This article has been accepted for publication in IEEE Transactions on Biometrics, Behavior, and Identity Science. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2023.3279859

Detecting Double-Identity Fingerprint Attacks

M. Ferrara, R. Cappelli, and D. Maltoni, *Senior Member, IEEE*

***Abstract*— Double-identity biometrics, that is the combination of two subjects' features into a single template, was demonstrated to be a serious threat against existing biometric systems. In fact, well-synthetized samples can fool state-of-the-art biometric verification systems, leading them to falsely accept both the contributing subjects. This work proposes one of the first techniques to defy existing double-identity fingerprint attacks. The proposed approach inspects the regions where the two aligned fingerprints overlap but minutiae cannot be consistently paired. If the quality of these regions is good enough to minimize the risk of false or miss minutiae detection, then the alarm score is increased. Experimental results carried out on two fingerprint databases, with two different techniques to generate double-identity fingerprints, validate the effectiveness of the proposed approach.**

***Index Terms*— Double-identity fingerprints, presentation attacks, ABC systems, eMRTD.**

I. INTRODUCTION

The term double-identity biometric denotes a biometric sample obtained by combining features of two subjects, so that it has high chance to be falsely matched with both. Enrolling a double-identity biometric into an e-MRTD (i.e., electronic Machine Readable Travel Documents) poses a serious security threat because it enables multiple subjects to cross borders under false identities [1] [2].

While face morphing remains the best-known (and most alarming) attack [3] [4], the feasibly of creating double-identity biometrics have been proved for other modalities such as fingerprint [5] and iris [6] [7]. In particular, in [5] we showed that two fingerprints can be combined at feature level (i.e., minutiae) or image level (i.e., pixel intensities) to produce realistic impressions able to fool state-of-the-art fingerprint recognition algorithms with high probability (about 90% chance of successful attacks against a system with a security level tuned according to FRONTEX guidelines [8]). Figure 1 shows an example of double-identity fingerprint obtained with the image-level combination method described in [5]. A well-manufactured fake fingertip can be then synthetized [9] and worn by a subject before placing his finger on the scanner during e-MRTD enrolment. To reduce the risk of such an attack, the officer attending the process should carefully supervise the process or a presentation attack detection (PAD) algorithm could be installed in the fingerprint acquisition system. Unfortunately, the fingerprint scanner is often positioned beyond a glass and it is not directly visible to the officer, and PAD algorithms are still far to be perfect. Therefore, an automated double-identity fingerprint detection module can provide an extra protection level.

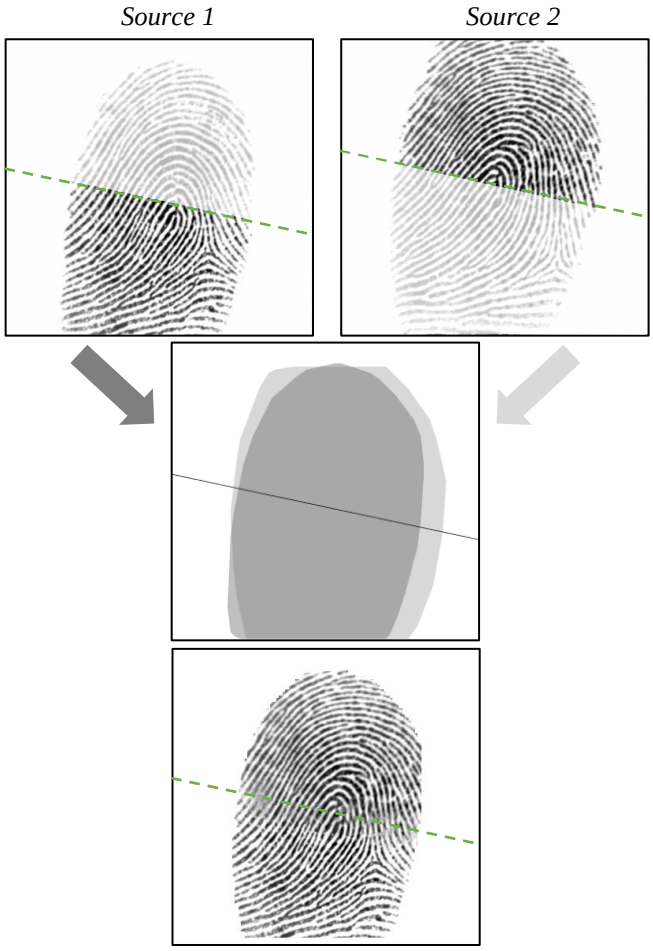

Fig. 1. Double-identity fingerprint creation using the image-level method described in [5]. From top to bottom: two source images (real fingerprints of different subjects), alignment of the two source patterns, and the resulting double-identity fingerprint. The dashed line is the "cutline" along which the two source fingerprints are combined (the top region of the double-identity fingerprint matches *Source 2*, while its bottom region matches *Source 1*.

This work is part of the iMARS project. The project received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 883356.

Disclaimer: this text reflects only the author's views, and the Commission is not liable for any use that may be made of the information contained therein.

Corresponding author: M. Ferrara.

The authors are with the Department of Computer Science and Engineering of the University of Bologna, Italy (e-mails: matteo.ferrara@unibo.it, raffaele.cappelli@unibo.it, and davide.maltoni@unibo.it).

In the context of face morphing, the detection approaches are denoted as MAD (Morphing Attack Detection) and can be categorized as single image (S-MAD) or differential (D-MAD) [10]; the former detect the alteration on a single image, while the latter require an additional "genuine" image to be compared with the probed one, to come to a final decision.

In this paper we introduce a novel double-identity fingerprint detection approach that can work in conjunction with an existing fingerprint verification system, as illustrated in Figure 2. According to the above MAD notation, our approach falls in the D-MAD category, since the detection takes place by comparing a second sample (i.e., the live fingerprint) with the probed one (i.e., the document fingerprint). Our detection approach was designed to defy existing fingerprint combination approaches whose basic idea is to combine two fingerprint portions. For example, in Figure 1 the lower portion of *Source 1* is combined with the upper portion of *Source 2*: as proved in [5], the selection of "compatible" patterns and the determination of an optimal cut-line makes the resulting pattern quite realistic. To tolerate involuntary finger displacement and to cope with lack of information in low quality regions (that can be produced by uneven finger pressure), state-of-the-art fingerprint matching algorithms usually do not enforce a strict feature correspondence across the entire pattern, but settle for a partial fingerprint matching. Hence, the basic idea of our method is inspecting the intersection of the foreground patterns (after alignment) and check the existence of good quality regions whose minutiae do not match (i.e., cannot be paired). To this purpose two maps are computed:

- the *expectation map* points out the places where, according to the foreground intersection after alignment and the existence of reliable minutiae, we expect to find minutiae pairings;
- the *alert map*, which is computed by subtracting from the expectation map the regions of actual minutiae pairings, and therefore, in case the probed fingerprint is bona fide, turns to be almost empty.

In our experiments, a simple threshold applied to the alert map allowed us to discriminate double-identity from bona fide fingerprints with good accuracy.

