Face Demorphing

Matteo Ferrara, Annalisa Franco, and Davide Maltoni, *Member, IEEE*

***Abstract*— The morphing attack proved to be a serious threat for modern automated border control systems where face recognition is used to link the identity of a passenger to his/her e-document. In this paper, we show that by exploiting the live face image acquired at the gate, the morphed face image stored in the document can be reverted (or demorphed) enough to reveal the identity of the legitimate document owner, thus allowing the system to issue a warning. A number of practical experiments on two data sets proves the efficacy of our approach.**

***Index Terms*— Automated border control, eMRTD, face demorphing, face morphing attack, face recognition.**

I. Introduction

We RECENTLY proved [1], [2] that face morphing can be exploited by a criminal to fool an Automated Border Control (ABC) system [3]. ABCs are nowadays installed in more than 180 airports across the globe [4], [5] and in the coming years most of the passenger controls will be delegated to them. Identity verification at an ABC relies on the comparison of a live face image with a digital face image stored in an electronic Machine Readable Travel Document (eMRTD) such as an e-passport. If a morphed image, which is similar enough to the face of two subjects, can be included in an eMRTD, then two persons can share the document. In this scenario a criminal could exploit the passport of an accomplice with no criminal records to overcome the security controls. In more details, the subject with no criminal records (i.e., the accomplice) could apply for an eMRTD by presenting the morphed face photo; if the image is not noticeably different from his/her face, the police officer accepts the photo and releases the document. It is worth noting that in this case the document is perfectly regular: in fact, the attack does not consist of altering the document content but in deceiving the officer at the stage of document issuing. The document released will thus pass all the integrity checks (optical and electronic) performed at the gates.

In [2] we demonstrated that two commercial face recognition systems can be deceived by morphed images with high chance (Morph Acceptance Rate $\geq$ 95% at FAR = 0.1%). Some further practical experimentations have been performed in the context of the Fidelity EU project [6] involving border guards and operational ABC at airports: the outcomes confirm the actuality of this threat and the need for countermeasures.

There are basically two families of approaches to deal with the morphing attack:

1) *Single-image*: detecting the presence of morphing alterations on i) the face image presented to officer at enrolment time or ii) on the face image read from an eMRTD during verification at an ABC.
2) *Two-images*: detecting an anomaly at an ABC when the live image of the passenger is compared with the morphed image stored in the eMRTD.

Interesting approaches belonging to the first family have been proposed in [7] and [8]. In our experience digital alterations (such as morphing) can be detected on digital images but they usually vanish during the printing/scanning process typical of passport issuance procedure, as confirmed in [8]; in fact, in many countries the photo ID provided by the citizen is printed on photographic paper and scanned by a police officer (see Section V). In this paper we focus on the second family of approaches: our aim is to design a technique able to raise a morphing warning in case a criminal tries to access an e-gate. We found out that a demorphing process can be put in practice to highly reduce the risk of this attack.

The basic idea of demorphing is trying to invert the morphing process. Here we provide a simple intuitive explanation; formal treatment is introduced in Sections III and IV. In case of morphing attack, image M stored in the document can be though as a linear combination $M = A + C$, where A and C are the accomplice and criminal face images respectively. On the other hand, in a genuine passport (with no morphing attack) we can think of M as the combination of two identical images ($M = C + C$), where C is here the legitimate user. At verification time we know M (stored in the document) and $\tilde{C}$ (a variant of C captured live), and we compute the demorphed image D by removing $\tilde{C}$ from M ($D = M - \tilde{C}$).

Then, comparing D against $\tilde{C}$ leads to:

- a low matching score if M is a morphed image; in fact, removing from M the presence of the criminal ($D = M - \tilde{C} = A + C - \tilde{C} \approx A$) makes the resulting image much more similar to the accomplice;
- a high matching score if M is not morphed; in this case removing from M the presence of legitimate user ($D = M - \tilde{C} = C + C - \tilde{C} \approx C$) leaves the underlying identity unaltered.

Actually, everything is much more complex in the reality: morphing is not a simple linear combination of image intensities and its reversibility with surrogate data ($\tilde{C}$ instead of C) needs to be proved, even if in the scenario of identity

Manuscript received September 26, 2017; accepted November 14, 2017. Date of publication November 23, 2017; date of current version January 3, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yunhong Wang. *(Corresponding author: Matteo Ferrara.)*

The authors are with the Department of Computer Science and Engineering, University of Bologna, 47521 Cesena, Italy (e-mail: matteo.ferrara@unibo.it; annalisa.franco@unibo.it; davide.maltoni@unibo.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2017.2777340

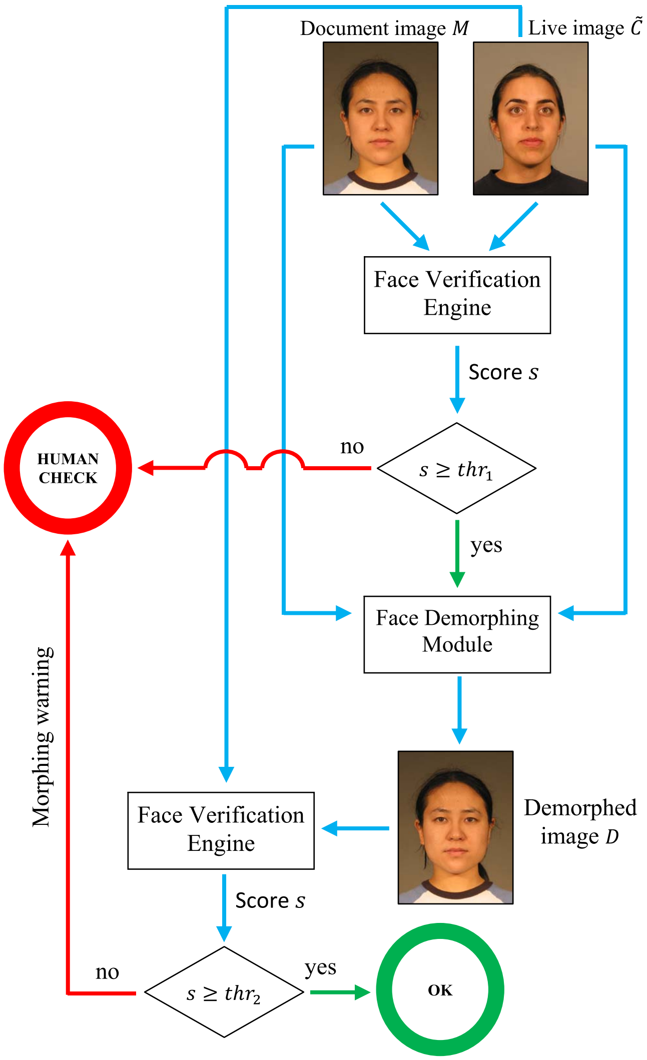


Fig. 1. Functional schema of the proposed face verification procedure (including the demorphing module) performed at ABC gates.

documents the image acquisition process is quite controlled and the pose/illumination variations are limited. Our experimental findings support the practical applicability of this idea.

Fig. 1 shows the overall workflow of the proposed approach. If the passenger passes the standard face verification stage, the demorphing step takes place: the document face image is demorphed and compared to the live image; in case of a negative match a "morphing" warning is issued to a second line officer. Of course, to be useful in practice, both the morphing acceptance rate and the amount of false morphing warnings must be sufficiently small.

The rest of this paper is organized as follows: Section II summarizes the state-of-the-art on face morphing detection. Section III defines the face morphing procedure and Section IV describes the novel demorphing process. In Section V, two new databases specifically created to evaluate morphing detection techniques are introduced. In Section VI, the efficacy of the proposed approach has been evaluated on the new two databases. Finally, Section VII draws some concluding remarks.

