Received: 29 October 2020 | Revised: 16 April 2021 | Accepted: 21 May 2021

IET Biometrics

DOI: 10.1049/bme2.12047

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Preventing face morphing attacks by using legacy face images

Ilias Batskos | Florens F. de Wit | Luuk J. Spreeuwers | Raymond J. Veldhuis

Department of Computer Science, Data Management & Biometrics group, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands

Correspondence

Ilias Batskos, Faculty of Electrical Engineering, Mathematics and Computer Science, Department of Computer Science, Data Management & Biometrics group, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands.
Email: I.batskos@utwente.nl

Abstract

Countries allow citizens to upload a face image or provide printed copies to authorities to issue their passport. This allows prior image manipulation with criminal intent. A composite image can be created by blending the images of two individuals before submitting the composite image to the authorities. Depending on several factors, the submitted morphed face image can fool the issuing officer to issue a legitimate document. The document can then be successfully used by either contributor to attack the automatic Face Recognition Systems (FRS) operating, for example, at Automatic Border Control (ABC) airport gates. This is known as a Morphing Attack (MA), an identity sharing scheme with serious consequences. Here, the security vulnerabilities due to MAs are identified and analysed, and an additional security measure that allows mitigating the risk or preventing MAs in certain scenarios is proposed. The measure introduces more comparisons by keeping the old passport or ID card image in the chip, in passport renewal applications or first time passport applications, respectively. This approach is implemented with two FRSs on a challenging dataset and the dramatic decrease in the vulnerability is shown. Finally, their performance is compared with a state-of-the-art MA detection algorithm on the same dataset.

1 | INTRODUCTION

Face morphing is the process of creating a composite face image containing information from two different contributing subjects. Information refers to texture and geometry. The ratio of texture and geometry information is in favour of both contributors, and consequently the similarity with either one can be easily controlled using blending and warping factors, respectively (see Figure 1).

The images can be post-processed to cover morphing traces that are both visible and invisible to the naked eye (see Figures 2 and 3). Details regarding the morphing process can be found in Section.

In most EU member states, a passport applicant has to go to either a municipality, an embassy or a police station in person and present a recent face image in the form of a printed ICAO-compliant photograph. A morphed image can be submitted by a passport applicant as being a bona fide face image. The passport issuing officer who receives the printed morphed face image will have to compare and verify it against the applicant. Under the right circumstances, such a morphed face image would be convincing enough to fool the issuing officers into verifying its genuineness. Once included in the passport, it can be used by both morphing contributors to fool border control officers as well as automatic Face Recognition Systems (FRS) to verify identity with alarming success [1–3]. Morphing Attacks (MA) pose an obvious threat to border security and biometric identity verification. We will refer to the passport applicant as the accomplice and to the other morphing contributor as the criminal. A blacklisted criminal could successfully use an accomplice's passport with a morphed face image. The higher the similarity between criminal and accomplice, the more probable it is for their morphed face image to fool both human and FRS inspection [4, 5].

Other EU member states allow online passport applications that in certain cases require just filling in a form and uploading a digital face image. The uploaded image is then verified against already existing face images from a public services card or a driving licence image database by an officer and/or an FRS [6]. In some cases, the applicant may be called for an interview in person [7]. In the UK, besides verification of identity by an officer's comparison of the new digital image

FIGURE 1 The two contributors (left and right) and three morphs in between with texture and geometry contribution ratios of 70:30, 50:50 and 30:70, respectively

FIGURE 2 Post-processed morphed face images of two of our team members both with 50:50 texture and geometry contribution ratio

FIGURE 3 Post-processed morphed face images of two of our team members both with 30:70 texture and geometry contribution ratio in favor of the accomplice

to an old one, an applicant may be required to have a third person (neighbour, colleague, friend) confirm their identity [8].

The root of the morphing problem in the aforementioned application procedures is the policy that allows citizens to provide passport images that have no verifiable trusted source, which makes image manipulation possible. With no known trusted source, photographic verification of someone's identity performed by either humans or machines is error prone, especially with the advent of face morphing.

In Finland, most photographers can digitally sign and submit a passport photograph for the applicant in the police licence administration's photograph server, which is then compared with any earlier ones. If the officer responsible for processing the application is unable to verify that the photographs are of the same person, they will ask the applicant to come to the police station to be identified in person. This security measure does not prevent silicon mask, prosthetics or classic print/replay attacks from happening if the photographer is complicit or coerced [9].

Live enrolment in controlled environments such as police stations or municipalities is the solution to the morphing problem, as it reinstates trust in the system. In Cyprus, live enrolment is optional. In Norway, it is mandatory. Although live enrolment would render MAs irrelevant, universal adoption will be hard and slow due to political issues (policy-making), standardisation, and economic costs (printer/scanner/photo-booth manufacturers, photographers, new enrolment equipment). Live enrolment through secure mobile applications would be easier to implement as the vast majority of the population has access to camera equipped mobile phones and would prevent digital manipulation. However, the problem of silicone masks, prosthetics, or classic print/replay attacks mentioned above remains. Note that even after we transition to live enrolment, the problem will exist until all passports with images captured in uncontrolled environments expire. Thus, it is important to mitigate the risk during the transition time.

In terms of Morphing Attack Detection (MAD), the morphing process inherently leaves some detectable traces on the created photograph. They can be either visible for example double exposure artefacts known as ghost artefacts, colour and texture inconsistencies, or invisible to the naked eye, for example double compression artefacts [10], camera sensor pattern disruption [11], suppression of high frequency components [12]. The vast majority of detection methods in the literature is based on detecting these traces using image forensics techniques [10], image descriptors [13], deep features [14], and a variety of combinations and tailor-made heuristics to construct such features and classify an image as either bona fide or morphed. This kind of MAD is known as Single image MAD or SMAD. Other solutions make use of two images, usually a probe image of the passport holder captured at the gate and a reference image read from the passport chip and compare these two images for example using face similarity [15]. This kind of MAD is known as Differential MAD or DMAD.

