Alma Mater Studiorum Università di Bologna
Archivio istituzionale della ricerca

On the Feasibility of Creating Double-Identity Fingerprints

(Article begins on next page)

06 September 2024

Rights / License:

On the Feasibility of Creating Double-Identity Fingerprints

Matteo Ferrara, Raffaele Cappelli, *Member, IEEE*, and Davide Maltoni, *Member, IEEE*

Abstract—**A double-identity fingerprint is a fake fingerprint created by combining features from two different fingers, so that it has a high chance to be falsely matched with fingerprints from both fingers. This paper studies the feasibility of creating double-identity fingerprints by proposing two possible techniques and evaluating to what extent they may be used to fool state-of-the-art fingerprint recognition systems. The results of systematic experiments suggest that existing algorithms are highly vulnerable to this specific attack (about 90% chance of success at FAR=0.1%) and that the fingerprint patterns generated might be realistic enough to fool human examiners.**

Index Terms—**Double-identity fingerprints, presentation attacks, ABC systems, minutiae, ridge-line orientations and frequencies.**

I. INTRODUCTION

DOCUMENT fraud has always been a key enabler for organized crime and terrorism. In the last decade, the security of e-MRTD (i.e., electronic Machine Readable Travel Documents) have been greatly improved by embedding electronic features (i.e. chips and encryption) that makes forgery very hard. Further, biometric modalities such as face and fingerprints have been adopted to link a document (i.e., a passport) to its legitimate owner [1].

While the high uniqueness of biometrics traits should ensure a 1-1 link between a document and an individual, recent studies demonstrated the feasibility of enrolling a double-identity biometrics in e-MRTD with the aim to link a single documents to two subjects. The attack described in [2] consists of enrolling a face image which is the result of a two persons morphing, so that at verification time (i.e. transit through an Automatic Border Control gate) the two persons can share the same document. Enrolling a double–identity face image is highly achievable since: i) in several countries face acquisition is not live but relies on printed face photo provided by the citizens; ii) officers cannot easily detect morphed faces (see experiments reported in [3]).

This work is aimed at studying the feasibly of creating double-identity fingerprints to carry out an attack similar to that described in [2]. In fact, even if (unlike face) fingerprint enrolment is always live (i.e., fingerprints are collected at the enrollment station), a well manufactured fake fingertip may be presented to the scanner if the enrolment procedure is not carefully supervised by an officer (often for logistic reasons the fingerprint scanner is beyond a glass and is not directly visible to the officer).

An inspiring work on this topic was carried out by Günter Schumacher, Jan Löschner and Javier Galbally at the European Commission Joint Research Center in Ispra, who first proved the feasibility of creating double-identity fingerprints[1]; however, since the creation approach used was manual, their conclusions are based on a small number of samples, and more systematic evaluations are necessary.

The idea of fingerprint combination was also explored by Othman and Ross in [4] with the aim of creating new virtual identities useful to preserve user privacy (by partially obscuring information) and to generate cancellable templates. It is worth noting that the aim of our technique is exactly the contrary: in fact, our double-identity fingerprint should produce a high comparison score with the native fingers, while Othman and Ross mixed fingerprints are designed to yield a low similarity score when compared with the original biometrics.

A double-identity fingerprint should meet two requirements: i) features should be combined in such a way that state-of-the-art fingerprint recognition algorithm wrongly attribute the resulting fingerprint to both subjects; ii) it should be visually realistic (i.e., without evident artifacts) to deceive the officer attending the enrolment (who normally has a live visual feedback of the user fingerprint).

Two different approaches (both addressed in this study) could be used to combine fingerprints:

- *Feature-level*: starts by local orientations, frequencies and minutiae derived from original fingerprints and then generates a synthetic fingerprint image.
- *Image-level*: directly blends portion of original fingerprint images.

The main contributions of this work are:

- Development of novel fully automatic approaches to combine two fingerprints at feature level and image-level;
- Comparison of feature- and image-level approaches;
- Systematic evaluation of the double-identity fingerprint attack in a verification scenario typical of an Automatic

The authors are with the Department of Computer Science and Engineering of the University of Bologna, Via Sacchi, 3 - 47521 Cesena (FC), Italy (e-mail: {matteo.ferrara, raffaele.cappelli, davide.maltoni}@unibo.it)

[1] The outcome of this research is described in a technical report that is not publicly available.

Border Control (ABC) system.

The rest of this paper is organized as follows. Section II describes the procedures to create double-identity fingerprints; Section III reports and comments the experimental results obtained; finally Section IV draws some concluding remarks.

II. DOUBLE-IDENTITY FINGERPRINT CREATION PROCESS

The aim of this process is to create a new fingerprint that includes features (i.e., minutiae, local orientations and frequencies) of two different fingers.

Given two fingerprints F^1 and F^2 from two different fingers, the following steps are carried out to produce the new fingerprint (Fig. 1):

A. The two fingerprints are superimposed and the best alignment is computed.

B. The optimal cutline is determined by maximizing the ridge pattern similarity nearby the cut.

C. The new double-identity fingerprint is generated.

The above steps are described in detail in the following sections. Table III in the Appendix provides a summary of the symbols used throughout this paper.

A. Fingerprint Alignment

The proposed technique aligns the two fingerprints by maximizing, for any reasonable translation and rotation, the ridge orientation similarity in their intersections.

The local orientations O^1 and O^2 (Fig. 1) of the two fingerprints are estimated blockwise (in steps of b_{size} pixels), along horizontal and vertical axes, by applying the gradient-based technique proposed in [5] with an averaging window of $w_{size} \times w_{size}$ pixels. Each orientation element $o_{i,j} = (\theta_{i,j}, r_{i,j})$ consists of an angle $\theta_{i,j} \in [0, \pi[$ and a value $r_{i,j} \in [0,1]$, denoting the reliability of the estimation ($r_{i,j}$ is zero for elements belonging to the background region).