II. Related Works

Digital image tampering is an important topic in digitals forensics and several approaches have been proposed in the literature to detect different kinds of forgery: see [9] for a recent survey. On the other hand, very few recent works specifically address the problem of face morphing detection in the context of identity documents: all published approaches belong to the "single-image" category. Raghavendra *et al.* [7] perform morphing detection based on facial micro-textures extracted using ad hoc filters. A progressive image degradation, obtained by JPG compression, is used in [10]: the basic idea is that genuine images are strongly affected by image degradation, while the impact on the morphed ones is lower, due to the blending operations used for morphing. The practical usability of deep networks for face morphing detection is analyzed in [11] where different architectures are compared. The previously mentioned algorithms work in the digital domain; unfortunately the printing/scanning process adopted in many cases during the document issuing procedure, determines a loss of the low-level details in the digital signal thus reducing the effectiveness of such techniques, as confirmed by [8]. To the best of our knowledge, the only approach dealing with printing/scanning issue is [12] where a transfer learning approach is adopted to detect morphed images based on a pre-trained D-CNN. Nevertheless, also in this case the printing/scanning process determines a significant performance degradation, thus confirming that morphing detection is still an open issue.

III. Face Morphing Process

In computer graphics and animations, morphing is a special effect that transforms an image into another through a seamless transition [13]; face morphing is a very common application of such technique. In this section, we describe a fully automated process to create a realistic morphed face, including the final retouching (a step that is often manually performed).

A. Morphing

Image morphing is a technique used to synthesize a fluid transformation from one image to another. It uses correspondence points between the images and distorts one image into the other as they crossfade. Given two images I_0 and I_1 (see Fig. 2.a and Fig. 2.f, respectively), the process generates a set of intermediate frames $\mathbb{M} = \{I_\alpha, \alpha \in \mathbb{R}, 0 < \alpha < 1\}$ (see Fig. 2.b to Fig. 2.e) representing the transformation of the first image (I_0) into the second one (I_1). Note that, to obtain realistic results, the two images need to be aligned in advance (e.g., by overlaying the eye centers). In general, each frame is a weighted linear combination of I_0 and I_1, obtained by: i) geometric warping [14] of the two images based on correspondence points and ii) pixel-by-pixel cross-dissolving (or blending). Formally:

$$I_\alpha(\mathbf{p}) = (1-\alpha)\cdot I_0\left(w_{P_\alpha \to P_0}(\mathbf{p})\right) + \alpha \cdot I_1\left(w_{P_\alpha \to P_1}(\mathbf{p})\right) \tag{1}$$

where:

- $\mathbf{p}$ is a generic pixel position;
- α is the frame weight factor;

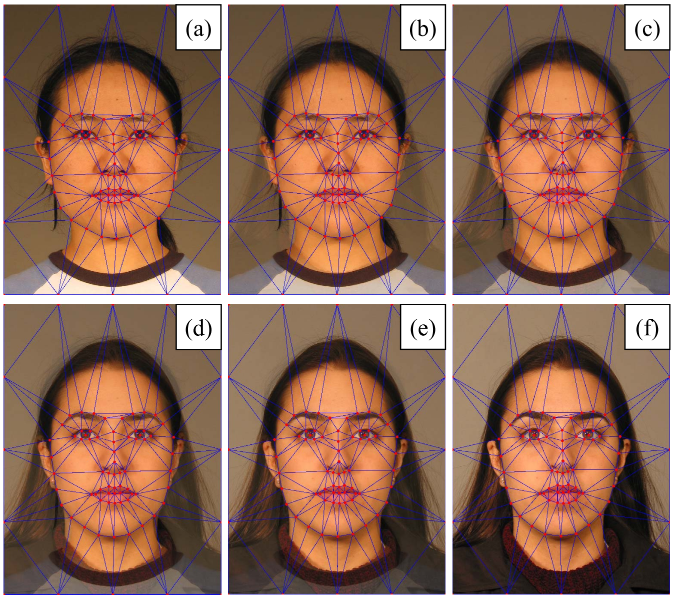


Fig. 2. Morphing of image I_0 (a) to I_1 (f). (b-e) are intermediate frames, obtained by the morphing procedure, gradually shading from I_0 to I_1. The correspondence points and the triangular meshes are highlighted in red and blue, respectively.

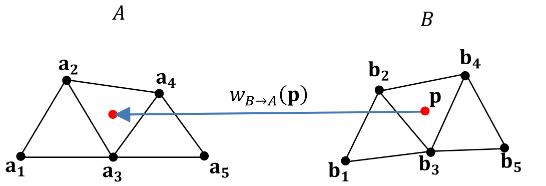


Fig. 3. Example of image warping using triangular meshes. The point $\mathbf{p}$ in the warped image is mapped into the original image using the inverse mapping of triangle $\Delta\mathbf{b_2b_3b_4}$ into $\Delta\mathbf{a_2a_3a_4}$.

- P_0 and P_1 are the two sets of correspondence points in I_0 and I_1, respectively (see Fig. 2.a and Fig. 2.f);
- P_α is the set of correspondence points aligned according to the frame weight factor α (see Fig. 2.b to Fig. 2.e);
- $w_{B\rightarrow A}(\mathbf{p})$ is a warping function.

Several warping techniques have been proposed in the literature [15]. A common approach consists in representing the two sets of points (A and B) by means of topologically equivalent (i.e., no folding or discontinuities are permitted) triangular meshes (see Fig. 2) and computing local spatial transformations that map each warped triangle to the corresponding original one [16]. Note that the meshes are constrained to cover the whole images and not to cause self-intersection (i.e., each pixel position is contained in exactly one mesh). A triangular mesh can be derived from a set of points via Delaunay triangulation [17]. Given a generic pixel position $\mathbf{p}$ in the warped image, the transformation used to map $\mathbf{p}$ onto the original image I is the local transformation corresponding to the warped triangle that contains $\mathbf{p}$ (see Fig. 3).

The set of aligned correspondence points P_α in Eq. (1) is computed as follows (see Fig. 4):

$$P_\alpha = \{\mathbf{r}_i | \mathbf{r}_i = (1-\alpha)\cdot\mathbf{u}_i + \alpha\cdot\mathbf{v}_i, \mathbf{u}_i \in P_0, \mathbf{v}_i \in P_1\} \quad (2)$$

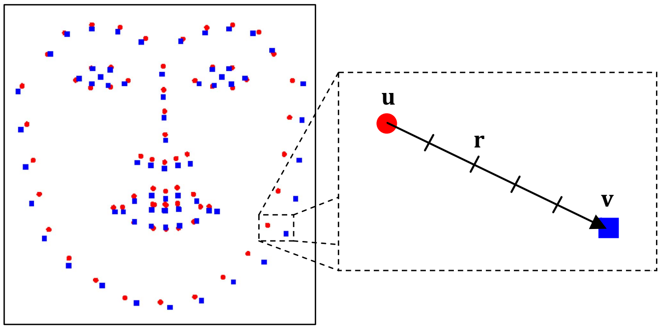


Fig. 4. Onthe left, P_0 (red circles) and P_1 (blue squares) are the corresponding points of images in Fig. 2.a and Fig. 2.f, respectively. On the right, the region containing points $\mathbf{u}$ and $\mathbf{v}$ is zoomed to show point $\mathbf{r}$ corresponding to morphed frame $I_{0.4}$ (see Fig. 2.c).

B. Automatic Retouching

As shown in Fig. 2, the intermediate morphed frames could present double exposure effects outside the facial region (e.g., background, hair, shoulders, body). This is due to different factors:

1) usually the correspondence points are chosen only inside the facial region (e.g., eye center and corners, eyebrows, nose tip, mouth corners, chin, etc.) and this may cause a misalignment outside the facial region;
2) the differences outside the facial region are much more evident (e.g., hairstyle, dresses) than inside.