Recent efforts to create MAD benchmarks [16, 17] are very important to estimate the magnitude of the threat by testing FRS vulnerabilities and current MAD algorithms' capabilities with a standardised way on a challenging range of realistic cases. Baseline results show that we are not quite close to satisfactory morphing detection with equal error rates ranging from 5% to 50% [16].

Due to the printing, scanning and heavy compression that a digital photograph undergoes before it is transferred to the passport chip, image degradation is so severe that it removes most, if not all texture-based features and hence their discriminatory power. This is evident from the considerable decrease in performance of detection methods when tested on printed and scanned databases [16–19]. Even though transitioning from printed and scanned to digital photographs would definitely make it a lot harder for a criminal to conceal all of the aforementioned morphing traces, it would not make it impossible. Amateur work with limited post-processing would be easily detected, but for each forensic technique a skilled actor could develop a counter-forensic one [11], and each detector whose feature space is known can be bypassed. Detection of morphing traces then becomes an arms race between researchers and criminals, in which the criminals are always one step ahead, because they have the opportunity to study published detection techniques and take counter measures to prevent detection. Under these circumstances, success or failure of detection depends mostly on the skill, time, knowledge and luck of the criminal rather than the effort of the researcher to detect it.

The use of additional biometric comparisons like fingerprints and/or iris patterns would definitely make presentation attacks a lot harder to achieve. Current passport chip technology provides this capability. However, it has been demonstrated that these too can be attacked [20] and universal implementation would be costly in economic (new equipment), efficiency (increased verification time and waiting queues) and political terms (privacy policies).

Proactivity and prevention are arguably the most fundamental aspects of security systems and practices. With this in mind, we propose a security measure to mitigate the risk of MAs in passport applications. More specifically, we propose to modify the passport enrolment process by keeping the old passport image of the applicant into the electronic passport chip besides uploading the newly submitted passport image. We will refer to the old passport image as legacy image. In other words, we are introducing a new comparison that benefits both FRSs and DMAD algorithms when the criminal attempts to use the passport at Automatic Border Control (ABC) gates that operate at airports for example. In case of first time passport applications, the legacy image will be the ID card image of the applicant.

In the following sections, we outline our methodology and show the significant effect of the approach on FRSs by testing a commercial FRS that currently operates at airports and an open source FRS with and without the measure and compare them to a state-of-the-art DMAD algorithm with a small but challenging dataset as a proof of concept. The approach can be adopted without major changes or disruption of current security practices, while affecting stakeholders' interests to a minimal extent. We argue that the measure will protect citizens from being targeted as potential morphing candidates, thus preventing criminals from succeeding. To the best of our knowledge, this is the first attempt that tries to motivate this enrolment and verification process modification as an MA counter-measure.

2 | METHODS

An MA is successful if the accomplice is verified against the morphed image at enrolment stage (AMA) and then the criminal is verified against the morphed image at the ABC stage (CMA). To evaluate the total risk of morphing attacks, we have to consider both security stages, enrolment and ABC, and both machine and human officers' detection capabilities. The latter is a complex task that needs to be investigated using properly designed tests, careful selection of participants, and realistic morphing attack scenarios. Human inspection usually takes place during the enrolment stage and at the ABC stage only when there is an FRS alert message or any other FRS problem. Experiments suggest that human morph detection capabilities are limited [1, 21]. In this paper, we do not evaluate human detection and thus we have to assume that our morphed images have successfully passed human inspection at the enrolment stage. Nonetheless, we use an FRS to replicate the enrolment stage verification by comparing a probe image of the accomplice to the morphed passport image. We then focus our experiments at ABC scenarios such as airport gates and only evaluate MAs in which the criminal attempts the attack (CMA, see Figure 4) given that the accomplice was successfully verified at enrolment stage by the same FRS. In other words, we evaluate Bona fide cases (Figure 5) and CMAs when the corresponding AMA was successful (see Figure 6).

We distinguish between first time passport applications and passport renewal applications and evaluate the effect of our method in these categories.

FIGURE 4 Example of a criminal morphing attack (CMA) with the ABC gate image of the criminal (left), the morphed new passport image (middle), and the legacy passport image of the accomplice (right)

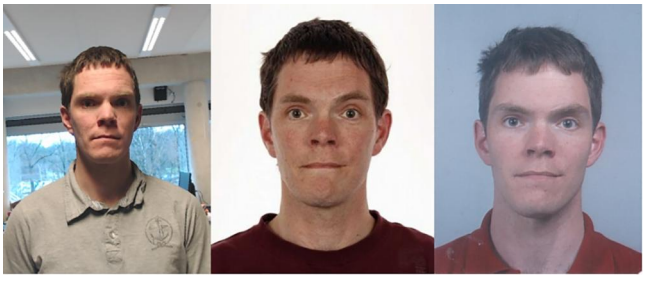

FIGURE 5 Example of a bona fide case with the ABC gate image (left), the new passport image (middle), and the legacy passport image (right)

FIGURE 6 Example of an accomplice morphing attack (AMA) of Figure 4 with the ABC gate image of the accomplice (left), the new morphed passport image (middle), and the legacy passport image of the accomplice (right)

2.1 | Passport renewal applications

A renewal requires that a passport already exists and that it either expires or it is lost. According to ICAO document 3903, part 9, section 4.1:

> Many States have a legacy database of facial images, captured as part of the digitised production of travel document photographs, which can be verified against new images for identity comparison purposes.

