# Face Morphing Versus Face Averaging: Vulnerability and Detection

R. Raghavendra Kiran B. Raja Sushma Venkatesh Christoph Busch [*]
Norwegian Biometrics Laboratory, NTNU, 2802 Gjøvik, Norway
Email: {raghavendra.ramachandra; kiran.raja; sushma.venkatesh; christoph.busch} @ntnu.no

## Abstract

*The Face Recognition System (FRS) is known to be vulnerable to the attacks using the morphed face. As the use of face characteristics are mandatory in the electronic passport (ePass), morphing attacks have raised the potential concerns in the border security. In this paper, we analyze the vulnerability of the FRS to the new attack performed using the averaged face. The averaged face is generated by simple pixel level averaging of two face images corresponding to two different subjects. We benchmark the vulnerability of the commercial FRS to both conventional morphing and averaging based face attacks. We further propose a novel algorithm based on the collaborative representation of the micro-texture features that are extracted from the colour space to reliably detect both morphed and averaged face attacks on the FRS. Extensive experiments are carried out on the newly constructed morphed and averaged face image database with* 163 *subjects. The database is built by considering the real-life scenario of the passport issuance that typically accepts the printed passport photo from the applicant that is further scanned and stored in the ePass. Thus, the newly constructed database is built to have the print-scanned bonafide, morphed and averaged face samples. The obtained results have demonstrated the improved performance of the proposed scheme on print-scanned morphed and averaged face database.*

## 1. Introduction

Face is one of the preferred biometric characteristics which is widely used in various applications for securing physical and logical access, border control, national identity card management, forensics identification among many others. Amongst all the applications, the most prevalent and important application corresponds to border control scenario in which the face characteristics are stored in the electronic passports (ePass) to establish the identity of the owner of ePass and also to verify the subject against the claimed identity through ePass. In the recent advancements of border control applications, Automatic Border Control (ABC) gates are designed to read the photos stored in the ePass to verify the identity of the subjects. The International Civil Aviation Organisation (ICAO) has laid the guidelines to use the face image from passport as mandatory mode of identity verification through Machine Readable Travel Document (MRTD) [12] due to which there are more than 800 million ePass instances from past ten years [9].

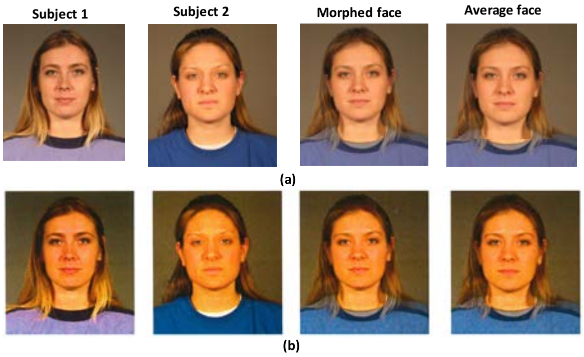


Figure 1: Example of face morphing and face averaging (a) digital version (b) print-scanned version

Most recently, the vulnerability of the ePass was identified by exploiting the loophole in the passport application and issuance protocol (or procedure) [7]. Specifically, owing to the fact that many countries issue or renew the ePass solely on the basis of photo provided by the applicant, it has to be noted that the applicant may obtain the passport by providing a photo of his vested interest. In order to leverage the shortcoming of passport issuance, the person with vested interest can morph his/her face image with another subject such that the submitted face image in passport can match to both the subjects used for morphing. To realize such morphing attacks, two different face images are considered which are geometrically aligned followed by mixing the image characteristics and correcting the color artefacts by photometric correction to generate a new morphed image that resembles characteristics of both constituent faces

[*] This work is carried out under the funding of the Research Council of Norway (Grant No. IKTPLUSS 248030/O70).

visually. The quality of the generated morphed face image is sufficient enough to challenge the human observers (including border guards) in mapping the morphed image to single constituent face image which was exemplified with experimental evaluation in earlier works [8] [21].

The failure of human observers in identifying such attacks puts the biometric systems operating in automatic manner into implicit risks towards morphing attacks. Thus, it is essential to detect such attacks to maintain the reliability and integrity of the biometric systems. In this regard, the automatic detection of the morphed face images is gaining popularity in the biometric community. Despite the severity of the problem, there exist limited works towards solving morphing attacks and they can be broadly classified in two categories: (1) **Morphed Face Image Detection in Digital Version:** In these set of works, morphed images (produced by combining two images) in digital version is presented to the system and correspondingly, the morph attack is detected through the use of pixel level information. The problem is highly relevant for the countries like New-Zealand, Ireland and Estonia who use the digital photograph to renew the passport which serves as a vulnerable point to use morphed image instead of actual face image. (2) **Print-Scanned Morphed Face Image Detection:** This scenario maps to the most prevalently used practices of passport issuance across many countries. In this scenario, the printed photo provided by applicant is scanned and stored in the ePass. The possibility of presenting the printed image provides a vulnerable point to submit a morphed image by the applicant. However, under this practice, it should be noted that the soft (pixel-level) information about morphing (unlike in digital version) is completely lost in the process of printing and scanning. The loss of soft information coupled with the introduction of other information due to print-scan process (such as noise, scan lines) increases the magnitude of challenge in detecting the morphed image where the real image and morphed image look highly similar.