To the best of our knowledge, there is almost no related literature on this subject. In [11], two fingerprints are combined, but with the totally different aim of generating new virtual identities and cancellable templates. In [12] experiments with GAN-based model are reported confirming the feasibility of double-identity fingerprint attacks, but no countermeasures are proposed. The only existent double-identity detection method for fingerprints was introduced in [13] by training a deep learning model. Unfortunately, the authors did not publish the resulting model and the dataset, making impossible a direct and fair comparison. Furthermore, based on our experience on face morphing, overfitting is a serious problem when training a large model to detect image alterations and several heterogeneous data sources would be necessary.

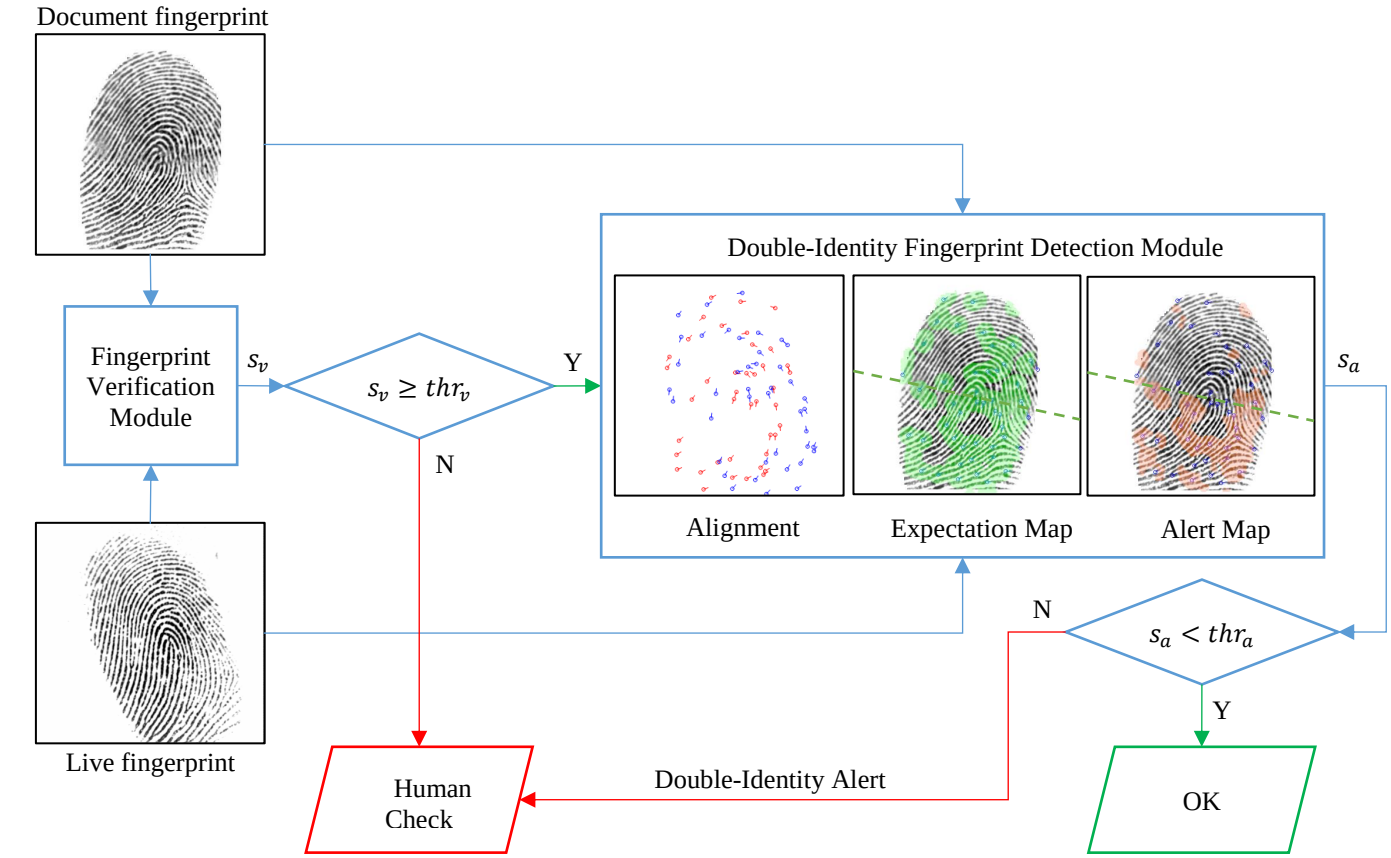

Fig. 2. Functional schema of the proposed fingerprint verification procedure (including the double-identity fingerprint detection module) performed at ABC gates.

In Section II we introduce our detection method by formally defining all the intermediate steps necessary to compute the final alert map. Section III reports and comments the experimental results obtained. Finally, Section IV draws some concluding remarks.

II. Proposed Approach

Given two greyscale fingerprints $\mathbf{F}^1$ and $\mathbf{F}^2$, the proposed approach computes the following data to calculate the alert score:

1. the two minutiae templates;
2. the parameters of the affine transform to align the two fingerprints;
3. the local quality map of the two fingerprints;
4. the minutia density map of the two fingerprints;
5. the density map of minutiae compatibility;
6. the expectation map;
7. the alert map.

Let $T^1 = \{m_i^1\}$ and $T^2 = \{m_j^2\}$ be the minutiae templates extracted from $\mathbf{F}^1$ and $\mathbf{F}^2$, respectively. Each minutia m is a triplet $m = (x, y, \theta)$ where x and y are the minutia location, and θ is the minutia angle in the range $[0,2\pi[$. T^1 and T^2 can be obtained using any state-of-the-art minutiae extraction algorithm [9]. Figure 3 shows two fingerprints and the corresponding minutiae templates: note that $\mathbf{F}^1$ is the double-identity fingerprint in Figure 1, while $\mathbf{F}^2$ is a live sample from *Source 2* (see Figure 1) different from that used to create $\mathbf{F}^1$.

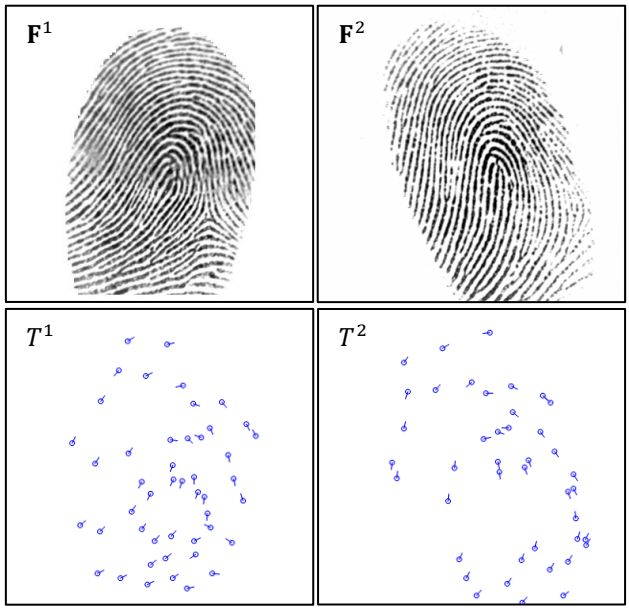

Fig. 3. Two fingerprints and the corresponding minutiae templates.