Previously used images are usually maintained in legacy databases until they are replaced with the new ones. Based on this, we propose to add a layer to the current security pipeline by using these legacy passport images in every passport renewal application. The enrolment process remains exactly the same, an applicant brings a recent face image to the issuing authority. The difference is that the legacy image is now kept together with the new passport image into the chip.

Current standards, technology (memory chip capacity), and infrastructure (operating FRSs) allow this legacy image to be stored in passport chips and accessed at an ABC gate without major modifications. Again, according to ICAO document 3903, part 9, section 5.1

> A State may use the storage capacity of the contactless IC in an eMRTD to expand the machine-readable data capacity of the eMRTD beyond that defined for global interchange. This can be for such purposes as providing machine readable access to breeder document information (e.g. birth certificate details), stored personal identity confirmation (biometrics) and/or document authenticity verification details.

This will allow the already employed FRS or a MAD algorithm at an ABC gate to do an additional comparison between the passport holder's ABC gate image and the legacy image. It requires minimal modification but has a significant effect. To evaluate the effect of the measure, we can further categorise citizens who apply for passport renewal into two categories. Citizens who have an expiring or lost passport with a bona fide face image and citizens who have an expiring or lost passport with an already morphed face image.

2.1.1 | Citizens with bona fide image passports

This category of citizens is arguably the overwhelming majority between the two and our primary concern. Our measure has a significant morphing preventive effect, which we will explain here and support with the results of our tests.

Let us assume that a potential criminal either targets or conspires with a citizen (potential morphing accomplice) with the purpose to use the morphed passport at an ABC gate. We assume that they create a decent morphed image, the accomplice applies for renewal and the passport is successfully issued. If the criminal would attempt to pass through an ABC gate, his/her gate image would have to match both the morphed new passport image and the legacy image, which is a bona fide image of the accomplice. Since they are two different people, the chances of a successful attack are quite low due to the new comparison, as they would have to be extremely similar in appearance (see Figure 4). Thus, the measure would render citizens who belong in this category terrible morphing candidates and would prevent them from either being targeted or conspiring for morphing. The vast majority of potential MAs are eliminated.

Passport validity periods is an issue that needs to be further examined. Countries usually issue passports with a validity period of five or 10 years. If we employ the new measure and set the new maximum passport validity period to 5 years, we will end up comparing probe and legacy images that might be 15 years apart for countries that have a current passport validity period of 10 years. This might increase false rejection rates (FRR) above accepted operational level. Comprehensive studies are limited due to scarce longitudinal face databases. Nonetheless, one such study indicates that the average subject can still be correctly verified at a false acceptance rate (FAR) of 0.01% across all 8 and 16 years of maximum elapsed time in the two face databases they used [22]. The same authors confirm this in a later study and infer that their FRS can verify 99% of the subjects at a false accept rate (FAR) of 0.01% for up to 8.5 years of elapsed time on one system and 10.5 on another. Beyond this time lapse of 8.5 years, there is a decrease in face recognition accuracy [23]. The images we acquired were read from currently valid ID documents. This is a limitation of our study as the capture time difference between the legacy and gate images of our cases is between 0 and 10 years instead of 10 and 15 years, which is required to examine FRR decrease. We will focus in such cases in future research.

2.1.2 | Citizens with morphed image passports

This category consists of citizens who have valid morphed image passports in circulation. Currently, we have no reliable

solution to detect MAs. It is likely that after a criminal successfully uses the morphed image passport to exit or enter a country, he/she will not continue to risk detection by continuing to use it for long, and the accomplice will declare the passport as lost and apply for renewal with a bona fide image. Our opportunity to detect the attack ends there. However, given our measure the morphed legacy image remains in the chip until the next renewal application. This might allow future detection with reliable MAD algorithms, if for example suspicion is raised after consecutive declarations of loss in a short period of time.

2.2 | First time passport applications

In every first time passport application, the legacy image can be the image of another valid ID document, preferably an ID card image. Most countries around the world require their citizens to have some form of identification, usually an ID card or a passport. According to a 2016 study commissioned and supervised by the European Parliament's Policy Department for citizens' rights and constitutional affairs, all EU member states except Denmark and Ireland have a national ID card. In 13 member states an ID card is mandatory and action for ID cards harmonisation is recommended [24]. A first time passport applicant is required to bring some kind of document that verifies identity. Thus, the only change in current procedures would be that the ID card image would be uploaded to the chip along with the new passport image. Arguably the primary motive for morphing is the ability to travel. Thus, it is unlikely for an ID card to be morphed, and if that were the case, our measure would have the same effect as in passport renewal applications. However, if an accomplice has a morphed ID card, the measure would not have an effect, besides providing MAD algorithms the additional comparison.

2.3 | Dataset creation

We have created a dataset based on 50 individuals. The dataset is a subset of a sequestered benchmark platform for MAD purposes [16] and thus cannot be shared. It contains the following images:

Enrolment images: We captured 2 bona fide images per individual using professional equipment. Photo ID Pro 8 was used to verify ICAO compliance. One of the images is used for morphing and the other one as the bona fide passport image.

Gate images: 10 bona fide face images per individual were captured with a mock ABC gate. They are used to verify that the passport holder is the rightful owner of the document. An example of a gate image can be seen in Figure 4 and the mock gate setup in the Appendix.

Chip images: Compressed face images stored on participants' identity documents (passport, ID, driving licence) were read and stored. These will be used as the legacy images.

Morphed face images: We created 25 exclusive pairs from the 50 individuals. Each of the two contributors can be put to the role of the criminal. Thus, we can have two morphed face images per pair with a single texture and geometry contribution ratio between criminal and accomplice as shown in Figures 2 and 3. We use a 50:50 and a 30:70 ratio in favour of the accomplice. The latter ratio is a realistic scenario, because it increases the issuance chance of the passport.

