

# The Magic Passport

Matteo Ferrara, Annalisa Franco, Davide Maltoni  
Department of Computer Science and Engineering  
Via Sacchi, 3 – 47521 Cesena (FC) - Italy  
{matteo.ferrara, annalisa.franco, davide.maltoni}@unibo.it

## Abstract

*Once upon a time there was a criminal; he was reading his e-mail when a banner caught his attention: low cost flights for the destination of his dreams! He had already started to book the trip when suddenly realized that, being wanted by the police, he could not use his passport without being arrested. What to do? He could not miss that opportunity, so he called a good friend and they started to think for a possible solution. Do you want to know if they succeeded? Read the rest of the paper and find it out.*

## 1. Introduction

In recent years electronic documents storing biometric features for machine-assisted identity verification have progressively replaced traditional paper documents. In 2002, with the Berlin resolution, face has been selected by the International Civil Aviation Organization (ICAO) as the primary globally interoperable biometric trait for machine-assisted identity confirmation in electronic Machine Readable Travel Documents (eMRTD) [1].

To facilitate the automatic identity verification process, the face image stored in an eMRTD has to satisfy very restrictive quality standards. Following ICAO guidelines, the International Standard Organization (ISO) defined a set of geometric and photometric requirements that a face image has to fulfil to be included into an eMRTD [2] [3].

Today, face photos to be included into an eMRTD can be provided in two ways (depending on the procedure adopted by the country issuing

the e-document): i) the face is acquired live with high-quality digital camera connected to the enrolment station; ii) the citizen provides a face ID photo printed on paper. While in the former case the ISO compliance verification is sufficient, in the latter further controls should be done to ensure that the printed photo has not been altered. Different kinds of photo alterations are possible. Some unintentional alterations could be introduced by the acquisition or printing devices (e.g., geometric distortions or image aspect ratio modifications) with the effect of changing the face geometry; other kinds of alterations, usually performed using image processing tools, may be intentionally realized to make the subject more attractive (i.e., beautification) or with the criminal intent of deceiving an automatic recognition system. Such alterations can have undesirable effects in terms of both security and efficacy of the recognition process.

Recently, the effects of some image alterations (i.e., geometric and beautification alterations) on face recognition performance have been studied in [4]. The results show that state-of-the-art face recognition algorithms are able to overcome limited alterations but are sensitive to more relevant modifications. In particular the above study shows that some geometric alterations and digital beautification can cause an increment of the false rejection rate: in an automatic verification scenario, (e.g., in an airport using an Automatic Border Control (ABC) system [5]) the system is not able to recognize the owner of the eMRTD thus requiring the intervention of a human operator; in a watch-list scenario, where a list of subjects wanted by the police has to be

checked in order to block the suspects, an intentional alteration could allow the suspect to bypass the control. With the widespread adoption of ABC systems [6], the risk of criminal attempts to bypass controls should be mitigated with appropriate countermeasures.

This study analyses the feasibility of an attack to ABC systems performed by using morphed face images obtained by combining faces of different subjects. At the time of verification at an ABC, a face image (acquired live) of the person presenting the travel document is matched against the face image stored in the eMRTD. If a morphed image included in an eMRTD can be successfully matched with the face of two or more subjects, then different persons can share the same document. In an ABC system scenario this would allow a criminal to exploit the passport of an accomplice with no criminal records to overcome the security controls. In more detail, the subject with no criminal records could apply for a eMRTD by presenting the morphed face photo; if the image is not noticeably different from the applicant face, the police officer could accept the photo and release the document (see Figure 1). It is worth noting that in this case the document is perfectly regular; the attack does not consist of altering the document content but in deceiving the officer at the moment of document issuing. The document released will thus pass all the integrity checks (optical and electronic) performed at the gates.

In this work we will evaluate: i) the feasibility of creating deceiving morphed face images and ii) the robustness of commercial recognition systems in the presence of morphing.

