related works

This section briefly reviews the state of the art on cohort normalization methods and presents the main challenges for the use of cohort normalization methods in ABC scenarios.

A. Cohort score normalization methods

In the literature, there are different studies on cohort-based score normalization methods that aim to increase the accuracy of biometric recognition systems [20], [33], with applications to fingerprint [34], face [35], palmprint [36], as well as multimodal biometric systems [21].

Many methods analyze the cohort matching scores using algorithmic approaches to normalize the matching score computed from the fresh and the enrolled template (fresh score). The method described in [36] compares the fresh score with the highest cohort score for palmprint biometrics. The study described in [34] presents two techniques for fingerprint recognition: the first one normalizes the fresh score using the first and second order moments of the cohort scores, while the second one is the T normalization. The method described in [21] computes the ratio between the fresh score and the maximum of the cohort scores in order to increase the accuracy of multimodal recognition systems. Another widely used statystical approach is the Z normalization [37].

More complex methods train computational intelligence classifiers to learn the relation between fresh and cohort scores. This approach has been applied to fingerprint recognition by using the maximum of the cohort scores or the "second best matching score" together with feed forward neural networks [33]. Other methods use the whole set of cohort scores, or a significant subset of it as input for a SVM classifier [23].

More recent approaches have shown that not only the most similar templates contain useful information, but also the most dissimilar ones can be exploited to increase the accuracy. For instance, the method described in [20] exploits this information by computing a polynomial regression of the cohort scores. In addition, the size, quality and number of users in a cohort set has a direct impact to the performance of the method [35].

B. Challenges to cohort normalization in ABC systems

Recent works in the literature highlighted several factors that can improve the accuracy of cohort normalization methods. However, most of these positive factors are not valid for ABC scenarios due to legislative as well as architectural issues:

- Experimental procedures perform both the training and testing phases using the same biometric database, which has been captured with the same sensor and with similar acquisition procedures. In ABC systems, it is not possible to train cohort normalization methods using images captured during the deployment, with the same sensor and with similar acquisition procedures, since the use of biometric data of the travelers is restricted by law.
- The evaluation procedures are performed on public databases, which have a limited number of samples, allowing the use of cross-validation procedures to test the performance of the method, and tune the parameters accordingly. In ABC systems, traditional cross-validation procedures cannot be applied since the biometric data of the travelers cannot be accessed.
- The use of biometric samples with similar quality can increase the accuracy of cohort-based methods [35]. In ACB scenarios, the biometric data stored in the electronic document and the samples captured at the e-Gate are obtained using different sensors, with different quality levels.

To the best of our knowledge, the proposed approach is the first one in the literature designed to work in these non-ideal conditions typical of ABC scenarios. The approach uses an external dataset to train cohort normalization methods and

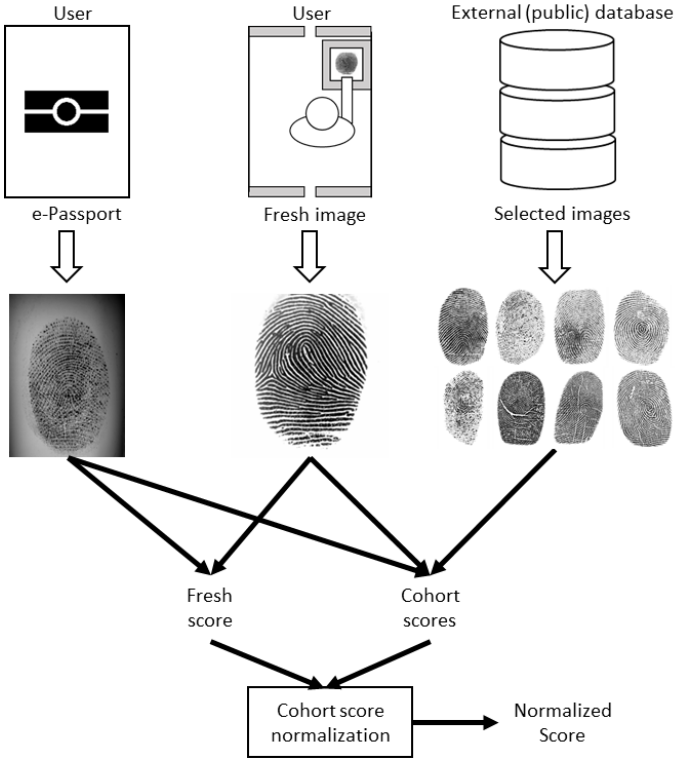

Fig. 1. Outline of the proposed privacy-compliant cohort score normalization approach. To comply with privacy protection regulations on biometric data in ABC systems, our approach uses an external dataset of templates to compute the cohort matching scores.

to compute the cohort scores. We also simulate the non-ideal conditions previously described in order to validate the applicability of cohort normalization methods in the considered application scenario. The used evaluation procedures simulate real conditions and are not based on cross-validation procedures. Moreover, the used biometric databases include samples of different quality acquired using different sensors.