Enrolment and morphed images were printed and scanned using the standard pipeline used in the Netherlands to simulate real case scenarios. Details can be found in the Appendix.

Although our dataset is small, it satisfies our purpose which is to demonstrate the advantages of the proposed measure. We have made a lot of effort to select candidates that are quite similar in terms of appearance, age and ethnicity, thus creating morphing attacks that resemble those of the real world. The most important criterion for a successful morphing attack besides age, gender and ethnicity is similarity between the two subjects, accomplice and criminal. To this end, we did extensive search on a casting agency website and selected 50 individuals to construct our 25 pairs. A demographic overview of the selected subjects is shown in Table 1.

We consider an MA successful if the accomplice is verified against the morphed image at enrolment stage and if then the criminal is verified against the morphed image at ABC stage. We conduct our accomplice verification tests with two FRSs, Cognitec's Facevacs SDK V9.4.0, an FRS currently used at airports with the proposed matching similarity threshold of 0.50003 with operational level performance [25] and Dlib's open source FRS [26] which performed well in the LFW benchmark [27] with the default similarity (1-distance) threshold of 0.4 and the parameter number-of-jitters set to 3. We conduct the final tests only with the cases that passed the enrolment stage control as shown in Table 2.

TABLE 1 Demographics of selected subjects

Attribute	Attribute	Count
Gender	Value	
	Female	26
	Male	24
Age (years)	18–35	18
	36–55	21
	56–75	11
Ethnicity	African	19
	East Asian	6
	European	19
	Middle Eastern	6

TABLE 2 Enrolment stage verification results

Attribute	Total Count	Successful with FaceVacs	Successful with Dlib
Bonafide	50	50	50
AMA's with 70:30 ratio	50	50	50
AMA's with 50:50 ratio	50	50	49

Abbreviation: AMA, accomplice morphing attack.

2.4 | ABC stage test cases

Only one of our 50:50 cases did not pass the enrolment stage verification with the Dlib FRS. As mentioned before, we evaluate the effect of our measure only at the ABC stage when the criminal attempts the attack (CMA) given that the accomplice successfully attacked the enrolment stage (AMA). Bona fide and CMA cases are as follows:

Bona Fide cases: both the passport and the legacy images are bona fide. The passport holder at the ABC gate is the legitimate holder. We created 50 bona fide cases as in Figure 5. We randomly select one gate image as probe.

Criminal morphing attack cases (CMA): the passport image is a morphed image of the criminal and the accomplice. The legacy image is a bona fide image of the accomplice. The passport holder at the ABC gate is the criminal as in Figure 4. The number of CMA cases corresponds to the number of successful AMA cases from Table 2. We randomly select one gate image as probe.

2.5 | Testing protocol

We test both FRSs with and without the proposed measure. The ABC test workflows with and without the measure are shown in Figures 7 and 8, respectively. The FRS compares a gate image to the passport image, and returns an answer match, no match. Given our measure, we do an additional comparison between the legacy image and the gate image. Here, we consider a match only if both comparisons result in a match.

Additionally, we test a state-of-the-art MAD algorithm [19] available at [28] which performed well in [16] with both FRSs as its backbone. It is a demorphing-based solution which tries to reverse-engineer the morphing process and uncover the accomplice based on the morphed passport image and the passport holder's image captured at the ABC gate. After the standard FRS verification, the gate image is compared with the demorphed image. A match is considered only after both comparisons result in a match. Its workflow is shown in Figure 9. One disadvantage of the demorphing method is that in real case scenarios, we lack prior knowledge regarding the ratio of information of the morphing contributors that an attacker could have used. Here we used a ratio of 40:60 as the demorphing parameter for both 30:70 and 50:50 cases and provided STASM landmarks [29] to the algorithm.