The rest of this paper is organized as follows. Section 2 describes the simulated attack to an ABC system, section 3 details the morphing procedure used to create the fake identity photos, finally section 4 reports and comments the experimental results obtained.

Please note that any association between subjects and the criminal role is purely accidental and not related to real facts.

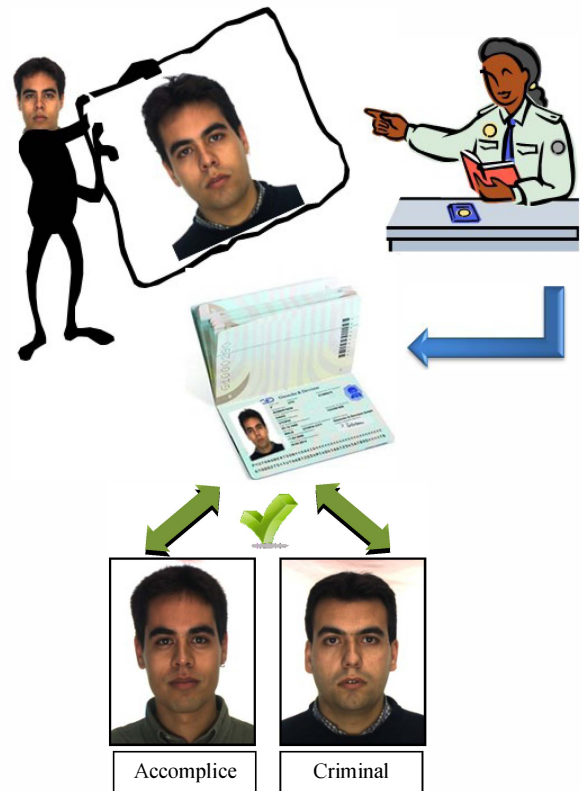


Figure 1: A possible attack realized by means of a morphed photo. The image is visually very similar to the applicant, but contains facial features of a different subject.

## 2. Attacking an ABC system

In this section, the robustness of automated face recognition system against morphing alterations has been evaluated. The experiments have been conducted using two commercial face recognition software tools: Neurotechnology VeryLookSDK 5.4 [7] and Luxand FaceSDK 4.0 [8]. In order to simulate a realistic attack to an ABC system, the operational thresholds of the face recognition software have been fixed according to the guidelines [5] provided by FRONTEX (the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union) [9]. In particular, for ABC systems operating in verification mode, the face verification algorithm has to ensure a security level in terms of the False Accept Rate (FAR) of at least 0.001 (i.e., 0.1 per cent). Both the SDKs used in the experiments provide an indication of

the score threshold to be used for face verification to reach a given FAR (i.e., 36 and 0.999 for Neurotechnology and Luxand SDKs, respectively), thus allowing to simulate the operating conditions of a real ABC system.

The attack was designed as follows:

- Two images of different subjects have been selected: we chose two persons with a some physical similarity but whose face images did not falsely match using the suggested threshold (for both SDKs); non matching images were used because in case of matching, no morphing operations are required.
- The two images were morphed into a new image as described in the following section.

The morphed image was matched to other two images of the two subjects (not those used for morphing) and the matching result was analyzed.

### 3. Morphing

In motion pictures and animations, morphing is a special effect that changes one image into another though a seamless transition [10]. Often morphing is used to depict one person turning into another.

To morph two face images the free GNU Image Manipulation Program v2.8 (GIMP) [11] and the GIMP Animation Package v2.6 (GAP) [12] have been used in this paper. The aim of morphing is, in this case, to produce a face image which is very similar to one of the two subjects (the applicant of the document) but that also includes facial features of the second subject. Of course this objective is easier to realize if the two subjects have similar faces, but the results will show that this condition is not strictly necessary.

Given two face images, the following steps are carried out to produce morphing:

1. The two faces are put as separate layers in the same image and are manually aligned by superimposing the eyes (see Figure 2).
2. A set of important facial points (e.g., eye corners, eyebrows, nose tip, chin, forehead etc.) are manually marked on the two faces

using the GAP morph tool (see Figure 3).