In general, the similarity between two local orientation images can be computed as follow:

$$S(O^1, O^2) = \frac{\Sigma_{(i,j) \in (V_{O^1} \cap V_{O^2})} (r_{i,j}^1 + r_{i,j}^2) \cdot \psi(\theta_{i,j}^1, \theta_{i,j}^2)}{\Sigma_{(i,j) \in (V_{O^1} \cap V_{O^2})} (r_{i,j}^1 + r_{i,j}^2)}, \quad (1)$$

where $\psi(\theta_1, \theta_2)$ is the similarity between two orientation angles θ_1, θ_2:

$$\psi(\theta_1, \theta_2) = 1 - \frac{2 \cdot |\theta_1 - \theta_2|}{\pi}, \quad (2)$$

and V_O contains the coordinates of foreground orientation elements of the local orientation image O.

$$V_O = \{(i,j) | o_{i,j} \in O \wedge r_{i,j} > 0\}. \quad (3)$$

In order to find the best alignment, all possible translations (in steps of b_{size} pixels) and rotations (in steps of δ_γ) of O^2 with respect O^1 are evaluated (Fig. 1) by maximizing the similarity (Eq. (1)) between O^1 and the aligned O^2. Moreover, to discard alignments with very small overlapping, the following condition is enforced:

$$\frac{|V_{O^1} \cap V_{O^2}|}{\max(|V_{O^1}|, |V_{O^2}|)} \geq min_{VR}. \quad (4)$$

B. Optimal Cutline Estimation

The optimal cutline is determined by attempting to simultaneously achieve the following objectives:

1. maximize the similarity of ridge pattern in the neighborhood of the cutline itself,
2. preserve a sufficient number of minutiae from both the original fingerprints.

The former objective is aimed at generating a fingerprint pattern that looks realistic to the human eye near the cutline (i.e., the most critical region). The latter helps to create a fingerprint that has a high chance to be matched with fingerprints from both the fingers.

Let (dx^*, dy^*, γ^*), be the best translation and rotation parameters computed as described in the previous section, then:

- F_A^2 and O_A^2 are obtained by aligning fingerprint F^2 and its local orientations O^2 according to (dx^*, dy^*, γ^*), respectively (Fig. 1).
- $\hat{F}^1$ and $\hat{F}^2$ are the intersection regions of F^1 and F_A^2, respectively (Fig. 1).
- $\hat{O}^1$ and $\hat{O}^2$ are the intersection regions of O^1 and O_A^2, respectively (Fig. 2).

The local ridge-line frequencies Υ^1 and Υ^2 of $\hat{F}^1$ and $\hat{F}^2$ are estimated as described in [5] (Fig. 3). Each frequency element is a value $v_{i,j} \in \mathbb{R}$, denoting the inverse of the average ridge-line period estimated in a neighborhood.

Minutiae templates T^1 and T^2 are extracted from $\hat{F}^1$ and $\hat{F}^2$, respectively, using the algorithm described in [6] (Fig. 4). Each minutia m is a quadruple $m = \{x_m, y_m, \theta_m, t_m\}$, where x_m and y_m are the minutia location, θ_m is the minutia direction and t_m is the minutia type (i.e., termination or bifurcation).

Let $\rho = (\rho_x, \rho_y)$ be the barycenter of the intersection region; the line l passing through p with angle β is defined as:

$$a_l \cdot x + b_l \cdot y + c_l = 0$$
$$a_l = \sin(\beta), b_l = \cos(\beta), c_l = -\rho_x \cdot \sin(\beta) - \rho_y \cdot \cos(\beta) \cdot \quad (5)$$

For each angle $\beta \in [0, \pi[$ (in steps of δ_β), the following score is computed:

$$S_c = \omega_o \cdot S_o + \omega_v \cdot S_v + \omega_m \cdot S_m, \quad (6)$$

where:

- S_o and S_v measure the similarity of the ridge orientations and frequencies, respectively, nearby the cutline l (with the aim of generating a pattern realistic to the human eye);
- S_m is a score derived from the two minutiae templates (described in the following paragraphs) with the aim of generating a fingerprint that matches with both fingers;
- $\omega_o, \omega_v, \omega_m \in [0,1], \omega_o + \omega_v + \omega_m = 1$ are three weighting factors.
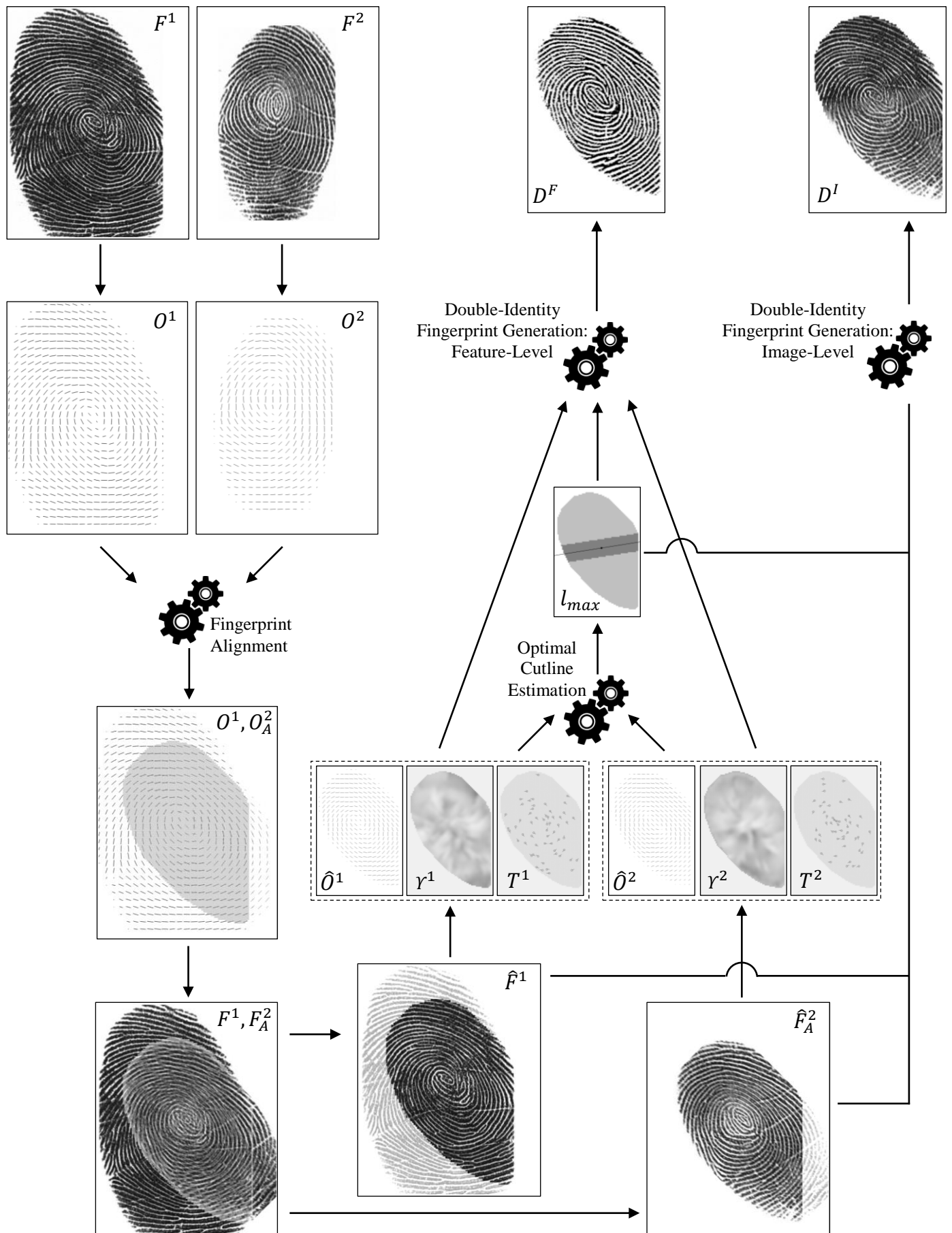
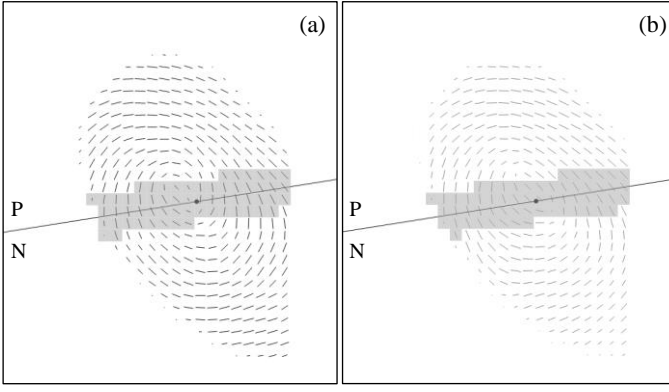Fig. 1 Functional schema of the double-identity fingerprint creation process.