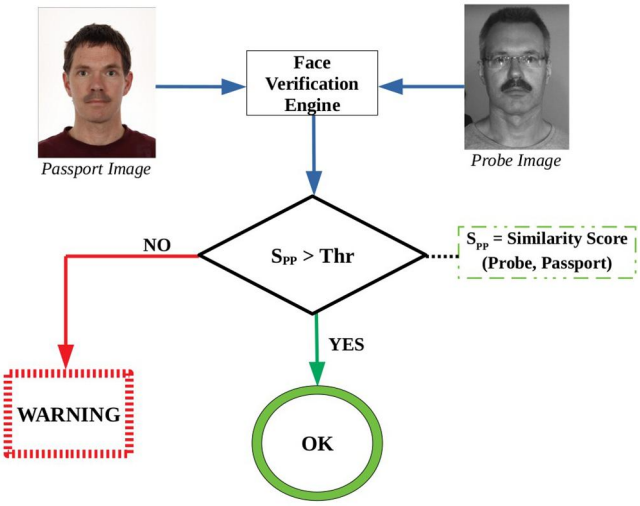

FIGURE 7 ABC test workflow of FRS without the measure

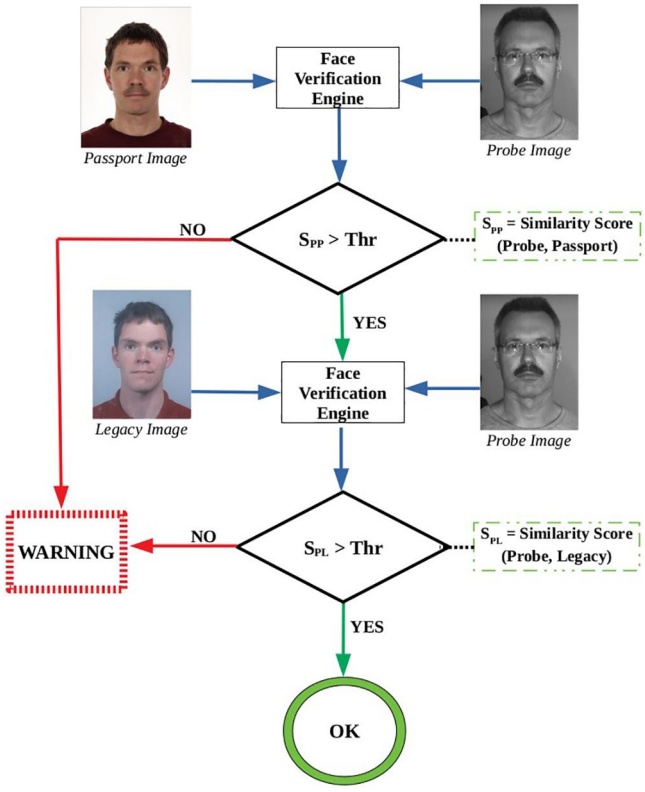

FIGURE 8 ABC test workflow of FRS with the measure

3 | RESULTS

To directly compare FRS and MAD performance, we use the standardised metrics of Attack Presentation Classification Error Rate (APCER) and Bona fide Presentation Classification Error Rate (BPCER) as defined in the International Standard ISO/IEC 30,107-3 [30]. APCER measures the proportion of MAs falsely classified as Bona fide and BPCER and the proportion of Bona fide cases falsely classified as MAs using the default threshold.

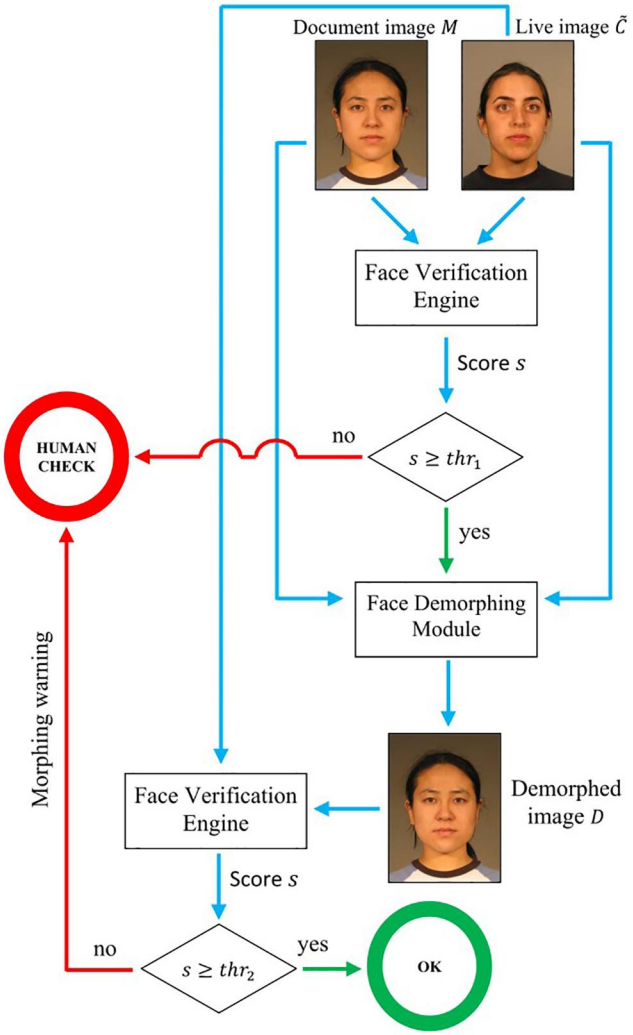

FIGURE 9 ABC test workflow of demorphing algorithm [19]

Additionally, we report the values of BPCER10, BPCER5, BPCER1 calculated from the detection error trade-off curves. BPCER10, measures the value of BPCER when APCER is equal to 10%. Accordingly, BPCER5 and BPCER1 measure BPCER when APCER equals 5% and 1%.

Results are shown in Tables 3, 4, 5 and 6. We observe from the results that 50:50 morphs (Tables 4 and 6) are harder to detect compared with 30:70 morphs (Tables 3 and 5) as expected. Except when we apply our measure in which case the morphing ratio is irrelevant because the final comparison is between the gate image and the legacy image which are the same in both 30:70 and 50:50 cases (the difference when using Dlib is due to 1 less case in the 50:50 set). This is another advantage of our approach. It is also obvious that Dlib's FRS performs far worse than FaceVacs, especially with the default threshold.

In Table 4, we observe an APCER of 4%, which means that two out of 50 morphed cases were falsely classified as bona fide even with our measure. These 2 cases consist of a pair of extremely similar looking siblings and should be considered very rare. In such cases, morphing might not even be necessary to fool an FRS.

TABLE 3 Results using FaceVacs as the FRS on 30:70 morphs

Workflow	APCER	BPCER	BPCER10	BPCER5	BPCER1
FRS only	24%	0%	0%	0%	8%
FRS + measure	4%	0%	0%	0%	2%
FRS + demorphing	4%	0%	0%	0%	12%

Abbreviations: APCER, attack presentation classification error rate; BPCER, bona fide presentation classification error rate; FRS, face recognition systems.

TABLE 4 Results using FaceVacs as the FRS on 50:50 morphs

Workflow	APCER	BPCER	BPCER10	BPCER5	BPCER1
FRS only	74%	0%	0%	10%	16%
FRS + measure	4%	0%	0%	0%	2%
FRS + demorphing	22%	0%	0%	0%	28%

Abbreviations: APCER, attack presentation classification error rate; BPCER, bona fide presentation classification error rate; FRS, face recognition systems.