Studies in the literature [35] have also shown that increasing the number of cohort scores improves the recognition accuracy up to a point where the performance stabilizes. In ABC systems, the number of templates in the cohort set cannot be increased indefinitely, as it is necessary to keep the passage time of the border as short as possible. We use an external dataset to compute the cohort scores, which can be composed of an arbitrary number of samples and we propose methods that can be executed in an interval of time that is less than the time in which the passenger accomplishes the border control procedure.

III. The proposed approach

In this section, we describe the proposed approach for cohort score normalization in ABC systems, with specific focus on fingerprint recognition. The approach has the features of being privacy-compliant and adaptive to different operational conditions (Fig. 1). To comply with privacy protection regulations on biometric data in ABC systems, our approach uses an external dataset of templates for computing the cohort matching scores. This dataset could be a public database or a dataset created and maintained secret by the vendor of the biometric technology.

The cohort score normalization procedure works as follows:

1) For a fresh sample s_i and a sample stored in the biometric document s_j, an identity comparison is performed to simulate the biometric verification performed in the e-Gate, and the fresh matching score g_{ij} is computed as follows:
$$g_{ij} = \mathrm{match}(s_i, s_j) \ , \tag{1}$$
where g_{ij} is the biometric similarity score obtained using the biometric matching function $\mathrm{match}(\cdot)$.
2) For each sample i, we extract a set E of n samples from an external database, and we compute the set M_i^C of impostor identity comparisons. The number of samples n is empirically selected as a tradeoff between accuracy and computational time. In our approach, n is constant for each identity comparison g_{ij}. Each matching score m_k^C of M_i^C is computed as follows:
$$m_k^C = \{s | s = \mathrm{match}(s_i, e_k)\} \ , \quad \{e_k\} \subseteq E \ , \tag{2}$$
where e_k is the k-th sample in the external fingerprint database E.
3) The final normalized matching score m_{ij} is obtained by applying a cohort normalization method. Table I summarizes the cohort normalization methods that we considered in this paper.

We chose the methods presented in Table I because they are well-known techniques in the literature. We did not use other well-known techniques that require to store additional information because they are not applicable in ABC scenarios.

In the following, we briefly describe the implemented cohort normalization methods.

- The *Max–rule* normalization method [21] computes the ratio between the fresh matching score g_{ij} and the maximum score in the set of cohort scores M_i^C. After computing the set of cohort scores M_i^C from the external dataset E, the maximum of the cohort scores is used to normalize the fresh matching score g_{ij}. The final normalized matching score is computed as follows:
$$m_{MaxRule} = g / \max(m_1^C, \cdots, m_n^C). \tag{3}$$
- In the *T–norm* cohort normalization method [34], the first order moment $\mu^C = \mathbb{E}_{m_k^C \in M_i^C}[m_k^C]$ and second order moment $(\sigma^C)^2 = \mathbb{E}_{m_k^C \in M^C}[(m_k^C - \mu^C)^2]$ of the cohort set M^C are used to normalize the fresh matching score g. The final normalized matching score is computed as follows:
$$m_{TNorm} = [(g - \mu^C)/\sigma^C, s.t.\ \mu^C, \sigma^C \in M_i^C]. \tag{4}$$
- The method *SVM–all–cohorts* classifies a feature set obtained using the samples s_i and s_j in two classes:

TABLE I
COHORT SCORE NORMALIZATION METHODS USED IN OUR APPROACH

Method	Description
Baseline	No normalization is performed
Max–rule [21]	Ratio of the raw score to the maximum of the cohort scores for each user.
T–norm [34]	The first and second order moments of the cohort scores are used to normalize the raw score.
SVM–all–cohorts	All the cohort scores for each user are used as input to a SVM classifier.
SVM–20–cohorts [23]	The 20 maximum cohort scores for each user are used as input to a SVM classifier.

genuines ($m_{SVM} = 1$) and impostors ($m_{SVM} = 0$). For each identity comparison between the samples s_i and s_j, the SVM takes in input a feature vector x_l composed of the fresh score g_{ij} and the cohort scores M_i^C. The feature vector therefore consists of $n + 1$ values.