Fig. 2 Detail of the intersection regions between the two aligned local orientations in Fig. 1. The orientation elements used to compute S_o are highlighted. P and N represent the positive and the negative side with respect to the cutline l_{max}.
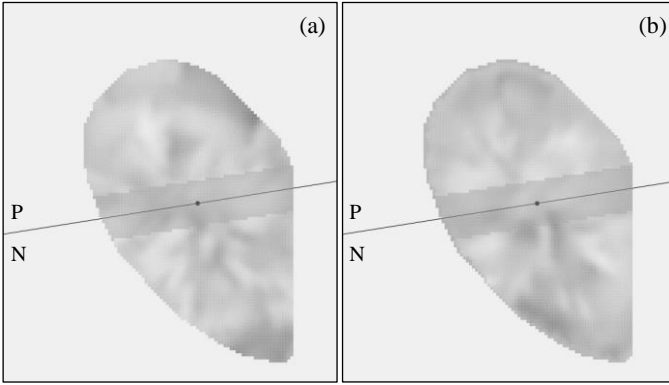

Fig. 3 Detail of the local ridge-line frequencies estimated from the intersection regions in Fig. 1. Light blocks denote higher frequencies. The elements used to compute S_v are highlighted. P and N represent the positive and the negative side with respect to the cutline l_{max}.
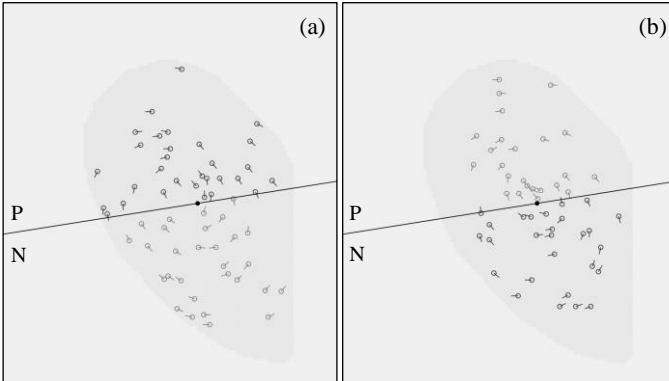

Fig. 4 Detail of the minutiae extracted from the intersection regions in Fig. 1. P and N represent the positive and the negative side with respect to the cutline l_{max}. The dark and gray minutiae are those used in Eq. (11) to compute $\zeta_m(T^1, T^2)$ and $\zeta_m(T^2, T^1)$, respectively.

$$S_o = \frac{\sum_{(i,j)\in C}\left(r_{i,j}^1 + r_{i,j}^2\right)\cdot\psi\left(\theta_{i,j}^1, \theta_{i,j}^2\right)}{\sum_{(i,j)\in C}\left(r_{i,j}^1 + r_{i,j}^2\right)}, \qquad (7)$$

$$S_v = \frac{\sum_{(i,j)\in C}\left(1 - \frac{|v_{i,j}^1 - v_{i,j}^2|}{(max_F - min_F)}\right)}{|C|}. \qquad (8)$$