To make morphed frames more realistic and compliant with ICAO specifications [18], and therefore more difficult to be detected by human officers during the issuing of the document, a manual retouching could be applied (see [1]).

Here we propose an automatic retouching procedure. The aim is not to make things simpler for perpetrators, but to enable automatic generation of large datasets of morphed images for evaluation purposes (see Section V).

In our procedure each frame is automatically corrected as follows:

$$\hat{I}_\alpha(\mathbf{p}) = \begin{cases} I_\alpha(\mathbf{p}) & \text{if } \mathbf{p} \in H_\alpha \\ I_0\left(w_{P_\alpha\rightarrow P_0}(\mathbf{p})\right) & \text{if } \mathbf{p} \notin H_\alpha \wedge \alpha \le 0.5 \\ I_1\left(w_{P_\alpha\rightarrow P_1}(\mathbf{p})\right) & \text{if } \mathbf{p} \notin H_\alpha \wedge \alpha > 0.5 \end{cases} \quad (3)$$

where H_α is the convex hull of the correspondence points in P_α.

The retouched morphed frame $\hat{I}_\alpha$ is obtained from I_α, by replacing the pixels outside the face region with those of the closest image (between I_0 and I_1). Of course replaced pixel need to be warped to preserve geometry (see Eq. (3)). Finally, to avoid visible edges in the boundary region, a weighted blending is applied near the facial region borders (not included for simplicity in Eq. (3)). The result of the automatic retouching is reported in Fig. 5.f.

IV. Demorphing Process

Given a morphed frame I_α, the original image I_1 and the correspondence points P_α and P_1, the morphing process can be fully reverted to obtain the original image I_0. This can be

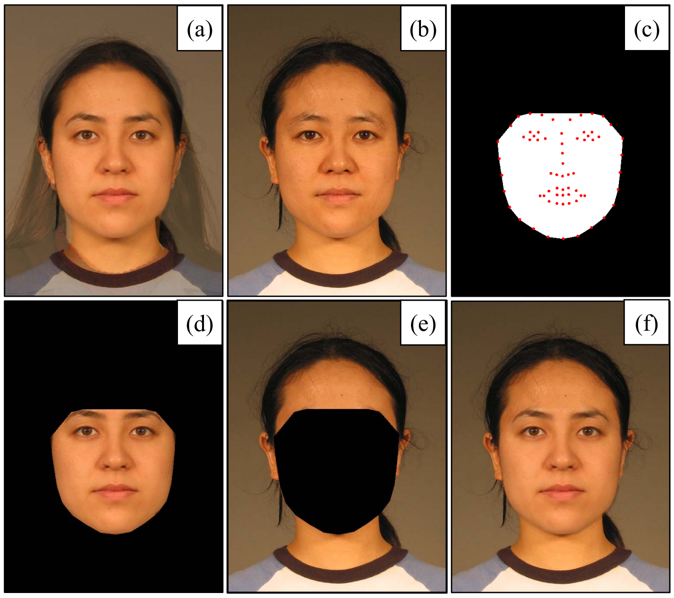


Fig. 5. Example of the automatic retouching process. The morphed frame $I_{0.4}$ (a) corresponding to Fig. 2.c; (b) the warped image obtained by warping I_1 to align P_1 to $P_{0.4}$; (c) the convex hull containing $P_{0.4}$; (d) the facial region of (a); (e) the background region of (b); (f) the retouched frame $\hat{I}_\alpha$ obtained by combining (d) and (e) and applying local blending near the borders.

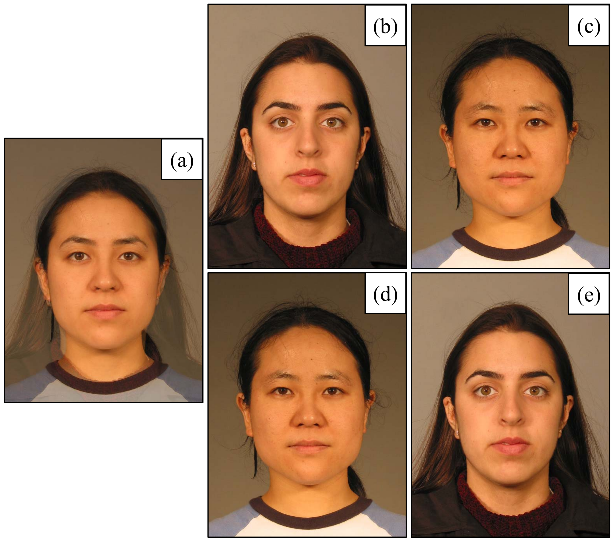


Fig. 6. Example of "exact" demorphing process. (a) the morphed frame $I_{0.4}$ corresponding to Fig. 2.c, (b) (c) the original images I_1 and I_0 (see Fig. 2.f and Fig. 2.a, respectively), and (d) (e) the recovered images: (d) obtained from (a) (b) and (e) obtained from (a) (c).

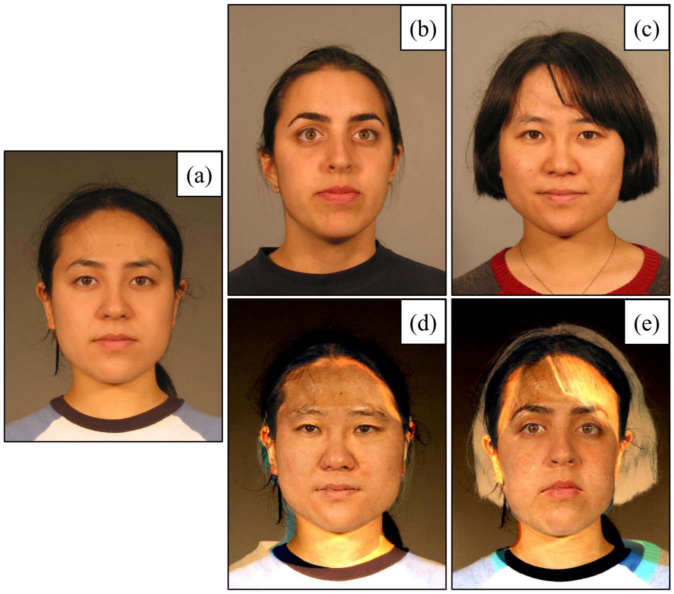


Fig. 7. Example of demorphing process in a real scenario. (a) the morphed photo stored in the travel document, (b) (c) images of the two subjects involved in the morphing process and, (d) (e) the corresponding demorphed images. The value of $\tilde{\alpha}$ to obtain (d) and (e) is here 0.5.

achieved by inverting Eq. (1) and (2) as follows:

$$I_0\left(w_{P_\alpha \to P_0}(\mathbf{p})\right) = \frac{I_\alpha(\mathbf{p}) - \alpha \cdot I_1(w_{P_\alpha \to P_1}(\mathbf{p}))}{(1-\alpha)} \quad (4)$$

By assuming $\mathbf{p} = w_{P_0 \to P_\alpha}(\mathbf{q})$ and replacing it in the above equation we obtain:

$$I_0\left(w_{P_\alpha \to P_0}\left(w_{P_0 \to P_\alpha}(\mathbf{q})\right)\right) = \frac{I_\alpha\left(w_{P_0 \to P_\alpha}(\mathbf{q})\right) - \alpha \cdot I_1\left(w_{P_\alpha \to P_1}\left(w_{P_0 \to P_\alpha}(\mathbf{q})\right)\right)}{(1-\alpha)} \quad (5)$$

that can be simplified by combining subsequent transformations:

$$I_0(\mathbf{q}) = \frac{I_\alpha\left(w_{P_0 \to P_\alpha}(\mathbf{q})\right) - \alpha \cdot I_1\left(w_{P_0 \to P_1}(\mathbf{q})\right)}{(1-\alpha)} \quad (6)$$

where:

$$P_0 = \left\{ \mathbf{u}_i | \mathbf{u}_i = \frac{\mathbf{r}_i - \alpha \cdot \mathbf{v}_i}{1-\alpha}, \mathbf{r}_i \in P_\alpha, \mathbf{v}_i \in P_1 \right\} \quad (7)$$

Similarly, I_1 can be obtained from I_α, I_0 and their correspondence points P_α and P_0.