Figure 1 illustrates the example of the digital (see Figure 1 (a)) and print-scanned version of morphed as shown Figure 1 (b). It can be evidently seen that, the quality of the print-scanned images are not only degraded but also the effects of morphing is less visible when compared to that of the digital version. Thus, the externally introduced noise due to the print and scan process make it challenging to detect the print-scanned morphed face images.

Further, most of the work reported in the literature are focused on detecting the morphed image straight-away in the digital domain. The first work [20] in this direction has explored the texture based features using Local Binary Patterns (LBP), Binarised Statistical Image Features (BSIF), Image Gradient magnitude (IG) and Local Phase Quantitation (LPQ) to detect the morphed face images automatically in the digital domain. Recently, the intrinsic characteristics of images in digital domain were explored by analysing the Benford features where the quantized DCT coefficients of JPEG compressed face images showed significant differences in morphed image and bonafide image in digital format[18]. The intrinsic features have indicated substantially good results in detecting the morphed face images as the data in the digital format keeps the effect of pixel alteration due to morphing process intact. Further, same work is extended [11] to detect the morphed face images that are degraded using the *stirTrace* technique to simulate the possible effects of print-scan procedure. The results indicated in [11] show the degraded performance of the intrinsic features in detecting the morphed face images after *stirTrace* process. In the similar manner, another work evaluated the severity in real-practice by printing and scanning the morphed face images [22]. In their work, they presented bonafide and the morphed image after print-scan process to the commercial-off-the-shelf (Neurotechnology [6]) system and the experiments indicated the fragile nature of face recognition systems which verified the morphed face image to both contributing images of morph image. Similar tendency, was observed in non-commercial (Open-face [4]) face recognition software which was found vulnerable to print-scanned morphed face images. It has to be noted that, the baseline evaluation carried out using micro-texture based features have reported high error rates in detecting the print-scanned morphed face images despite the fact that face images used in their work was gray-scale only and further, the images were upscaled and adjusted to match ICAO standards from already processed images [22]. Such cases of using the morphed gray-scale images do not correspond to realistic use case of face images in passport which is a shortcoming to deduce any conclusions.

### 1.1. Our contributions

Identifying the shortcomings from existing works, it can be noted that the use of intrinsic image features can be useful to detect the digitally morphed face images but fails to detect morphing after print-scan process due to the noise introduced in the process of printing and scanning. The vulnerability of the face recognition systems was further evaluated by non-standard face data printed and scanned in gray-scale. However, in the real case, the face images stored on the passport after print-scan process are expected to be ICAO compliant color image. Thus, it is very essential to employ the ICAO compliant face images in color format to evaluate the full spectrum of the problem. In this work, we present systematic study to demonstrate the vulnerability of face recognition systems resembling real-life scenario (passport issuance). To this extent, we have constructed a new print-scanned morphed face database from 163 unique subjects (derived from high quality FRGCv2.0 database [19]). We then generated the morphed face images using a conventional morphing technique coupled with region bounded refinement (henceforth referred as *Morphed Image*, refer Section 2.2). Further, to assess the vulnerability of the face recognition systems towards such attacks, we also create a corresponding image dataset simply by averaging the images based on facial landmarks (henceforth referred as *Averaged Image*). A realistic quality averaged images are demonstrated in the last row of Figure 1. The vulnerability analysis is therefore presented on both morphed and averaged image set using a commercial face recognition software by Cognitec [2] following the real-life scenario. Further, we propose a novel scheme for detecting both morphed and averaged face images by exploring the collaborative representation of the micro-texture features in different colour spaces. Thus, following are the main contributions of this paper:

- Presents the analysis of simple averaging based attacks on face recognition system to establish the vulnerability of biometric systems as compared to attacks using complex and conventional face morphing technique. To the best of our knowledge, this is the first work to demonstrate the vulnerability of face recognition systems towards simple averaged images.

- A novel algorithm is presented to detect the morphed and averaged images by leveraging the collaborative representation of micro-texture features and deriving the information from different color spaces to detect print-scanned images generated using both conventional morphing and averaging technique. This is the first work to show the significance of using color spaces to detect such attacks and can be easily adapted in the real-life passport issuance procedure.