C contains the element coordinates whose distance from l is less or equal to d_{max} and where both local orientation images

present non-null elements (see the highlighted regions in Fig. 2 and Fig. 3):

$$C = \left\{(i,j)|\ (i,j)\in\left(V_{\hat{O}^1}\cap V_{\hat{O}_A^2}\right)\wedge dist_l(i,j)\le d_{max}\right\}, \qquad (9)$$

$$dist_l(x,y) = \frac{|a_l\cdot x + b_l\cdot y + c_l|}{\sqrt{a_l^2 + b_l^2}}, \qquad (10)$$

$$S_m = \max\left(\zeta_m(T^1, T^2), \zeta_m(T^2, T^1)\right), \qquad (11)$$

$$\zeta_m(A,B) = \frac{Z\left(|A|_l^P, \mu_m, \tau_m\right) + Z\left(|B|_l^N, \mu_m, \tau_m\right)}{2}, \qquad (12)$$

where $|T|_l^P$ and $|T|_l^N$ denote the cardinalities of the minutiae in T that fall in the positive or negative side of line l, respectively (see Fig. 4):

$$|T|_l^P = \left|\{m\in T|\ \phi_l(m_x, m_y)\ge 0\}\right|, \qquad (13)$$

$$|T|_l^N = \left|\{m\in T|\ \phi_l(m_x, m_y) < 0\}\right|. \qquad (14)$$

Z is a sigmoid function, controlled by two parameters (μ_m and τ_m), that limits the contribution of the cardinality operator ($|\cdot|$), and ensures that the final value is in the range $[0,1]$. The sigmoid function is defined as:

$$Z(v,\mu,\tau) = \frac{1}{1+e^{-\tau(v-\mu)}}. \qquad (15)$$

Finally, the line l_{max} with the maximum score S_c is selected as the cutline.

C. Double-Identity Fingerprint Generation

Two different approaches for generating double-identity fingerprints are described. Starting from the information computed in Sections II.A and II.B, the former approach creates a new synthetic fingerprint starting from combined local orientations, frequencies and minutiae, while the latter produces a new fingerprint by directly blending the two original fingerprints.

1) Feature-level Approach

As described in [7] [8], a realistic fingerprint can be synthetically reconstructed starting from the information available in a standard minutiae template and attempting to estimate various aspects of the original unknown fingerprint (i.e., fingerprint area, local orientations and frequencies).

Given the cutline l_{max}, the fingerprint information used to reconstruct the positive (p) and the negative (n) portions of the new image is selected, on the basis of the resulting number of minutiae (see Eq. (12)), as follows:

$$(p,n) = \begin{cases}(1,2) & \text{if } \zeta_m(T^1, T^2)\ge\zeta_m(T^2, T^1) \\ (2,1) & \text{otherwise}\end{cases}. \qquad (16)$$

The double-identity local orientations $\tilde{O}$, frequencies $\tilde{Y}$ and minutiae template $\tilde{T}$ (see Fig. 5) are then computed by merging the corresponding positive and negative portions:

$$\tilde{O}(x,y) = w_{x,y}^{l_{max}} \cdot \hat{O}^p(x,y) + \left(1 - w_{x,y}^{l_{max}}\right) \cdot \hat{O}^n(x,y), \quad (17)$$

$$\tilde{Y}(x,y) = w_{x,y}^{l_{max}} \cdot Y^p(x,y) + \left(1 - w_{x,y}^{l_{max}}\right) \cdot Y^n(x,y), \quad (18)$$

$$\tilde{T} = \{m \in T^p, \phi_{l_{max}}(m_x, m_y) \geq 0\} \cup \{m \in T^n, \phi_{l_{max}}(m_x, m_y) < 0\}, \quad (19)$$

where $w_{x,y}^{l_{max}} \in [0,1]$ is a weighting factor to balance the blending nearby the cutline l_{max}:

$$w_{x,y}^{l_{max}} = \begin{cases} 1 - \max\left(0, \frac{d_{max} - dist_{l_{max}}(x,y)}{2 \cdot d_{max}}\right) & \text{if } a_{l_{max}} x + b_{l_{max}} y + c_{l_{max}} \geq 0 \\ \max\left(0, \frac{d_{max} - dist_{l_{max}}(x,y)}{2 \cdot d_{max}}\right) & \text{otherwise} \end{cases}. \quad (20)$$

Note that, to avoid angle circularity problems [9], the computation of angles $\tilde{O}$ (17) is actually performed as explained in [10] (i.e., by doubling the angles and summing x and y components separately).

Finally, the double-identity fingerprint D^F (see Fig. 5.d) is synthetically generated by the method proposed in [7], using $\tilde{O}$, $\tilde{Y}$ and $\tilde{T}$ as input.
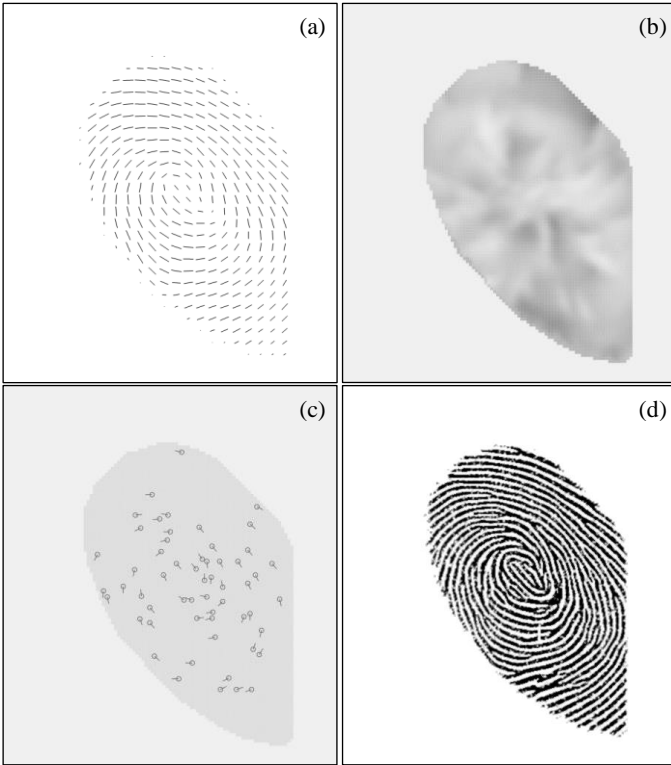

Fig. 5 Local orientations $\tilde{O}$ (a), frequencies $\tilde{Y}$ (b) and minutiae $\tilde{T}$ (c), derived from the fingerprints in Fig. 1 used to synthetically generate the double-identity fingerprint D^F (d).

