Challenges for Automated Face Recognition Systems

Christoph Busch[1,2*]

[1*]Norwegian Biometrics Laboratory (NBL),
Norwegian University of Science and Technology (NTNU),
Teknologiveien 22, Gjøvik, 2802, Norway .
[2]Computer Science Department, Hochschule Darmstadt (HDA),
Schoefferstrasse 3, Darmstadt, 64295, Hesse, Germany.

Corresponding author(s). E-mail(s): christoph.busch@h-da.de;

Abstract

Purpose: Face recognition as a process of the human visual system, analyses face properties and contextual information such as body shape. An automated recognition process replicates the human process and processes a face image, which is typically acquired with a visible spectrum sensor. This review addresses challenges of biometric recognition systems, which are based on face image analysis.

Performance and Quality: When dealing with operational systems, the quality of captured face images is relevant as it will impact the recognition accuracy. Thus, it is required to measure the utility of a face sample with a quality score but also with complementary measures that can provide actionable feedback.

Attacks and Security: A serious challenge for face recognition systems is the vulnerability to presentation attacks for instance with silicon masks. For reliable recognition in non-supervised environments robust presentation attack detection is required. Further enrolment attacks that morph the face images of two subjects raised concerns. Such attacks merge the content of two parent images into one. This is problematic, as many countries still allow in the passport application analogue images, i.e., a printed photo. Last not least biometric templates must be protected

Acceptability and Fairness: Acceptability of biometric systems requires fairness of biometric algorithms and artificial neural networks that are used. It is important to determine if face recognition systems are/are not biased towards a specific demographic group.

Keywords: Biometric face recognition systems, Sample quality, Presentation attack detection, Morphing attack detection, Biometric fairness

1 Introduction

Biometric applications have the primary purpose, to provide access control with a non-delegable authentication factor. These applications are more convenient for users of IT systems on the one hand and increase the security of access control on the other hand. Biometric recognition, which is understood as the automated recognition of individuals based on their behavioural and biological characteristics [1], exploits the rich set of anatomical characteristics related to the structure of the body (finger pattern, iris pattern etc.). A biometric recognition process requires that an individual (i.e. the natural person) is known by the system in advance (*enrolment*) to create the necessary reference data. This is done in the enrolment procedure. Biometric systems can either be designed as verification systems or as identification systems. In a verification system, the user specifies an identity to which - he claims - exists a reference in the system. If biometric systems are combined with an authentication document (e.g. some sort of identity card), the biometric reference (e.g. a passport photo) may be stored on this document. At the time of verification, a comparison of a biometric probe with exactly this one reference image is performed (*1:1 comparison*). On the other hand in the case of an identification system, the captured probe image is compared with many images that have been enrolled, and the most similar reference record is determined from this set (*1:n comparison*). However, the similarity between two images must reach a pre-defined threshold, so that a reliable assignment of the identity associated with the most similar reference image can be done. For the face capture process it is relevant to have the same constraints for enrolment samples and recognition samples: the capture subject should frontally face the capture device to ensure the same frontal pose, neutral facial expression and appropriate lighting conditions.

Face recognition today is widely adopted and has reached high significance in a variety of applications, ranging from authentication with smart personal devices (e.g. mobile phones), over access control (e.g. and border crossing) to forensic applications (e.g. video surveillance), which all constitute relevant operational systems.

When dealing with operational face recognition systems, three aspects need to be considered.

First the performance of the biometric system in terms of low transaction times, which becomes specifically relevant for large scale identification systems, where a probe will be compared to billions of biometric references. Workload reduction techniques are essential for such systems [2]. Moreover biometric performance is addressing the recognition accuracy in terms of low error rates for false positive of false negative errors [3]. In order to reach a good recognition accuracy the quality of biometric samples plays an important role. Only when both reference and probe samples are of good quality a reliable comparison score can be achieved. This will be discussed in Section 2 that provides a common sense about biometric quality assessment.

Second biometric identification and verification systems must be secure and trustworthy, specifically when integrated with other security technologies, in order to enforce a security policy (e.g. that an authentication factor can not be delegated. This requires that capture devices can not be fooled by artefacts (e.g. gummi fingers) and that attacks against the enrolment process are reliably detected. This is important to prevent impersonation attack targeted at misusing credentials of a victim. This will be reviewed in Section 3 and 4 respectively. In addition identification systems are potentially exposed to attacks that leak reference data in a central storage or even replace biometric reference data, such that impersonation attacks are supported. Preventing such security risks is fundamental and will therefore be addressed in Section 5.

Third biometric systems can only be successful, if they are well adopted by the target population. At the beginning of this century, our society was rather reluctant with respect to biometrics applications, as such were primarily associated with forensic investigations, which indeed constituted the major deployed systems from more than one hundred years. Moreover the storage of biometric data in central databases caused concerns [4]. Over the last decade the public perception of biometrics improved a lot, as Smartphones with fingerprint- or face recognition have demonstrated the increase in usability and security and moreover constrain the storage of reference data under the full control of the data subject. However a remaining challenge is that biometric algorithms shall treat different demographic groups in a fair manner, meaning with the same recognition accuracy. Addressing this challenge is fundamental to reach wide acceptability of biometrics in society.

Partially this article is discussing existing solutions, which should be deployed in operational systems and partly solutions are merely proposed and the need for further research is indicated.

2 Face image quality

For two dimensional (2D) face recognition capture requirements have been formulated in the international standard ISO/IEC 39794-5 such as a decent resolution [5], a full frontal perspective, good contrast, and good lighting. Furthermore certain acquisition criteria such as a neutral facial expression or the precondition that the face region and specifically the landmarks shall not be covered by hair, and the absence of (reflective) glasses or headgear should be met. If compliance of a face image with these requirements is not fulfilled, then the biometric system may recognize the capture subject only with low probability. Not very often the pose (i.e. perspective) and the expression of the face is fully identical in the reference and in the presented probe sample. In essence the drawback of the 2D approach is: the biometric performance is sensitive to pose variations, illumination changes, sensor conditions, and other disturbance factors that degrade the image quality.

It can be assumed that a biometric comparison algorithm delivers good and reliable results when high-quality images are presented and, conversely, delivers worse results when low-quality images are presented. While the quality assessment of fingerprint images has been a subject of research and development for 20 years [6–8], only recently strong innovation is observable for face image quality assessment. One of the driving

factors is the launch of the European Entry Exit System (EES)[9] which requires that the EU member states will conduct the biometric enrolment at border control points in accordance with Implementing Decision 2019/329 [10].