To comply with privacy laws, the classifier is trained using only data belonging to the external dataset E.

For each element of the training set, which represents a comparison between the fingerprint images e_i and e_j pertaining to the external dataset E, the cohort set M_i^C is computed as the set of matching scores obtained from all the possible impostor comparisons between the sample e_j and the samples pertaining to E.

The training set is composed of $n \cdot (n - 1)$ elements representing all the possible combinations of identity comparisons between the n samples belonging to the external dataset E. The number of samples n of E is equal to $x \cdot y$, where x is the number of individuals and y is the number of samples per individual. The training dataset is therefore composed of $x \cdot y$ genuines and $x^2(y - 1)y$ impostors.

The application of SVM classifiers to the training dataset can obtain poor results, because the class distribution is very imbalanced. To cope with this problem, we use an ensemble learning approach that combines the decisions of 25 SVM classifiers using a voting approach that chooses the most voted class, following the work in [38]. The set of impostor comparisons is divided into 25 subsets obtained by random sampling without substitution, where each subset contains $2 \cdot x \cdot y$ impostor comparisons. Each SVM is trained using the whole set of genuine comparisons combined with one of the impostor comparisons subsets.

- The method *SVM–20–cohorts* [23] is similar to SVM–all–cohorts but it uses a reduced feature set composed of g_{ij} and the 20 highest values of M_i^C. We chose to use 20 cohorts because studies in the literature shown that this number allows to obtain a good tradeoff between accuracy and computational time [23].

IV. EXPERIMENTAL RESULTS

In this section we analyze three test scenarios to evaluate the proposed method. First, we illustrate the applicability of cohort normalization methods in a general scenario. Second, we evaluate the feasibility of the proposed approach for ABC systems. Last, we simulate a deployment performance analysis using the procedure proposed by Frontex [3], which is compliant with privacy protection regulations. We also present an analysis of the computational time required by the proposed approach. Other score normalization techniques are not compared with cohort normalization methods because techniques based on the analysis of genuine matching scores cannot be applied in ABC systems due to privacy protection regulations on the use of biometric data.

We evaluated the accuracy of the proposed approach in terms of FMR (False Matching Rate) and FNMR (False Non-Matching Rate). As error measures, we considered the EER (Equal Error Rate), and FMR_{1000} (the higher FNMR for FMR $\leq 0.1\%$) [13]. We also evaluated the accuracy of biometric recognition techniques by using ROC (Receiver Operating Characteristic) curves.

A. Used databases

Biometric samples stored in e-Passports and captured at e-Gates can be acquired in a wide variety of non-ideal situations, can present poor quality due to acquisition problems, and can be captured using different acquisition sensors [14], [15]. In order to simulate these problems and evaluate the performance of the proposed approach, we used several fingerprint datasets. The used data pertain both to public biometric databases and to sets of samples acquired in our laboratory by simulating border crossings in ABC scenarios. All the datasets include images captured with an optical sensor and at a resolution of 500 ppi, according to the ICAO specifications [4], [39].

- *Dataset–A (ABC lab best-case scenario)*: this dataset simulates good-quality acquisitions performed in ABC scenarios. We created this dataset in our laboratory by acquiring biometric images using an optical four finger scanner and a software currently adopted in real ABC systems [40]. The images represent the best finger skin conditions in ABC scenarios [14]. In particular, we collected 1504 biometric samples from 188 fingers in two situations:
  - 752 images (4 samples per finger). The volunteers were asked to place their fingers on the sensor as they are, with no specific variations in behavioral or environmental conditions.
  - 752 images (4 samples per finger). The volunteers were asked to clean their fingers before performing biometric acquisitions.
- *Dataset–B (ABC lab worst-case scenario)*: this dataset simulates poor-quality acquisitions performed in ABC scenarios. We created this dataset in our laboratory by acquiring biometric images using an optical four finger scanner and a software currently adopted in real ABC

systems [40]. The images represent poor finger skin conditions in ABC scenarios or uncomfortable acquisition conditions [14]. In ABC scenarios, passengers can carry a luggage and their fingers can be dirty after touching dusty, unclean surfaces (e.g., hand rails) or food covered in flour (e.g., donuts, croissants). To simulate these conditions, we collected 1504 biometric samples from 188 fingers in two situations:

  - 752 images (4 samples per finger). To simulate fingertips dirtied by touching dusty, unclean surfaces (e.g., hand rails) or food covered in flour (e.g., donuts, croissants), we acquired the fingerprint samples after dirtying the fingers with flour.
  - 376 images (2 samples per finger). To simulate the grease on the hands typically present after eating fast foods (e.g., sandwiches, mayonnaise, pizza) or using hand creams, we acquired the fingerprint samples after applying a hand cream.
  - 376 images (2 samples per finger). To simulate uncomfortable conditions, we acquired the fingerprints while the users ere holding a 4 kg bag on the same shoulder as the finger used for the acquisition.