- Introducing a new print-scanned morphed face images' dataset that has 1000 bonafide images, 1423 morphed face images and corresponding 1423 averaged face images generated from 163 unique subjects to mimic the most realistic scenario of high quality attack image generation. To the best of our knowledge, this is the largest database created to evaluate the print-scanned morphing attacks on face recognition systems with two different attacks (morphed and averaged).

- Extensive experiments are carried out and presented systematically along with the arguments and motivation for analysing the vulnerability. Correspondingly, the motivation for attack detection mechanism is presented with justifying results to indicate the applicability of proposed approach.

The rest of the paper is organised as follows: Section 2 describes the new database construction, Section 3 describes the proposed method to detect the print-scanned attack images. Section 4 presents the experimental results of the proposed scheme and vulnerability analysis using newly constructed database. Section 5 draws the conclusion and lists out the key remarks.

## 2. Database construction

In many of the existing passport issuance system, the enrolment images are obtained from the subjects by scanning the printed picture for passport. The picture submitted by any person is further scanned, digitized and stored in the memory chip on the epassport which is used for identifying the subject in subsequent authentication attempts. Motivated by the severity of the problem in detecting the morph/average images in a real-life operating scenario, we have created a new database of morphed and averaged images in this work. The newly created Morph and Averaged Face Image (MAFI) database consists of face images from FRGC v2.0 face database. The MAFI database derived from FRGC v2.0 consists of subset of 163 unique subjects whose images are captured in multiple sessions. The subset of face images from 163 unique subjects is chosen carefully to have the ideal quality images for creating the morph images and has a gender distribution of 52 female subjects and 111 male subjects. Further, the image set are divided in three disjoint subsets corresponding to development set, training set and testing set which consist of 23, 70 and 70 subjects correspondingly. The exact distribution of the MAFI database is presented in the Table 1. Figure 2 presents the schematic of database creation in-lines with the ICAO standards and sequence of steps involved are discussed in the following subsections.

Table 1: Summary of database distribution.

| | Development Set | Training Set | Testing Set |
|---|---|---|---|
| Total | 23 | 70 | 70 |
| Male | 16 | 50 | 45 |
| Female | 7 | 20 | 25 |

### 2.1. Bonafide Image Database

In order to generate the high quality images meeting the specification standards recommended by ICAO used in passport application, we perform a series of operations as indicated below. In the first step, high quality images with high resolution from a set of images corresponding to a subject from MAFI database is considered. The image generally consists of uniformly illuminated background, face and parts of the upper torso. However, the passport quality picture must contain the facial image with a minimal amount of neck and torso, specifically in a upright position. Thus, we first normalize the face image to correct any tilt and rotation

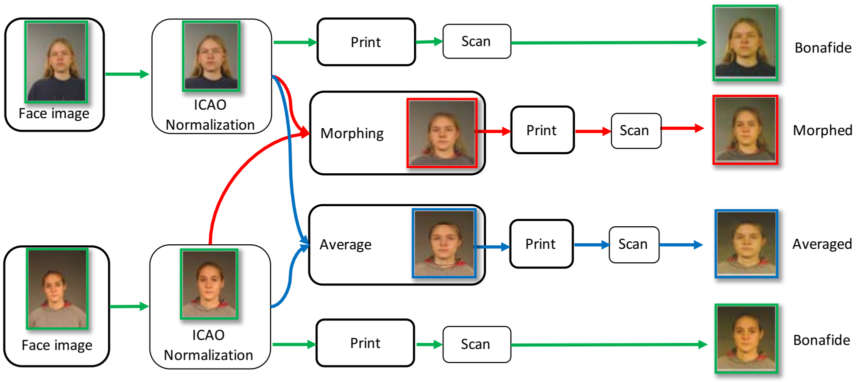


Figure 2: Detailed illustration of database generation; The path illustrated by green arrow indicates the generation of bonafide images (green border), path indicated by red arrow indicates morphed image (red border) and path indicated by blue color indicates the averaged image (blue border).

in the head to meet the requirements of ICAO. Further, the passport image quality as recommended by ICAO should have a between-eye distance of $> 120$ pixels [13]. In-order to comply to such standards, we crop the rotation normalized image and scale it to have the recommended between-eye distance manually. Thus, the set of all the high quality digital images are transformed to ICAO compliant passport quality image carefully. Further, to simulate the process of passport-issuance, we print the digital image and scan it to create the enrolment database. To produce the realistic use case, we followed the guidelines of ISO/IEC 19794-5 [16] that recommends the deployment of face biometrics in the electronic passport in which a facial image is to be scanned with $300dpi$. We employed the high-quality laserjet printer *RICOH MPC 6003 SP* to print the images using high quality photo paper with $300gms$ density. We then scan the printed passport photo using a photo-quality scanner from *HP Photosmart 5520* at $300dpi$ as recommended by ICAO [14]. The entire sequence of the steps involved in creating the high quality images for bonafide set are indicated using the green colored arrow as shown in Figure 2.