2) Image-level Approach

The double-identity fingerprint is generated by fusing $\hat{F}^1$ and $\hat{F}^2$ according to the cutline l_{max}. Let $\hat{F}^p$ and $\hat{F}^n$ be the positive and the negative aligned original fingerprints (with respect to l_{max}), respectively, selected on the basis of the resulting number of minutiae (see Eq. (16)), the double-identity fingerprint D^I (see Fig. 6) is then generated as:

$$D^I(x,y) = w_{x,y}^{l_{max}} \cdot \hat{F}^p(x,y) + \left(1 - w_{x,y}^{l_{max}}\right) \cdot \hat{F}^n(x,y). \quad (21)$$

Fig. 6 Double-identity fingerprint D^I generated starting from the fingerprints in Fig. 1 using the image-level approach.

III. EXPERIMENTAL EVALUATION

This section describes the experiments carried out to evaluate the possibility of success of the proposed attack by estimating the behaviour of automatic fingerprint recognition in presence of double-identity fingerprints.

A. Database and Testing Protocol

The experiments have been carried out on the FVC2002 DB1 database [11], containing 800 fingerprints from 100 fingers (8 impressions per finger) captured at 500dpi using the optical scanner "TouchView II" by Identix. This dataset has been selected because of its clean background, that is typical of high quality scanners used for electronic document enrolment.

For each generation approach, 100 double-identity fingerprints (see examples reported in Fig. 7) have been produced as follows:

1. The first impression F_i of each finger i is aligned (see Section II.A) with the first impression of 10 other randomly chosen fingers and the optimal cutline is computed as described in Section II.B. The first impression F_j of finger j ($j \neq i$) presenting the maximum ridge pattern similarity score S_c with F_i (see Eq. (6)) is selected as the optimal companion for fusion. We limited to 10 the size of the search set to prove that finding a reasonably good companion fingerprint for creating an effective double-identity fingerprint is quite simple.

2. F_i and F_j are fused into a new fingerprint ($D_{i,j}^F$ or $D_{i,j}^I$) following the procedures described in Section II.C.
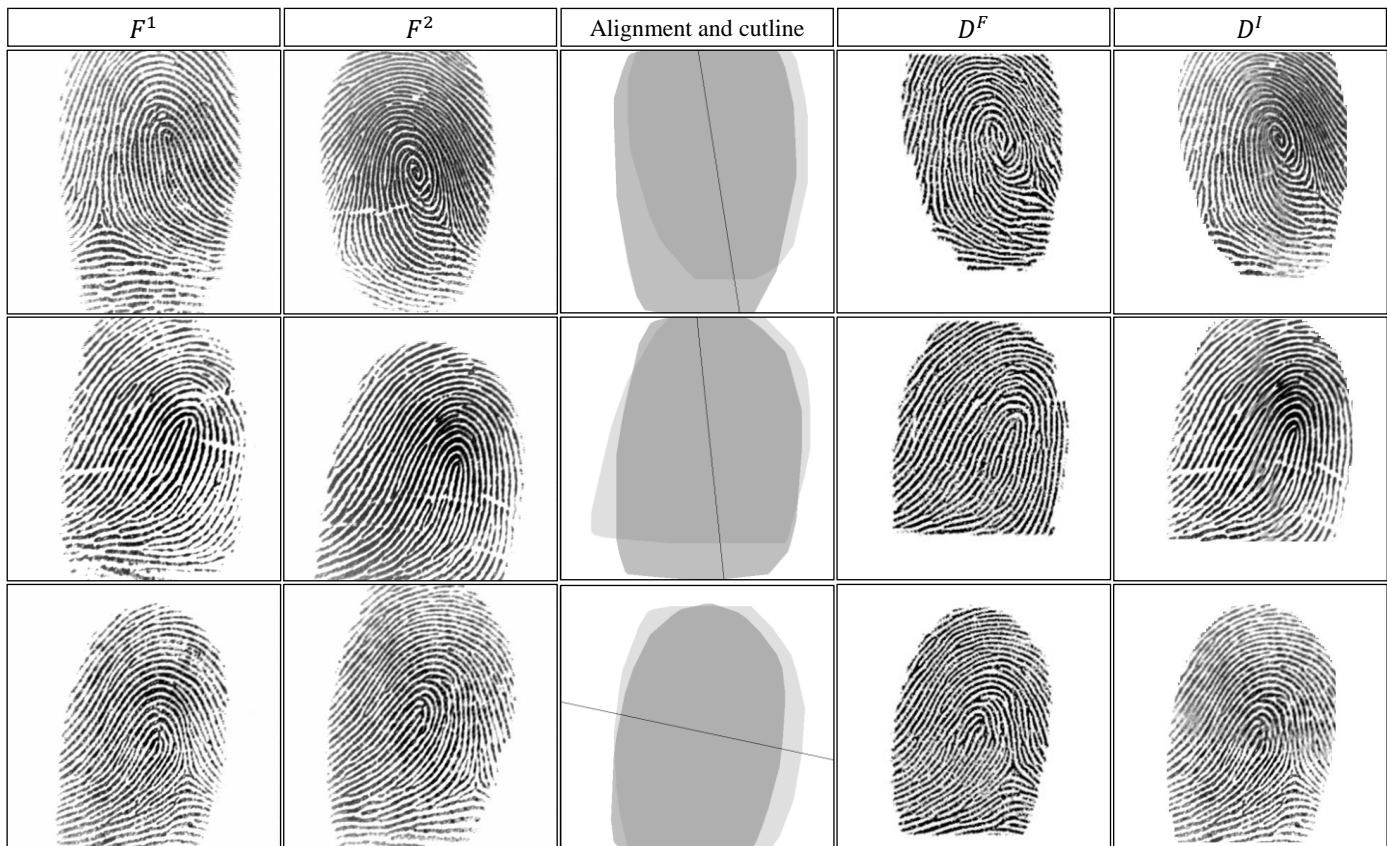
Fig. 7 Double-identity fingerprints: the results obtained with three fingerprint couples. Two input images (columns F^1 and F^2), the corresponding best alignment and the optimal cutline, and the resulting feature- and image-level double-identity fingerprints (columns D^F and D^I) are reported for each row.

Finally, the following comparisons are performed:

- *genuine* – 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 genuine comparisons is 2800.

- *impostor* – the first impression of each finger is compared against the first impression of the remaining fingers. 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 impostor comparisons is 4950.

- *double-identity* – each double-identity fingerprint ($D_{i,j}^F$ or $D_{i,j}^I$) is compared against all other seven impressions of fingers i and j. The total number of double-identity comparisons is 1400 for each generation approach.