- *Dataset–C*: this dataset is composed of fingerprint images collected from a greater number of individuals with respect to Dataset–A and Dataset–B. We used samples pertaining to the CASIA Fingerprint Image Database Version 5.0 [41]. We extracted 2000 images by selecting the first two samples of the left and right indexes of all the 500 individuals of the CASIA database. We selected the two indexes of each individual because they are the two fingers most frequently enrolled in e-Passports [42].

To compute the cohort scores in a manner compliant with privacy laws, we used a set of samples E corresponding to the public database FVC (Fingerprint Verification Database) 2002 DB1 [13], composed of fingerprint samples acquired using a legacy optical sensor with a resolution of 500 ppi. The set is composed of a total of $n = 800$ images acquired from $x = 100$ fingers ($y = 8$ samples per finger).

B. Test 1: validation based on a single dataset

To prove the applicability of cohort normalization techniques in a general application scenario, we evaluated the performance of different methods by using an iterative validation procedure that uses the samples pertaining to a biometric dataset for both the training and testing processes [43]. In particular, for each considered dataset (Dataset–A, Dataset–B and Dataset–C), the samples of 50% of the fingers are used for computing the cohort scores, and the remaining samples are used for testing. We computed the training feature set needed by SVM classifiers from the partition used to compute the cohort scores. The evaluation is carried out 10 times and the results are averaged. Similar procedures are widely used in the literature to validate score normalization methods [23], [43].

Table II summarizes the results achieved using the considered cohort score normalization methods and the described validation strategy based on a single biometric dataset. This table shows that cohort normalization methods increased the accuracy of the used fingerprint recognition software (baseline) for each considered dataset. Moreover, the performance improved in terms of EER as well as of FMR_{1000}. In particular, the methods based on SVM classifiers achieved the best accuracy for all the performed tests. This result could be due to the generalization capability of SVM classifiers, which allowed to achieve greater robustness to noisy data with respect to the other normalization methods. Nevertheless, the method T–Norm, which does not require a training step, achieved satisfactory results for all the performed tests. As an example, the method SVM–20–cohorts decreased the EER from 1.61% to 1.38% for Dataset–A, from 3.88% to 3.02% for Dataset–B, and from 3.61% to 3.07% for Dataset–C.

C. Test 2: proposed privacy-compliant approach

We evaluated the performance of the proposed privacy-compliant approach using Dataset–A, Dataset–B and Dataset–C. For each user, the sample set E was used to compute the cohort scores and to train SVM classifiers. It is important to note that the obtained results are not directly comparable to those presented in the previous section, because the evaluation procedure is different. In this case, the performance of each cohort normalization method is computed once using all the samples pertaining to the considered datasets.

Table III summarizes the achieved results. This table shows that the proposed approach increased the accuracy of the used fingerprint recognition software (baseline) for each implemented cohort normalization method in terms of both EER and FMR_{1000}. Also in this case, SVM classifiers achieved the greatest performance improvements. In particular, SVM classifiers achieved the best FMR_{1000} for each evaluated dataset. FMR_{1000} is a particularly relevant figure of merit for evaluating the performance of biometric technologies for high security applications, like ABC systems. As an example, the method SVM–20–cohorts decreased the FMR_{1000} from 1.71% to 1.59% for Dataset–A, the method SVM–all–cohorts decreased the FMR_{1000} from 7.62% to 6.87% for Dataset–B, and the method SVM–20–cohorts decreased the FMR_{1000} from 7.50% to 6.50% for Dataset–C.

Fig. 2 shows the ROC curves obtained by our approach using the cohort normalization methods that achieved the best performance in term of FMR_{1000} for Dataset–A, Dataset–B and Dataset–C. The ROC curves show that the proposed approach increased the accuracy of the used fingerprint recognition software for all the operational points of the biometric system by using SVM classifiers.