3. A sequence of frames showing the transition from one face to the other is automatically generated using the GAP morph function (see Figure 4).
4. The selection of the final frame is done by scanning the frames (starting from the applicant photo) and continuing until the current frame gets a matching score with the criminal subject greater than or equal to the matching thresholds. For frame selection the similarity with the applicant of the document was privileged to maximize the probability of acceptance in the enrollment stage, under the hypothesis of face verification at unattended gates. Of course it is possible to use an intermediate morphed image for other scenarios such as attended gates.
5. Finally, the frame selected is manually retouched to make it more realistic (see Figure 5), in order it can be accepted as a genuine ICAO photo. To this purpose one should eliminate the ghost shadows and other small defects.

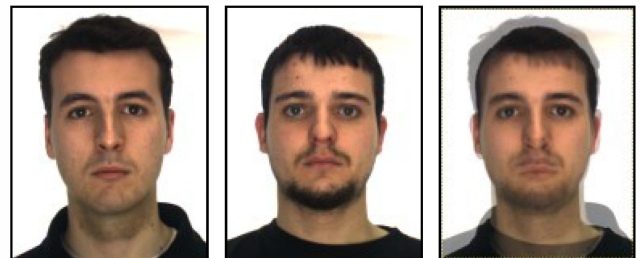


Figure 2: The first step for morphing - aligning the two images according to the eyes position.



Figure 3: The facial points labeled for the two images before morphing; such points will allow to obtain a better alignment between the two faces and a smoother morphing.

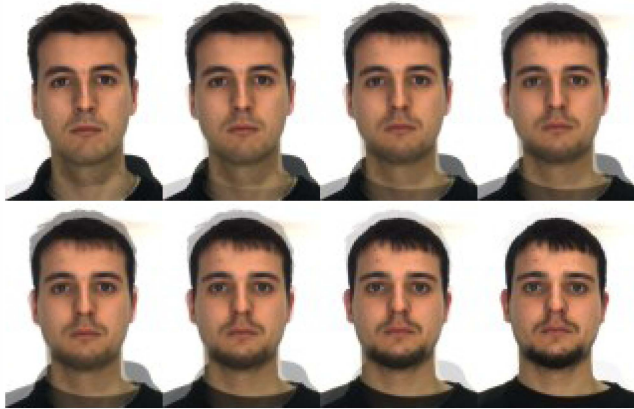


Figure 4: Frames obtained by the morphing procedure, gradually shading from subject 1 (applicant) to subject 2 (criminal).

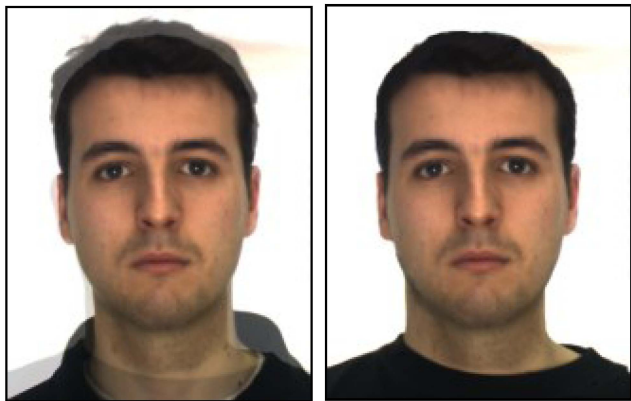


Figure 5: The frame selected for matching before and after manual photo retouch.

#### 4. Experimental results

This section presents the results obtained. The experiments have been carried out on the AR face database [13], chosen because it contains several images compliant to the quality standards in use for eMRTD. The database consists of 4,000 frontal images taken under different conditions in two sessions separated by two weeks. In particular, poses 1 and 14 are selected for the morphing experiments since they present neutral expression and good illumination.