With the aim of aligning the two fingerprints, a least-square approach is used to find an affine transform M of T^2 that superimposes its minutiae to T^1. M is determined starting from a set of minutiae correspondences $P = \{(i_k, j_k)\}$, where i_k and j_k are the minutia-indices in T^1 and T^2, respectively (see Figure 4). P can be found by any state-of-the-art minutiae comparison algorithm [9]. In the following, $\hat{T}^2$ denotes the set of minutiae obtained by aligning T^2 according to M (see Figure 5).

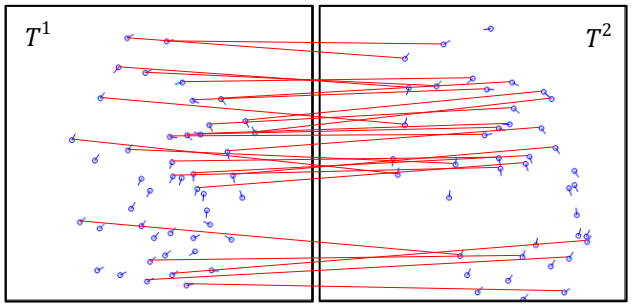

Fig. 4. The set P of minutiae correspondences between T^1 and T^2 is graphically displayed by red lines.

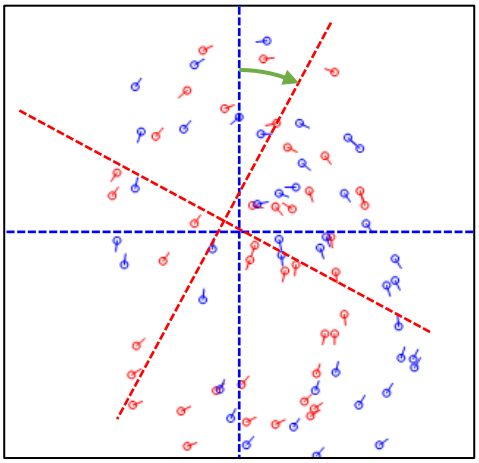

Fig. 5. The affine transform M applied to minutiae in T^2 (in blue color) to obtain the aligned template $\hat{T}^2$ (in red).

The proposed method, beside minutiae, relies on the fingerprint local quality [9] to concentrate the analysis where the fingerprint pattern is more reliable. Let $\mathbf{Q}^1$ be the local quality map (pixel-wise) of $\mathbf{F}^1$, and $\mathbf{Q}^2$ be the one obtained by applying M to the local quality map of $\mathbf{F}^2$. Figure 6 shows $\mathbf{Q}^1$ and $\mathbf{Q}^2$ for the fingerprint images in Figure 3.

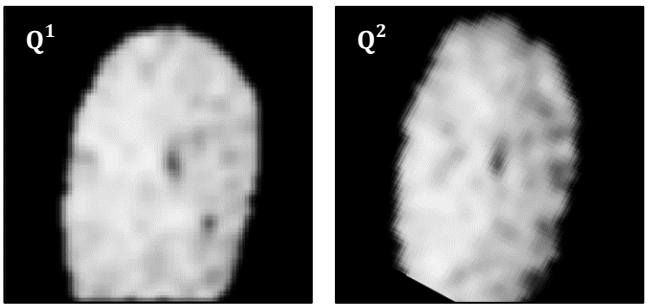

Fig. 6. The pixel-wise local quality maps of $\mathbf{F}^1$ and $\mathbf{F}^2$. Note that $\mathbf{Q}^2$ is aligned according to M.

Local quality maps $\mathbf{Q}^1$ and $\mathbf{Q}^2$ are then binarized according to a fixed threshold τ_Q. Hereafter any binary image $\mathbf{I}$ is formally

represented as the set containing the coordinates of non-zero pixels: $\mathbb{I} = \{(x,y)|\, \mathbf{I}[x,y] \neq 0\}$. This makes the notation simpler when set operations and morphological operators are applied [14].

Let $\mathbb{Q}^1$ and $\mathbb{Q}^2$ be the sets containing the coordinates of good-quality pixels according to τ_Q: $\mathbb{Q}^t = \text{binarize}(\mathbf{Q}^t, \tau_Q)$ where $\text{binarize}(\mathbf{X}, \tau) = \{(x,y)|\mathbf{X}[x,y] \geq \tau\}$ (see Figure 7).

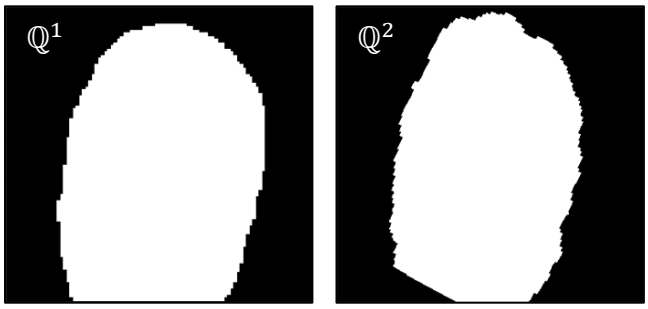

Fig. 7. The binary images corresponding to sets $\mathbb{Q}^1$ and $\mathbb{Q}^2$ obtained from $\mathbf{Q}^1$ and $\mathbf{Q}^2$ in Figure 6.

The next step consists in computing the minutia density maps from T^1 and $\hat{T}^2$. The minutia density map $\mathbf{D}^1$ is a matrix with the same size of $\mathbf{F}^1$ whose elements $\mathbf{D}^1_{i,j}$ denote the likelihood of finding minutiae in T^1 close to position $(x \equiv j, y \equiv i)$:

$$\mathbf{D}^1_{i,j} = \mathrm{z}_{\mu_D,\beta_D}\left(\sum_{m \in T^1} \mathrm{B}_{i,j}(m)\right) \quad (1)$$

with

$$\mathrm{B}_{i,j}(m) = \mathrm{g}_{\sigma_B}\left(\mathrm{d}_{i,j}(m)\right) \quad (2)$$

where:

- $\mathrm{d}_{i,j}(m)$ is the Euclidean distance between position (j,i) and the location of minutia m;
- $\mathrm{g}_\sigma(v) = e^{-\frac{v^2}{2\sigma^2}}$ is a Gaussian function with zero mean, σ standard deviation and a maximum value of one;
- $\mathrm{z}_{\mu,\beta}(v) = \frac{1}{1+e^{-\beta\cdot(v-\mu)}}$ is a sigmoid function controlled by two parameters (μ and β), that limits the contribution of dense minutiae clusters, to ensure that the final value is in the range $[0,1]$.

$\mathbf{D}^1_{i,j}$ is obtained by summing the contribution $\mathrm{B}_{i,j}(m)$ of each minutia $m \in T^1$, which depends on the Euclidean distance between m and (j,i).

$\mathbf{D}^2$ is computed in the same way, starting from the aligned minutiae template $\hat{T}^2$. Figure 8 shows the two maps $\mathbf{D}^1$ and $\mathbf{D}^2$ as well as the corresponding minutiae in T^1 and $\hat{T}^2$.