In order to prove the statistical significance of the results achieved by the proposed approach with respect to the baseline method, we estimated the confidence bounds of the error rates achieved for each curve shown in Fig. 2 by using a method based on the central limit theorem [44] with 95% confidence limits. In particular, we observed that the confidence bounds estimated for our approach and for the baseline method present very limited overlapping regions (FMR$< 0.1\%$ for Dataset–A

TABLE II
RESULTS OF THE SCORE NORMALIZATION USING THE VALIDATION TECHNIQUE BASED ON A SINGLE DATASET (2-FOLD VALIDATION ITERATED 10 TIMES)

Method	Test database					
	Dataset–A (Simulated ABC, best-case)		Dataset–B (Simulated ABC, worst-case)		Dataset–C (1000 fingers, public dataset)	
	EER (%)	FMR_{1000} (%)	EER (%)	FMR_{1000} (%)	EER (%)	FMR_{1000} (%)
Baseline (test 1)	1.61	1.86	3.88	7.31	3.61	7.42
Max–rule	1.46	1.77	3.39	6.54	3.43	6.40
T–norm	1.45	1.84	3.25	6.47	3.08	5.89
SVM–all–cohorts	1.38	1.80	3.16	7.14	3.23	6.96
SVM–20–cohorts	1.38	1.73	3.02	6.55	3.07	6.25

and Dataset–B and FMR$< 1\%$ for Dataset–C). These results confirm that our approach can increase the performance of a commercial fingerprint recognition technology currently used in ABC systems.

The proposed approach decreased the EER from $1,49\%$ to $1,21\%$ for Dataset–A. Therefore, our approach could reduce the number of identity recognitions performed by human operators in cases of false non matches at ABC gates of around 19% when applied to samples of good quality (Dataset–A). Considering the huge amount of identity verifications performed daily at international borders, this result can be considered as positive because it can reduce the efforts of guards in performing non-critical identity controls.

D. Test 3: Privacy-compliant testing

Since the proposed approach could be applied in already deployed ABC systems, we also tested its accuracy by simulating a scenario evaluation. This analysis is also useful to illustrate the process that should be followed to evaluate a real ABC deployment, in which it is not possible to perform a performance evaluation using the mostly adopted strategies in the literature.

Scenario / operational evaluations of biometric technologies for ABC systems are difficult processes because privacy protection regulations impose strict limitations in storing samples and templates obtained from biometric documents as well from live acquisitions, thus making difficult to compute traditional figures of merit in an accurate manner.

To simulate a scenario evaluation, we used the privacy-compliant test methodology proposed by Frontex [3]. This procedure allows to store only the last 10 fresh templates in order to estimate the biometric recognition accuracy of a system. Moreover, it requires that each finger is presented only once to the system in order to obtain a single genuine score between the fresh sample and the one stored in the biometric document. This scenario evaluation procedure assumes that only genuine attempts of crossing the board are performed.

We simulated this test methodology by implementing a procedure that compares each biometric sample with the last 10 acquired fresh samples, using a first-in first-out (FIFO) structure. Moreover, we used a dataset with two samples per finger (Dataset–C) and considered the first sample as the one enrolled in the biometric document and the second sample as the fresh data acquired at the ABC e-Gate. For each simulated access attempt, we computed a single genuine matching score and a maximum of more than 10% impostor identity comparisons (a maximum of 10 impostor matching scores obtained comparing the fresh sample and the samples stored in the FIFO structure, and a maximum of 10 impostor matching scores obtained comparing the sample enrolled in the biometric document and the samples stored in the FIFO structure).

We evaluated the performance of the proposed approach using the external dataset E for each considered cohort normalization method. Table IV summarizes the obtained results, confirming that the proposed approach can increase the recognition accuracy of the fingerprint recognition software in ABC systems.

E. Computational time

Since it is not possible to store additional biometric data in e-Passports or in the ABC system, the cohort scores should be computed for each access attempt. In order to validate the feasibility of the proposed approach in ABC systems, we evaluated the computational time required by the used commercial matching software [32] and by the SVM classifiers for the computation of the normalized matching score. We performed this test using an Intel Xeon 3.6 GHz with 32 GB of RAM working with Windows 10 and Matlab R2015b. The time required to compute the cohort scores from E (800 identity comparisons) is 0.24 s. The classification time required by the Matlab toolbox for SVM is 0.02 s for SVM–20–cohorts and 0.342 s for SVM–all–cohorts. The obtained results suggest that the proposed approach could be used in ABC applications without increasing the time in which the passengers accomplish the border control procedure. We should study techniques to reduce the computational complexity and the number of cohort scores in future work.