Fig. 6 shows an example of the demorphing process on the morphed frame reported in Fig. 2.c. It is worth noting that the recovered images (see Fig. 6.d and Fig. 6.e) are identical to the original ones, except for minor numerical approximation.

Assuming that I_1 coincides with the original criminal face image C and I_0 with the original accomplice face image A. Then I_α is the intermediate frame obtained by the morphing I_0 and I_1 with morphing factor α (Eq. (1)). Unfortunately, in a real identity verification scenario at an ABC, the information needed to perform an "exact" demorphing (i.e., I_α, P_α, I_1, P_1 and α) is not available. In fact:

- image M stored in the document can be slightly different from I_α because of the final retouching (compare Fig. 7.a with Fig. 6.a);
- live face image I_1 ($\tilde{C}$ in the introduction) can be quite different from C because of variation in pose, lighting, expression, make-up, aging, etc. (compare Fig. 7.b with Fig. 6.b). While ICAO specifications on face enrolment [18] and Frontex guidelines for ABC deployment [19] should reduce the impact of pose, lighting and expression variation, make-up changes and aging are still possible and much more difficult to address;
- the morphing factor α initially used to produce I_α (and M) is unknown; however, a related demorphing factor $\tilde{\alpha}$ could be estimated based on some practical assumptions. A detailed discussion about the demorphing factor $\tilde{\alpha}$ is given in Section VI;

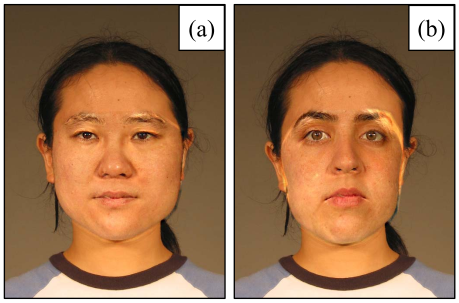


Fig. 8. Retouching applied to demorphed images shown in Fig. 7.d and Fig. 7.e, respectively.

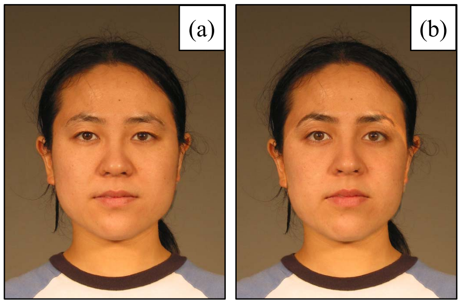


Fig. 9. (a) (b) demorphing applied to the morphed image in Fig. 7.a using Fig. 7.b and Fig. 7.c as live image, respectively. Proper selection of demorphing factor (here $\tilde{\alpha} = 0.25$) and final retouching lead to much better results (compare with Fig. 7.d, Fig. 7.e, Fig. 8.a and Fig. 8.b).

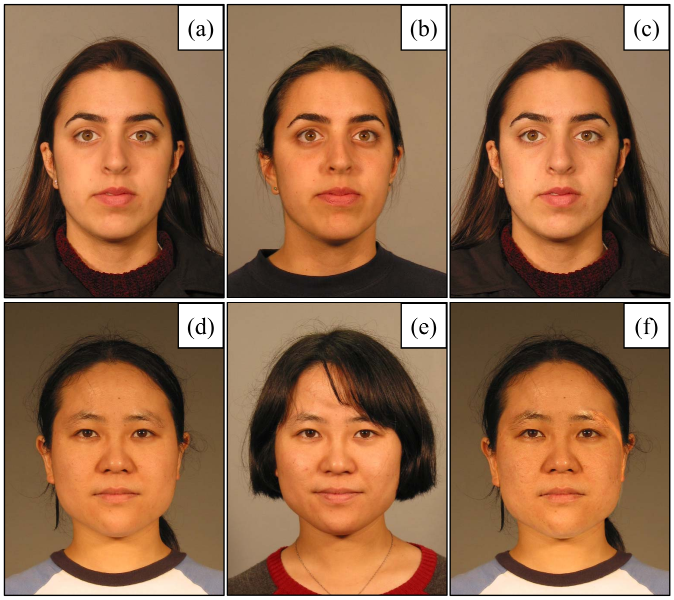


Fig. 10. Two examples (one per row) of the demorphing process applied to genuine (not morphed) images. (a) (d) are the images M stored in the document, (b) (e) the images $\tilde{C}$ acquired live at the ABC gate, and (c) (f) the demorphed images obtained with demorphing factor $\tilde{\alpha} = 0.25$.

- finally, the set of correspondence points P_α and P_1 can be estimated by extracting facial landmarks from M and $\tilde{C}$ respectively.

Fig. 7 shows an example of demorphing in a real scenario. It is evident that, when the original information is missing, the obtained result is not satisfactory (see Fig. 7.d and Fig. 7.e), mainly due to evident artefacts introduced outside the face region. To mitigate this effect and reduce the chance of false morphing warnings in case of genuine images, the demorphed image can be retouched by applying the process described in Section III-B (see Eq. (3)). The result of retouching applied to Fig. 7.d and Fig. 7.e is reported in Fig. 8.

The obtained images are visually better but still affected by anomalies because of the choice of a non-optimal demorphing factor $\tilde{\alpha}$. Fig. 9 shows the result of demorphing with a more appropriate value of $\tilde{\alpha}$ with respect to that used in Fig. 8. A specific discussion on the selection of $\tilde{\alpha}$ is reported in Section VI.

Finally in Fig. 10 we show that the demorphing process applied to genuine (not morphed) images does not alter them (and the underlying identity) significantly as hypothesized in the introduction.

V. Databases

Face morphing emerged only recently as a serious security threat and for this reason the research community lacks of public benchmarks for morphing detection. Databases collected by researchers working on this problem are still not available for performance comparison. In our previous works [1], [2] we introduced a preliminary benchmark (named FMC-1.0). In FMC-1.0 the morphed images were generated using the GIMP software [20], [21] after a manual labeling of the correspondence points and a first manual alignment based on eyes superimposition; a final manual retouch was carried out to remove visible artifacts. Since the aim of that preliminary study was to demonstrate the feasibility of the morphing attack, the morphed images were created to maximize the probability of success for both subjects (i.e., accomplice and criminal) as follows:

- only pairs of very similar subjects were manually selected for morphing;
- the final retouch (manual) was often aimed at increasing the similarity of the morphed image with the criminal subject;
- in several cases the selected morphed frame was halfway between the accomplice and the criminal (i.e., a morphing factor $\alpha \approx 0.45$). Operating with such an α maximizes the probability of fooling the automatic recognition system (at the gate), but reduces the possibility of fooling the officer during enrollment (see Fig. 11 and Fig. 12 with α close to 0.45). Based on our experience and on the results obtained with human experts and algorithms, we believe that a good tradeoff to fool both an officer and the ABC is working with a value of α in the range $[0.20; 0.30]$. Such claim is also supported by the study in [22] where extensive tests with humans lead to the same conclusion.