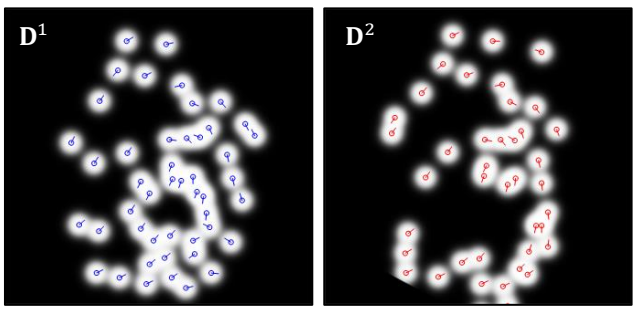

Fig. 8. The pixel-wise density maps of T^1 and $\hat{T}^2$. Minutiae points are superimposed to the two maps to better highlight how they have been computed. Note the saturation produced by the sigmoid in the overlapping regions.

The two density maps are then binarized into $\mathbb{D}^1$ and $\mathbb{D}^2$ to determine high-density locations, according to a given threshold τ_D: $\mathbb{D}^t = \text{binarize}(\mathbf{D}^t, \tau_D)$, see Figure 9.

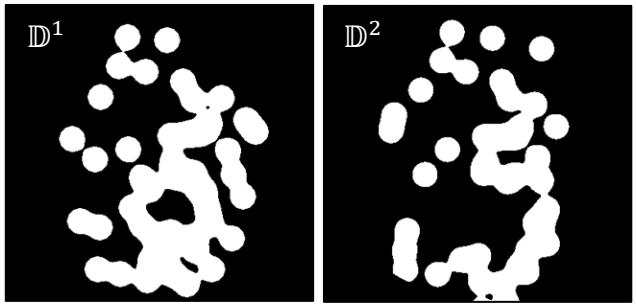

Fig. 9. The binary images corresponding to sets $\mathbb{D}^1$ and $\mathbb{D}^2$ obtained from $\mathbf{D}^1$ and $\mathbf{D}^2$ in Figure 8.

The density map of minutiae compatibility $\mathbf{D}$ is a matrix with the same size of $\mathbf{F}^1$, where each element $\mathbf{D}_{i,j}$ is the likelihood of finding compatible minutiae pairs near position (j,i), see Figure 10. Two minutiae (one from T^1 and the other from $\hat{T}^2$) are considered compatible if their positions are close and their angles are similar.

$$\mathbf{D}_{i,j} = \mathrm{z}_{\mu_D,\beta_D}\left(\frac{\mathrm{K}_{i,j}(T^1,\hat{T}^2)+\mathrm{K}_{i,j}(\hat{T}^2,T^1)}{2}\right) \quad (3)$$

with

$$\mathrm{K}_{i,j}(T,T') = \sum_{m' \in T'} \mathrm{B}_{i,j}(m') \cdot \mathrm{C}(m',T) \quad (4)$$

and

$$\mathrm{C}(m',T) = \mathrm{z}_{\mu_C,\beta_C}\left(\sum_{m \in T} \mathrm{g}_{\sigma_E}\left(\mathrm{d}_E(m,m')\right) \cdot \mathrm{g}_{\sigma_\theta}\left(\mathrm{d}_\theta(m,m')\right)\right) \quad (5)$$

where:

- $\mathrm{d}_E(m,m')$ is the Euclidean distance between minutiae m and m';
- $\mathrm{d}_\theta(m,m')$ is the difference between the angles of minutiae m and m'.

Equation (3) computes $\mathbf{D}_{i,j}$ similarly to how Equation (1) calculates each element of the minutia density map for a single template: the same sigmoid function ($\mathrm{z}_{\mu_D,\beta_D}$) is applied to the sum of the contribution $\mathrm{B}_{i,j}$ of each minutia. In this case, however:

- for each minutia $m' \in T'$, its contribution $\mathrm{B}_{i,j}(m')$ is weighted by the compatibility measure $\mathrm{C}(m',T)$ of m' with respect to the positions and angles of all minutiae in the other template T, see Equations (4) and (5);
- since function $\mathrm{K}_{i,j}$, defined by Equation (4) on two templates, is a non-commutative operation, the average of $\mathrm{K}_{i,j}(T^1,\hat{T}^2)$ and $\mathrm{K}_{i,j}(\hat{T}^2,T^1)$ is used in Equation (3).

The density map of minutiae compatibility $\mathbf{D}$ is then binarized to determine the set of pixel coordinates close to compatible minutiae, according the same threshold τ_D used to binarize the minutia density maps: $\mathbb{D} = \text{binarize}(\mathbf{D}, \tau_D)$, see Figure 11.

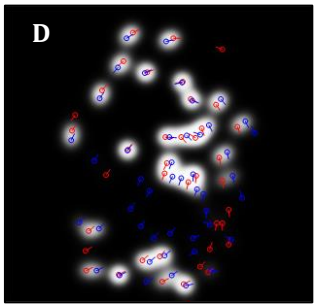

Fig. 10. The pixel-wise density map of minutiae compatibility between T^1 and $\hat{T}^2$. Minutiae points of both templates are superimposed to the map (T^1 minutiae in blue, and $\hat{T}^2$ ones in red).

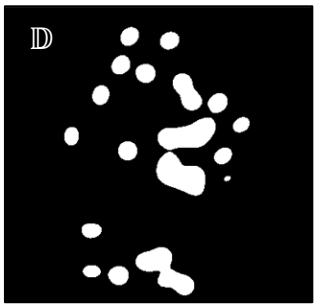

Fig. 11. The binary image corresponding to set $\mathbb{D}$ obtained from **D** in Figure 10.

The last step consists in computing the expectation map $\mathbb{E}$ and the alert map $\mathbb{A}$:

$$\mathbb{E} = (\mathbb{D}^1 \cup \mathbb{D}^2) \cap (\mathbb{Q}^1 \cap \mathbb{Q}^2) \quad (6)$$

$$\mathbb{A} = (\mathbb{E} \backslash \mathbb{D}) \circ \mathbb{S}_d \quad (7)$$

In Equation (6), $\mathbb{D}^1 \cup \mathbb{D}^2$ denotes regions where minutiae are present at least in one of the fingerprints, and $\mathbb{Q}^1 \cap \mathbb{Q}^2$ represents regions where the quality is good in both fingerprints. Hence, we can say that the expectation map $\mathbb{E}$ denotes the good quality regions where minutiae are present at least in one of the fingerprints, see Figure 12.

In fingerprint comparisons where $\mathbf{F}^1$ is a bona fide fingerprint, it is expected that $\mathbb{E} \approx \mathbb{D}$, since in good quality regions any minutia should find a compatible minutia in the other template. For this reason, the alert map is based on the set difference between $\mathbb{E}$ and $\mathbb{D}$ (i.e., $\mathbb{E} \backslash \mathbb{D}$: the relative complement of $\mathbb{D}$ in $\mathbb{E}$). An opening morphological operation $\circ$ (with a circular structuring element $\mathbb{S}_d$ of diameter d) is also applied to remove small artefacts that may be present due to the variability of fingerprint patterns, skin deformation and other alterations. The bottom-right image in Figure 12 shows the alert map for the two fingerprints in Figure 3.

