Biometrics in the Era of COVID-19: Challenges and Opportunities

Marta Gomez-Barrero[a,*], Pawel Drozdowski[b], Christian Rathgeb[b], Jose Patino[c], Massimiliano Todisco[c], Andreas Nautsch[c], Naser Damer[d], Jannis Priesnitz[b], Nicholas Evans[c], Christoph Busch[b]

[a]*Hochschule Ansbach, Germany*
[b]*da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany*
[c]*EURECOM, France*
[d]*Fraunhofer Institute for Computer Graphics Research IGD, Germany*

Abstract

Since early 2020 the COVID-19 pandemic has had a considerable impact on many aspects of daily life. A range of different measures have been implemented worldwide to reduce the rate of new infections and to manage the pressure on national health services. A primary strategy has been to reduce gatherings and the potential for transmission through the prioritisation of remote working and education. Enhanced hand hygiene and the use of facial masks have decreased the spread of pathogens when gatherings are unavoidable. These particular measures present challenges for reliable biometric recognition, e.g. for facial-, voice- and hand-based biometrics. At the same time, new challenges create new opportunities and research directions, e.g. renewed interest in non-constrained iris or periocular recognition, touch-less fingerprint- and vein-based authentication and the use of biometric characteristics for disease detection. This article presents an overview of the research carried out to address those challenges and emerging opportunities.

Keywords: COVID-19, Biometrics, Mask, Hygiene, Touchless biometrics, Remote authentication, Mobile biometrics

1. Introduction

Since early 2020, the world has been grappling with the COVID-19 pandemic caused by the new SARS-CoV-2 coronavirus. At the time of writing, there have been more than 80 million confirmed infections while almost 2 million have succumbed to the virus or related complications [1]. The main vector of disease transmission is exposure to respiratory particles resulting from direct or close physical contact with infected individuals. Transmission can also occur from the transfer of viral particles from contaminated surfaces or objects to the eyes, nose or mouth [1].

Various preventive measures have been adopted worldwide to help curb the spread of the virus by reducing the risk of new infections. These include local, national and international travel restrictions, the banning of large gatherings and the encouragement of physical distancing, remote working and education, and strict quarantine policies, see e.g. [2]. Two of the most broadly adopted measures are the (sometimes mandatory) use of protective facial coverings or masks [3] and enhanced hand hygiene (handwashing or disinfection using hydroalcoholic gel). Facial masks, such as those illustrated in Fig. 1, can reduce viral transmission through respiratory particles [4], while enhanced hand hygiene can reduce the rate of new infections through contact with contaminated surfaces or objects. Preventive measures, as well as the virus itself, have necessitated consequential shifts and disruption to daily life, with potentially long-lasting repercussions impacting individuals, social and professional practices and processes, businesses both small and large, as well as the global economy.

Such measures have had a considerable impact in our daily lives. For instance, the use of facial masks covering the mouth and nose in public spaces can decrease the usefulness of surveillance systems or prevent us from unlocking our smartphone using face recognition technologies. In this context, this article focuses on the impact of the COVID-19 pandemic on **biometric recognition**. Biometric technologies can be used for automated identity verification and to distinguish individuals based on their personal biological and behavioural characteristics (e.g. face and voice respectively). Biometric solutions frequently supplement or replace traditional knowledge- and token-based security systems since, as opposed to passwords and access cards, biometric characteristics cannot be forgotten or lost. Furthermore, biometrics inherently and seamlessly enable diverse application scenarios which are either difficult or infeasible using more traditional methods, e.g. continuous authentication [6, 7], forensics [8], and surveillance [9].

Biometrics technologies have come to play an integral role in society, e.g., for identity management, surveillance, access

*Corresponding author
Email addresses: marta.gomez-barrero@hs-ansbach.de (Marta Gomez-Barrero), pawel.drozdowski@h-da.de (Pawel Drozdowski), christian.rathgeb@h-da.de (Christian Rathgeb), jose.patino@eurecom.fr (Jose Patino), massimiliano.todisco@eurecom.fr (Massimiliano Todisco), andreas.nautsch@eurecom.fr (Andreas Nautsch), naser.damer@igd.fraunhofer.de (Naser Damer), jannis.priesnitz@h-da.de (Jannis Priesnitz), nicholas.evans@eurecom.fr (Nicholas Evans), christoph.busch@h-da.de (Christoph Busch)

(a) Surgical mask [5] (b) Cloth mask [5] (c) Filter mask[1] (d) Printed mask[2]

Figure 1: Examples of typical protective face masks

Table 1: Overview of popular biometric characteristics in the context of COVID-19.