Table I reports the parameter values used; all parameters have been calibrated on a separate data set containing 80 fingerprints from 10 fingers (8 impressions per finger). The calibration procedure consisted in an exhaustive search over a reasonable range of values.

B. Automatic Fingerprint Recognition SDKs Evaluated

The experiments have been conducted using two state-of-the-art fingerprint recognition SDKs: the Neurotechnology VeriFinger SDK v6.0 (VF) [12] and the Minutia Cylinder-Code SDK v2.0 (MCC) [13] [14]. Since the MCC SDK works directly with minutiae templates, the minutiae extraction algorithm described in [6] has been used to create minutiae templates.

TABLE I
PARAMETER VALUES USED IN THE EXPERIMENTATION

Parameter(s)	Description	Value
b_{size}, w_{size}	Block and window size used in local orientation and frequency estimation (in pixel)	4, 23
δ_γ	Rotation step used when searching for the best alignment	$\frac{\pi}{36}$
min_{VR}	Minimum overlapping between two local orientation images to be a candidate for a valid alignment	0.6
δ_β	Rotation step used during the optimal line estimation	$\frac{\pi}{60}$
$\omega_o, \omega_v, \omega_m$	Weight parameters in (6)	$\frac{1}{3}, \frac{1}{3}, \frac{1}{3}$
min_F, max_F	Minimum and maximum frequency in (8)	$\frac{1}{15}, \frac{1}{5}$
d_{max}	Maximum distance used to define the neighborhood of the cutline (in pixel)	30
μ_m, τ_m	Sigmoid parameters in (12)	$15, \frac{3}{10}$

In order to simulate a realistic attack to an ABC system, the operational thresholds of both fingerprint recognition software have been set according to the FRONTEX guidelines [15]

[16]. In particular, for ABC systems operating in verification mode, the fingerprint verification algorithm has to ensure a False Acceptance Rate (FAR) equal to 0.1% and a False Rejection Rate (FRR) lower than 3%. VF provides the corresponding score thresholds in its documentation, whereas for MCC, the score thresholds have been computed on the basis of about 110000 impostor comparisons performed on a disjoint database.

Table II reports score thresholds for both SDKs and different values of FAR.

TABLE II
THRESHOLDS TO ACHIEVE DIFFERENT VALUES OF FAR FOR BOTH SDKs

SDK	FAR (%)		
	1	0.1	0.01
VF	24	36	48
MCC	0.1083	0.1205	0.1329

C. Results

Fig. 8 and Fig. 9 show the score distribution graphs for VF and MCC, respectively. Fig. 10 and Fig. 11 report the values of Double-identity Acceptance Rate (DAR) and FRR at different values of FAR for VF and MCC SDKs, respectively. It is quite evident that for both the SDK the majority of attack scores are higher than the FRONTEX recommended thresholds corresponding to FAR = 0.1%.

While MCC seems to be slightly more robust than VF (compare DAR's in Fig. 10 and Fig. 11), both algorithms demonstrate high vulnerability to double-identity fingerprint attacks.
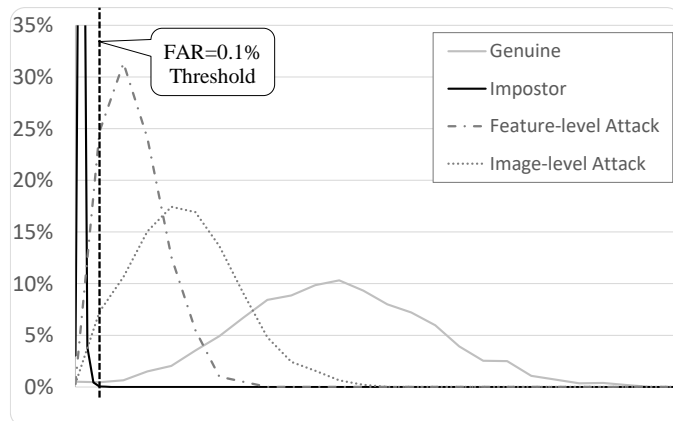

Fig. 8 The VF score distribution graph on the FVC2002 DB1 dataset.

The image-level approach proved to be more effective than feature-level approach in terms of percentage of successful attacks. This behavior is probably due to the particular nature of the synthetic generation technique used in the feature-level approach [7]. In fact, in order to generate a realistic pattern, it involves an iterative filtering procedure that may cause some original minutiae to be slightly shifted or completely removed, or false minutiae to be introduced. On the other hand, the image-level approach exactly preserves the positions of all the minutiae that are not close to the cutline, often resulting in a higher chance of successful attacks. Furthermore, the image-level approach allows to generate more realistic images

(compare the last two columns of Fig. 7), even if in a few cases $D_{i,j}^{I}$ presents more artifacts than $D_{i,j}^{F}$ (see Fig. 12).
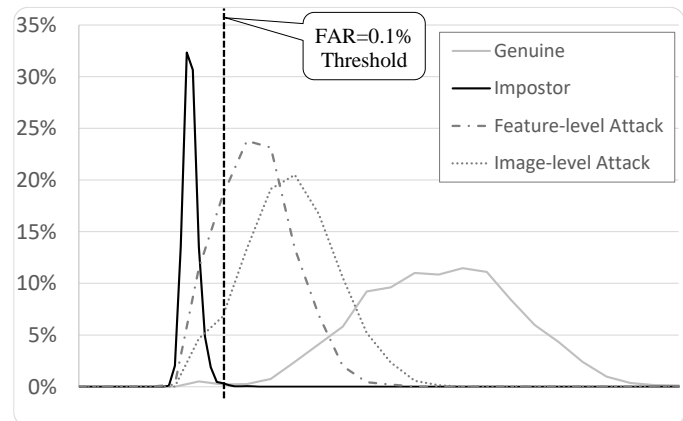

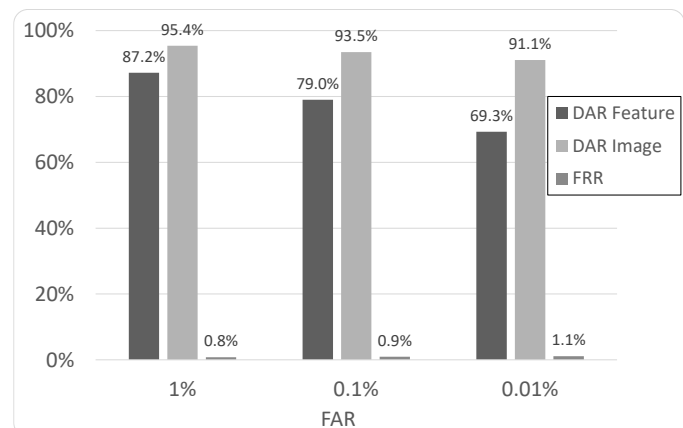Fig. 9 The MCC score distribution graph on the FVC2002 DB1 dataset.