In this subset of bonafide images, there are approximately $5-6$ images per subject (total subjects - 163) which result in a total number of 1000 bonafide images. From the set of $5-6$ images per subject, we consider one image for generating the morph and average image, and another image for assessing the vulnerability of the face recognition systems. Rest of the $3-4$ images per subject are used for evaluation of the proposed technique.

## 2.2. Morphed and Average Image Database

In order to create a morphed or averaged image database, we consider high quality images from the set of processed (ICAO compliant) images as mentioned in the previous subsection.

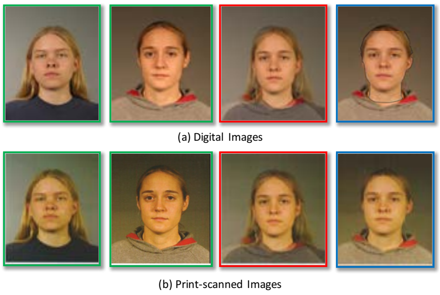
- To retain the disjoint nature of database as mentioned in Table 1, the morphed and averaged face images are created pertaining to each partition of development, training and testing.
- Within each partition, we further divide the set into gender based sub-sets to map the realistic use case of morphing.
- For each gender subset, we create morphed and averaged face images by carefully morphing every subject with 4 random subjects.
- To generate high quality morph images, we obtain the facial landmarks to align composite images contributing to generate the morphed image such that there are no geometric misalignment.
- With the help of facial landmark points of both contributing images, we create a morphed image using triangulation based tight morphing [3]. In the similar manner, we also create another image corresponding to two contributing images using a simple principle of averaging [1].
- In compliance with ISO standards [15], we remove the high frequency components from the images using a Gaussian filter.
- Finally, generated morphed and averaged face images are printed using the high-quality laser jet printer *RICOH MPC 6003 SP* on a high-quality photo paper with $300gms$ density. The printed passport photo is further scanned using a photo-quality scanner from *HP Photosmart 5520* at 300dpi. Note that, same printer, same

print quality paper and same scanner with 300dpi is used to generate all print-scanned version of *bonafide, averaged* and *morphed* face images.

Table 2: Summary of Morphed and Averaged images from MAFI database.

| | Development Set | Training Set | Testing Set |
|---|---|---|---|
| Morphed | 150 | 693 | 580 |
| Average | 150 | 693 | 580 |

The total number of morphed images in this work amounts to 1423 images of which the development set consists of 150 images, training set consists of 693 images and testing set consists of 580 images. Further, the averaged image set also have similar number of images and the complete distribution is provided in Table 2.


(a) Digital Images

(b) Print-scanned Images

Figure 3: Sample images from the new database; (a) corresponds to digital images and (b) corresponds to images obtained after printing and scanning. The images in green border indicate the bonafide images of two subjects, images with red border indicates morphed image and images with blue border indicate the averaged image.

Figure 3 illustrates the sample images in the MAFI database. The images in the top row of Figure 3(a) demonstrates the digital images and Figure 3(b) demonstrates the print-scanned version of the same images. It has to be noted that the images with green border indicate the bonafide images, images with red border indicate the morphed images and images with blue color indicate the averaged images (Also refer Fig.2). In this work, we have used the images as indicated in Figure 3(b), i.e., print-scanned images for rest of the experiments to simulate the realistic use-case of detecting attacks on passport face systems.

## 3. Proposed Method

Figure 4 shows the block diagram of the proposed attack detection on the face recognition scheme based on the collaborative representation of the micro-texture information extracted from two different colour spaces. As the process of printing and scanning of the digital photos result in multi-level distortions modifying the intensity component of the image, it is our assertion that the use of colour space, especially HSV and YCbCr space can separate the intensity components from colour components on which the micro-texture features can reveal the morphing and averaging face artefacts.

Figure 5 illustrates the individual color channel's output corresponding to HSV and YCbCr space employed in this work. Figure 5 (a) provides the example of color channel output corresponding to bonafide (print-scanned ) and Figure 5 (b) illustrates the color channel output corresponding to morphed face image (print-scanned). Similarly, Figure 5 (c) corresponds to average face image (print-scanned). For the sake of better illustration, we have included the morphed and averaged face data that was generated from the same subjects. As observed from the Figure 5, the distinctive information between bonafide, morphed and averaged face image can be visually observed in color channels. Thus, the use of color space information can be justified to detect the print-scanned face images corresponding to morphed and averaged image.