Biometric characteristic	Data acquisition hardware	Application area				Operational prevalence	Impact of COVID-19
		mobile devices	access control	forensics	surveillance		
Face	commodity hardware	✓	✓	✓	✓	wide	high
NIR Iris	special sensor	(✓)	✓			wide	low
VIS Iris	commodity hardware	✓	(✓)			low	low
Touch-based Fingerprint	special sensor	✓	✓	✓		wide	high
Touchless Fingerprint	commodity hardware	✓	✓			low	low
Touch-based Hand Vein	special sensor		✓			low	low
Touchless Hand Vein	special sensor	(✓)	✓			low	low
Voice	commodity hardware	✓	✓	✓	✓	wide	medium

control, social and welfare management, and automatic border control, with these applications alone being used either directly or indirectly by billions of individuals [10, 11, 12, 13]. While reliance upon biometric technologies has reached a profound scale, health-related measures introduced in response to the COVID-19 pandemic have been shown to impact either directly or indirectly upon their reliability.

Table 1 provides a brief overview of the operational prevalence and COVID-19-related impacts and technological challenges in the context of the most widely (in operational systems) used biometric characteristics. They are reviewed and discussed in further detail in the remainder of this article, including a short introduction and description for each characteristic for the non-expert readers. The rest of the article is organised as follows. The impact of facial masks on biometrics technologies is discussed in Section 2. Section 3 addresses impacts upon mobile and remote biometric authentication. Section 4 describes new opportunities and applications that have emerged as a result of the COVID-19 pandemic. Concluding remarks are presented in Section 5.

2. Influence of facial coverings on biometric recognition

The use of facial coverings, such as masks, occlude a substantial part of the lower face. Such occlusions or obstructions change dramatically the operational conditions for numerous biometric recognition technologies. Such changes can make biometric recognition especially challenging. A review of the impacts of facial coverings is presented in this section, with a focus upon facial, periocular, iris, and voice biometrics.

2.1. Face recognition

The natural variation among individuals yields a good inter-class separation and thus makes the use of facial characteristics for biometric recognition especially appealing. Traditional solutions rely upon handcrafted features based on texture, key-points, and other descriptors for face recognition [14]. More recently, the use of deep learning and massive training datasets has led to breakthrough advances. The best systems perform reliably even with highly unconstrained and low-quality data samples [15, 16]. Relevant to the study presented here is a large body of research on occluded face detection [17] and recognition [18], though occlusion-invariant face recognition remains challenging [19]. Most work prior to the COVID-19 pandemic addresses occlusions from, e.g., sunglasses, partial captures, or shadows which typify unconstrained, 'in-the-wild' scenarios. The use of facial masks therefore presents a new and significant challenge to face recognition systems, especially considering the stringent operating requirements for application scenarios in which face recognition technology is often used, e.g. automated border control. The requirement for extremely low error rates typically depend on the acquisition of unoccluded images of reasonable quality.

The most significant evaluation of the impact of masks upon face recognition solutions was conducted by the National Institute of Standards and Technology (NIST) [20, 21]. The evaluation was performed using a large dataset of facial images with superimposed, digitally generated masks of varying size, shape,

[1]Source: `www.ikatehouse.com`
[2]Source: `www.thenationalnews.com`

and colour. The evaluation tested the face recognition performance of algorithms submitted to the ongoing Face Recognition Vendor Test (FRVT) benchmark in terms of biometric verification performance (i.e., one-to-one comparisons). The false-negative error rates (i.e., false non-match rate) for algorithms submitted prior to the pandemic [20], where observed to increase by an order of magnitude, even for the most reliable algorithms. Even some of the best-performing algorithms (as judged from evaluation with unmasked faces) failed almost completely, with false-negative error rates of up to 50%.