The morphing experiment has been carried out for 5 couples of male subjects (see Figure 6) and 5 female (see Figure 7). Moreover two extra experiments have been conducted mixing i) one man and one woman (see Figure 8); ii) three men

(see Figure 9).

All the attacks were successful: for both SDKs the matching score between the morphed face image and each of the test images (see Table 1) is higher than the recommended threshold (see Section 2). A visual inspection of the morphed images (see the second column in Figures 6 and 7) confirms that the attack is perfectly feasible since the morphed image is very similar to one of the two subjects (ID1) and also the human expert issuing the passport could be easily fooled.

Table 1. Matching scores of the test images and the morphed image for the subjects in Figures 6 (M1-M5), 7 (F1-F5) and 8 (MF).

	VeryLookSDK 5.4		LuxandSDK 4.0	
	T1 - M	T2 - M	T1 - M	T2 - M
<b>M1</b>	280	191	1.00000	0.99999
<b>M2</b>	846	75	1.00000	0.99998
<b>M3</b>	686	61	1.00000	0.99946
<b>M4</b>	360	49	1.00000	0.99967
<b>M5</b>	412	100	1.00000	0.99995
<b>F1</b>	390	119	0.99999	0.99957
<b>F2</b>	311	67	0.99998	0.99939
<b>F3</b>	339	130	0.99975	0.99904
<b>F4</b>	615	98	1.00000	0.99992
<b>F5</b>	182	292	0.99996	0.99908
<b>MF</b>	285	203	0.99996	0.99966

As an outcome of this study, we can affirm that giving to the citizens the possibility of providing a printed face photo poses serious concerns in terms of security: proper countermeasures have to be taken to avoid storing digitally altered photos in eMRTDs. The alterations shown in this work suggest that even a human expert can be easily fooled; in our opinion at today the best solution to the problem of altered face photo is to directly acquire the face photo to be stored in the ePassport at the enrolment station using a high quality camera in a controlled environment, and following the recommendations listed in [2] (Informative Annex C.2). At the time this paper is being written we are conducting further experiments, in cooperation with government agencies, to assess the feasibility of this threat in operational ABC.