In order to design a more appropriate benchmark to study morphing attacks to ABCs, we introduce here two new databases: PMDB and MorphDB. Note that PMDB includes most of the FMC-1.0 original images, but the morphing generation is here done according to the precise protocol described hereafter.

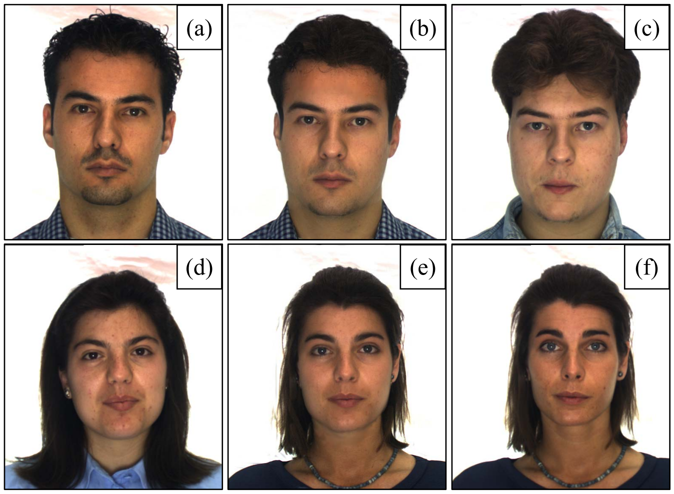


Fig. 11. Examples from FMC-1.0 database. (b) (e) two morphed images generated from (a) (c) and (d) (f), respectively. It is worth noting that the morphed image is quite different from both subjects and it will hardly fool a human expert (as reported in [2]).

A. PMDB - Progressive Morphing Database

This database was automatically generated starting from existing face images. Thanks to the fully automatic generation, we can produce a large number of samples and at the same time precisely control the morphing factor α.

PMDB consists of a collection of datasets, each containing the same set of genuine (not morphed) images G and a specific set of morphed images M_α obtained applying the morphing process described in Section III with morphing factor α and automatic retouching:

$$PMDB = \{MDB_\alpha, \alpha \in \{0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4, 0.45\}\}$$

where $MDB_\alpha = G \cup M_\alpha$.

The morphed images have been generated starting from the AR [23], FRGC [24] and Color Feret [25], [26] databases which contains images of males and females taken under different acquisition conditions. The selected images have been manually checked to ensure they fulfil ISO/ICAO specifications [18]. Moreover, the subjects wearing glasses have been excluded since the resulting morphing could be affected by visible artifacts. The final number of subjects is 280: 80 for AR (34 males and 46 females) and 100 for both FRGC and Color Feret (50 males and 50 females each). Two images of each subject have been selected: the former used for morphing generation and the latter for testing.

The set of genuine images G contains overall 1334 images including the two images of each subject used for morphing and additional ISO/ICAO [18] compliant images of other subjects from the same databases.

Analogously to [27], the selection of candidate images to produce morphing cases was performed as follows:

1) the first image of each subject (i.e., the criminal) is compared with the first image of other k subjects of the same gender (i.e., possible accomplices) randomly chosen from the same source database (i.e., AR, FRGC or Color Feret). The subject presenting the maximum similarity with the criminal is selected as the optimal accomplice for morphing. The comparisons have been performed using the commercial face recognition software Neurotechnology VeriLook SDK 6.0 [28] (VL-SDK). This choice is aimed at maximizing the probability of fooling the face verification software at the gate. A visual inspection of the selected pairs confirms a good degree of similarity between the two subjects.
2) The first image of the criminal and of the optimal accomplice are morphed following the procedure described in Section III. The result is a set of morphed frames, one for each value of α (see Fig. 12).
3) The generated images are compared against the original images of both subjects using VL-SDK. In case of non-match with at least one of the two originals, we discarded the morphing due to the low chance of success (of the morphing attack). To this purpose the similarity threshold was set to 48 (corresponding to a FAR=0.01% [28]).

TABLE I

CARDINALITY OF THE SET OF MORPHED IMAGES M_α AS A FUNCTION OF THE VALUE OF α. THE SECOND ROW QUANTIFIES THE MORPHING GENERATION SUCCESS RATE FOR EACH VALUE OF α

	α							
	0.10	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
$\lvert M_\alpha \rvert$	67	239	547	849	1001	1087	1102	1108
%	5.98	21.34	48.84	75.80	89.38	97.05	98.39	98.93

The above procedure is repeated t times (4 in our experiments) for each subject to increase the number of morphed images. Each time the optimal accomplices used in the previous iterations are excluded from the random selection. PMDB has been generated with $k = 10$ to simulate a realistic scenario where a criminal can find 10 very good friends with no criminal records who accept to play the role of possible accomplices [27]. However, in the experimental section we also show and discuss the impact of k on the probability of success of the morphing attack.

Table I summarizes the number of successfully generated morphed images (absolute value and percentage with respect to the total attempt number: 1120) as function of α. The percentage value represents the probability of automatically generating a "valid" morphed image given an accomplice chosen according to the previous procedure at a specific value of α. Of course, lower values of α yields to morphed images which are very similar to the accomplice and in most cases the "small" presence of the criminal is not sufficient to produce a positive match. However for α in the range [0.2; 0.3] the chance of generating a "valid" morphing from two subjects is fairly high (i.e., in [48.8%; 89.4%]) and the resulting images are similar enough to the accomplice to fool a human officer.

PMDB will be used to setup a new benchmark on the FVC-onGoing platform [29], [30].

B. MorphDB

A second database, named *MorphDB*, has been created starting from controlled images of the Color Feret [25], [26] and FRGC [24] databases, to produce a set of very accurate morphed images. The aim of this dataset is also to reproduce

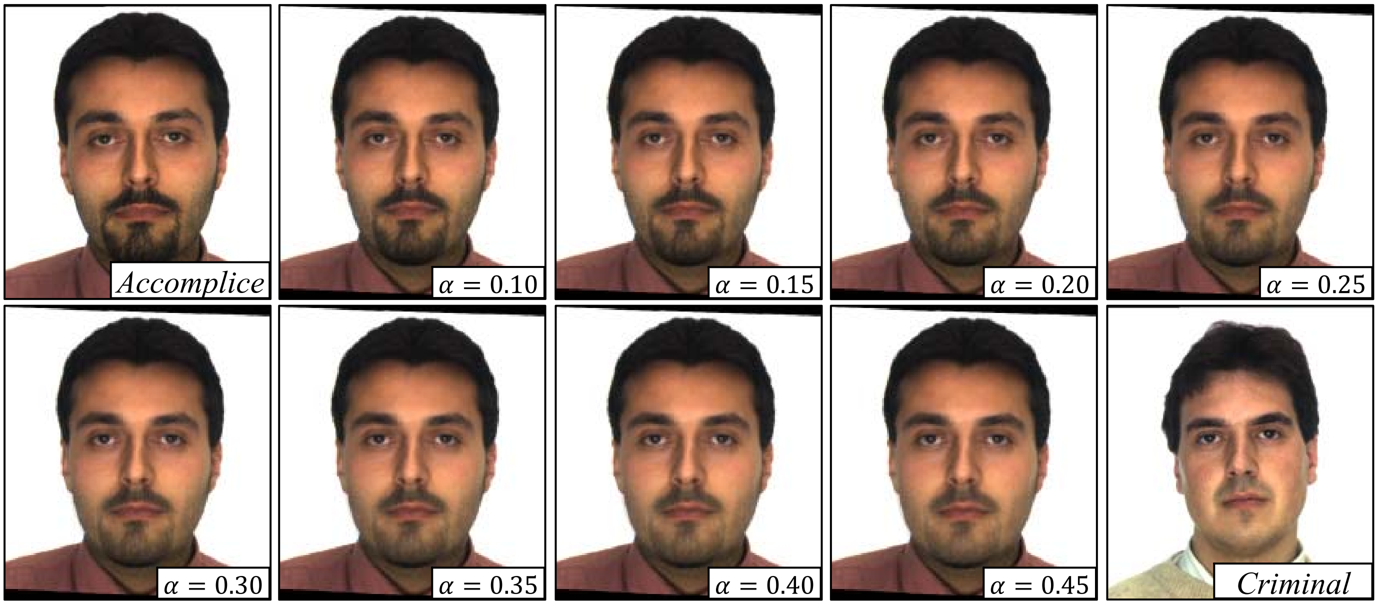


Fig. 12. Example images from the PMDB. The morphed images are obtained combining the accomplice and the criminal with different mixing factors (α). The morphed image is always rather similar to the accomplice, even if for higher values of α the image could raise some suspicion in the human officer.

the typical scenario where the ID photo is provided by the citizens printed on photographic paper and then scanned by the officer during the issuing process (*P&S* process). To maximize precision and to emulate the *P&S* process, the collection of this database requires several manual steps.