An overview of methods to assess face image quality was recently given in [11]. These methods focus on unified quality scoring approaches that describe the utility of an image for face recognition. The algorithms should have predictive power, meaning that a low quality score indicates a low comparison score to be expected, if that image is used in a biometric comparison. Such low score should prevent the face image to be inserted in the EES enrolment database. But also complementary measures are needed that allow actionable feedback to the capture subject such as the correctness of the pose or information to the biometric attendant such as the sharpness of the face image (among many others). Nevertheless, the requirements for a face image to be compliant to a canonical face image definition following the ICAO travel document specification (MRTD) [12], are expressed in the Biometric Data Interchange Standard ISO/IEC 19794-5:2011 as *Frontal image type* [13] and in the more recent Extensible Biometric Data Interchange Standard ISO/IEC 39794-5 in Annex D.1 [14] [1].

The prediction capability of a unified quality score is determined with Error-versus-Discard-characteristic curve (EDC)[15] based on the false-non-match rate (FNMR)[3] as an expression of recognition performance (i.e. false negative outcomes). The EDC can illustrate, how quickly the FNMR will decrease, when poor quality samples are discarded from the dataset in a step-wise manner. This is illustrated in the example in Figure 1, where for a chosen discard fraction the FNMR decreases faster for the MagFace algorithm [16] (the green line) as compared to the CR-FIQA(S) algorithm (the orange line) [17] indicating for MagFace a better prediction of the biometric recognition performance[2]. For this analysis it is important to demonstrate that a unified quality scoring method can generalise over many recognition algorithms [20].

At the time of this writing a standardisation process for a unified quality algorithm and complementary quality measures (i.e. actionable feedback) is about to be completed with ISO/IEC 29794-5 [21]. The quality score is a holistic measure for the entire sample, which is predictive of recognition performance and is an integer number in the range 0 to 100 (with higher being better). Along with the standard ISO/IEC 29794-5 the Open Source Face Image Quality (OFIQ) project does provide an open-source reference implementation of standardised algorithms, which was recently released in March 2024. This open source software can be deployed in commercial and governmental applications[3]. The MagFace algorithm, which was selected for the unified quality scoring, derives the quality measure directly from the magnitude of the face recognition feature vector [16].

For the optimisation of the capture process and the involved individuals, namely the capture subject and the biometric attendant, actionable feedback should be provided. Quality components (e.g. the pose angle) are assessing properties of the biometric sample and the compliance with the requirements for a canonical face image

[1] According to ICAO TAG/TRIP/4 decision from October 2023, passport inspection system must be able to handle ISO/IEC 39794-5 face image data by 2026-01-01

[2] The FNMR in Figure 1 is computed with the open source face recognition system ArcFace-R100-MS1MV2[18] on the LFW dataset[19]

[3] For more information on OFIQ visit the BSI website:https://bsi.bund.de/dok/OFIQ-e

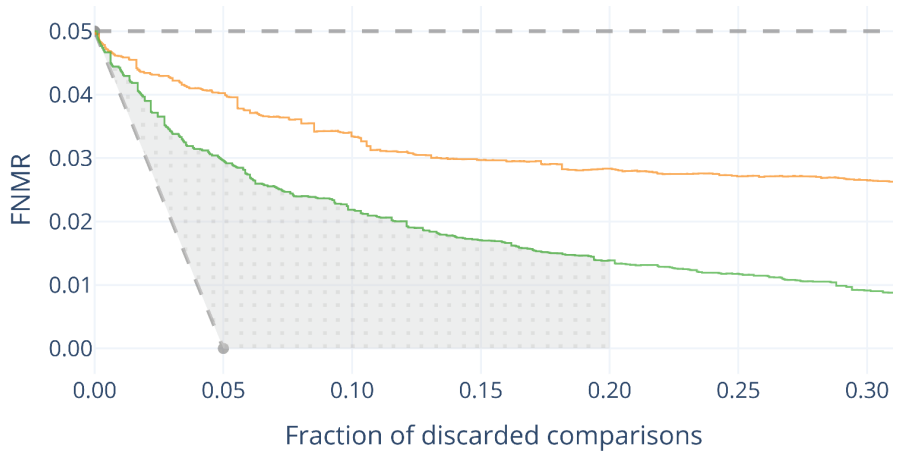

Fig. 1 Example of an EDC-curve, indicating that for a chosen discard fraction of poor quality images the FNMR will decrease faster for the green algorithm as compared to the orange algorithms. Highlighted in gray is the partial Area Under the Curve (pAUC), which spans from 0% up to 20% discard fraction. The smaller the pAUC the better is the quality assessment algorithm.

(e.g. frontal perspective to the capture device with zero pose angle). Component measures on the biometric sample may also contribute to the computation of a unified quality score [22]. Next to the pose angle also the deviation from expression neutrality is important, as it has a strong impact on recognition accuracy for many face recognition systems [23, 24].

Beyond subject related measures also capture device related measures are of interest primarily for the capture system set-up and calibration. Here the standard provides algorithms to assess the sharpness / focus of the camera. A further choice of parameters of the capture device could cause image compression artefacts. Such impact analysis for face image compression and the resulting recognition performance was first discussed in Funk et al. [25]. More recently the effect of more modern file compression techniques like JPEG-XL was investigated by Schlett et al. [26].

3 Presentation attack detection

While lacking face image quality may result in an operational risk for biometric systems, there are additional aspects specifically related to the robustness of image acquisition devices, which constitutes a security risk, if not addressed properly. As it is sketched in many science fiction films, access control sensors can be fooled by presenting a photo up to the camera or rendering a video of an authorized person on a laptop. In experiments, even the low image quality offered by a Smartphone was sufficient to present the pretended "*face biometric characteristic*" to a face capture device. There are yet too few systems that include a liveness detection and would thus prevent the faking of an identity using an inanimate object (i.e. a flat representation on a display). Consequently the reliable usage of this technology in non-supervised environments is still not feasible, specifically when biometrics are integrated with other

security technologies that expect that a biometric authentication factor can not be delegated.

More than 20 years ago this was documented in the literature with regards to fingerprint capturing [27–29]. Such attacks became a major concern when operational systems developed towards unsupervised enrolment or verification procedures. A presentation attack (PA) can be conducted from any outsider that interacts with a biometric capture device. However, the need to develop a harmonized perspective for presentation attacks that are conducted by biometric capture subjects became obvious. The biometric community has developed a multipart standard 'ISO/IEC 30107 Biometric presentation attack detection' [30–32]. The intention of this standard is to provide a harmonized definition of terms and a taxonomy of attack techniques. Beyond that it defines a data format that can transport measures of robustness against said attacks and a testing methodology that can evaluate PAD mechanisms.