Figure 13 shows $\mathbb{E}$ and $\mathbb{A}$ superimposed to $\mathbf{F}^1$. As already described in Section I, $\mathbf{F}^1$ is a double-identity fingerprint created by blending the fingerprints of two different fingers (*Source 1* and *Source 2* in Figure 1). $\mathbb{E}$ and $\mathbb{A}$ have been obtained by comparing $\mathbf{F}^1$ to $\mathbf{F}^2$, which, in this example, is another impression of the finger used to make the top half of $\mathbf{F}^1$ (*Source 2*). As a consequence, the alert map has several active zones in the bottom part of $\mathbf{F}^1$, whose minutiae are mostly not compatible with those of $\mathbf{F}^2$.

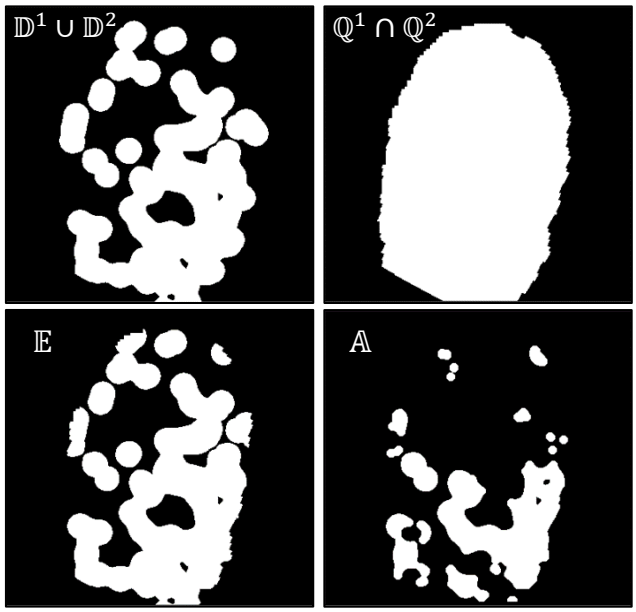

Fig. 12. From top to bottom, from left to right: the binary images corresponding to sets $\mathbb{D}^1 \cup \mathbb{D}^2$, $\mathbb{Q}^1 \cap \mathbb{Q}^2$, $\mathbb{E}$, and $\mathbb{A}$.

Fig. 13. From left to right: the expectation map $\mathbb{E}$ and the alert map $\mathbb{A}$ superimposed to $\mathbf{F}^1$ and its minutiae. The cutline used to create the double-identity fingerprint $\mathbf{F}^1$ is also reported (see Figure 1).

Finally, the alert score $s_a \in [0,1]$ is computed as the ratio between the cardinalities of $\mathbb{A}$ and $\mathbb{E}$:

$$s_a = \frac{|\mathbb{A}|}{|\mathbb{E}|}. \quad (8)$$

The higher the alert score, the more likely it is that $\mathbf{F}^1$ is a double-identity fingerprint.

The alert score obtained for the example in Figure 13 is 0.50. As a reference, Figure 14 shows a bona fide comparison: the alert map exhibits much fewer active zones with respect to Figure 13, resulting in a significantly lower alert score: 0.09.

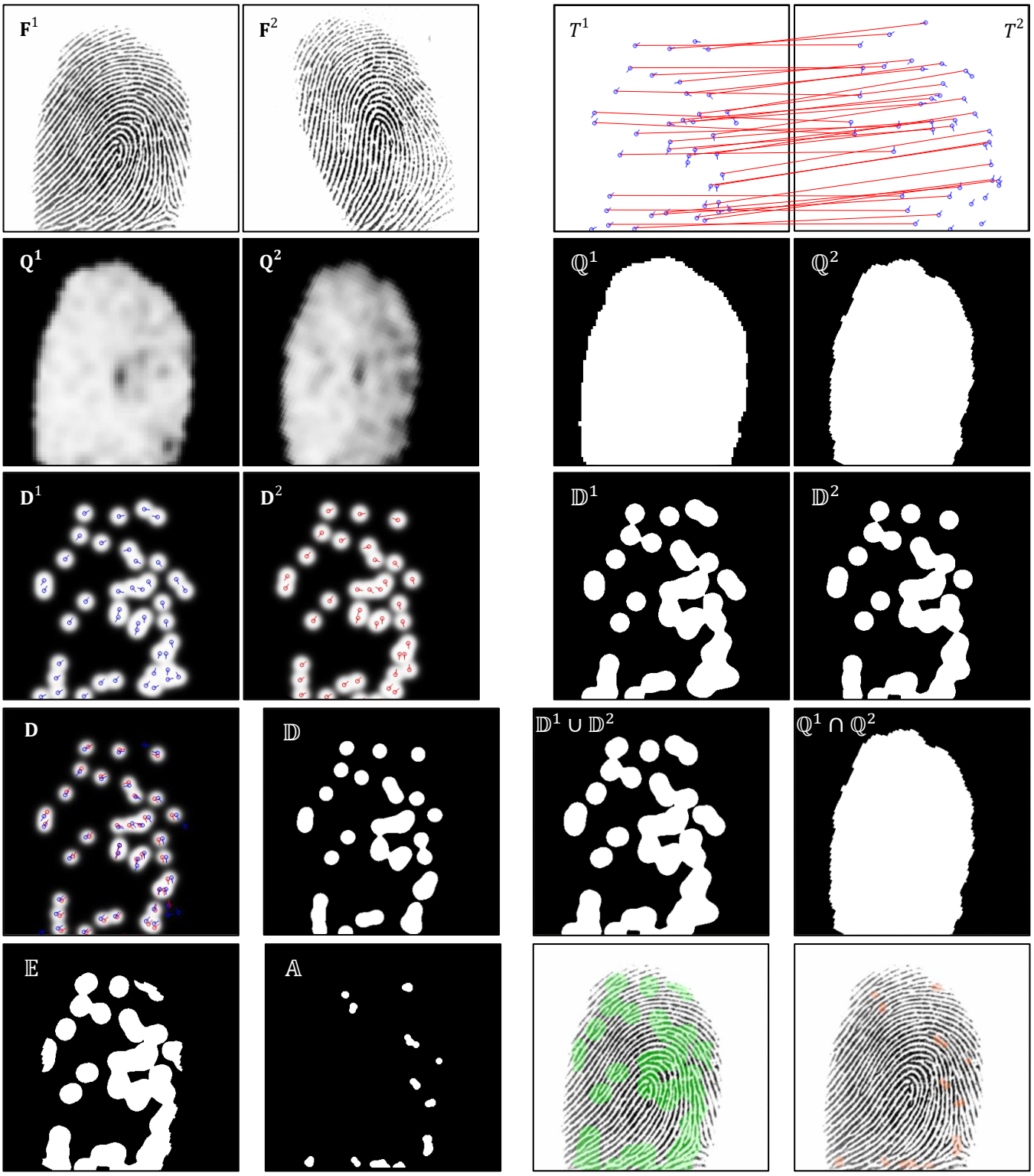

Fig. 14. An example of the proposed method applied to a bona fide comparison. From top to bottom, from left to right: two fingerprints ($\mathbf{F}^1$ and $\mathbf{F}^2$) from the same finger, the correspondences between the two minutiae templates between T^1 and T^2, the local quality maps $\mathbf{Q}^1$ and $\mathbf{Q}^2$, the corresponding binary images $\mathbb{Q}^1$ and $\mathbb{Q}^2$, the minutiae density maps $\mathbf{D}^1$ and $\mathbf{D}^2$, the corresponding binary images $\mathbb{D}^1$ and $\mathbb{D}^2$, the density map of minutiae compatibility $\mathbf{D}$, its corresponding binary image $\mathbb{D}$, the images corresponding to $\mathbb{D}^1 \cup \mathbb{D}^2$ and $\mathbb{Q}^1 \cap \mathbb{Q}^2$, the expectation map $\mathbb{E}$, the alert map $\mathbb{A}$, and finally $\mathbb{E}$ and $\mathbb{A}$ superimposed to $\mathbf{F}^1$.