Of course, these results may not be entirely surprising given that systems designed prior to the pandemic are unlikely to have been optimised for masked face data. The study itself also had some limitations, e.g. instead of using genuine images collected from mask-wearing individuals, it used synthetically generated images where masks were superimposed using automatically derived facial landmarks. Despite the shortcomings, the study nonetheless highlights the general challenges to biometric face recognition from face coverings and masks. The general observations are that: 1) the degradation in verification reliability increases when the mask covers a larger proportion of the face including the nose; 2) reliability degrades more for mated biometric comparisons than for non-mated comparisons, i.e. masks increase the rate of false non-match rate more than the false match rate; 3) different mask shapes and colors lead to differences in the impact upon verification reliability, a finding which emphasises the need for evaluation using genuine masked face data; 4) in many cases, masked faces are not even detected.

A follow-up study [21], also conducted by NIST, evaluated systems that were updated with enhancements designed to improve reliability for masked faces. In addition to greater variability in mask designs, the study also considered both masked probe as well as masked reference face images. While reliability was observed to improve for masked faces, it remained substantially degraded compared to unmasked faces (approximately an order of magnitude lower). The degraded performance of masked faces was equivalent to that for unmasked faces and state-of-the-art systems from 2017. Increases in false-match rates were also observed when both reference, as well as probe faces are masked. Full details and results are available from the NIST FRVT Face Mask Effects website [22].

Results from the related DHS Biometric Rally show similar trends [23]. The DHS study was conducted in a setup simulating real operational conditions using systems submitted by commercial vendors. Significant difficulties in image acquisition as well as general degradation in biometric performance were observed for masked faces. Like the NIST study, the DHS study too found that, even with masked faces, today's systems perform as well as state-of-the-art systems from only a few years ago [23] tested with unmasked face images.

These US-based studies are complemented by a number of academic studies. Two datasets [5, 24] of masked face images have been collected in Europe and China to support research efforts. While [24] provides data, however, it does not provide a formal evaluation of the effect of masks on face recognition performance. Moreover, this study did not address a specific usecase scenario, e.g. collaborative face verification. Damer *et al.* [5] released a database of real masked face images that were collected in three collaborative sessions. They include realistic variation in the capture environment, masks, and illumination. Evaluation results show similar trends exposed by the NIST study [20]: difficulties in face detection and greater impacts upon mated comparisons than non-mated comparisons. While significantly smaller than the NIST dataset in the number of data subjects and images, the use of real instead of synthetically generated masked faces images increases confidence in results.

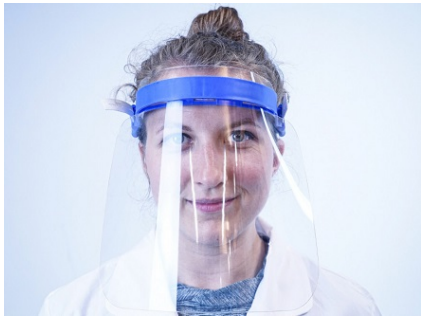
From a technical perspective, face masks can be considered as a subset of general face occlusions, and thus previous works on this issue are relevant. A number of works have proposed to automatically detect, and synthetically in-paint, the occluded face areas. This aimed at generating realistic and occlusion-free face images, as well as enabling a more accurate face recognition. Most of the better performing face completion solutions are based on deep generative models [25, 26]. A recent study by Mathai *et al.* [27] has shown that face completion can be beneficial for occluded face recognition accuracy, given that the occlusions are detected accurately. They have also pointed out that the completion of occlusions on the face boundaries did not have significant effect, which is not the case of face mask occlusions. Thus, these results indicate that face image completion solutions are possible candidates to enhance masked face recognition performance.

The use of transparent masks or shields may combat to some extent the impact of opaque masks upon face recognition systems. Transparent masks, such as those shown in Fig. 2, allow some portion of the masked face to remain visible but even their impact is likely non-trivial. Transparent masks can cause light reflections, visual distortions and/or blurring. Both opaque and transparent masks, as well as strategies to counter their impact, may increase the threat of presentation attacks. For example, it is conceivable that masks with specific patterns could be used to launch concealment or impersonation attacks, e.g. using concepts similar to those in [28].