TABLE 5 Results using Dlib as the FRS on 30:70 morphs

Workflow	APCER	BPCER	BPCER10	BPCER5	BPCER1
FRS only	64%	0%	4%	4%	24%
FRS + measure	38%	0%	4%	6%	8%
FRS + demorphing	30%	0%	2%	6%	56%

Abbreviations: APCER, attack presentation classification error rate; BPCER, bona fide presentation classification error rate; FRS, face recognition systems.

TABLE 6 Results using Dlib as the FRS on 50:50 morphs

Workflow	APCER	BPCER	BPCER10	BPCER5	BPCER1
FRS only	96%	0%	14%	24%	50%
FRS + measure	40%	0%	2%	2%	8%
FRS + demorphing	45%	0%	20%	22%	68%

Abbreviations: APCER, attack presentation classification error rate; BPCER, bona fide presentation classification error rate; FRS, face recognition systems.

Results also indicate that when moving the threshold to optimise the detection error trade-off, both FRSs without the measure are far from reaching operational levels on this dataset. The demorphing approach has good results on 30:70 morphs with both FRSs as its backbone, however, on 50:50 morphs, the most challenging set; it struggles with Dlib on all 3 metrics and with FaceVacs on BPCER1, which is the most important.

4 | DISCUSSION

We have demonstrated the effectiveness of our approach. The approach is not a MAD in the strict sense. It is an enrolment and verification processes modification that acts as

a morphing preventive measure by utilising a bona fide legacy image of a citizen and thus leaving little chance for MA success. The results of the approach are to be expected. This is the very reason we consider it. It is quite straight forward and can be easily implemented and tested with any operational FRS. We cannot overcome cases of extreme 'lookalikes' (e.g. siblings like the two cases in our dataset) with our approach, however in such cases morphing might not be necessary. The 'lookalikes' problem at ABC gates–potentially including the face mask problem (liveness/skin detection) - is generally easier to tackle. Current FRSs operate with <5% False Rejection Rate at 0.1% False Acceptance Rate, and human officers can perform quite well in liveness/skin detection with close inspection.

Regarding privacy, there should be no additional concerns, since passport face image verification is already accepted worldwide. A rational and comprehensive explanation of the new step should suffice to satisfy privacy rights advocates' scepticism.

The new comparison would theoretically double the time of passenger verification, but with significantly increased detection performance in return. It would also double the necessary storage capacity of legacy databases. However, considering rapid technological advancements, the aforementioned disadvantages will be quickly mitigated.

Passport producers, who in many cases are also FRS vendors, have to coordinate with governments and make all necessary adjustments, namely upload the legacy image to the chip and modify ABC gate software to enable the new comparison. However, this does not mean adding infrastructure or changing the whole architecture and pipeline, but rather adapting it, which is quite straightforward. FRS software updates are not uncommon.

Although universal adoption of such a measure is always hard, countries that will adopt it automatically mitigate their internal MA risk, protect their citizens and strengthen their passport documents' security level.

With the two aforementioned modifications, namely the use of legacy images and the restriction of the document's validity period to 5 years, there is still a way that someone could successfully attack an FRS with a morphed image passport. This could happen if an accomplice applied for a passport with a morphed face image, declared it lost without the criminal ever using it and then re-applied with another morphed face image. That would result in both the legacy and the new passport images being morphed. To solve this last issue, when someone declares a loss and re-applies for a passport while the lost passport is still within its validity period, the re-issued passport should contain the same images as the lost one. That way the bona fide legacy image would remain in the passport for the rest of the validity period.

5 | CONCLUSION

Our measure protects citizens that currently have bona fide passports as well as citizens who do not have a passport but have a bona fide ID card from being targeted as potential morphing candidates in the future. The possibility of a successful MA for these categories of citizens becomes quite low as explained in Section 2 and shown in Section 3. In other words, we limit the options of potential criminals to find proper morphing candidates. To the best of our knowledge, this is the first time in which the use of legacy images to mitigate the risk of MAs is proposed and investigated.

Additionally, keeping legacy images which are currently discarded extends MAD capabilities. It enables more than one comparisons and provides the possibility to detect morphed passports in circulation in the future when MAD algorithms mature and become more effective.

It should be clear that bold and urgent policy actions are needed to overcome this threat, especially while some EU member states provide the ability to non-EU citizens to purchase EU passports, and the refugee crisis is more relevant than ever. The proposed solution is a good compromise between all involved parties until global live enrolment in controlled environments becomes a reality or another effective and easily applicable measure emerges. Until then, we need to take steps towards mitigating the risk of potential attacks. We believe our approach is a step in that direction.

ACKNOWLEDGEMENTS

We would like to thank the University of Bologna for conducting the tests on their benchmarking platform and providing us with the results and Cognitec Systems GmbH. for supporting our research by providing the FaceVACS SDK V9.4.0 software. Results obtained for FaceVACS SDK V9.4.0 should not be construed as a vendor's maximum effort full-capability result.