III. Experiments

This section describes the experiments designed to assess the capability of the proposed approach to deal with double-identity fingerprints.

Databases

To the best of our knowledge, there are no publicly available fingerprint databases for testing double-identity attacks. The experiments of this study were carried out on the following databases:

- *TestDB1* - the double-identity fingerprint database generated in [5]. This database was created starting from the FVC2002 DB1 set A [15], containing 800 fingerprints from 100 fingers (8 impressions per finger), captured at 500dpi using the optical scanner "TouchView II" by Identix. Besides the real fingerprints, it contains two sets of 100 double-identity fingerprints, produced using feature- and image-level generation approaches, respectively (see [5]).
- *TestDB2* – a double-identity fingerprint database created starting from the V300 Fingerpass database [16], containing 8640 fingerprints from 720 fingers (12 impressions per finger), captured at 500dpi using the optical scanner "Verifier 300" by CrossMatch. Besides the real fingerprints, it contains two sets of 720 double-identity fingerprints, produced using feature- and image-level generation approaches, respectively (see [5]).
- *TrainDB* – a double-identity fingerprint dataset obtained from FVC2002 DB1 set B [15]. It contains 80 bona fide fingerprints (from ten different fingers) and ten double-identity fingerprints generated using the image-level approach described in [5]. Note that this database is completely disjoint from *TestDB1* database, since there are no common fingers between set A and B of FVC2002 DB1.

Figure 15 shows an example of bona fide images from *TestDB1* and *TestDB2*.

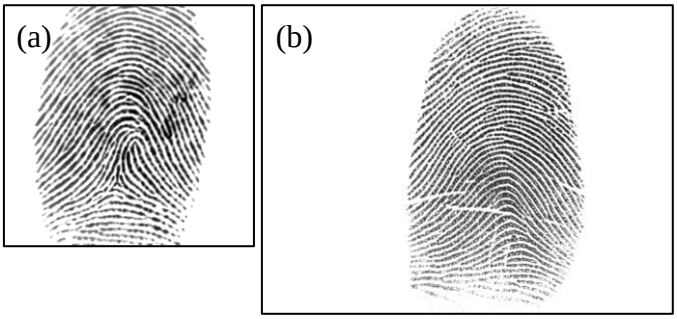

Fig. 15. Examples of bona fide images from *TestDB1* (a) and *TestDB2* (b).

Parameters

Table I reports the parameter values used; all parameters were calibrated on *TrainDB*. The calibration procedure consisted in an exhaustive search over a reasonable range of values.

TABLE I
Parameter Values Used in the Experimentation

Parameter(s)	Description	Value
τ_Q	Quality map binarization threshold	15
μ_D, β_D	Sigmoid parameters in (1) and (3)	$\frac{1}{5}$, 4
σ_B	Standard deviation in (2)	8
τ_D	Density map binarization threshold	$\frac{1}{2}$
μ_C, β_C	Sigmoid parameters in (5)	$\frac{1}{4}$, 15
σ_E	Standard deviation of the position difference in (5)	8
σ_θ	Standard deviation of the angle difference in (5)	15°
d	Diameter of the structuring element used in (7).	11

Evaluation of the Attack Potential

This section describes the experiments carried out to evaluate the attack potential of the double-identity fingerprints contained in the two test databases. The recently-introduced Morphing Attack Potential (MAP) metric [17] was applied to analyze the impact of multiple samples and different fingerprint recognition systems (FRSs). MAP is defined as a matrix whose generic element MAP$[r, c]$ is the proportion of double-identity fingerprints that can successfully reach a match decision with both source fingers in at least r verification attempts by at least c FRSs [17]. Two state-of-the-art FRSs were use: the Minutia Cylinder-Code SDK v2.0 (MCC) [18] [19] and the VeriFinger SDK v12.1 (VF) [20]. In order to simulate a realistic attack to an ABC gate, the operational thresholds of both FRSs were set, according to the FRONTEX guidelines [8], to ensure a False Acceptance Rate (FAR) equal to 0.1%.

Tables II and III report MAP results on *TestDB1* and *TestDB2*, respectively. It is well evident that the attack potential of double-identity fingerprints is very high: if just a single successful match decision is required (as it often happens in ABC), on both databases the attack is effective in almost all the cases with the image-level generation approach and in more than 85% of the cases with the feature-level one. Even with a stricter requirement of three successful match decisions, the attack is quite dangerous both on *TestDB1* (93% and 59% on image- and feature-level sets, respectively), and *TestDB2* (98% and 78% on image- and feature-level sets, respectively). In general, the attack potential of the image-level approach is higher than that of the feature-level one. It is also worth noting that the attacks tend to be more successful on *TestDB2*. This is probably due to the different acquisition area of the fingerprint sensors (see Figure 15). In particular, the sensor used to acquire *TestDB2* images has a larger area, hence acquired fingerprint patterns tend to be larger and contain more minutiae, thus increasing the success changes of the attack.

The results reported in Table II are in line with those reported in [5] using a different metric: the Double-identity Acceptance Rate (DAR), which is computed analogously to the well-known False Acceptance Rate (FAR), see [5] for more details. For completeness, tables IV and V report results using DAR metric, for both FRSs, at different values of FAR on *TestDB1* and *TestDB2*, respectively. Note that results on Table IV are exactly the same reported in [5].

TABLE II
MORPHING ATTACK POTENTIAL (%) ON *TESTDB1*

		Feature-level		Image-level	
		# FRSs		# FRSs	
		1	2	1	2
# Attempts	1	99.0	86.0	100.0	100.0
	2	96.0	73.0	100.0	98.0
	3	89.0	59.0	100.0	93.0
	4	84.0	50.0	100.0	88.0
	5	80.0	41.0	96.0	83.0
	6	69.0	27.0	93.0	63.0
	7	26.0	9.0	56.0	23.0

TABLE III
MORPHING ATTACK POTENTIAL (%) ON *TESTDB2*

		Feature-level		Image-level	
		# FRSs		# FRSs	
		1	2	1	2
# Attempts	1	97.2	89.7	100.0	99.9
	2	95.6	82.4	100.0	99.3
	3	92.9	77.8	100.0	98.2
	4	89.9	72.4	99.9	97.1
	5	86.3	66.3	99.6	95.7
	6	82.6	59.7	99.3	94.2
	7	77.5	53.1	98.5	88.9
	8	70.3	43.6	96.7	81.8
	9	61.8	32.9	93.1	73.6
	10	49.2	23.5	86.0	61.8
	11	30.4	11.1	72.5	39.4

TABLE IV
DOUBLE-IDENTITY ACCEPTANCE RATE (%) ON *TESTDB1*

Set	@FAR$_{1\%}$		@FAR$_{0.1\%}$		@FAR$_{0.01\%}$	
	MCC	VF	MCC	VF	MCC	VF
Feature-level	80.6	87.2	69.3	79.0	54.5	69.3
Image-level	92.6	95.4	88.5	93.5	81.1	91.1

TABLE V
DOUBLE-IDENTITY ACCEPTANCE RATE (%) ON *TESTDB2*

Set	@FAR$_{1\%}$		@FAR$_{0.1\%}$		@FAR$_{0.01\%}$	
	MCC	VF	MCC	VF	MCC	VF
Feature-level	85.4	92.9	73.1	85.6	58.5	74.9
Image-level	95.6	98.8	91.4	97.4	85.3	95.8

Feature Extraction

In order to compute the proposed alert score, the fingerprint recognition SDK VeriFinger 12.1 [20] was used to extract minutiae and to pair them during the alignment step (see Section II). The local quality (necessary to create quality maps $\mathbf{Q^1}$ and $\mathbf{Q^2}$) was estimated as the local orientation reliability, i.e. the coherence of a set of orientation estimations in a given neighbourhood [9].