Literature and science tends to struggle in general, and specifically in a multidisciplinary community as biometrics, with a clear and non-contradicting use and understanding of its terms. Therefore, ISO/IEC has developed a Harmonized Biometric Vocabulary (HBV) ISO/IEC 2382-37 [1] that includes terms and definitions useful in the context of presentation attacks. Some of the definitions in the HBV are relevant for the taxonomy on presentation attack detection (PAD).

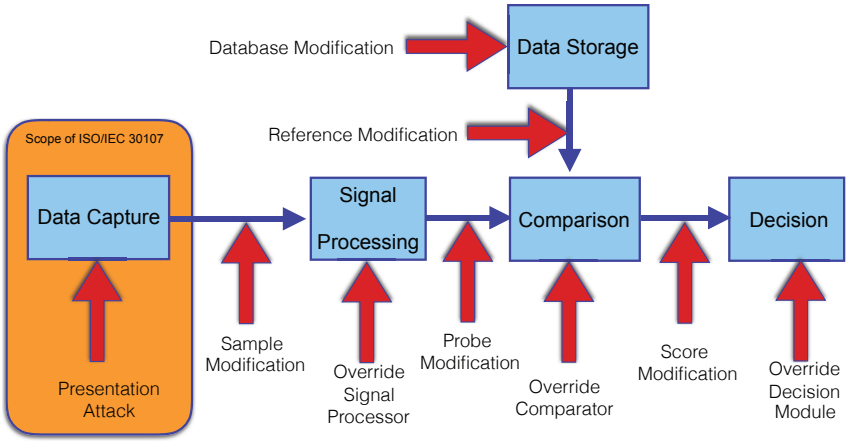

Fig. 2 Potential targets (indicated by the red arrows) of attacks against a generic biometric system. The schematic is drawn following what is reported in Reference [30]

In addition the standards ISO/IEC 30107-1 [30] and ISO/IEC 30107-3 [31] have established terms that are used to describe security properties of a biometric system. Relevant terms are contained in the Glossary at the end of this manuscript.

Figure 2 illustrates the potential targets in a generic biometric system [33] that could be attacked by a PA. We distinguish two types of attacks [30]: the Active Impostor Presentation Attack, and the Identity Concealer Attack.

- The *Active Impostor Presentation Attack* attempts to subvert the correct and intended policy of the biometric capture subsystem. Here, the attacker aims to be recognized as a specific data subject known to the system (*i.e.*, an impersonation attack).
- In an *Identity Concealer Presentation Attack*, on the other hand, the attacker aims to avoid being matched to his/her own biometric reference in the system.

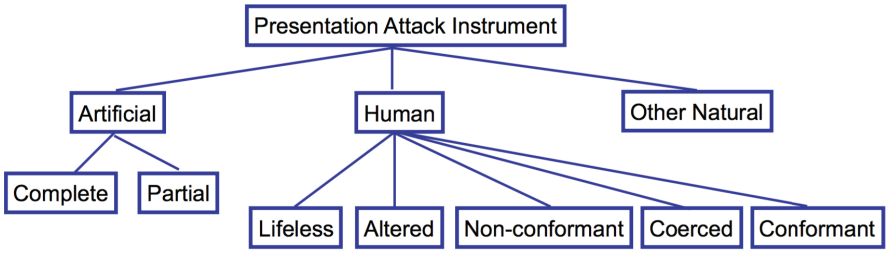

Fig. 3 A biometric system may be attacked with presentation attack instruments, which could be artefacts but also (altered) human body parts or other natural material

The potential of the attack (to succeed) will depend on the attacker's knowledge, the window of opportunity, and other factors, to create the object (i.e. PAI) used in the attack. The object that is employed in the attack can be of manifold nature: from *silicone masks* to categories of alterations of the biometric characteristic itself (e.g. makeup manipulations). See Figure 3. An *Identity Concealer* could be interested to cover his face by a silicone mask. A form of alteration of the biometric characteristic itself could be the manipulation of the facial appearance by a makeup artist [34, 35]. An overview of presentation attack detection for face capturing is given in [36].

4 Morphing attack detection

A morphing attack can be considered as an enrolment attack, that exploits the absence of live enrolment (see Section 4.3) and undermine the function of the passport as a trust anchor for identity control. Practically such attack enables a criminal to take over the identity of an accomplice, without taking the effort of an impersonation attack, as it was described in Section 3.Therefore, detection methods for morphing attacks are needed.

Face image manipulations can occur in the physical and digital domain [37, 38]. They can be applied to alter the appearance of face portraits, thereby adversely affecting the recognition accuracy of face recognition systems. Methods of facial modifications include substitution or re-enactment, often referred to as *face-swapping* or *deep-fakes*. In addition, morphing methods for transforming image content are known from film animation. Implementations of morphing methods are freely available and can be used to create a *morph* from two parent face images of two subjects. In the vast majority of countries, the face image submitted in the application process for an

identity document is provided by the applicant in an analogue form, i.e. as a printed photo. Some countries even allow photographs to be uploaded in the digital process when the document is re-issued. Therefore, an attacker can morph his face image with the face image of an accomplice. The result of this morphing process is shown in Figure 4. The morph face image (in the center) looks equally similar to the left and to the right parent image. It should be noted that morphed face images can fool face recognition systems as well as human examiners [39]. In order to constitute a high morphing attack potential [40], parent images are selected from individuals that have the same gender, similar age and a corresponding skin color.

Fig. 4 Face images of the two parent subjects (left and right), as well as a morphed face image (middle), which could be stored in the passport

The merging of face images (face morphing attack) threatens the core function of the passport as a document for identity verification. A significant number of passports with morphed facial images have been in circulation in recent years. The detection of such manipulated passports by human expert visual inspection is hardly possible. Extensive investigations have shown that even trained experts can rarely detect more than 60% of the manipulated photographs [41, 42]. Therefore, the development and deployment of Morphing Attack Detection (MAD) software is of great benefit. MAD is implemented using a suitable combination of features to describe textures, noise patterns or geometrical changes in a face image. In addition, deep learning methods are used to extract further features from the facial images. The influences of the printing and scanning process must also be taken into account.

This is a rather young field of research that was only established in the last decade. Numerous approaches for the automated detection of morphing attacks (MAs) have been proposed. In order to achieve reliable detection, the diversity of MAs must be taken into account. For example, the methods FaceMorpher, OpenCV, UBO-Morpher or MIPGAN are used for MAs [43]. FaceMorpher and OpenCV are open source implementations that perform landmark detection in the face image. Delaunay triangles are formed from these landmarks, which are distorted and their color values averaged. The generated morphs show strong artefacts, especially in the area of the eyes and pupils. Landmarks are also used in the UBO morpher. The morphs are created by triangulation, averaging and blending. To avoid the artefacts in the area outside the face, the morphed facial area is copied to the background of the original accomplice image. The MIPGAN method is derived from the StyleGAN Generative Adversarial Network

and averages the latent vectors of the two parent images of the attacker and accomplices in the latency space [44]. A loss function is used in the training, which takes into account perceptual quality and the identity preservation, ensuring a high-quality morphed face image as a result with only minimal artefacts. A detailed overview of MA and MAD is given by Scherhag et al. [39].