For each pair of subjects, Sqirlz Morph 2.1 [31] has been used to generate a sequence of 20 morphed frames; the facial landmarks used as correspondence points in the morphing process have been automatically extracted using VL-SDK. Then, for each morphing sequence, the best candidate has been manually retouched to remove at best any visible artifact. The morphed frame candidates have been manually selected to maximize the probability of easily fooling both the human expert (at the passport issuing stage) and the automatic face recognition software (at the verification stage) (see Fig. 13.a-c). Then the morphed images have been printed on high quality photographic paper by a professional photographer, following the standard procedure used for ID photos. Finally, the printed images have been scanned at 600 DPI and rescaled to the original size. In spite of the high quality printing/scanning, the *P&S* process usually modifies the image texture, introducing a blurring effect and often reducing the contrast (see Fig. 13. d-f).

Overall, the MorphDB consists of 100 morphed images (50 males and 50 females) and, for each of them, includes the two original images used for morphing and a variable number of test images of the two subjects. In the following, we will refer to:

- *MorphDB_D* to indicate the MorphDB where all the images are used in digital format;
- *MorphDB_P&S* to indicate the MorphDB where the morphed images and the original images are printed and scanned (to simulate images stored in the document), while the test images are digital (to simulate images acquired live at the ABC gate).

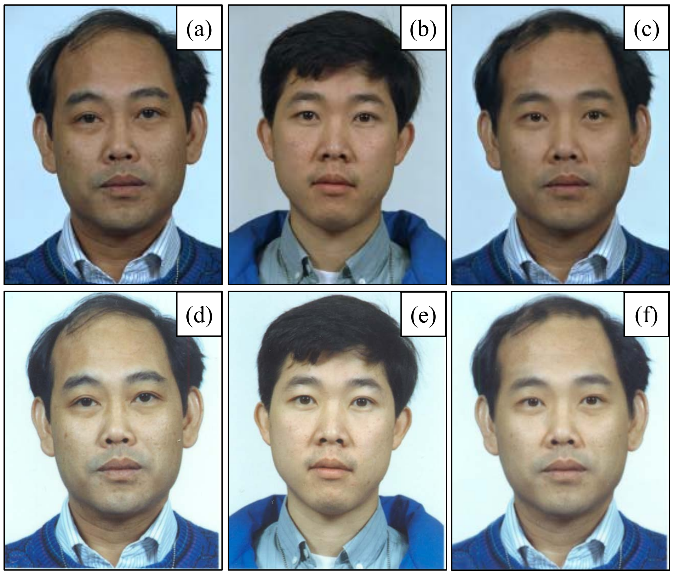


Fig. 13. Original images of two subjects (a) and (b) and the resulting morphing image in digital format (c). In the second row, the printed and scanned version of the previous images is provided (d-f).

MorphDB will be made available to the scientific community on our website [32] to promote further studies on this important topic.

VI. Experimental Evaluation

In this section, we describe the experiments carried out on PMDB and MorphDB, specifically designed for “two-images” techniques. No other approaches of this category have been proposed until now, so we cannot perform a comparative evaluation.

The experiments have been conducted using the commercial face recognition software VL-SDK. In order to simulate a realistic attack to an ABC system, the operational threshold

TABLE II

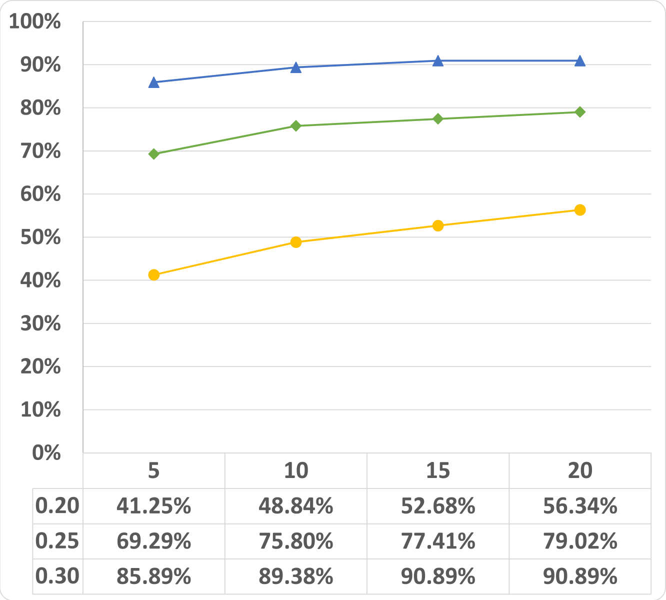
GENUINE ACCEPTANCE RATE ON PMDB. THE RESULT WITHOUT DEMORPHING (COLUMN NO DEMORPHING) IS COMPARED TO THOSE OBTAINED WITH DIFFERENT VALUES OF DEMORPHING FACTOR $\tilde{\alpha}$

No demorphing	$\tilde{\alpha}$							
	0.10	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
99.9%	99.6%	99.3%	99.0%	98.2%	97.9%	95.7%	91.6%	89.2%

TABLE III

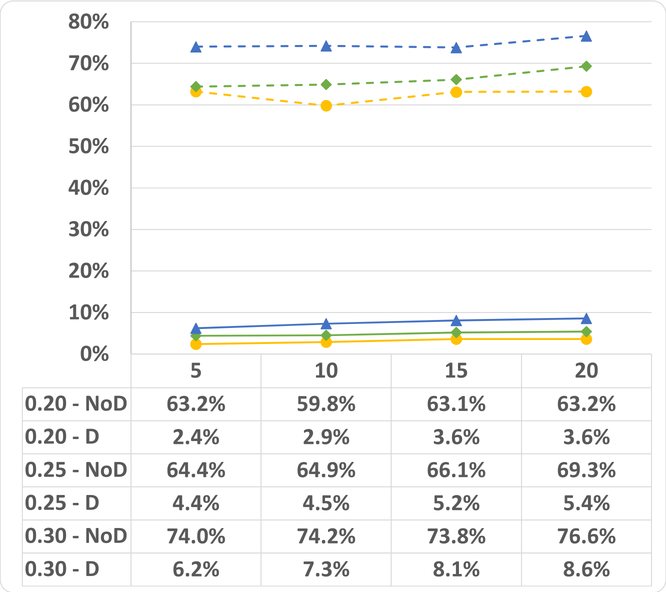
CRIMINAL MORPH ACCEPTANCE RATE ON PMDB AT DIFFERENT VALUES OF MORPHING FACTOR α. THE RESULT WITHOUT DEMORPHING (COLUMN NO DEMORPHING) IS COMPARED TO THOSE OBTAINED WITH DIFFERENT VALUES OF DEMORPHING FACTOR $\tilde{\alpha}$