Regardless of the exact type of face mask, wearing one can have an effect on the face image quality. Most biometric systems estimate the quality of a detected face image prior to feature extraction [29]. This quality estimation indicates the suitability of the image for recognition purposes [30]. For existing systems, the quality threshold configurations might lead to disregarding samples with face masks and thus increase the failure to extract rate. This link between face occlusions and face image quality has been probed in previous works, however, not exclusively for mask occlusions. One of these works, presented by Lin and Tang [31], built on the assumption that occlusions negatively effect the face image quality, in order to detect such occlusion. A recent study by Zhang *et al.* [32] has demonstrated the effect of occlusion on the estimated face mage quality, along with presenting an efficient multi-branch face quality assessment algorithm. The authors pointed out that images with alignment distortion, occlusion, pose or blur tend to obtain lower quality scores.

The studies conducted thus far highlight the challenges to face recognition systems in the COVID-19 era and raise nu-

(a) Transparent mask[3]



(b) Face shield[4]

Figure 2: Examples of alternative protective masks

merous open questions. These include, but are not limited to large-scale tests using images with real and not digitally generated masks, identification (i.e. one-to-many search), demographic differentials, presence of additional occlusions such as glasses, the effect on face image quality, unconstrained data acquisition in general, as well as effects on the accuracy of human examiners [21].

2.2. *Iris recognition*

The human iris, an externally visible structure in the human eye, exhibits highly complex patterns which vary among individuals. The phenotypic distinctiveness of these patterns allow their use for biometric recognition [33]. The acquisition of iris images typically requires a camera with near-infrared (NIR) illumination so that sufficient detail can be extracted for even darkly pigmented irides. Recent advances support acquisition in semi-controlled environments from at a distance even from only reasonably cooperative data subjects on the move (e.g. while walking) [34, 35].

Solutions to iris recognition which use mobile devices and which operate using only visible wavelength illumination have been reported in recent years [36, 37, 38]. Attempts to use image super-resolution, a technique of generating high-resolution images from low resolution counterparts, have also shown some success by increasing image quality [39]. However, iris recognition solutions seem more dependent than face recognition solutions upon the use of constrained scenarios that lead to the acquisition of high quality images [15, 16]. Nevertheless, iris recognition systems have now been in operation worldwide for around two decades. Near-infrared iris recognition has been adopted in huge deployments of biometrics technology, e.g. in the context of the Indian Aadhaar programme through which more than 1 billion citizens have been enrolled using iris images [40] in addition to other biometric data. Due to their high computational efficiency and reliability [41], iris recognition systems are used successful within the Aadhaar programme for intensive identification (1-*N* search) and de-duplication (*N*-*N* search) [11].

Figure 3: IrisGuard Inc. UAE enrolment station[5]

The success of automated border control systems used in the United Arab Emirates [10], where it is common for individuals to conceal a substantial part of their face on account of religious beliefs, serve to demonstrate the robustness of iris recognition systems to face coverings. In these scenarios, such as that illustrated in Fig. 3, whereas face recognition systems generally fail completely, iris recognition systems may still perform reliably so long as the iris remains visible. They are also among the least intrusive of all approaches to biometric recognition. This would suggest that, at least compared to face recognition counterparts, the reliability of iris recognition systems should be relatively unaffected as a consequence of mask wearing in the COVID-19 era.

It is worth mentioning that the usefulness of the anatomy of the human eye with regard to biometrics is not limited to the irides. For example, the retinal blood vessels are suitable for the purposes of biometric recognition. However, retinal imaging requires close proximity of a highly cooperative data subject to the specialised acquisition device which sends a beam of light inside the eye to fully illuminate the retina (see e.g. [42]). Although retinal structures exhibit a high degree of distinctiveness and hence good biometric performance, the need for a specialised sensor and the perceived intrusiveness of the acquisition process have been considered as obstacles to adoption of this biometric characteristic. The blood vessels present in the ocular surface have also been shown to exhibit some discriminative power and hence suitability of biometric recogni-

[3] Source: `https://www.theclearmask.com/product`

[4] Source: `https://3dk.berlin/en/covid-19/474-kit-for-face-shield-mask-with-two-transparent-sheets.html`

[5] Source: `https://en.wikipedia.org/wiki/File:IrisGuard-UAE.JPG`

tion [43]. The acquisition process for those, albeit less arduous than for the retinal images, still requires a high-resolution camera and subject cooperation in gazing in the required directions. Thus far, however, biometric recognition with ocular vasculature received relatively little attention beyond academic studies.