Since implemented MAD methods are largely not made publicly available, a comparative and independent evaluation of the detection performance became only possible, when the NIST FATE MORPH testing program was launched in 2019 [45]. Moreover the state of the art of MAD can be continuously benchmarked with the online platform provided by the University of Bologna (BOEP)[4]. The evaluation platform from Bologna includes high quality enrolment images but also operational probe images of mixed quality that were taken with ABC gates in three EU countries [43][5]. In addition, further possible post-processing by an attacker was simulated, such as image post-processing techniques, e.g. image sharpening, compression and the relevant print-scan transformation. In those evaluations both scenarios can be addressed, which are either based on a single suspicious face image (S-MAD) or, if an image pair is present, based on a differential image analysis (D-MAD). The latter scenario is illustrated in Figure 5 and is more robust, as it is based on the trusted live capture from the ABC gate. The results from NISTIR 8292 show that MAD with low error rates now become available [45].

4.1 Detection methods

In order to detect morphing attacks (MA), methods for morphing attack detection (MAD) are required, which allow a distinction between morphs and bona fide (unprocessed pristine face images, i.e. stemming directly from the camera) photographs. If a morph is detected at the border, a more detailed inspection can be carried out by a human examiner in a second step and a suspicious case, at least for European travel documents, can be clarified in a *second line inspection* by comparing the finger images, as these are also stored in the document. In order to distinguish bona fide face images submitted by the applicant or extracted from a bona fide traveler's travel document from morphs, several complementary features can be evaluated. In the first MAD step, artifacts that arise directly from the morphing process (so-called morphing shadows) are to be detected if they are still present. In the next step, an extensive analysis is carried out with the help of texture descriptors [46, 47]. Examples of implementation methods for analyzing MAs and their description are given in Table 1.

A simplistic approach is to analyse the sharpness of the face image that is usually reduced by the averaging of two images in the morphing process. In addition, an evaluation of geometric relationship is helpful: If face images of two individuals are merged, then for each parent image the geometric proportions (e.g. distance between the eyes and the length of the nose) are impacted. An average of these two ratios will be computed for the morphed image [48]. At the point of morphing attack control, it can be analysed if the geometric proportions of the passport holder are different from those in the photograph in the passport. Another MAD evaluation relies on a

[4] https://biolab.csr.unibo.it/fvcongoing/UI/Form/BOEP.aspx
[5] Both evaluations operate on a sequestered dataset, which can not be provided to researchers

Table 1 Categories of Morphing Attack Detection Methods

Method	Description
Analysis with texture descriptors	Detecting texture differences of the skin, sharpness and alike
Analysis of the geometry	Detecting transformations of landmark position
Forensic analysis	Detecting noise patterns of one or multiple cameras
Deep-Learning analysis	Detecting differences in latent vectors

forensic analysis of the camera noise. If the noise pattern of two cameras is found in the suspected face image, this is an indication that a morphing attack took place [49, 50]. Finally, latent vectors that have already been learned by deep neural networks on millions of bona fide photographs can also be used in the MAD evaluation [51, 52].

The design of MAD methods needs to consider the vulnerability of face recognition systems to MAs. It must be taken into account that good face recognition systems, which have a desired tolerance, meaning a robustness to expected variations in facial images, e.g. due to different lighting or face expression, are specifically vulnerable. This has been confirmed in the NIST FATE MORPH report [45] showing that face recognition algorithms that have a very good recognition performance are also more vulnerable to MAs due to their tolerance.

In security systems, risk assessment in terms of Common Criteria Testing is relevant. This requires quantifying an attack potential in terms of the attacker's expertise, knowledge of the target, and access to equipment. Recently evaluation methodologies have been developed to quantify the resistance of face recognition systems with respect to a morphing attack [40, 53, 54]. This methodology enables a quantification of the risk a certain morphing attack creates.

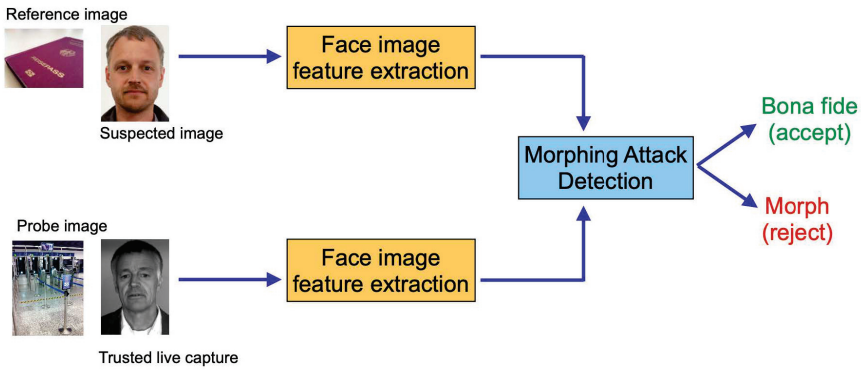

Fig. 5 Differential Morphing Attack Detection (D-MAD), as it can take place at border control. The suspected image from the passport is compared with the trusted live capture from the ABC-Gate

4.2 Deepfake generation attacks

Another form of enrolment attack can be executed, when the capabilities of synthetic face image generation tools are exploited [55]. Such tools benefit from the quality of artificial neural networks such as Generative Adversarial Networks (GAN) [56, 57] and more recently diffusion models [58]. These networks can be used to create high quality face images in diverse environments [59]. The attack is posing a severe risk for our society as they have already been used to influence voters[6], politicians[7] and lastly the public opinion. Detection of deep fakes remains a challenge for both human experts [42] and also trained algorithms [37]. Specifically when detection of unknown mechanisms is expected, the detection rate is modest, as generalisation capabilities of detectors are limited [60]. While the diversity of synthetic algorithms may be unlimited the more promising approach are one-class, which are trained to distinguish bona fide (i.e. pristine) images from any sort of attack images [61].

4.3 Need for live enrolment

Only a very small number of passport issuing authorities (e.g. in Europe Norway, Sweden, Hungary) will be able to prevent a morphing attack or a deep fake attack through live enrolment in the application process. Only in these few countries the face image is taken under the supervision of an officer of the authorities. Many passports with morphed facial images are already in circulation. The authorities in Europe are aware of at least 1000 cases detected in the past five years[8]. Until further notice, the use of MAD software is required at all border checkpoints, to ensure the security of our borders.