V. CONCLUSION

In this work, we proposed a privacy-compliant and adaptive cohort score normalization approach for enhancing the accuracy of fingerprint recognition in ABC systems. The proposed approach can be applied in existing ABC systems in accordance to the privacy protection regulations and without requiring hardware or software modifications. The

TABLE III
ACCURACY OF THE PROPOSED PRIVACY-COMPLIANT APPROACH USING DIFFERENT COHORT NORMALIZATION METHODS

Method	Test database					
	Dataset–A (Simulated ABC, best-case)		Dataset–B (Simulated ABC, worst-case)		Dataset–C (1000 fingers, public dataset)	
	EER (%)	FMR_{1000} (%)	EER (%)	FMR_{1000} (%)	EER (%)	FMR_{1000} (%)
Baseline (test 2)	1.49	1.71	3.97	7.62	3.59	7.50
Max–rule	1.31	1.63	3.57	6.90	3.27	6.98
T–norm	1.31	1.61	3.46	7.06	3.34	6.60
SVM–all–cohorts	1.22	1.61	3.34	6.87	3.40	6.85
SVM–20–cohorts	1.21	1.59	3.37	7.13	3.42	6.50

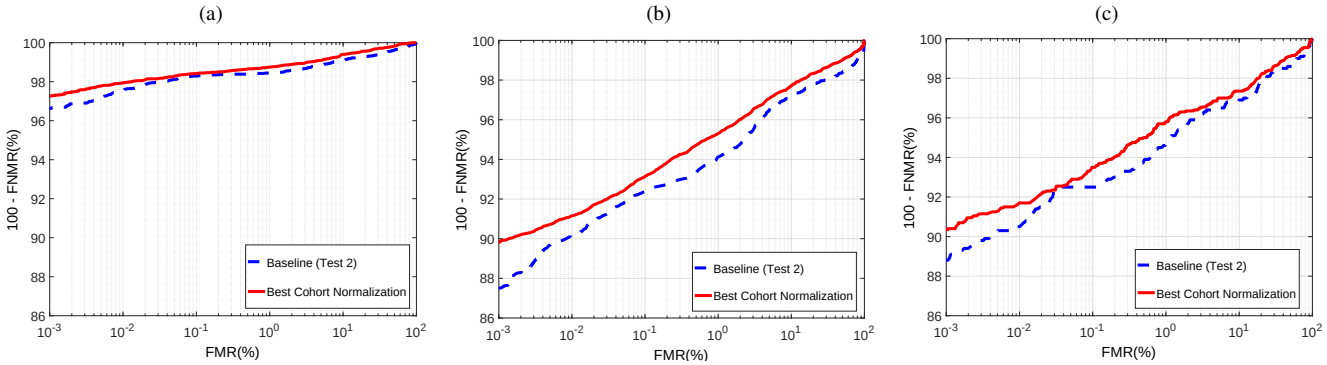

Fig. 2. ROC curves of the proposed privacy-compliant approach using the cohort normalization methods that achieved the best performance in term of FMR_{1000}: (a) SVM–20–cohorts for Dataset–A, (b) SVM–all–cohorts for Dataset–B, and (c) SVM–20–cohorts for Dataset–C. The higher the values along the vertical axis ($100 - \text{FNMR}(\%)$) are, the better is the accuracy. The proposed approach increased the recognition accuracy with respect to the baseline for each operational point of the biometric system.

TABLE IV
ACCURACY OF THE PROPOSED PRIVACY-COMPLIANT APPROACH USING DIFFERENT COHORT NORMALIZATION METHODS AND THE PRIVACY-COMPLIANT TEST METHODOLOGY PROPOSED BY FRONTEX [3]

Method	**Test database**	
	Dataset–C (1000 fingers, public dataset)	
	EER (%)	FMR_{1000} (%)
Baseline (test 3)	3.69	7.50
Max–rule	3.27	6.50
T–norm	3.17	5.70
SVM–all–cohorts	3.29	6.50
SVM–20–cohorts	3.18	6.00

approach computes cohort scores from an external dataset and uses computational intelligence to learn and improve the matching score distribution. We performed a technological and a scenario evaluation using biometric samples acquired by simulating different non-ideal conditions present in the case of people moving through a border crossing point. For all the performed tests, the proposed approach increased the accuracy of the commercial matching software used. In particular, the configurations of our approach based on SVM-based classifiers achieved the best accuracy for the evaluated datasets by taking advantage of the generalization capability of classification techniques based on machine learning. We also evaluated the required computational time, obtaining satisfactory performance. The obtained results suggest that cohort normalization methods could be effectively applied in ABC systems in a privacy-compliant manner. Furthermore, the number of identity recognition performed by human operators in cases of false non matches could be reduced of up to 19%.