2.3. Periocular recognition and soft-biometrics

Periocular recognition, namely recognition observing biometric characteristics from the area surrounding the eye [44], offers potential for a compromise between the respective strengths and weaknesses of face and iris recognition systems. Unlike face recognition, periocular recognition can be reliable even when substantial portions of the face are occluded (opaque masks) or distorted (transparent masks). Unlike iris recognition, periocular recognition can be reliable in relatively unconstrained acquisition scenarios. Compared to alternative ocular biometrics, periocular recognition systems are also less demanding in terms of subject cooperation.

Due to those and other properties, periocular recognition was explored extensively during the last decade. Similarly to work in iris recognition, much of it has direct relevance to biometrics in the COVID-19 era, in particular with regards the wearing of face masks. In fact, one of the most popular use cases thus far for periocular recognition involves consumer mobile devices [45, 46] which can readily capture high quality images of the periocular region with onboard cameras. This approach to biometric recognition, e.g. to unlock a personal device, is of obvious appeal in the COVID-19 era when masks must be worn in public spaces and where tactile interactions, e.g. to enter a password or code, must preferably be avoided.

In most works, reliable verification rates can be achieved by extracting handcrafted features from the periocular region. However, the error rates are not yet as good as those yielded by face verification schemes under controlled scenarios. Nevertheless, the periocular features can be used to improve the performance of unconstrained facial images as shown in [46]. Similarly, Park *et al.* showed in [47] how the rank-1 accuracy was multiplied by a factor of two in a similar scenario using a synthetic dataset of face images treated artificially to occlude all but the face region above the nose. In other words, the success chances of correctly identifying a person within a group are doubled when the periocular information is analysed in parallel to the global face image.

In addition to the aforementioned works, some multimodal approaches combining face, iris, and the periocular region have been proposed for mobile devices [48], also incorporating template protection in order to comply with the newest data privacy regulations such as the European GDPR [49].

As pointed out in Sect. 2.2, in such uncontrolled conditions where the iris cannot always be used due to a low quality or resolution of the samples, that lack of quality of acquired biometric information can be addressed using super-resolution. Even though some approaches have already been proposed for the periocular region, based mostly on deep learning models [50, 39], there is still a long way ahead before they are deployed in practical applications.

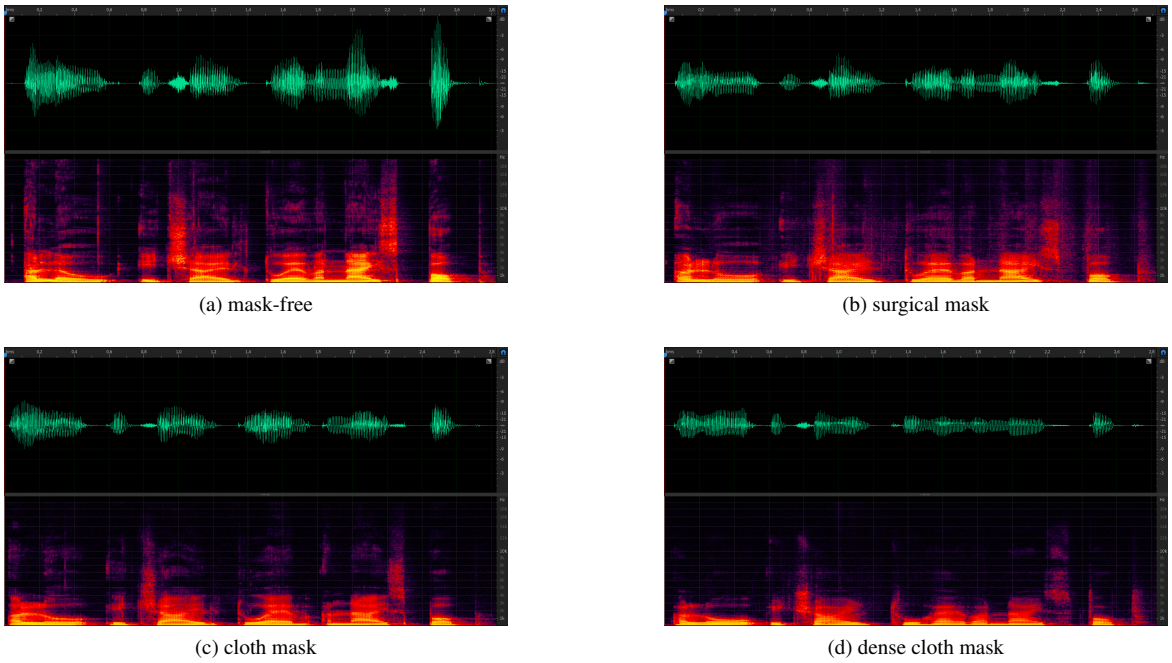
In addition to providing identity information, facial images can also be used to extract other soft biometric information, such as age range, gender, or ethnicity. Alonso-Fernandez *et al.* benchmarked the performance of six different CNNs for soft-biometrics. Also for this prupose, the results obtained indicate the possibility of performing soft-biometrics classification using images containing only the ocular or mouth regions, without a significant drop in performance in comparison to using the entire face. Furthermore, it can be observed in their study how different CNN models perform better for different population groups in terms of age or ethnicity. Therefore, the authors indicated that the fusion of information stemming form different architectures may improve the performance of the periocular region, making it eventually similar to that of unoccluded facial images. Similarly, the periocular region can be also utilised to estimate emotions using handcrafted textural features [51] or deep learning [52].