5 Biometric template protection

Operational biometric systems must demonstrate a balanced relationship between the advantages of biometric systems and the disadvantage of the more or less unmutable property of the biometric characteristic. Therefore the attack point of the biometric reference database needs to be investigated as it could be exploited in order to leak references or to even modify the stored enrolment records. To mitigate the risk that such attacks are exploited Biometric Template Protection (BTP) techniques are needed [62]. The goals for template protection have been anchored in the International Standard ISO/IEC 24745:2022 *Biometric information protection* [63] and constitute:

- Irreversibility such that no biometric sample can be reconstructed from the stored reference
- Non-leakage of additional information such as medical information related to the capture subject
- Secrecy, meaning that the comparison can be executed in the protected domain
- Diversification of references in space (unlinkability) and in time (*renewability*).

[6] CNN report about fake profile of a politician running for US congress: https://edition.cnn.com/2020/02/28/tech/fake-twitter-candidate-2020/index.html

[7] The Guardian report about European politicians duped into deepfake video calls: https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko

[8] the number of unreported cases is probably many times higher

In addition it is required that a protection mechanism does not cause a decrease of the biometric performance in terms of recognition accuracy (i.e. FMR and FNMR) Technically speaking biometric template protection can be achieved by transformations in the feature space, as it was successfully shown with the Bloom-Filter approach [64, 65] or using Homomorphic Encryption, that allows mathematical operations in the context of a biometric comparison trial to take place in the encrypted domain [65, 66]. Then a decryption of the sensitive data prior to the comparison is not needed. Only the result of the operation, the comparison score, is decrypted and handed over to the access control system.

5.1 Anticipate future change of operator control

As an outlook into the future, operators should anticipate that leakage of biometric references can happen as a consequence of undesired and/or unintentional change of the controller of the data storage subsystem, which might lead to enforcement of different policies. Such situation was experienced, when the NATO troops left Afghanistan in Summer 2021. The fast exit caused that biometric data (iris images, face images and fingerprint images) were left behind and coming under control of the Taliban[9] Such situation must be considered as a severe function creep. The fear is that these datasets and the corresponding capture devices will eventually reveal, which Afghan citizens had been serving for the NATO coalition forces. Reflecting the impact that these incidents had for the enrolled data subject, this experience should motivate operators, to store biometric data on central servers only, once proper biometric template protection methods are in place.

6 Biometric fairness

The successful deployment of biometric systems requires good acceptability in the target population respectively in the society, when it comes to public biometric system operations. Acceptability in turn requires on the one hand that the interaction of individuals with capture devices is considered as convenient. Meaning a good usability of the interaction scheme, and also free of medical concerns, meaning that frequent interaction does not impact the health status of the capture subject. Acceptability on the other hand also requires that data subjects have confidence that they are treated in a fair manner by the biometric algorithm. With the artificial intelligence (AI) evolution and the intensive use of AI algorithms in biometric systems the question has been in focus, whether the incorporated artificial neural networks are treating different demographic groups in the same manner. A prominent case has been reported in the 2020 documentary film *Coded Bias* [10], that illustrated how a face detection algorithm, which worked well for individuals with white skin, suddenly failed for individuals with dark skin. Fairness is moreover expected for biometric recognition algorithms. The NISTIR

[9] MIT technology review on the Afghan biometric databases (August 2021). See https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/

[10] The documentary film is described at:https://en.wikipedia.org/wiki/Coded_Bias

8280 investigated to which extend the biometric performance[11] for face recognition systems shows a differential performance[12], meaning a difference in the mated and non-mated comparison score distributions. Such investigation is specifically of interest for categorical demographic variables[13] as the gender categories *male*, *female* or *neutral*. Another interest is the differential performance related to continuous demographic variables[14] such as the skin color of an individual. While skin color has been in the past considered as categorical classes (e.g. the Fitzpatrick Skin Tpyes (FST) [68]) the recent literature considers alternative face area lightness measures (FALM) constituting a continuous variable as more appropriate [69].

It is important to validate prior to deployment that a face recognition system is not biased towards a specific demographic group. An overview of the effect of algorithmic bias in biometric systems and a survey on the recent literature is given in [70]. The reasons for bias are manifold and range from unbalanced training datasets to systematic effects in the training procedures [71–73].

On the path to reach fair biometric systems, a testing methodology is needed. Recent proposals for fairness measures [72, 74] are now under consideration to become the testing methodology in the draft International Standard ISO/IEC DIS 19795-10 [67].

However the challenge remains open, as bias mitigation concepts that can ensure a fair biometric system are still in their infancy. The immediate approach, to reach a balanced size of demographic subsets in the training [67] does not fully solve the problem due to the complexity of training procedures. Also score normalisation [75] and fusion of face recognition algorithms [76] are promising approaches yet have limited mitigation success. Finally also the fairness of face image quality assessment algorithms [77, 78] needs further exploration, as indicated in Section 2.

7 Conclusion

This review article has looked at challenges of current face recognition systems. Factors that are impacting the recognition accuracy such as the quality of captured face images are identified and discussed. Face recognition systems that are expected to increase the security level of an access control application may in turn contain some security weaknesses that have been looked at in this review, namely the vulnerability of capture devices to presentation attacks (e.g. with artefacts that replicate a biometric characteristic), a morphing attack against the enrolment process and potentially leaking biometric references for the enrolment database. Countermeasures are needed and are still subject to current research activities. Face recognition systems should not be operated unless strong and tested defense subsystems are integrated in the

[11] Following the International Standard ISO/IEC 19795-1 [3] biometric performance is reported in terms of false match rate (FMR) and false non-match rate (FNMR) for verification systems and in terms of false positive identification rate (FPIR) and false negative identification rate (FNIR) for identification systems

[12] The draft International Standard ISO/IEC DIS 19795-10 [67] defines differential performances as "difference in biometric system metrics across different demographic groups"

[13] The draft International Standard ISO/IEC DIS 19795-10 [67] defines categorical demographic variable as "demographic characteristic of an individual that is nominally or ordinally described"

[14] The draft International Standard ISO/IEC DIS 19795-10 [67] defines continuous demographic variable as "demographic characteristic of an individual that is observable, measurable, and that is not necessarily constrained to discrete categories"

overall system. Finally biometric systems can only be operated, if they are accepted by the target population. The perception will reflect the advancements in machine learning algorithms (and whether such are considered as beneficial or non-beneficial) and the impact of evolving privacy laws on operational systems. Thus the validation of algorithm fairness is fundamental. It remains important to demonstrate that face recognition algorithms are not biased towards a specific demographic group. One should note that the challenges performance and quality, attacks and security as well as acceptability and fairness are all closely related, meaning that it is not sufficient to address one or the other only. On the contrary for operational systems all challenges need to be addressed.