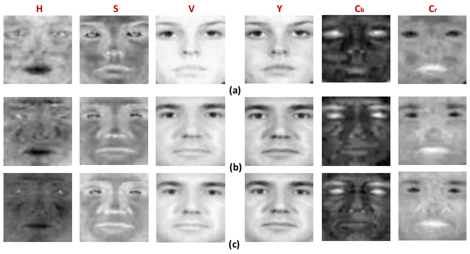


Figure 5: Example of HSV and YCbCr colour channels for print -scanned (a) Bonafide sample (b) Morphed sample (c) Averaged sample

Given the color face image $I_f$, the first step is to decompose the $I_f$ into six different color channels using HSV and YCbCr space that results in six different images denoted as $CI_i = \{CI_1, CI_2, CI_3, \ldots, CI_6\}$. In the next step, we extract the micro-texture features from each of the $CI_i$ color channels by employing Local Binary Patterns (LBP). Given the color channels of image $CI_i$, we extract the texture features using $LBP_{8,2}^{U2}$ by dividing the whole images into 40 blocks with an overlapping of 30(%). Since the size of $CI_i$ is 250 × 250 pixels, the $LBP_{8,2}^{U2}$ will result in a feature dimension of $1 \times 2891$ and this procedure is repeated for $i = 1, 2, \ldots, 6$ and all the obtained features are combined by concatenation to form a single feature vector of dimension $1 \times 2891 \times 6 = 17346$. Let the LBP features computed from $CI_i$ be $F_i$, then the concatenated features can be represented as: $F_i = \{F_1||F_2||F_3||F_4||F_5||F_6||\}$. The fused feature vector is classified using the Probabilistic Collaborative Representation Classifier (Pro-CRC) [5] that maximize the likelihood ratio of test sample jointly with other

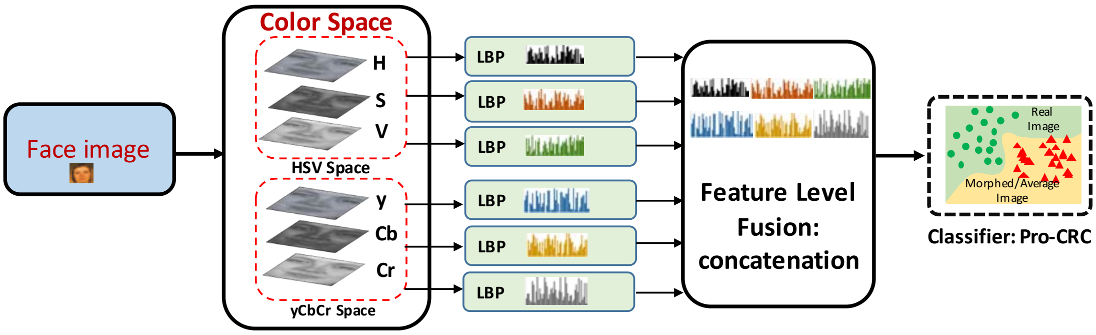


Figure 4: Schematic of proposed method to detect the morphing/averaging attacks

classes to perform the classification [5]. The Pro-CRC used in this work utilizes the Regularized Least Square Regression (RLSR) on the learned feature vectors versus the probe feature vectors [5] formulated as:

$$\widehat{F} = argmin_{\alpha} \left\| F_t - \mathscr{D}\alpha \right\|_2^2 + \lambda \left\| \alpha \right\|_2^2 \qquad (1)$$

where the $F_t$ is the feature vector of the test image, $\mathscr{D}$ is the learned collaborative subspace dictionary using $F_i$, $\alpha$ is coefficient vector and $\lambda$ is the regularization parameter. The distance obtained is used as the comparison score to obtain the attack face detection performance.