α	**No demorphing**	**Demorphing Factor** $\tilde{\alpha}$							
		0.10	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
0.10	53.7%	16.4%	10.4%	3.0%	1.5%	1.5%	3.0%	4.5%	3.0%
0.15	53.1%	18.0%	9.6%	4.2%	2.5%	2.1%	2.1%	3.8%	4.6%
0.20	59.8%	21.9%	10.6%	5.3%	4.2%	2.9%	2.4%	2.9%	2.9%
0.25	64.9%	30.5%	17.1%	10.5%	6.1%	4.5%	3.2%	2.6%	1.8%
0.30	74.2%	44.5%	31.5%	18.8%	11.5%	7.3%	5.1%	4.2%	3.0%
0.35	82.4%	60.5%	47.5%	33.8%	23.1%	15.1%	10.1%	7.5%	6.3%
0.40	88.7%	74.0%	64.4%	51.9%	39.7%	30.0%	20.3%	14.1%	9.5%
0.45	94.2%	84.2%	76.2%	67.7%	57.7%	45.9%	34.7%	26.2%	17.3%



	5	10	15	20
0.20	41.25%	48.84%	52.68%	56.34%
0.25	69.29%	75.80%	77.41%	79.02%
0.30	85.89%	89.38%	90.89%	90.89%

Fig. 14. Morphing generation success rate at different values of k. The curves refer to the following values of α: 0.20 (yellow circles), 0.25 (green diamond) and 0.30 (blue triangle).



	5	10	15	20
0.20 - NoD	63.2%	59.8%	63.1%	63.2%
0.20 - D	2.4%	2.9%	3.6%	3.6%
0.25 - NoD	64.4%	64.9%	66.1%	69.3%
0.25 - D	4.4%	4.5%	5.2%	5.4%
0.30 - NoD	74.0%	74.2%	73.8%	76.6%
0.30 - D	6.2%	7.3%	8.1%	8.6%

Fig. 15. C-MAR values with (D, solid lines) and without (NoD, dashed lines) demorphing for different values of k. The curves refer to the following α: 0.20 (yellow circles), 0.25 (green diamond) and 0.30 (blue triangle). The demorphing factor $\tilde{\alpha}$ is 0.30.

of the face recognition software have been fixed according to the Frontex guidelines [3]. In particular, for ABC systems operating in verification mode, the face recognition algorithm has to ensure a *False Acceptance Rate* (FAR) equal to 0.1% and a *False Rejection Rate* (FRR) lower than 5%. During the experimentation, a score threshold of 36 (for both thr_1 and thr_2 in Fig. 1) has been used, since this is the value indicated by the SDK documentation to achieve FAR=0.1%. To compute performance, the following comparisons have been executed:

- *Genuine attempts* – non-morphed face images of the same subject are compared to compute the *Genuine Acceptance Rate* (GAR).
- *Criminal morph attempts* – morphed face images are compared against face images of the criminal subject to compute the Criminal Morph Acceptance Rate (C-MAR).

It is worth noting that:

- referring to ISO/IEC 30107-3 [33] and in general to Presentation Attach Detection (PAD) literature, C-MAR corresponds to IAPMR (Imposter Attack Presentation Match Rate). In the specific case of morphing attacks, C-MAR corresponds to MMPMR (Mated Morph Presentation Match Rate) [34].
- In the considered scenario, comparing morphed images against the accomplice is of no interest, since the

TABLE IV

ACCEPTANCE RATES ON MORPHDB_D. THE RESULT WITHOUT DEMORPHING (COLUMN NO DEMORPHING) IS COMPARED TO THOSE OBTAINED WITH DIFFERENT VALUES OF DEMORPHING FACTOR $\tilde{\alpha}$

	No demorphing	**Demorphing Factor $\tilde{\alpha}$**							
		0.10	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
GAR	100.0%	100.0%	100.0%	99.6%	99.6%	99.3%	98.1%	97.6%	95.9%
C-MAR	66.4%	32.1%	20.7%	15.9%	11.4%	9.6%	9.1%	8.1%	6.1%

TABLE V

ACCEPTANCE RATES ON MORPHDB_P&S. THE RESULT WITHOUT DEMORPHING (COLUMN NO DEMORPHING) IS COMPARED TO THOSE OBTAINED WITH DIFFERENT VALUES OF DEMORPHING FACTOR $\tilde{\alpha}$

	No demorphing	**Demorphing Factor $\tilde{\alpha}$**							
		0.10	**0.15**	**0.20**	**0.25**	**0.30**	**0.35**	**0.40**	**0.45**
GAR	100.0%	100.0%	99.9%	99.1%	98.8%	98.4%	97.8%	96.2%	94.0%
C-MAR	50.5%	18.9%	14.4%	9.1%	6.3%	4.8%	4.3%	3.0%	2.5%

accomplice is here considered the legitimate document owner, and as such is entitled to pass the gate.

A. Results on PMDB

The main objective of the experimentation on this database is to evaluate the range of feasible values for the morphing factor α (see Section III) and the demorphing factor $\tilde{\alpha}$ (see Section IV). The number of genuine attempts in this database is 667, while the number of criminal morph attempts, for a given α, corresponds to the related entry in Table I (in fact each morphed images is compared against the test image of the criminal subject).

Table II reports the GAR for different values of the demorphing factor $\tilde{\alpha}$. Note that GAR (i.e., 1-FRR) includes both false rejections independent of the demorphing process (see first column "No demorphing") and false morphing warnings. To distillate false morphing warnings, we should remove from GAR the contributions of the first column. For example at $\tilde{\alpha} = 0.25$ we have GAR $= 98.2\% \rightarrow$ FRR $= 1.8\%$, and false morphing warnings $= 1.7\%$.

In order to be applicable in real scenarios the rate of false morphing warnings should be as small as possible; ideally the total FRR (1-GAR) should continue to fulfill the Frontex requirements (FRR$<$5%). [3]. Looking at the results in Table II, $\tilde{\alpha}$ values up to 0.35 would be acceptable, but a prudent choice suggests not exceeding the value of 0.3. Anyway, a more general analysis, including the effects of $\tilde{\alpha}$ on the morph acceptance rate, is needed to maximize the effectiveness of the demorphing technique without affecting the recognition performance.

Table III reports C-MAR as function of both the morphing factor α used to generate the morphed images and the demorphing factor $\tilde{\alpha}$ used to demorph them. The results obtained without demorphing (column "*No demorphing*") confirm that, as expected, the chance of a criminal to fool an automatic recognition system is directly proportional to the value of α (i.e., the presence of the criminal in the morphed image). Here too, a visual inspection of the morphed images suggests that values of α in the range [0.2; 0.3] represent the best trade-off between the probability of acceptance of the morphed image by the human officer in the enrollment stage and the possibility of success in the verification stage. As to the parameter $\tilde{\alpha}$, it is evident that higher values are more effective in reducing C-MAR. Again, interesting results can be achieved with $\tilde{\alpha}$ in the range [0.2; 0.3]: in fact, in this case a drastic reduction of C-MAR can be observed (from about 60-75% to 3-6%) without a significant degradation of GAR (from about 99.9% to 98%).

To evaluate the impact of the number of possible accomplices involved in the morphing generation procedure (parameter k in Section V-A), additional tests have been carried out by re-generating the PMDB database for different values of k (5, 15 and 20). Fig. 14 shows the probability of automatically generating a "valid" morphed image for different k and α. As expected, the probability of success increases with α and k, but the influence of k is much lower than α. Fig. 15 shows C-MAR for $\tilde{\alpha} = 0.30$ (GAR $= 97.9\%$) for various k. It is worth noting that increasing k results in a minor increment of C-MAR. Overall, the demorphing process drastically reduces the C-MAR with respect to an "unprotected" ABC (as clearly visible by a comparison of solid and dashed lines).