8 Acknowledgements

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

9 Competing interests policy

There is no competing interest.

10 Glossary terms

- biometric characteristic: biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition
- biometric feature: number or label extracted from biometric samples and used for comparison
- biometric capture: obtaining and recording of, in a retrievable form, signal(s) of biometric characteristic(s) directly from individual(s), or from representation(s) of biometric characteristic(s)
- biometric capture device: device that collects a signal from a biometric characteristic and converts it to a captured biometric sample
- biometric capture process: series of actions undertaken to effect a biometric capture
- biometric capture subject: individual who is the subject of a biometric capture process
- biometric attendant: agent of the biometric system operator who directly interacts with the biometric capture subject
- PA - presentation attack / AP - attack presentation: presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system

- bona fide presentation: biometric presentation without the goal of interfering with the operation of the biometric system
- PAI - presentation attack instrument: biometric characteristic or object used in a biometric presentation attack
- PAD - presentation attack detection: automated discrimination between bona-fide presentations and biometric presentation attacks
- artefact: artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns
- comparison: estimation, calculation or measurement of similarity or dissimilarity between a biometric probe(s) and a biometric reference(s)
- comparison score: numerical value (or set of values) resulting from a comparison
- biometric recognition: automated recognition of individuals based on their biological and behavioural characteristics
- biometric sample: analogue or digital representation of biometric characteristics prior to biometric feature extraction
- biometric reference: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison
- biometric probe: biometric sample or biometric feature set input to an algorithm for comparison to a biometric reference(s)
- biometric utility: degree to which a biometric sample supports biometric recognition performance
- quality component: measurement on the biometric sample that may contribute to the computation of a unified quality score
- quality measure: quality score or quality component
- quality score: quantitative value of the fitness of a biometric sample to accomplish or fulfil the comparison decision
- biometric impostor: subversive biometric capture subject who performs a biometric imposter attack
- biometric concealer: subversive biometric capture subject who performs a biometric concealment attack
- EDC - Error-versus-Discard-Characteristic curve: method to evaluate the efficacy of quality assessment algorithms by quantifying how efficiently discarding samples with low quality scores results in improved (i.e., reduced) false non-match rate
- canonical face image: face image conformant to an external standard or specification of a reference face image

- FNMR - false non-match rate: proportion of the completed biometric mated comparison trials that result in a false non-match
- FMR - false match rate: proportion of the completed biometric non-mated comparison trials that result in a false match
- MA - morphing attack: biometric image manipulation attack through merging two or more facial images by means of morphing
- MAD - morphing attack detection: detecting traces of a face image morphing attack conducted by some algorithms and/or human examiner

References

[1] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 2382-37:2022 Information Technology - Vocabulary - Part 37: Biometrics. International Organization for Standardization, (2022). International Organization for Standardization

[2] Drozdowski, P., Rathgeb, C., Busch, C.: Computational workload in biometric identification systems: An overview. IET Biometrics **8**(6), 351–368 (2019)

[3] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 19795-1:2021. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework. International Organization for Standardization, (2021). International Organization for Standardization

[4] Meints, M., Biermann, H., Bromba, M., Busch, C., Hornung, G., Quiring-Kock, G.: Biometric systems and data protection legislation in Germany. In: IEEE Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP09), pp. 1088–1093 (2008)

[5] Funk, W., Arnold, M., Busch, C., Munde, A.: Evaluation of image compression algorithms for fingerprint and face recognition. In: Proc. IEEE Information Assurance Workshop (2005)

[6] Tabassi, E., Wilson, C.: A novel approach to fingerprint image quality. In: 2005 Intl. Conf. on Imag Processing (ICIP 2005), pp. 37–40 (2005)

[7] Olsen, M., Šmida, V., Busch, C.: Finger image quality assessment features - definitions and evaluation. IET Biometrics **5**(2), 47–64 (2016)

[8] Tabassi, E., Olsen, M., Bausinger, O., Busch, C., Figlarz, A., Fiumara, G., Henniger, O., Merkle, J., Ruhland, T., Schiel, C., Schwaiger, M.: NIST interagency report 8382. NIST Interagency Report 8382, National Institute of Standards and Technology (July 2021)

[9] European Council: Regulation 2017/2226 of the European Parliament and of the Council of 30 November 2017 on establishing an Entry/Exit System (EES) to

register entry and exit data and refusal of entry data of third-country nationals (2017)

[10] European Council: Commission Implementing Decision 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES) (2019)

[11] Schlett, T., Rathgeb, C., Henniger, O., Galbally, J., Fierrez, J., Busch, C.: Face image quality assessment: A literature survey. ACM Computing Surveys (CSUR) (2021)

[12] International Civil Aviation Organization NTWG: Machine Readable Travel Documents – Part 3 – Specifications for Electroncally Enabled MRtds with Biometric Identification Capability. http://www.icao.int/publications/Documents/9303_p3_cons_en.pdf. Last accessed: 2024-01-15 (2021)

[13] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 19794-5:2011. Information Technology - Biometric Data Interchange Formats - Part 5: Face Image Data. International Organization for Standardization, (2011). International Organization for Standardization

[14] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 39794-5:2019 Information Technology - Extensible Biometric Data Interchange Formats - Part 5: Face Image Data. International Organization for Standardization, (2019). International Organization for Standardization

[15] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 29794-1 Information Technology - Biometric Sample Quality - Part 1: Framework. International Organization for Standardization, (2024). International Organization for Standardization

[16] Meng, Q., Zhao, S., Huang, Z., Zhou, F.: MagFace: A universal representation for face recognition and quality assessment. In: 2021 IEEE/CVF Conf. on Computer Vision and Pattern Recognition (CVPR) (2021)

[17] Boutros, F., Fang, M., Klemt, M., Fu, B., Damer, N.: CR-FIQA: Face image quality assessment by learning sample relative classifiability. In: Conf. on Computer Vision and Pattern Recognition (CVPR), pp. 5836–5845 (2023). IEEE

[18] Deng, J., Guo, J., Zafeiriou, S.: ArcFace: Additive angular margin loss for deep face recognition. In: Conf. on Computer Vision and Pattern Recognition (CVPR) (2019)

[19] Huang, G.B., Ramesh, M., Berg, T., Learned-Miller, E.: Labeled faces in the wild: A database for studying face recognition in unconstrained environments. In: Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition (2008)