2.4. Voice recognition

Progress in voice recognition has been rapid in recent years [53, 54, 55, 56, 57]. Being among the most convenient of all biometrics technologies, voice recognition is now also among the most ubiquitous, being used for verification across a broad range of different services and devices, e.g. telephone banking services and devices such as smart phones, speakers and watches that either contain or provide access to personal or sensitive data.

The consequences of COVID-19 upon voice recognition systems depend largely on the effect of face masks on the production of speech. Face masks obstruct the lower parts of the face and present an obstacle to the usual transmission of speech sounds; they interfere with the air pressure variations emanating from the mouth and nose. The effect is similar to acoustic filters such as sound absorbing fabrics used for soundproofing or automobile exhaust mufflers [58]. Since masks are designed to hinder the propagation of viral particles of sub-micron size, typically they consist of particularly dense fabric layers. The effect on speech is an often-substantial attenuation and damping. A study on the impact of fabrics on sound is reported in [59, 60], which shows how acoustic effects are influenced by the particular textile and its thickness, density and porosity. Denser structures tend to absorb sound at frequencies above 2 kHz, while thicker structures absorb sound of frequencies below 500 Hz. With these bands overlapping that of human speech, masks attenuate and distort speech signals and hence degrade the reliability of voice biometric systems that are trained with normal (unmasked) speech.

Masks can also have a negative impact on presentation attack detection (PAD) systems, which present countermeasures to discriminate bonafide vs spoofed speech. These systems are based on spectral features obtained from the two classes. It becomes clear that any modification/deviation of the bonafide spectrum results in greater difficulty in detecting it. Moreover, other countermeasure systems are based on the detection of the POP noise [61]: a bonafide user emits pop noise which naturally incurred while speaking close to the microphone. This



(a) mask-free (b) surgical mask

(c) cloth mask (d) dense cloth mask

Figure 4: Examples of four spectrograms of the utterance: *allow each child to have an ice pop*, pronounced by the same speaker wearing different types of masks: (a) mask-free, (b) surgical, (c) cloth and (d) dense cloth mask.

noise is attenuated by the mask and, consequently, PAD performance decreases.

Fig. 4 shows speech waveforms and corresponding spectrograms derived using the short-time Fourier transform (STFT) for four different recordings of read speech. The text content is identical for all four recordings: *allow each child to have an ice pop*. The first is for a regular, mask-free recording while the other three are for the same speaker wearing a surgical mask, a thin or light cloth mask and a dense cloth mask. Note that the word *pop* pronounced at the end of the sentence becomes less and less noticeable as you wear heavier masks. Another notable effect concerns the attenuation of high frequencies for heavier masks, which affects not only recognition performance but also speech intelligibility [62].