## 4. Experimental results and discussion

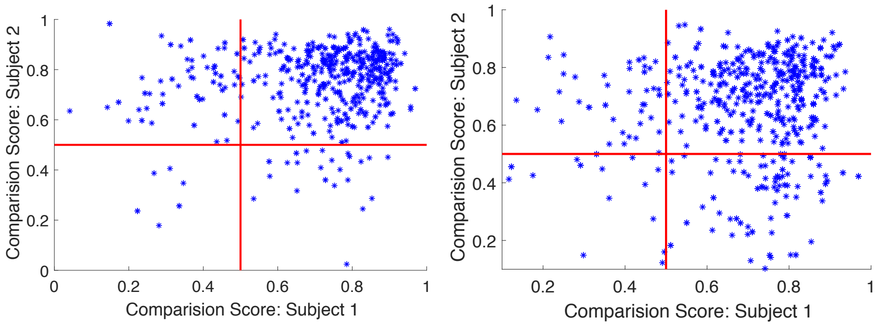
In this section, we present the vulnerability and the quantitative performance of the proposed attack face detection (morphed and averaged). The vulnerability analysis is carried out on both print-scanned morphed and averaged face images from our newly constructed database. The evaluation of the proposed morphed and averaged face detection is carried out using only training and testing set. While development set is used to tune the parameters of the proposed scheme and the regularization parameter of the Pro-CRC. The performance of the vulnerability and morphed face detection is measured following the metrics proposed in IS0/IEC 30107-3 [17] to be in-line with the works reported earlier on this problem.

### 4.1. Vulnerability Analysis

To effectively evaluate the vulnerability of the print-scanned morphed and averaged face images from new database, we employed the commercial face recognition system from Cognitec FaceVACS version 9.1.4 [2]. Cognitec FaceVACS is a commercial face recognition system, which is well tested, for example by the Face Recognition Vendor Test of the National Institute of Standards and Technology (NIST) [10] and employed in various border control scenarios and passport control applications. The vulnerability analysis will determine the impact of the generated morphed and average face images on the commercial face recognition system. According to [17], the vulnerability (or attack success rate) of the biometrics systems under attacks can be quantified using the metric - Imposter Attack Presentation Match Rate (IAPMR) which is defined as *the proportion of imposter attack presentations using the same Attack Instrument species (morphed or averaged) in which the target reference is matched in a full-system evaluation of a verification system.* The higher the value of IAPMR, the higher is the vulnerability of FRS.

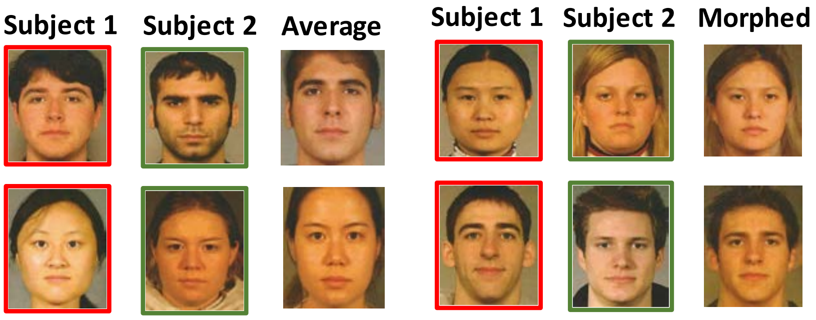
Figure 6 shows the scatter plot of the corresponding scores obtained using commercial FRS from Cognitec FaceVACS 9.1.4 separately on morphed and averaged face images. Figure 6 (a) illustrates the vulnerability of the averaged face image in which the comparison score are obtained by enrolling the print-scanned averaged face image and probing the print-scanned face images corresponding to the subjects that are used to generate the averaged face (constituent subjects). As noted from the Figure 6 (a), most of the comparison scores lie in the top-right corner of the graph indicating the vulnerability of the FRS to the averaged face image with an $IAPMR = 90.33\%$. Similar observation is also noted with the morphed face image as shown in the Figure 6 (b) that indicates the $IAPMR = 83.62\%$. Thus, based on the obtained IAPMR, it is evidently demonstrated that the FRS is vulnerable to both averaged and morphed face images. As an important remark, the averaged face images have shown the higher value of IAPMR and thus, pose higher risks to FRS.

Introspection of the lower values of comparison scores resulting in the failure to verification of averaged or morphed face image against bonafide subjects led to following notes: (1) There exist very few cases of failed verification of both subjects when compared against morphed /averaged face images. However, larger failure is observed on morphed face images. (2) The majority of the failed verification is due to failure exhibited by any one of the contributing subjects for morph (or average). Figure 7 shows the exam-



(a) Vulnerability of Averaged face images (b) Vulnerability of Morphed face images

Figure 6: Vulnerability study by analysing the comparison scores calculated using Cognitec FaceVACS