[20] Schlett, T., Rathgeb, C., Tapia, J., Busch, C.: Considerations on the evaluation of biometric quality assessment algorithms. Trans. on Biometrics, Behavior, and Identity Science (TBIOM) (2023)

[21] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC DIS 29794-5 Information Technology - Biometric Sample Quality - Part 5: Face Image Data. International Organization for Standardization, (2024). International Organization for Standardization

[22] Chandaliya, P., Raja, K., Raghavendra, R., Busch, C.: Unified face image quality score based on iso/iec quality components. In: Proc. Intl. Conf. of the Biometrics Special Interest Group (BIOSIG), pp. 1–11 (2023)

[23] Grimmer, M., Rathgeb, C., Veldhuis, R., Busch, C.: Neutrex: A 3d quality component measure on facial expression neutrality. In: Proc. Intl. Joint Conf. on Biometrics (IJCB), pp. 1–8 (2023). IEEE

[24] Grimmer, M., Veldhuis, R., Busch, C.: Efficient expression neutrality estimation with application to face recognition utility prediction. In: Proc. Intl. Workshop on Biometrics and Forensics (IWBF), pp. 1–8 (2024)

[25] Funk, W., Arnold, M., Busch, C., Munde, A.: Evaluation of image compression algorithms for fingerprint and face recognition systems. In: Proc. IEEE SMC Information Assurance Workshop, pp. 72–78 (2005)

[26] Schlett, T., Schachner, S., Rathgeb, C., Tapia, J., Busch, C.: Effect of lossy compression algorithms on face image quality and recognition. In: Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP) (2023)

[27] Zwiesele, A., Munde, A., Busch, C., Daum, H.: BioIS study - comparative study of biometric identification systems. In: 34th Annual 2000 IEEE Intl. Carnahan Conf. on Security Technology (CCST) (2000)

[28] Matsumoto, T., Matsumoto, H., Yamada, K., Yoshino, S.: Impact of artificial "gummy" fingers on fingerprint systems. In: SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275–289 (2002)

[29] Schuckers, S., Hornak, L., Norman, T., Derakhshani, R., Parthasaradhi, S.: Issues for liveness detection in biometrics. In: Proc. of Biometric Consortium Conf. (2002)

[30] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-1. Information Technology - Biometric Presentation Attack Detection - Part 1: Framework. International Organization for Standardization, (2023). International Organization for Standardization

[31] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-2. Information Technology

- Biometric Presentation Attack Detection - Part 2: Data Formats. International Organization for Standardization, (2017). International Organization for Standardization

[32] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3. Information Technology - Biometric Presentation Attack Detection - Part 3: Testing and Reporting. International Organization for Standardization, (2023). International Organization for Standardization

[33] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC SC37 SD11 General Biometric System. International Organization for Standardization, (2008). International Organization for Standardization

[34] Rathgeb, C., Drozdowski, P., Busch, C.: Detection of makeup presentation attacks based on deep face representations. In: Proc. Int. Conf. on Pattern Recognition (ICPR), pp. 3443–3450 (2020)

[35] Rathgeb, C., Drozdowski, P., Busch, C.: Makeup presentation attacks: Review and detection performance benchmark. IEEE Access **8**, 224958–224973 (2020)

[36] Raghavendra, R., Busch, C.: Presentation attack detection methods for face recognition systems: A comprehensive survey. ACM Comput. Surv. **50**(1), 1–37 (2017)

[37] Rathgeb, C., Tolosana, R., Vera, R., Busch, C. (eds.): Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, 1st edn. Advances in Computer Vision and Pattern Recognition. Springer, Switzerland (2022)

[38] Rathgeb, C., Dantcheva, A., Busch, C.: Impact and detection of facial beautification in face recognition: An overview. IEEE Access **7**, 152667–152678 (2019)

[39] Scherhag, U., Rathgeb, C., Merkle, J., Breithaupt, R., Busch, C.: Face recognition systems under morphing attacks: A survey. IEEE Access (2019)

[40] Ferrara, M., Franco, A., Maltoni, D., Busch, C.: Morphing attack potential. In: 10th Intl. Workshop on Biometrics and Forensics (IWBF) (2022)

[41] Godage, S., Løvåsdal, F., Venkatesh, S., Raja, K., Raghavendra, R., Busch, C.: Analyzing human observer ability in morphing attack detection — where do we stand? IEEE Trans. on Technology and Society **4**(2), 125–145 (2023)

[42] Nichols, R., Rathgeb, C., Drozdowski, P., Busch, C.: Psychophysical evaluation of human performance in detecting digital face image manipulations. IEEE Access **10**, 31359–31376 (2022)

[43] Raja, K., Ferrara, M., Franco, A., Spreeuwers, L., Batskos, I., et al.: Morphing attack detection - database, evaluation platform and benchmarking. IEEE Trans. on Information Forensics and Security (2020)

[44] Zhang, H., Venkatesh, S., Raghavendra, R., Raja, K., Damer, N., Busch, C.: MIPGAN – generating strong and high quality morphing attacks using identity prior driven GAN. IEEE Trans. on Biometrics, Behaviour and Identity (2021)

[45] Ngan, M., Grother, P., Hanaoka, K., Kuo, J.: Face analysis technology evaluation (FATE) part 4: MORPH - performance of automated face morph detection. NIST Interagency Report 8289, National Institute of Standards and Technology (October 2023)

[46] Raghavendra, R., Raja, K., Busch, C.: Detecting morphed face images. In: 2016 IEEE 8th Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS). IEEE, New York (2016). 8th IEEE Intl. Conf. on Biometrics: Theory, Applications and Systems (BTAS-2016)

[47] Scherhag, U., Kunze, J., Rathgeb, C., Busch, C.: Face morph detection for unknown morphing algorithms and image sources: a multi-scale block local binary pattern fusion approach. IET Biometrics **9**(6), 278–289 (2020)

[48] Scherhag, U., Budhrani, D., Gomez-Barrero, M., Busch, C.: Detecting morphed face images using facial landmarks. In: Intl. Conf. on Image and Signal Processing (ICISP) (2018)

[49] Debiasi, L., Scherhag, U., Rathgeb, C., Uhl, A., Busch, C.: PRNU-based detection of morphed face images. In: 6th Intl. Workshop on Biometrics and Forensics, pp. 1–6 (2018)

[50] Scherhag, U., Debiasi, L., Rathgeb, C., Busch, C., Uhl, A.: Detection of face morphing attacks based on PRNU analysis. Trans. on Biometrics, Behavior, and Identity Science (TBIOM) (2019)