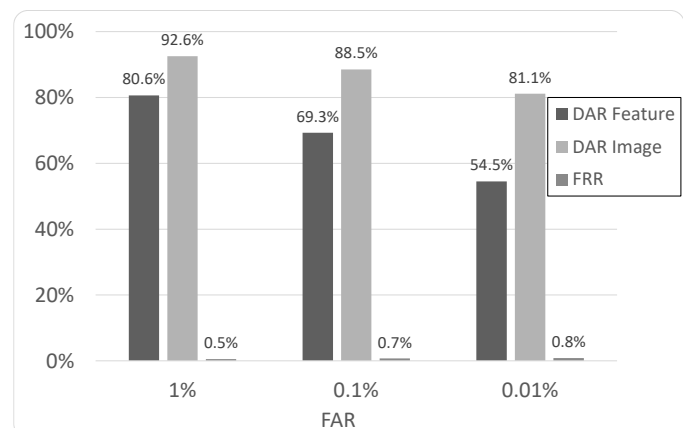Fig. 10 DAR and FRR values computed at different levels of FAR for VF SDK on the FVC2002 DB1 dataset.

Fig. 11 DAR and FRR values computed at different levels of FAR for MCC SDK on the FVC2002 DB1 dataset.
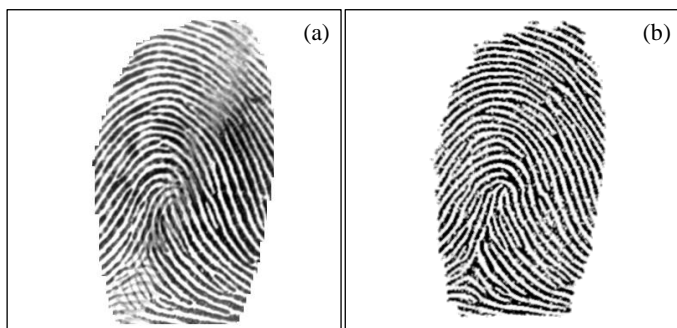
Fig. 12 Example of a double-identity fingerprint where the cutline and the blending region are more evident in the image-level result (a), than in the feature-level one (b). In particular, note the presence of orthogonal ridge lines in the bottom left corner of (a).

IV. CONCLUSION

In this paper we introduced two automated approaches to create double-identity fingerprints by combining two real ones. As discussed in [2] [3], two individuals, a criminal and an accomplice (with no criminal record) could combine their fingerprints and introduce the resulting double-identity fingerprint in an electronic document to be used (by both persons) to pass Automatic Border Control gates. We proved that two state-of-the-art fingerprint recognition algorithms are highly vulnerable to this specific attack (about 90% chance of success at FAR = 0.1%) and we guess that the majority of existing fingerprint recognition algorithms are vulnerable as well.

To mitigate the risk of this attack, particular care should be taken by officers in charge of the enrolment process to avoid the possibility that a citizen provides fake fingerprints. Presentation attack detection techniques (hardware/software) are being continuously improved but nowadays they are still far to be perfect [17] so visual inspection of the finger surface still remains the preferred option.

Developing software countermeasures, to detect if a given fingerprint is a double-identity fingerprint or not, seems feasible, and probably not too hard if the input were a digital image such as those printed in Fig. 7. However, we believe that the approach in reality is much more complex because the digital double-identity fingerprint is used only as starting point to fabricate a fake finger whose surface will be acquired by a live scanner, thus loosing much of the digital traces that could have been detected.

Finally, fingerprint recognition algorithms to be used in ABC could be extended/improved to detect "anomalies" (i.e., atypical partial matches) during unattended fingerprint recognition. We plan to dedicate some of our future research to investigate this option, to explore its efficacy and evaluate the risk of FRR increase. For instance, a feasible approach could be based on the analysis of minutiae correspondence groups, looking for suspicious partial matches with respect to the foreground intersection.