(a) Averaged face images (b) Morphed face images

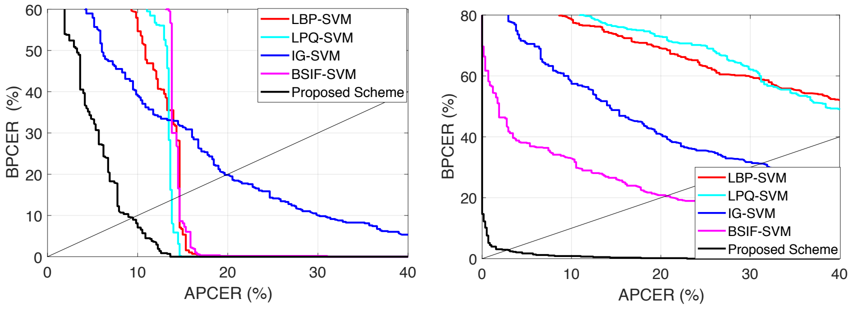
Figure 7: Example subjects that failed to get verified with the FRS (green color indicates the successful verification with the corresponding averaged or morphed face image and red color indicates the unsuccessful verification.)

ple of the subjects in which one of them is verified to the averaged and/or morphed face while other fails to get verified with FRS employed in this work. A detailed review of the scores indicated that most of the failure to verification was stemming from morphed or averaged images generated with the non-correlating ethnicity. However, this observation comes with a caveat of few such samples to fully validate the claim.

### 4.2. Morphed and Averaged face detection performance

In this section, we present the performance of the proposed scheme for detecting the morphed and averaged face images. Quantitative results of the proposed scheme is obtained by following the experimental protocol described in Table 2. The results are presented using the metrics: *Bonafide Presentation Classification Error Rate (BPCER) and Attack Presentation Classification Error Rate (APCER)* along with the corresponding ROC curves (APCER versus BPCER) as described in IS0/IEC 30107-3 [17]. **BPCER** is defined as proportion of bonafide presentations incorrectly classified as presentation attacks at the attack detection subsystem in a specific scenario while **APCER** is defined as proportion of attack face images incorrectly classified as bonafide images at the attack detection subsystem in a specific scenario. Besides, we also report the performance of the system by reporting the value of BPCER by fixing the APCER to 5% and 10% corresponding to realistic operating values of commercial face recognition systems.

Table 3 and Table 4 depicts the quantitative performance of the proposed scheme and the State-Of-The-Art (SOTA) algorithms on the print-scanned Morphed and Averaged Face Image (MAFI) database. Figure 8 shows the ROC curve indicating the performance of the proposed scheme together with SOTA on print-scanned morphed and averaged face images in MAFI database. The results are also presented using Equal Error Rate (%) computed from APCER versus BPCER, specifically at BPCER @ APCER = 10% and BPCER @ APCER = 5%. Table 3 depicts the quantitative performance of the proposed scheme on the morphed face detection. As noted from the Table 3, the proposed method has demonstrated the best performance when compared with four different SOTA texture based methods



(a) Morphed face images

(b) Averaged face images

Figure 8: ROC curves showing the performance of the proposed scheme

with EER = 9.48%, BPCER = 8.11 @APCER = 10% and BPCER = 35.12 @APCER = 5%. The performance of the SOTA schemes are severely degraded when compared to the performance of the proposed scheme that indicates the efficiency of the proposed method in detecting print-scanned morphed face images.

Table 3: Detection performance of the proposed algorithms on morphed face image

| Algorithms | EER (%) | BPCER (%) @ | |
|---|---|---|---|
| | | APCER = 10% | APCER = 5% |
| LBP-SVM | 14.65 | 55.51 | 74.13 |
| LPQ-SVM | 13.79 | 67.58 | 87.41 |
| BSIF-SVM | 14.65 | 87.41 | 96.55 |
| IG-SVM | 19.74 | 38.96 | 58.78 |
| **Proposed Scheme** | **9.48** | **8.11** | **35.12** |

Table 4 depicts quantitative performance of the proposed scheme on the print-scanned averaged face image database. It is interesting to note that, the proposed scheme has demonstrated the outstanding performance with the lowest EER of 2.93%, BPCER = 0.86% @APCER = 10% and BPCER = 1.72% @APCER = 5% when compared with the performance of rest of the SOTA methods. Thus, based on the extensive experiments carried out on the newly developed print-scanned morphed and averaged face image database, the proposed detection method has emerged as the best method on both print-scanned morphed and averaged face images with the lowest error rates. The performance of the SOTA schemes indicate the degraded performance on the averaged images when compared to that of the morphed face images. However, the proposed method shows good detection performance on both averaged and morphed face images.