[51] Raghavendra, R., Raja, K., Venkatesh, S., Busch, C.: Transferable deep-cnn features for detecting digital and print-scanned morphed face images. In: IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1822–1830 (2017)

[52] Scherhag, U., Rathgeb, C., Merkle, J., Busch, C.: Deep face representations for differential morphing attack detection. IEEE Trans. on Information Forensics and Security (2020)

[53] Scherhag, U., Nautsch, A., Rathgeb, C., Gomez-Barrero, M., Veldhuis, R.N.J., Spreeuwers, L., Schils, M., Maltoni, D., Grother, P., Marcel, S., Breithaupt, R., Raghavendra, R., Busch, C.: Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In: Intl. Conf. of the

Biometrics Special Interest Group BIOSIG 2017, pp. 1–7 (2017)

[54] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC CD 20059. Information Technology – Methodologies to Evaluate the Resistance of Biometric Recognition Systems to Morphing Attacks. International Organization for Standardization, (2023). International Organization for Standardization

[55] Joshi, I., Grimmer, M., Rathgeb, C., Busch, C., Bremond, F., Dantcheva, A.: Synthetic data in human analysis: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1–20 (2024) https://doi.org/10.1109/TPAMI.2024.3362821

[56] Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A.C., Bengio, Y.: Generative adversarial nets. In: Neural Information Processing Systems (2014). https://api.semanticscholar.org/CorpusID:261560300

[57] Karras, T., Aittala, M., Laine, S., Härkönen, E., Hellsten, J., Lehtinen, J., Aila, T.: Alias-free generative adversarial networks. CoRR **abs/2106.12423** (2021) 2106.12423

[58] Dhariwal, P., Nichol, A.: Diffusion models beat gans on image synthesis. In: Ranzato, M., Beygelzimer, A., Dauphin, Y., Liang, P.S., Vaughan, J.W. (eds.) Advances in Neural Information Processing Systems, vol. 34, pp. 8780–8794 (2021). https://proceedings.neurips.cc/paper_files/paper/2021/file/49ad23d1ec9fa4bd8d77d02681df5cfa-Paper.pdf

[59] Melzi, P., Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., Lawatsch, D., Domin, F., Schaubert, M.: Gandiffface: Controllable generation of synthetic datasets for face recognition with realistic variations. In: 2023 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), pp. 3078–3087. IEEE Computer Society, Los Alamitos, CA, USA (2023). https://doi.org/10.1109/ICCVW60793.2023.00333 . https://doi.ieeecomputersociety.org/10.1109/ICCVW60793.2023.00333

[60] Khodabakhsh, A., Ramachandra, R., Raja, K., Wasnik, P., Busch, C.: Fake face detection methods: Can they be generalized? In: 2018 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–6 (2018). https://doi.org/10.23919/BIOSIG.2018.8553251

[61] Ibsen, M., Rathgeb, C., Marcel, S., Busch, C.: Multi-channel cross modal detection of synthetic face images. In: Proc. Intl. Workshop on Biometrics and Forensics (IWBF), pp. 1–8 (2024)

[62] Breebart, J., Busch, C., Grave, J., Kindt, E.: A reference architecture for biometric template protection based on pseudo identities. In: BIOSIG 2008: Biometrics and Electronic Signatures, pp. 25–37 (2008)

[63] ISO/IEC JTC1 SC27 Security Techniques: ISO/IEC 24745:2022. Information Technology - Security Techniques - Biometric Information Protection. International Organization for Standardization, (2022). International Organization for Standardization

[64] Rathgeb, C., Breitinger, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive Bloom filters. In: 2013 Intl. Conf. on Biometrics (ICB), pp. 1–8 (2013)

[65] Gomez-Barrero, M., Rathgeb, C., Galbally, J., Fierrez, J., Busch, C.: Protected facial biometric templates based on local Gabor patterns and adaptive Bloom filters. In: 2014 22nd Intl. Conf. on Pattern Recognition (ICPR), pp. 4483–4488 (2014)

[66] Kolberg, J., Drozdowski, P., Gomez-Barrero, M., Rathgeb, C., Busch, C.: Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption. In: Intl. Conf. of the Biometrics Special Interest Group (BIOSIG) (2020)

[67] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC DIS 19795-10. Information Technology – Biometric Performance Testing and Reporting – Part 10: Quantifying Biometric System Performance Variation Across Demographic Groups. International Organization for Standardization, (2023). International Organization for Standardization

[68] Fitzpatrick, T.: The validity and practicality of sun-reactive skin types I through VI. Archives of Dermatology **124**(6), 869–871 (1988)

[69] Howard, J., Sirotin, Y., Tipton, J., Vemury, A.: Reliability and validity of image-based and self-reported skin phenotype metrics. Trans. on Biometrics, Behavior, and Identity Science (TBIOM) **3**(4), 550–560 (2021)

[70] Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., Busch, C.: Demographic bias in biometrics: A survey on an emerging challenge. Trans. on Technology and Society (TTS) **1**(2), 89–103 (2020)

[71] Drozdowski, P., Rathgeb, C., Busch, C.: The watchlist imbalance effect in biometric face identification: Comparing theoretical estimates and empiric measurements. In: Intl. Conf. on Computer Vision Workshops (ICCVW), pp. 1–9. IEEE, New York (2021)

[72] Howard, J., Laird, E., Rubin, R., Siroting, Y., Tipton, J., Vemury, A.: Evaluating proposed fairness models for face recognition algorithms. In: Proc. Intl. Conf. on Pattern Recognition (2022)

[73] Rathgeb, C., Drozdowski, P., Frings, D.C., Damer, N., Busch, C.: Demographic fairness in biometric systems: What do the experts say? IEEE Technology and

Society Magazine **41**, 71–82 (2022)

[74] Kotwal, K., Marcel, S.: Fairness index measures to evaluate bias in biometric recognition. In: Proc. Intl. Conf. on Pattern Recognition (2022)

[75] Terhörst, P., Kolf, J., Damer, N., Kirchbuchner, F., Kuijper, A.: Post-comparison mitigation of demographic bias in face recognition using fair score normalization. Pattern Recognition Letters (PRL) (2020)

[76] Kolberg, J., Schäfer, Y., Rathgeb, C., Busch, C.: On the potential of algorithm fusion for demographic bias mitigation in face recognition. IET Biometrics (2023)

[77] Terhörst, P., Kolf, J., Damer, N., Kirchbuchner, F., Kuijper, A.: Face quality estimation and its correlation to demographic and non-demographic bias in face recognition. In: Intl. Joint Conf. on Biometrics (IJCB), 2020 (2020)

[78] Babnik, Z., Struc, V.: Assessing bias in face image quality assessment. In: European Signal Processing Conf. (EUSIPCO) (2020)