Future works should test the effects of age, gender, and different quality of the fingerprint samples on the cohort normalization procedures. Moreover, we will consider the use of synthetically generated databases for cohort score normalization methods in a fully privacy-compliant way. We should also study techniques to optimize the computational time.

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 Computing Surveys*, vol. 49, no. 2, pp. 24:1–24:39, June 2016.

[2] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Advanced design of Automated Border Control gates: Biometric system techniques and research trends," in *Proc. of the 2015 IEEE Int. Symp. on Systems Engineering (ISSE 2015)*, September 2015, pp. 412–419.

[3] Frontex Agency, *Best Practice Technical Guidelines for Automated Border Control (ABC) Systems*. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, 2016.

[4] ICAO, "ICAO Doc 9303: Machine Readable Travel Documents (seventh edition) - Part 9: Deployment of biometric identification and electronic storage of data in eMRTDs," 2015.

[5] D. Cuesta Cantarero, D. A. Pérez Herrero, and F. Martín Méndez, "A multi-modal biometric fusion implementation for ABC systems," in *Proc. of the European Intelligence and Security Informatics Conf. (EISIC 2013)*, August 2013, pp. 277–280.

[6] L. J. Spreeuwers, A. J. Hendrikse, and K. J. Gerritsen, "Evaluation of automatic face recognition for Automatic Border Control on actual data recorded of travellers at Schiphol Airport," in *Proc. of the Int. Conf. of the Biometrics Special Interest Group (BIOSIG 2012)*, September 2012, pp. 1–6.

[7] A. Krupp, C. Rathgeb, and C. Busch, "Social acceptance of biometric technologies in germany: A survey," in *Proc. of the 2013 Int. Conf. of the Biometrics Special Interest Group (BIOSIG 2013)*, September 2013, pp. 1–5.

[8] J. Sánchez del Río, C. Conde, A. Tsitiridis, J. Raúl Gómez, I. Martín de Diego, and E. Cabello, "Face-based recognition systems in the ABC e-gates," in *Proc. of the 2015 9th Annual IEEE Int. Systems Conf. (SysCon 2015)*, April 2015, pp. 340–346.

[9] C. Conde, I. Martín de Diego, and E. Cabello, "Face recognition in uncontrolled environments, experiments in an airport," in *Proc. of the Int. Joint Conf. on E-Business and Telecommunications (ICETE 2011) - Revised Selected Papers*, M. S. Obaidat, J. L. Sevillano, and J. Filipe, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 20–32.

[10] R. Raghavendra and C. Busch, "Improved face recognition by combining information from multiple cameras in Automatic Border Control system," in *Proc. of the 2015 12th IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS 2015)*, August 2015, pp. 1–6.

[11] J. S. del Rio, D. Moctezuma, C. Conde, I. M. de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Computers & Security*, vol. 62, pp. 49 – 72, 2016.

[12] J. Daugman, "Iris recognition at airports and border crossings," in *Encyclopedia of Biometrics, Second Edition*, 2015, pp. 998–1004.

[13] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, 2nd ed. Springer, 2009.

[14] 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 the 2015 IEEE Symp. on Computational Intelligence in Biometrics and Identity Management (CIBIM 2015)*, December 2015, pp. 354–361.

[15] C. Riley, G. Johnson, H. McCracken, and A. Al-Saffar, "Instruction, feedback and biometrics: The user interface for fingerprint authentication systems," in *Proc. of the 12th IFIP TC 13 Int. Conf. on Human-Computer Interaction (INTERACT 2009)*, August 2009, pp. 293–305.

[16] D. Lee, K. Choi, S. Lee, and J. Kim, "Fingerprint fusion based on minutiae and ridge for enrollment," in *Proc. of the 4th Int. Conf. on Audio- and Video-based Biometric Person Authentication (AVBPA 2003)*, 2003, pp. 478–485.

[17] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*, ser. International Series on Biometrics. Springer, 2006, vol. 6.

[18] J. Yang, N. Xiong, and A. V. Vasilakos, "Two-stage enhancement scheme for low-quality fingerprint images by learning from the images," *IEEE Trans. on Human-Machine Systems*, vol. 43, pp. 235–248, March 2013.

[19] N. Poh, J. Kittler, S. Marcel, D. Matrouf, and J. F. Bonastre, "Model and score adaptation for biometric systems: Coping with device interoperability and changing acquisition conditions," in *Proc. of the 2010 20th Int. Conf. on Pattern Recognition (ICPR 2010)*, August 2010, pp. 1229–1232.