Table 4: Detection performance of the proposed algorithms on averaged face image

| Algorithms | EER | BPCER @ | |
|---|---|---|---|
| | | APCER = 10% | APCER = 5% |
| LBP-SVM | 46.89 | 78.44 | 84.82 |
| LPQ-SVM | 44.65 | 82.24 | 86.41 |
| BSIF-SVM | 20.51 | 32.58 | 38.10 |
| IG-SVM | 31.12 | 85.34 | 70.86 |
| **Proposed Scheme** | **02.93** | **0.86** | **01.72** |

## 5. Conclusion

The evolving technology in generating the morphed face images has raised a potential threat, especially for the passport control application. As many countries issue the electronic passport based on the photo submitted by the applicant, the use of face-morphing technology can be effectively used to conceal the identity. In this work, we introduced a new potential attack on the passport control systems by introducing the averaged face that is obtained by taking the average of corresponding pixels value from the face images corresponding to two subjects. We built a new database following the real-life scenario of the passport issuance to have print-scanned images corresponding to bonafide, averaged and morphed face images. Extensive experiments were carried out to evaluate the vulnerability of the newly developed database of print-scanned averaged and morphed face images using a commercial FRS. Our experiments revealed that generating a morphed/averaged images with different ethnicity and different capture scenario (variation of indoor or studio lighting) may not contribute to the success of the attacks. Further, we also proposed a novel morphed/averaged face detection algorithm based on the collaborative representation of the micro-texture features extracted from the colour space. The performance of the proposed scheme is compared with four different SOTA algorithms. Extensive evaluation of the proposed morphed/averaged detection algorithm has indicated the outstanding performance in detecting the averaged face attacks and also the improved results in detecting the morphed face attacks.

## References

[1] Average face : Opencv. http://www.learnopencv.com/average-face-opencv-c-python-tutorial/, 2017. Accessed: 2017-04-10.

[2] Cognitech : Face vacs. http://www.cognitec.com/technology.html/, 2017. Accessed: 2017-04-10.

[3] Face morph using opencv. http://www.learnopencv.com/face-morph-using-opencv-cpp-python/, 2017. Accessed: 2017-04-10.

[4] Free and open source face recognition with deep neural networks. https://cmusatyalab.github.io/openface/.html, 2017. Accessed: 2017-04-10.

[5] S. Cai, L. Zhang, W. Zuo, and X. Feng. A probabilistic collaborative representation based approach for pattern classification. 2016.

[6] F. COTS. Verilook cots. http://www.neurotechnology.com/verilook.html, 2015. Accessed: 2015-02-08.

[7] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *IEEE International Joint Conference on Biometrics*, pages 1–7. IEEE, sep 2014.

[8] M. Ferrara, A. Franco, and D. Maltoni. *Face Recognition Across the Imaging Spectrum*, chapter On the Effects of Image Alterations on Face Recognition Accuracy, pages 195–222. Springer International Publishing, 2016.

[9] Frontex. Best Practice Technical Guidelines for Automated Border Control ( ABC ) Systems. Technical report, 2012.

[10] P. Grother and M. Ngan. Face Recognition Vendor Test ( FRVT ) Performance of Face Identification Algorithms. *National Institute of Standards and Technology (NIST)*, apr 2014.

[11] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann. Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.

[12] International Civil Aviation Organisation. Machine Readable Travel Documents - Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs. Technical report, ICAO, Montreal, 2006.

[13] INTERNATIONAL CIVIL AVIATION ORGANIZATION. PORTRAIT QUALITY (REFERENCE FACIAL IMAGES FOR MRTD). Technical Report Version: 0.8, Authority of the Secretary General, INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2017. Date published: 2017-04-01.

[14] International Civil Aviation Organization NTWG. Machine Readable Travel Documents – Part 1 Volume 1 – Passports with Machine Readable Data Stored in Optical Character Recognition Format. http://www.icao.int/publications/pages/publication.aspx?docnum=9303, 2006.

[15] International Organization for Standardization. Information technology – Biometric sample quality – Part 1: Face image data. ISO/IEC 29794-5:2010, JTC 1/SC 37, Geneva, Switzerland, 2010.

[16] International Organization for Standardization. Information technology – Biometric data interchange formats – Part 5: Face image data. ISO/IEC 29794-5:2011, JTC 1/SC 37, Geneva, Switzerland, 2011.

[17] International Organization for Standardization. Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting. ISO/IEC DIS 30107-3:2016, JTC 1/SC 37, Geneva, Switzerland, 2016.

[18] A. Makrushin, T. Neubert, and J. Dittmann. 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 - Volume 6: VISAPP, (VISIGRAPP 2017)*, pages 39–50, 2017.

[19] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. *Proceedings - 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2005*, I:947–954, 2005.

[20] R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In *8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, pages 1–8, 2016.

[21] D. Robertson, R. S. Kramer, and A. M. Burton. Fraudulent id using face morphs: Experiments on human and automatic recognition. *PLoS ONE*, 12(3):1–12, 2017.

[22] U. Scherhag, R. Raghavendra, K. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch. On the vulnerability of face recognition systems towards morphed face attack. In *International Workshop on Biometrics and Forensics (IWBF 2017)*, pages 1–6, 2017.