Testing Protocol and Performance Indicators

For each double-identity set of both test databases, bona fide and double-identity fingerprints were used to compute the Bona fide Presentation Classification Error Rate (BPCER) and the Attack Presentation Classification Error Rate (APCER). As defined in [21], BPCER is the proportion of bona fide presentations falsely classified as presentation attacks, while APCER is the proportion of double-identity attack presentations falsely classified as bona fide presentations. The following performance indicators are reported:

- EER (detection Equal-Error-Rate): the error rate for which BPCER and APCER are identical;
- BPCER$_{10}$: the lowest BPCER for APCER≤10%;
- BPCER$_{20}$: the lowest BPCER for APCER≤5%;
- BPCER$_{100}$: the lowest BPCER for APCER≤1%.

To calculate the above indicators, alert scores were computed, as described in Section II, for the following types of comparisons:

- *bona fide* – each fingerprint is compared against the remaining ones of the same finger. If fingerprint F_A is compared against F_B, the symmetric comparison is not executed to avoid correlation in the scores. The total number of bona fide comparisons is 2800 for *TestDB1* and 47520 for *TestDB2*.
- *double-identity* – each double-identity fingerprint is compared against all other impressions of both fingers involved in the generation process. The total number of double-identity comparisons, for each double-identity set, is 1400 for *TestDB1* and 15840 for *TestDB2*.

Results

The proposed approach was compared to a baseline method which, after the alignment step, computes the alert score as the ratio between the number of non-paired minutiae and the total number of minutiae. Tables VI and VII report the performance indicators of the proposed approach and the baseline method on both double-identity sets of *TestDB1* and *TestDB2*, respectively. In general, we observe that the proposed approach was quite effective in detecting double-identity attacks and outperformed the baseline in all cases. On *TestDB1*, at the highest security level considered (BPCER$_{100}$), in the worst case less than 5% bona fide attempts were erroneously rejected; on *TestDB2*, at the same security level, only about 11% of bona fide attempts were erroneously rejected.

TABLE VI
PERFORMANCE INDICATORS ON *TESTDB1*

Double-identity set	Method	EER	BPCER$_{10}$	BPCER$_{20}$	BPCER$_{100}$
Feature-level	Baseline	2.18%	1.07%	1.50%	3.29%
	Proposed	0.95%	0.14%	0.39%	0.93%
Image-level	Baseline	3.36%	2.61%	3.18%	18.86%
	Proposed	1.95%	0.46%	0.93%	4.64%

TABLE VII
PERFORMANCE INDICATORS ON *TESTDB2*

Double-identity set	Method	EER	$BPCER_{10}$	$BPCER_{20}$	$BPCER_{100}$
Feature-level	Baseline	9.57%	9.49%	11.36%	14.83%
	Proposed	5.11%	4.00%	5.13%	7.56%
Image-level	Baseline	13.53%	14.75%	17.16%	23.24%
	Proposed	6.81%	6.01%	7.48%	11.33%

It is wort noting that double-identity fingerprints generated with the feature-level approach were easier to be detected for both approaches. This may be due to the presence of spurious minutiae which often appear during the generation process (see [5] for more details).

An analysis of the errors of the proposed approach at $BPCER_{100}$ was carried out to understand their main causes.

- Almost all attack presentation classification errors were due to incorrect placement of the finger on the acquisition device (see Figure 16).
- As to bona fide presentation classification errors, most of them were due to skin distortion (see Figure 17), a few other errors depended on low quality regions not correctly detected (see Figure 18) or on a small number of paired minutiae. Errors due to skin distortion were particularly common on *TestDB2*, resulting in a BPCER higher than *TestDB1* at the same APCER. This explains the better performance of our approach on *TestDB1* (see Tables VI and VII).

Some ideas to further reduce the above errors are discussed in the following section.

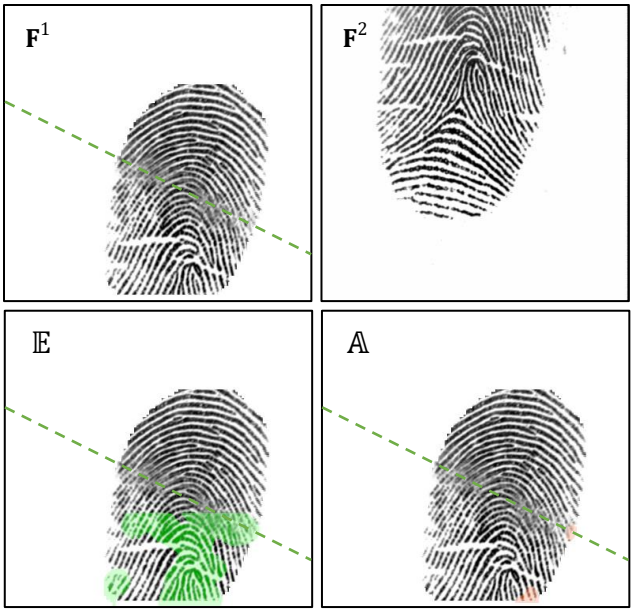

Fig. 16. An example of double-identity attack not detected by the proposed approach at $BPCER_{100}$. The live fingerprint ($\mathbf{F}^2$) corresponds to the lower part of $\mathbf{F}^1$ but, due to an incorrect finger placement, the upper portion of $\mathbf{F}^2$ is not present (see the expectation map $\mathbb{E}$). For this reason, the alert map $\mathbb{A}$ is almost empty and the alert score is very low.