ORCID

Ilias Batskos https://orcid.org/0000-0002-3389-0535

REFERENCES

1. Robertson, D.J., Kramer, R.S.S., Burton, A.M.: Fraudulent ID using face morphs: Experiments on human and automatic recognition. PLoS ONE, 12(3), e0173319, (2017). https://doi.org/10.1371/journal.pone.0173319
2. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE International Joint Conference on Biometrics, pp. 1–7. IEEE, Clearwater (2014). https://doi.org/10.1007/978-3-319-28501-6_9
3. Ferrara, M., Franco, A., Maltoni, D.: On the effects of image alterations on face recognition accuracy, In Bourlai, T. (Ed.): Face Recognition Across the Imaging Spectrum. Springer International Publishing, pp. 195–222. (2016). https://doi.org/10.1007/978-3-319-28501-6_9
4. Scherhag, U., et al.: Face recognition systems under morphing attacks: a survey, IEEE Access, 7, pp. 23012–23026. (2019). https://doi.org/10.1109/ACCESS.2019.2899367
5. Damer, N., et al.: To detect or not to detect: The right faces to morph. In: 2019 International Conference on Biometrics (ICB), pp. 1–8. IEEE, Crete (2019). https://doi.org/10.1109/ICB45273.2019.8987316
6. Online FAQs - Department of Foreign affairs, https://www.dfa.ie/passportonline/onlinefaqs/. Accessed July 2020
7. Poliisi - more information on applying for a passport, https://www.poliisi.fi/passport/more/information_on_applying_for_a4_passport. Accessed July 2020
8. Confirming someone's identity: how to confirm someone's identity – apply for a passport – GOV.UK, https://www.passport.service.gov.uk/help/confirming-identity/how-to-confirm-identity. Accessed July 2020

9. Bhattacharjee, S., Mohammadi, A., Marcel, S.: Spoofing deep face recognition with custom silicone masks. In: 2018 IEEE 9th International Conference on Biometrics Theory, Applications And Systems (BTAS), pp. 1–7. IEEE, Redondo Beach (2018). https://doi.org/10.1109/BTAS.2018.8698550
10. Makrushin, A., Neubert, T., Dittmann, J.: Automatic generation and detection of visually faultless facial morphs. In: Proceedings of the 12th International Joint Conference on Computer vision, imaging and Computer Graphics theory and applications, pp. 39–50. SCITEPRESS - Science and Technology Publications, Porto (2017). https://doi.org/10.5220/0006131100390050
11. Scherhag, U., et al.: Detection of face morphing attacks based on PRNU analysis, IEEE Trans. Biom. Behav. Identity Sci. 1(4), 302–317. (2019). https://doi.org/10.1109/TBIOM.2019.2942395
12. Spreeuwers, L., Schils, M., Veldhuis, R.: Towards robust evaluation of face morphing detection. In: 2018 26th European Signal Processing Conference (EUSIPCO), pp. 1027–1031. IEEE, Rome (2018). https://doi.org/10.23919/EUSIPCO.2018.8553018
13. Scherhag, U., Rathgeb, C., Busch, C.: Morph deterction from single face image: a multi-algorithm fusion approach. In: Proceedings of the 2018 2nd International Conference on Biometric Engineering And Applications - ICBEA '18', pp. 6–12. ACM Press, New York (2018). https://doi.org/10.1145/3230820.3230822
14. Seibold, C., et al.: Detection of face morphing attacks by deep learning, In Kraetzer, C. et al. (Eds.): Digital Forensics and Watermarking. Springer International Publishing, pp. 107–120. (2017). https://doi.org/10.1007/978-3-319-64185-0_9
15. Wandzik, L., Kaeding, G., Garcia, R.V.: Morphing detection using a general- purpose face recognition system. In: 2018 26th European Signal Processing Conference (EUSIPCO)' 2018 26th European Signal Processing Conference (EUSIPCO), pp. 1012–1016. IEEE, Rome (2018). https://doi.org/10.23919/EUSIPCO.2018.8553375
16. Raja, K., et al.: Morphing attack detection - database, evaluation platform and benchmarking.IEEE Transactions on Information Forensics and Security, pp. 1–1, (2020). https://doi.org/10.1109/TIFS.2020.3035252
17. FRVT MORPH, https://pages.nist.gov/frvt/html/frvt_morph.html. Accessed July 2020
18. Ferrara, M., Franco, A., Maltoni, D.: Face morphing detection in the presence of printing/scanning and heterogeneous image sources. University of Bologna, (2019). https://doi.org/10.1049/bme2.12021
19. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing, IEEE Trans. Inform.Forensic Secur. 13(4), pp. 1008–1017. (2018). https://doi.org/10.1109/TIFS.2017.2777340
20. Kolberg, J., et al.: Presentation attack detection for finger recognition, In Uhl, A. et al. (Eds.): Handbook of Vascular Biometrics. Springer International Publishing, pp. 435–463. (2020). https://doi.org/10.3390/s18082601
21. Kramer, R.S.S., et al.: 'Face morphing attacks: investigating detection with humansand computers'Cogn. Research, 4(1), p. 28, (2019). https://doi.org/10.1186/s41235-019-0181-4
22. Best-Rowden, L., Jain, A.K.: Longitudinal study of automatic face recognition, IEEE Trans Pattern Anal Mach Intell, 40(1), pp. 148–162. (2018). https://doi.org/10.1109/TPAMI.2017.2652466
23. Deb, D., Best-Rowden, L., Jain, A.K.: Face recognition performance under ageing. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 548–556. IEEE, Honolulu (2017). https://doi.org/10.1109/CVPRW.2017.82
24. Adamis-Csaszar, K., et al.: The legal and political context for setting up a European identity document, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/556957/IPOL_STU(2016)556957_EN.pdf. Accessed July 2020
25. Frontex, Best practice operational Guidelines for automated border control (ABC) systems, http://op.europa.eu/en/publication-detail/-/publication/e81d082d-20a8-11e6-86d0-01aa75ed71a1/language-en/. Accessed July 2020
26. Dlib C++ Library. http://dlib.net/. Accessed March 2021
27. LFW: Results. http://viswww.cs.umass.edu/lfw/results.html. Accessed March 2021
28. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing Tool. http://biolab.csr.unibo.it/facedemorphingtools.html. Accessed March 2021
29. Milborrow, S., Bishop, T.E., Nicolls, F.: Multiview active shape models with SIFT descriptors for the 300-W face landmark challenge. In: 2013 IEEE International Conference on Computer Vision Workshops, pp. 378–385. Sydney (2013). https://doi.org/10.1109/ICCVW.2013.57
30. ISO/IEC 30107-3: Information technology — biometric presentation attack detection — Part 3: testing and reporting. (2017)
31. Pérez, P., Gangnet, M., Blake, A.: Poisson image editing. ACM Transactions on Graphics. 22(3), 313–318 (2003). http://dx.doi.org/10.1145/882262.882269
32. GIMP, https://www.gimp.org/. Accessed July 2020