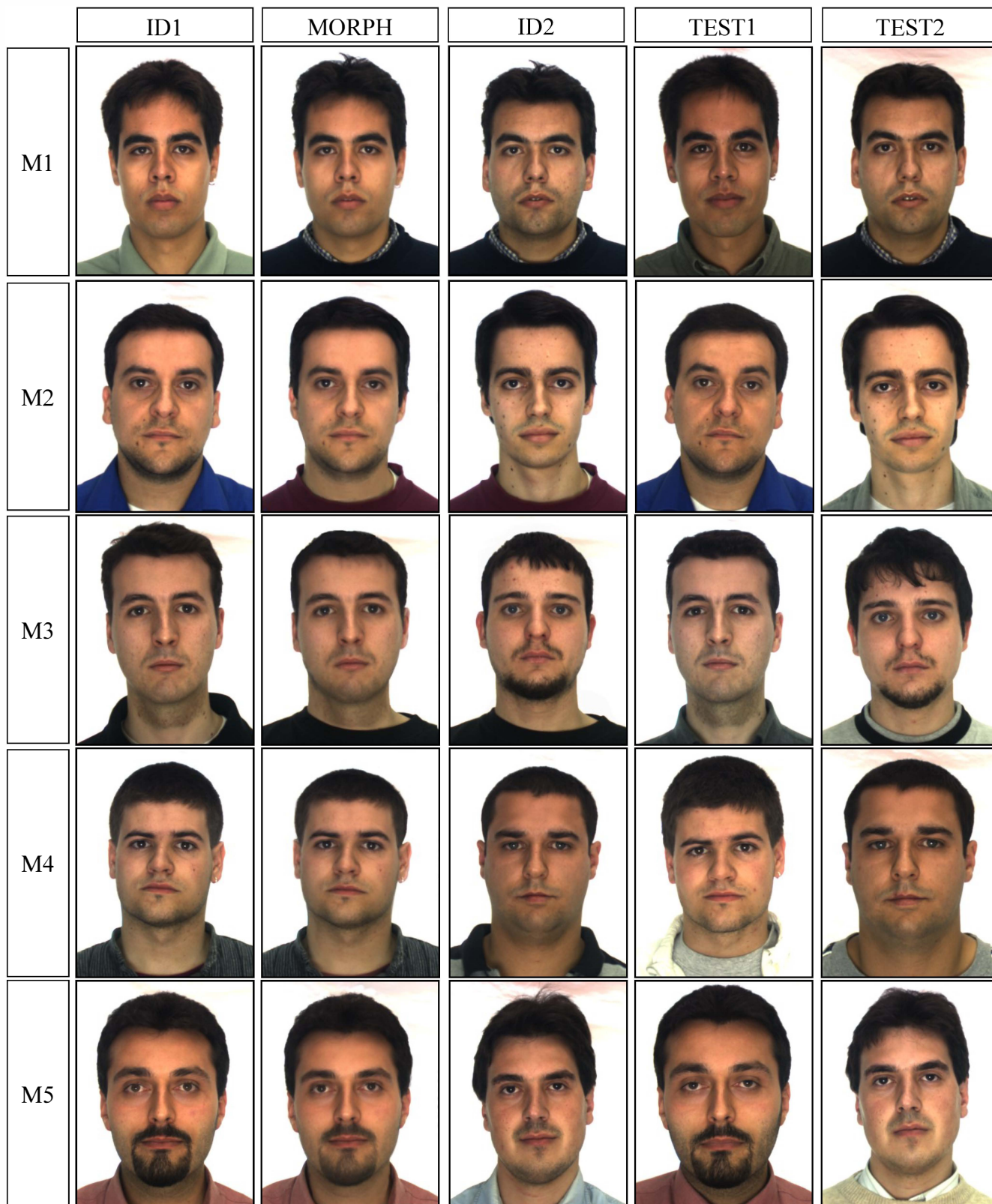


Figure 6: Example of morphed images: the results obtained with five male couples. In particular, for each row the following images have been reported: the two images used for morphing (columns ID1 and ID2), the resulting morphed face image (column MORPH) and the two images used for the matching test (columns TEST1 and TEST2).