[20] A. Merati, N. Poh, and J. Kittler, "User-specific cohort selection and score normalization for biometric systems," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 4, pp. 1270–1277, 2012.

[21] G. Aggarwal, N. K. Ratha, R. M. Bolle, and R. Chellappa, "Multi-biometric cohort analysis for biometric fusion," in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP 2008)*, March 2008, pp. 5224–5227.

[22] A. E. Rosenberg, J. DeLong, C.-H. Lee, B.-H. Juang, and F. K. Soong, "The use of cohort normalized scores for speaker verification," in *Proc. of the Second Int. Conf. on Spoken Language Processing (ICSLP 1992)*, October 1992.

[23] G. Aggarwal, N. K. Ratha, and R. M. Bolle, "Biometric verification: Looking beyond raw similarity scores," in *Proc. of the 2006 Conf. on Computer Vision and Pattern Recognition Workshop (CVPRW 2006)*, June 2006, pp. 31–31.

[24] R. Donida Labati, V. Piuri, and F. Scotti, *Touchless Fingerprint Biometrics*. CRC Press, August 2015.

[25] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Toward unconstrained fingerprint recognition: a fully-touchless 3-d system based on two views on the move," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 2, pp. 202–219, February 2016.

[26] V. Piuri and F. Scotti, "Fingerprint biometrics via low-cost sensors and webcams," in *Proc. of the 2008 IEEE Int. Conf. on Biometrics: Theory, Applications and Systems (BTAS 2008)*, September 2008, pp. 1–6.

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

[28] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*.

[29] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "Privacy-preserving fingercode authentication," in *Proc. of the 2010 ACM Workshop on Multimedia and Security*, September 2010, pp. 231–240.

[30] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Proc. of the 2010 IEEE Int. Conf. on Biometrics: Theory Applications and Systems (BTAS 2010)*, September 2010, pp. 1–7.

[31] A. Anand, R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Enhancing the performance of multimodal Automated Border Control systems," in *Proc. of the 15th Int. Conf. of the Biometrics Special Interest Group (BIOSIG 2016)*, September 2016.

[32] Dermalog, "DERMALOG High Speed AFIS." [Online]. Available: http://www.dermalog.com/en/products_solutions/afis/

[33] S. Tulyakov, Z. Zhang, and V. Govindaraju, "Comparison of combination methods utilizing t-normalization and second best score model," in *Proc. of the IEEE Computer Society Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW 2008)*, June 2008, pp. 1–5.

[34] N. Poh, A. Merati, and J. Kittler, "Making better biometric decisions with quality and cohort information: a case study in fingerprint verification," in *Proc. of the 2009 17th European Signal Processing Conf. (EUSIPCO 2009)*, August 2009, pp. 70–74.

[35] M. Tistarelli, Y. Sun, and N. Poh, "On the use of discriminative cohort score normalization for unconstrained face recognition," *IEEE Trans. on Information Forensics and Security*, vol. 9, no. 12, pp. 2063–2075, 2014.

[36] A. Kumar, "Incorporating cohort information for reliable palmprint authentication," in *Proc. of the Sixth Indian Conf. on Computer Vision, Graphics & Image Processing (ICVGIP 2008)*, December 2008, pp. 583–590.

[37] M. Tistarelli and Y. Sun, "Cohort-based score normalization," in *Encyclopedia of Biometrics*, Z. S. Li and K. A. Jain, Eds. Springer US, 2014, pp. 1–9.

[38] R. Batuwita and V. Palade, "Class imbalance learning methods for support vector machines," *Imbalanced learning: Foundations, algorithms, and applications*, pp. 83–99, 2013.

[39] ISO/IEC, "ISO/IEC 19794 (all parts): Biometric data interchange formats," 2011.

[40] Dermalog, "LF10 Fingerprint Scanner." [Online]. Available: http://www.dermalog.com/en/products_solutions/fingerprintscanner/lf10.php

[41] CASIA, "Fingerprint Image Database Version 5.0." [Online]. Available: http://biometrics.idealtest.org/dbDetailForUser.do?id=7

[42] Frontex Agency, "BIOPASS II Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate," 2010.

[43] K. Nandakumar, Y. Chen, S. C. Dass, and A. Jain, "Likelihood ratio-based biometric score fusion," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 30, no. 2, pp. 342–347, February 2008.

[44] A. J. Mansfield and J. L. Wayman, "Best practices in testing and reporting performance of biometric devices," National Physical Laboratory, Tech. Rep., August 2002.