APPENDIX

TABLE III

DESCRIPTIONS OF SYMBOLS USED IN THIS PAPER

Symbol	Description	First introduced in Section
F^1, F^2	The two fingerprints (from two different fingers) to be mixed	II
O^1, O^2	Local orientation maps of F^1 and F^2	
b_{size}	Block size used in local orientation and frequency estimation	
w_{size}	Window size for local orientation and frequency estimation	
$o_{i,j} = (\theta_{i,j}, r_{i,j})$	An orientation element $[i,j]$ with ridge orientation $\theta_{i,j}$ and reliability $r_{i,j}$	
$S(O^1, O^2)$	Similarity between two local orientation images	II.A
$\psi(\theta_1, \theta_2)$	Similarity between two orientation angles θ_1, θ_2	
V_O	Coordinates of foreground orientation elements of O	
δ_γ	Rotation step used when searching for the best alignment	
min_{VR}	Minimum allowed overlapping between two orientation images	
(dx^*, dy^*, γ^*)	Best translation and rotation parameters	
F_A^2	Result of aligning F^2 according to (dx^*, dy^*, γ^*) parameters	
O_A^2	Result of aligning O^2 according to (dx^*, dy^*, γ^*) parameters	
$\hat{F}^1$	Portion of F^1 that lies in the intersection with F_A^2	
$\hat{O}^1, \Upsilon^1$	Orientations and frequencies of $\hat{F}^1$, respectively	
$\hat{F}^2$	Portion of F_A^2 that lies in the intersection with F^1	
$\hat{O}^2, \Upsilon^2$	Orientations and frequencies of $\hat{F}^2$, respectively	
$\nu_{i,j}$	Average ridge-line frequency estimated in $[i,j]$	
T^1, T^2	Minutiae templates extracted from $\hat{F}^1$ and $\hat{F}^2$	
$m = \{x_m, y_m, \theta_m, t_m\}$	A minutia with location (x_m, y_m), direction θ_m, and type t_m	
$\rho = (\rho_x, \rho_y)$	Barycenter of the intersection region	
β	Angle that line l forms with the horizontal axis	
l	Line passing through ρ with angle β, as in Eq. (5)	
δ_β	Rotation step used during the optimal line estimation	II.B
S_o	Similarity of the ridge orientations nearby line l as in Eq. (7)	
S_ν	Similarity of the ridge frequencies nearby line l as in Eq. (8)	
min_F, max_F	Minimum and maximum ridge frequency	
S_m	Score derived from the number of minutiae in T^1 and T^2 as in Eq. (11)	
$\omega_o, \omega_\nu, \omega_m$	Three weighting factors in Eq. (6)	
S_c	Score maximized to select the optimal cutline	
C	Coordinates of foreground neighborhood elements of line l	
d_{max}	Parameter controlling neighborhood size of line l	
$dist_l(x, y)$	Euclidean distance of point (x, y) from line l	
$|T|_l^P, |T|_l^N$	Number of minutiae in T that fall in the positive (P) or negative (N) side of line l	
$Z(v, \mu, \tau)$	Sigmoid function, see Eq. (15)	
μ_m, τ_m	Sigmoid parameters in Eq. (12)	
l_{max}	Cutline selected by maximizing S_c	
$\tilde{O}, \tilde{\Upsilon}, \tilde{T}$	Double-identity orientations, frequencies, and minutiae	
$w_{x,y}^{l_{max}}$	Blend weighting factor in Eq. (20)	II.C.1
D^F	The double-identity fingerprint generated using the feature-level approach	
D^I	The double-identity fingerprint generated using the image-level approach	II.C.2

REFERENCES

[1] ICAO, "Biometric Deployment of Machine Readable Travel Documents," TAG MRTD/NTWG, May 2004.

[2] 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.

[3] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of

Image Alterations on Face Recognition Accuracy," in *Face Recognition Across the Electromagnetic Spectrum*.: Springer, 2016, pp. 195-222.

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

[5] R. Cappelli, M. Ferrara, and D. Maio, "A Fast and Accurate Palmprint Recognition System based on Minutiae," *IEEE Transactions on Systems, Man and Cybernetics - Part B*, vol. 42, no. 3, pp. 956-962, June 2012.

[6] R. Cappelli and M. Ferrara, "A fingerprint retrieval system based on level-1 and level-2 features," *Expert Systems with Applications*, vol. 39, no. 12, pp. 10465–10478, September 2012.

[7] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," *IEEE Transactions on Pattern Analysis Machine Intelligence*, vol. 29, no. 9, pp. 1489-1503, September 2007.

[8] J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez, "Fake fingertip generation from a minutiae template," in *International Conference on Pattern Recognition*, Tampa, FL, 2008, pp. 1-4.

[9] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. New York, NJ, USA: Springer-Verlag, 2009.

[10] M. Kass and A. Witkin, "Analyzing oriented patterns," *Computer Vision, Graphics, and Image Processing*, vol. 37, no. 3, pp. 362-385, March 1987.

[11] 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.

[12] Neurotechnology Inc. (2016, October) Neurotechnology Web Site. [Online]. http://www.neurotechnology.com/

[13] BioLab. (2016, October) MCC SDK Web Site. [Online]. http://biolab.csr.unibo.it/mccsdk.html

[14] 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.

[15] FRONTEX - Research and Development Unit, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems - v2.0," FRONTEX, ISBN: 978-92-95033-58-0, DOI: 10.2819/26969, August 2012.

[16] FRONTEX. (2016, October) FRONTEX Web Site. [Online]. http://frontex.europa.eu/

[17] (2016, October) LivDet - Liveness Detection Competition Series Web Site. [Online]. http://livdet.org/

Matteo Ferrara is an assistant professor at the Department of Computer Science and Engineering of the University of Bologna, Italy. He received the Bachelor degree cum laude in Computer Science from the University of Bologna in 2004, the Master degree cum laude in 2005 and the PhD degree in 2009. He is member of the Biometric System Laboratory and he is one of the organizers of the international performance evaluation initiative named "FVC-onGoing". Moreover, he is one of the authors of the well-known fingerprint recognition algorithm named "Minutia Cylinder-Code" (MCC). His research interests are in the areas of pattern recognition, computer vision and biometric systems. He is author of several scientific papers and book chapters, and holds a patent in fingerprint recognition. He took part to national and European research projects and to consultancy projects between the University of Bologna and foreign universities and companies.

Raffaele Cappelli (M'09) is an associate professor at the Department of Computer Science and member of the Biometric System Laboratory of the University of Bologna. He is in charge of the "Image processing" course at the Laurea degree in Computer Science, University of Bologna, Cesena. His research activity focuses on biometric systems and he mainly works on fingerprint recognition. He is author of various scientific papers and book chapters, and holds two patents in fingerprint recognition. He is one of the organizers of the international fingerprint verification competitions (FVC200-FVC2006, FVC-onGoing) and one of the authors of the synthetic fingerprint generation method named "SFinGe". He took part to several national and European research projects and to various consultancy projects between the University of Bologna and foreign universities and companies. Raffaele Cappelli received the Laurea degree cum laude in Computer Science in 1998, and his PhD in 2002.

Davide Maltoni (M'05) is a Full Professor with the Department of Computer Science and Engineering (DISI), University of Bologna, Italy, and Chair of DISI Unit in Cesena. His research interests are in the areas of pattern recognition, computer vision, and computational neuroscience. He is the Codirector of the Biometric Systems Laboratory (BioLab) at the University of Bologna, which is internationally known for its research and publications in the field. Several original techniques have been proposed by BioLab team for fingerprint feature extraction, matching, and classification, hand shape verification, face location, and performance evaluation of biometric systems. He coauthored the book entitled Handbook of Fingerprint Recognition (Springer, 2009), and holds three patents on fingerprint recognition. He was elected as a fellow of the International Association for Pattern Recognition in 2010.