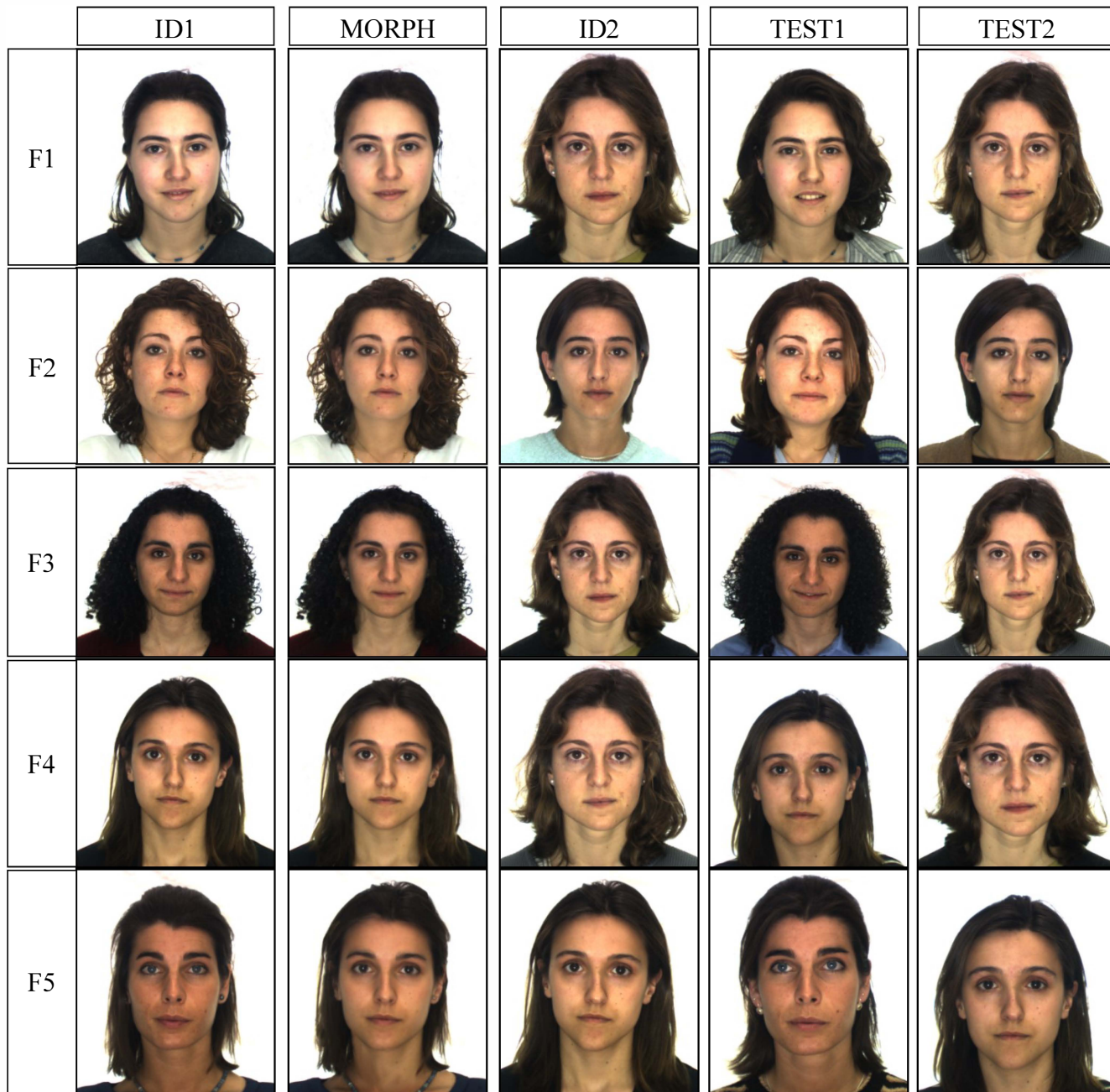


Figure 7: Example of morphed images: the results obtained with five female couples.



Figure 8: Example of morphed images: the results obtained mixing one man and one woman (MF).