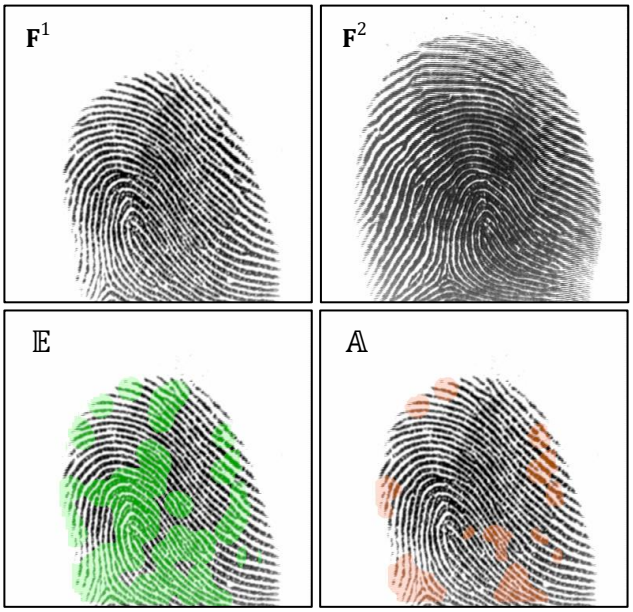

Fig. 17. An example of bona fide comparison erroneously detected as a double-identity attack at $BPCER_{100}$. The large amount of skin distortion in fingerprint $\mathbf{F}^2$ prevents several minutiae from being paired, resulting in a quite high alert score.

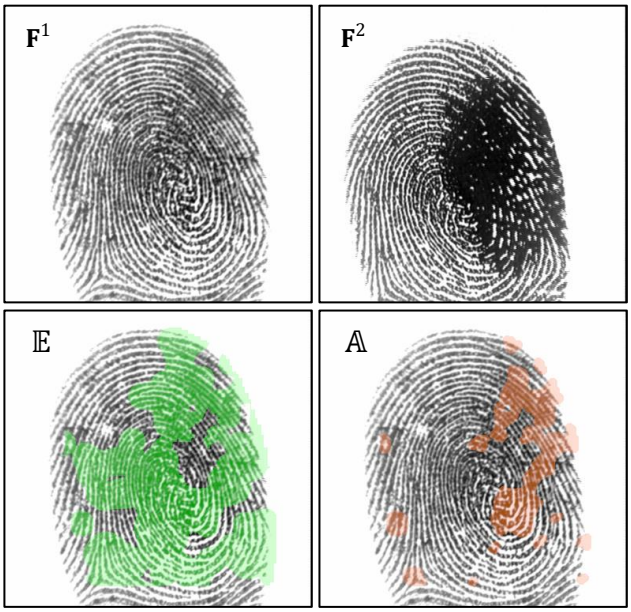

Fig. 18. An example of bona fide comparison erroneously detected as a double-identity attack at $BPCER_{100}$. In this case, the local quality estimator is unable to correctly discard most of the low-quality region in $\mathbf{F}^2$. This can be observed in the expectation map $\mathbb{E}$, where only a small part of the low-quality region is not present. Therefore, since minutiae cannot be reliably extracted from that region, no pairing with minutiae in $\mathbf{F}^1$ can be found, resulting in many active zones in the alert map $\mathbb{A}$.

IV. Conclusion

In this paper we proposed the first differential approach to detect double-identity fingerprint attacks. This approach was specifically designed to counteract double-identity generation methods based on the combination of two fingerprint portions (as the two techniques introduced in [5]). The idea of looking at non-matching minutiae in the aligned intersection of the two fingerprints proved to be very effective: in the worst case considered, the proposed method is able to detect 99% of the attacks with a BPCER less than 12%. On the other hand, the proposed method may not behave as well with double-identity fingerprints generated by attack techniques not based on contiguous minutiae regions; investigating this issue is beyond the aims of this work.

From the in-depth error analysis carried out, most of the undetected attacks were due to large displacement of some samples in the datasets, leading to small area overlapping. In a practical deployment, this problem could be addressed by enforcing a correct placement of the live finger over the acquisition device. Most of the bona fide presentation classification errors were due to skin distortion: this problem may be addressed by adopting a distortion-tolerant minutia matching algorithm in the alignment step.

Our future research in this field will be focused on improving the proposed method with respect to the weaknesses highlighted in the experimental section and to design a new single image detector checking for anomalies in fingerprint texture and features.

References

[1] M. Ferrara, A. Franco, and D. Maltoni, "The Magic Passport," in *IEEE International Joint Conference on Biometrics (IJCB)*, Clearwater, Florida, USA, 2014, pp. 1-7.

[2] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of Image Alterations on Face Recognition Accuracy," in *Face Recognition Across the Electromagnetic Spectrum*. Switzerland: Springer International Publishing, 2016, ch. 9, pp. 195-222.

[3] M. Ferrara and A. Franco, "Morph Creation and Vulnerability of Face Recognition Systems to Morphing," in *Handbook of Digital Face Manipulation and Detection*.: Springer, 2022, ch. 6, pp. 117-137.

[4] K. Raja et al., "Morphing Attack Detection - Database, Evaluation Platform and Benchmarking," *accepted on IEEE Transactions on Information Forensics and Security (TIFS)*, 2020.

[5] M. Ferrara, R. Cappelli, and D. Maltoni, "On the Feasibility of Creating Double-Identity Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 892-900, April 2017.

[6] C. Rathgeb and C. Busch, "On the feasibility of creating morphed iris-codes," in *IEEE International Joint Conference on Biometrics (IJCB)*, Denver, CO, USA, 2017.

[7] R. Sharma and A. Ross, "Image-Level Iris Morph Attack," in *IEEE International Conference on Image Processing (ICIP)*, Anchorage, AK, USA, 2021.

[8] FRONTEX - R&D Unit, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems," FRONTEX, Warsaw, Poland, ISBN: 978-92-95205-50-5, DOI: 10.2819/39041, September 2015.

[9] D. Maltoni, D. Maio, A. K. Jain, and J. Feng, *Handbook of Fingerprint Recognition*, 3rd ed.: Springer Cham, 2022.

[10] M. Ferrara, A. Franco, and D. Maltoni, "Face Demorphing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008-1017, April 2018.

[11] A. Othman and A. Ross, "On Mixing Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260-267, January 2013.

[12] A. Makrushin, M. Trebeljahr, S. Seidlitz, and J. Dittmann, "On feasibility of GAN-based fingerprint morphing," in *23rd International Workshop on Multimedia Signal Processing (MMSP)*, Tampere, Finland, 2021.

[13] I. Goel, N. B. Puhan, and B. Mandal, "Deep Convolutional Neural Network for Double-Identity Fingerprint Detection," *IEEE Sensors Letters*, vol. 4, no. 5, May 2020.

[14] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed.: Pearson, 2017.

[15] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "FVC2002: Second fingerprint verification competition," in *International Conference on Pattern Recognition*, vol. 16, 2002, pp. 811-814.

[16] X. Jia, X. Yang, Y. Zang, N. Zhang, and J. Tian, "A cross-device matching fingerprint database from multi-type sensors," in *proceedings of 21st International Conference on Pattern Recognition (ICPR)*, Tsukuba, Japan, 2012, pp. 3001-3004.

[17] M. Ferrara, A. Franco, D. Maltoni, and C. Busch, "Morphing Attack Potential," in *IEEE International Workshop on Biometrics and Forensics*, Salzburg, Austria, 2022.

[18] BioLab. (2023, January) MCC SDK Web Site. [Online]. http://biolab.csr.unibo.it/mccsdk.html

[19] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 12, pp. 2128 - 2141, December 2010.

[20] Neurotechnology Inc. (2022, September) Neurotechnology Web Site. [Online]. https://www.neurotechnology.com/

[21] International Organization for Standardization (ISO), "Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting," Geneva, Switzerland, ISO/IEC FDIS 30107-3:2017 JTC 1/SC 37, 2017.