How to cite this article: Batskos, I., et al.: Preventing face morphing attacks by using legacy face images. IET Biome. 10(4), 430–440 (2021). https://doi.org/10.1049/bme2.12047

APPENDIX

The printing, scanning and compressing pipeline is shown in Table A.1. The mock ABC gate setup and the enrolment image acquisition setup are shown in Figures A.1 and A.2 respectively.

We use the SOTA morphing pipeline that we created for [16]. First, locations of corresponding facial landmarks are automatically extracted from the two contributing faces using STASM [29], and averaged to create the morphed face landmarks as shown in Figure A.3.

Next, Delaunay triangles are created using these average landmarks, the vertices of which are used to create corresponding triangles on the contributors' faces. Corresponding contributors' triangles and their content are then warped using affine transformation functions to take the shape of the target triangle as in Figure A.4.

Finally, the content of corresponding triangles is overlaid to create the morphed face image in Figure A.5.

To avoid double exposure (ghost) artefacts as seen in Figure A.5, the facial region is transferred automatically to both contributors' background. To overcome colour, illumination and texture inconsistencies between the transferred facial region and the background, we use generic interpolation machinery based on solving Poisson equations for seamless editing of image regions [31]. The two resulting morphed images are manually retouched with GIMP [32] to conceal any other obvious traces.

TABLE A.1 Official print, scan and compress steps that a passport image undergoes in the Netherlands

#	Process
1	Print with printer Dmb DS-RX1HS at 300 x 300 dpi, matte
2	Scan using Epson V600 at 300 dpi
3	Crop to 413 x 531 pixels
4	Compress using JPEG2000, max file size = 15kb, RGB 24 BIT

FIGURE A.1 Mock ABC gate setup

FIGURE A.2 Enrolment image acquisition setup

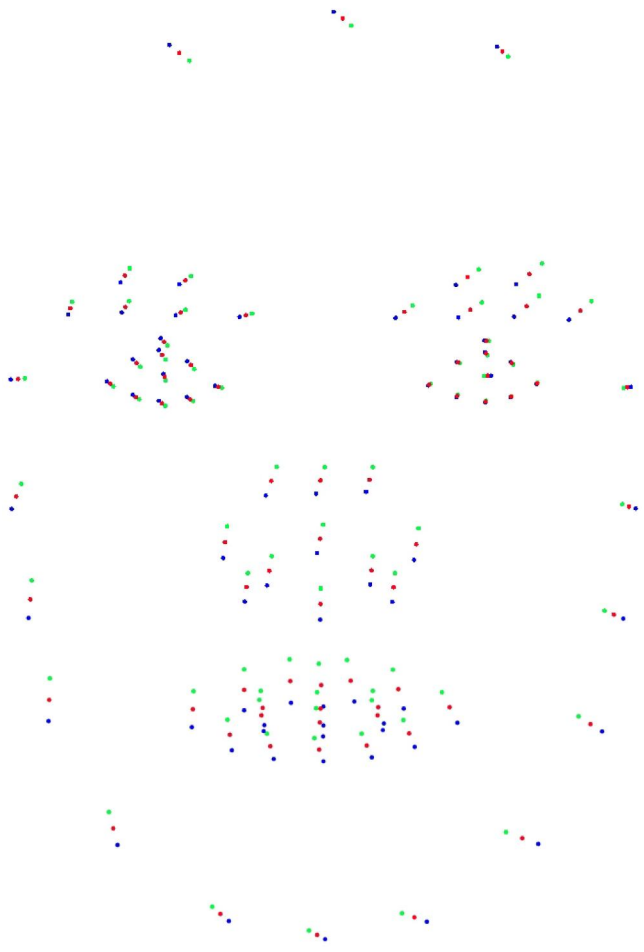

FIGURE A.3 The average landmarks with red colour and contributors' landmarks with green and blue colour

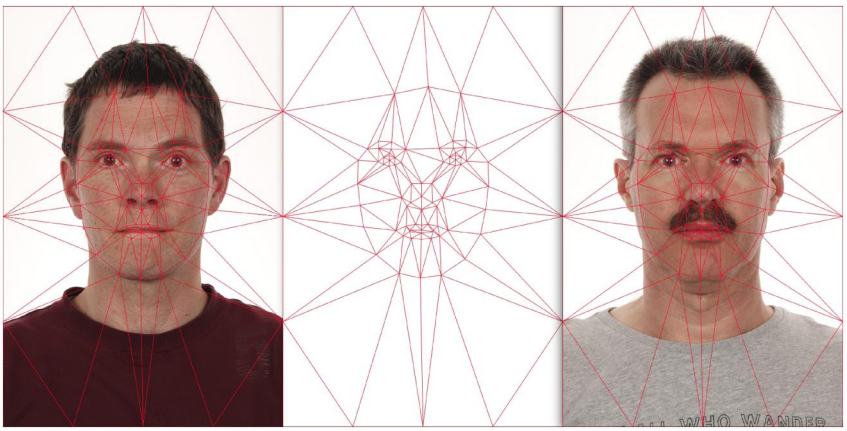

FIGURE A.4 Two contributors (left and right) adapted to the average face geometry (middle)

FIGURE A.5 Morphed face image without post-processing