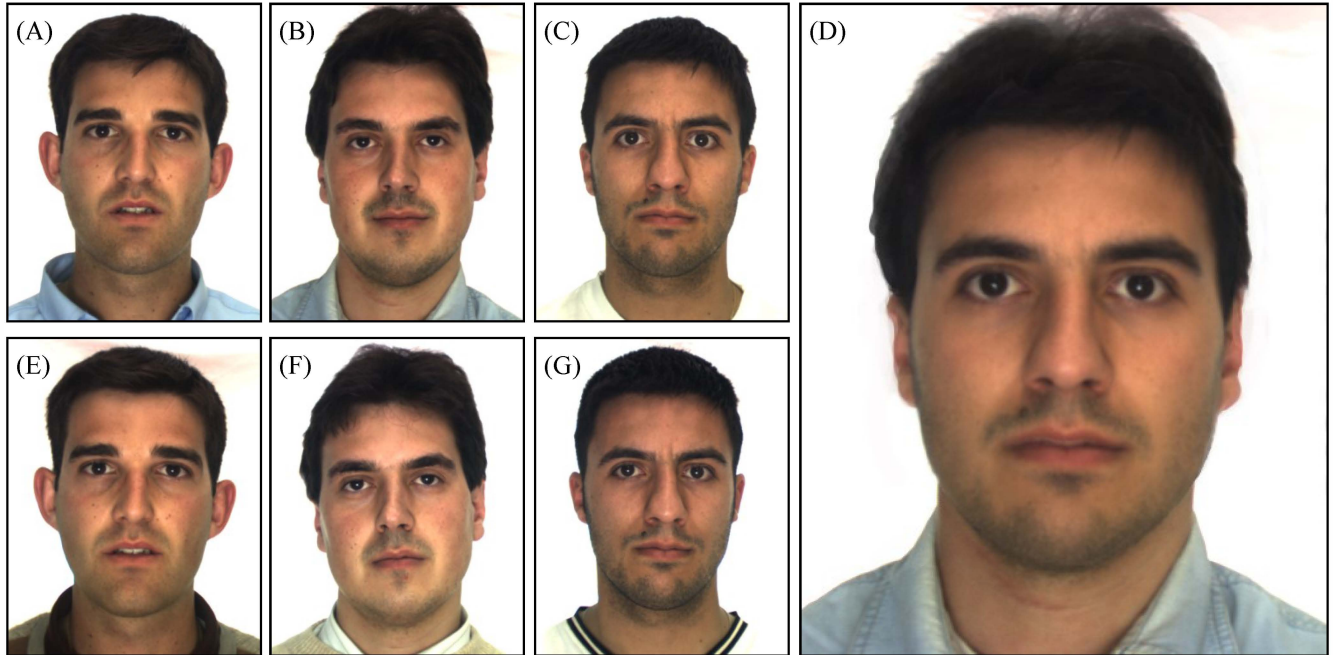


Figure 9: Example of morphed image generated using three men photos: the three images used for morphing (A, B and C), the resulting morphed face image (D) and the three images used for the matching test (E, F and G). In this example the subject in (C, G) is the applicant. The matching scores between test images (E, F, G) and the morphed one (D) are 51, 72 and 565 using VeryLookSDK and 0.99965, 0.99904 and 1.00000 using LuxandSDK.

## 5. Conclusion

The poor criminal nervously put the magic passport close to the scanner and looked at the camera trying to hide his hesitation. His heart jumped when the green light turned on: no more obstacles to the deserved holiday!

*The End*

## Acknowledgment

The work leading to these results has received funding from the European Community's Framework Programme (FP7/2007-2013) under grant agreement n° 284862.

## References

- [1] ICAO, "Biometric Deployment of Machine Readable Travel Documents," TAG MRTD/NTWG, May 2004.
- [2] ISO/IEC 19794-5, Information technology - Biometric data interchange formats - Part 5: Face image data, 2011.
- [3] M. Ferrara, A. Franco, D. Maio, and D. Maltoni, "Face Image Conformance to ISO/ICAO standards in Machine Readable Travel Documents," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1204-1213, August 2012.
- [4] M. Ferrara, A. Franco, D. Maltoni, and Y. Sun, "On the Impact of Alterations on Face Photo Recognition Accuracy," in *proceedings of the International Conference on Image Analysis and Processing (ICIAP2013)*, Naples, 2013, pp. 743-751.
- [5] FRONTEX - Research and Development Unit, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems," - v2.0, 2012.
- [6] IATA. (2014, July) Airport with Automated Border Control Systems. [Online]. <http://www.iata.org/whatwedo/stb/maps/Pages/passenger-facilitation.aspx>
- [7] Neurotechnology Inc. (2014, July) Neurotechnology Web Site. [Online]. <http://www.neurotechnology.com/>
- [8] Luxand Inc. (2014, July) Luxand Web Site. [Online]. <http://luxand.com>
- [9] FRONTEX. (2014, July) FRONTEX Web Site. [Online]. <http://frontex.europa.eu/>
- [10] Wikipedia. (2014, July) Morphing. [Online]. <http://en.wikipedia.org/wiki/Morphing>
- [11] GIMP. (2014, July) GNU Image Manipulation Program Web Site. [Online]. <http://www.gimp.org/>
- [12] GIMP. (2014, July) GIMP Animation Package. [Online]. <http://registry.gimp.org/node/18398>
- [13] A. M. Martinez and R. Benavente, "The AR face database," Computer Vision Center, CVC Technical Report 1998.