B. Results on MorphDB

The experiments on *MorphDB* are aimed at measuring the efficacy of face demorphing on high quality morphed images and to evaluate the impact of the *P&S* process on the accuracy. In this database the number of testing images varies for the different subjects; overall the tests consist of 756 genuine attempts and 396 criminal morph attempts.

The results obtained are summarized in Table IV and Table V for MorphDB_D and MorphDB_P&S, respectively. The values of C-MAR without demorphing on the MorphDB_D are close to those obtained on PMDB with $\alpha = 0.2$ (about 67%). The demorphing algorithm, with values of $\tilde{\alpha}$ in the range [0.2; 0.3] produces also in this case a significant reduction of the C-MAR (from 66.4% to 11.4% for $\tilde{\alpha} = 0.25\%$) with only little impact on GAR. With respect to PMDB the demorphing approach is slightly less accurate; this can be related to the higher quality of morphing (manual selection, manual retouch, etc.) which makes the process inversion more complex. The results on the printed and scanned version of the database show that the *P&S* process tends to reduce a little bit the incidence of C-MAR (from 66.4% to 50.5%) but confirms the efficacy of the demorphing process (from 50.5% to 6.3% for $\tilde{\alpha} = 0.25$).

VII. Conclusion

In this paper we proposed a face demorphing approach to protect Automated Border Control systems against morphing attacks.

Our experimental results show that demorphing can substantially reduce (from 60-70% to 6-10%) the chance that a criminal can fool an ABC system while keeping the amount of false morphing warnings quite limited (1-2%).

Two new datasets have been created to study the efficacy of morphing detection. Particular care has been devoted to the subject selection and morphing generation procedures to ensure that the generated images are challenging both for human officers (at enrolment) and face recognition algorithms (at the gate). Both databases will be made available to the research community: PDMB as a new benchmark through the FVC-onGoing platform and MorphDB as full download.

Further experiments are necessary to ensure that our assumptions are valid and that the face variations in AR, FRGC and Color Feret (used as sources for PDMB and MorphDB) are representative of face recognition at ABC. In fact, factors such as face aging and different acquisition settings between enrolment and live capture (only partially covered in our experiments) could be hurting for demorphing; on the other hand, the possibility of capturing and demorphing multiple frames during the live check at the gate could make the approach more robust. To better investigate these issues, we are going to setup an experiment in an operational scenario at a real e-gate.

References

[1] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Clearwater, FL, USA, Sep. 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 Imaging Spectrum*. Cham, Switzerland: Springer, 2016, pp. 195–222.

[3] *Best Practice Technical Guidelines for Automated Border Control (ABC) Systems—V2.0*, FRONTEX, Warsaw, Poland, Aug. 2012, doi: 10.2819/26969.

[4] *The Global Automated Border Control Industry Report: Airport eGates & Kiosks*, Acuity Market Intelligence, St. Louisville, CO, USA, 2014.

[5] International Air Transport Association (IATA). (Nov. 2017). *IATA Automated Border Control Map*. [Online]. Available: http://www.iata.org/whatwedo/passenger/Pages/automated-border-control.aspx

[6] (Nov. 2017). *FIDELITY European Project Web Site*. [Online]. Available: http://www.fidelity-project.eu/

[7] R. Raghavendra, K. B. Raja, and C. Busch, "Detecting morphed face images," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Niagara Falls, NY, USA, Sep. 2016, pp. 1–7.

[8] U. Scherhag *et al.*, "On the vulnerability of face recognition systems towards morphed face attacks," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Coventry, U.K., 2017, pp. 1–7.

[9] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Invest.*, vol. 10, no. 3, pp. 226–245, Oct. 2013.

[10] T. Neubert, "Face morphing detection: An approach based on image degradation analysis," in *Proc. Int. Workshop Digit. Watermarking (IWDW)*, Magdeburg, Germany, 2017, pp. 93–106.

[11] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in *Proc. Int. Workshop Digit. Watermarking (IWDW)*, Magdeburg, Germany, 2017, pp. 107–120.

[12] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Transferable deep-CNN features for detecting digital and print-scanned morphed face images," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Honolulu, HI, USA, Jul. 2017, pp. 1822–1830.

[13] Wikipedia. (Nov. 2017). *Morphing*. [Online]. Available: http://en.wikipedia.org/wiki/Morphing

[14] Wikipedia. (Nov. 2017). *Image Warping*. [Online]. Available: http://en.wikipedia.org/wiki/Image_warping

[15] G. Wolberg, *Digital Image Warping*, 1st ed. Los Alamitos, CA, USA: IEEE Computer Society Press, 1994.

[16] D. F. Rogers and J. A. Adams, *Mathematical Elements for Computer Graphics*, 2nd ed. New York, NY, USA: McGraw-Hill, 1989.

[17] B. Delaunay, "Sur la sphère vide. A la mémoire de Georges Voronoï," *Bulletin l'Académie Sciences l'URSS, Classe Sciences Mathématiques Naturelles*, no. 6, pp. 793–800, 1934.

[18] *Information Technology—Biometric Data Interchange Formats—Part 5: Face Image Data*, document ISO/IEC 19794-5, 2011.

[19] *Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems*, FRONTEX, Warsaw, Poland, 2011.

[20] GIMP. (Nov. 2017). *GNU Image Manipulation Program*. [Online]. Available: http://www.gimp.org/

[21] GIMP. (Nov. 2017). *GIMP Animation Package*. [Online]. Available: http://registry.gimp.org/node/18398

[22] D. J. Robertson, R. S. S. Kramer, and A. M. Burton, "Fraudulent ID using face morphs: Experiments on human and automatic recognition," *PLoS ONE*, vol. 12, no. 3, p. e0173319, Mar. 2017.

[23] A. Martínez and R. Benavente, "The AR face database," Univ. Autònoma Barcelona, Bellaterra, Spain, Tech. Rep. #24, 1998.

[24] P. J. Phillips *et al.*, "Overview of the face recognition grand challenge," in *Proc. IEEE Comput. Vis. Pattern Recognit.*, vol. 1. Jun. 2005, pp. 947–954.

[25] P. J. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image Vis. Comput.*, vol. 16, no. 5, pp. 295–306, 1998.

[26] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 10, pp. 1090–1104, Oct. 2000.

[27] M. Ferrara, R. Cappelli, and D. Maltoni, "On the feasibility of creating double-identity fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 892–900, Apr. 2017.

[28] Neurotechnology Inc. (Nov. 2017). *Neurotechnology*. [Online]. Available: http://www.neurotechnology.com/

[29] B. Dorizzi *et al.*, "Fingerprint and on-line signature verification competitions at ICB 2009," in *Proc. 3rd IAPR/IEEE Int. Conf. Biometrics (ICB)*, Alghero, Italy, Jun. 2009, pp. 725–732.

[30] BioLab. (Nov. 2017). *FVC-on Going*. [Online]. Available: http://biolab.csr.unibo.it/fvcongoing

[31] Xiberpix. (Nov. 2017). *Sqirlz Morph 2.1*. [Online]. Available: http://www.xiberpix.net/SqirlzMorph.html

[32] BioLab. (Nov. 2017). *Biometric System Laboratory*. [Online]. Available: http://biolab.csr.unibo.it

[33] *Information Technology—Biometric Presentation Attack Detection—Part 3: Testing and Reporting*, document ISO/IEC FDIS 30107-3:2017 JTC 1/SC 37, International Organization for Standardization (ISO), Geneva, Switzerland, 2017.

[34] U. Scherhag *et al.*, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2017, pp. 1–7.

Authors' photographs and biographies not available at the time of publication.