Related to these aforementioned issues, a study of the impact of face coverings upon the voice biometrics is reported in [63]. It assessed and analysed the acoustic properties of four coverings (motorcycle helmet, rubber mask, surgical mask and scarf). The impact of all four coverings was found to be negligible for frequencies less than 1 kHz, while substantial levels of attenuation were observed for frequencies above 4 kHz; 4 kHz is not a general mark, since peaks at 1.8 kHz are reported for some masks. Face coverings were shown to degrade the accuracy of an i-vector/PLDA speaker recognition system. However, the treatment of speech data with inverted mask transfer functions was shown to improve accuracy to a level closer to the original. Similarly, face masks distort speech data above 4 kHz. The degradation to performance, however, is modest since the substantial effects are at higher frequencies where speech energy (and discriminative biometric information) is typically lower than it is at lower frequencies where the effects are much milder.

To reflect the current issues in the voice biometrics community, the 2020 findings of the 12th Computational Paralinguistics Challenge (COMPARE) considered a mask detection subchallenge. System fusion results for the challenge baselines show that the task is far from being solved. Speech signals, in this context, are not only relevant to voice biometrics but are usable to detect signal distortions.

The existing work stands to show that facial masks do affect voice-based technologies, and there is potential to compensate these effects. Thus the relevance of speaker recognition increases in this time, since it is unintrusive and touchless , that is, it can be done at distance, without any physical interaction (over the phone).

3. Remote and mobile biometric recognition

The COVID-19 pandemic has caused disruptions to many aspects of life. As a result of physical interactions being necessarily limited or even forbidden, many have had no alternative but to work remotely or to receive education online. With authentication being needed to access many services and resources, and without the possibility of physical means to identification, the deployment of biometric solutions for remote authentication has soared in recent times [64]. Remote biometric authentication has already attracted significant attention [9, 65] and is already being exploited for, e.g., eBanking, eLearning, and eBoarders. With an increasing percentage of personal mobile devices now incorporating fingerprint, microphone and imaging sensors, remote biometric authentication is deployable even without the need for costly, specialist or shared equipment. The latter is of obvious appeal in a pandemic, where the use of

touchless, personal biometric sensors and devices can help reduce spread of the virus.

Some specific biometric characteristics lend themselves more naturally to remote authentication than others. They are dictated by the level of required user cooperation and the need for specialist sensors. Face, voice, and keystroke/mouse dynamics are among the most popular characteristics for remote biometric authentication [66, 67]. These characteristics can be captured with sensors which are likely to be embedded in the subjects' devices, e.g. camera, microphone, keyboard and mouse. As discussed in the following, remote biometric authentication entails a number of specific challenges related to mobile biometrics, remote education, as well as security and privacy.

3.1. Mobile biometrics

The ever-increasing number of smartphones in use today has fueled research in mobile biometric recognition solutions, e.g. mobile face recognition [68] and mobile voice recognition [69, 70, 71]. Numerous biometric algorithms specifically designed or adapted to the mobile environment have been proposed in the literature [72]. Additionally, commercial solutions for mobile biometric recognition based on inbuilt smartphone sensors or hardware/software co-design are already available.

Proposed solutions can be categorized depending on where the comparison of biometric data takes place:

- Biometric comparison is performed on the client side, as proposed by the Fast IDentity Online (FIDO) Alliance [73]. An advantage of this scheme is that biometric data is kept on the user device, leading to improved privacy protection. On the other hand, users may require specific sensors and installed software to enable authentication.

- Biometric comparison is performed on the server side. Server side comparisons depend upon the secure transmission of biometric data (see Section 3.3), with relatively little specific software being required on the user device.

One limiting factor of mobile biometrics stems from processing complexity and memory footprints. Whereas server side computation capacity and memory resources are typically abundant, mobile devices resources running on battery power are relatively limited. Many state-of-the-art biometric recognition algorithms are based on large (deep) neural networks which require a large amount of data storage and are computationally expensive, thereby prohibiting their deployment on mobile devices. This has spurned research in efficient, and low footprint approaches to biometric computation, e.g. using smaller, more shallow neural networks [74]. A number of different approaches to compress neural networks have been proposed, e.g. based on student-teacher networks [75] or pruning [76]. These approaches trade model size and inference time against system performance. However, this trade-off still has to be optimized for mobile systems, while the implications of limited resources extend to other biometric sub-processes too, e.g. PAD and segmentation.

Figure 5: BioID® Identity Proofing for e-learning platforms [82]

In summary, mobile biometric authentication clearly has a role to play in the COVID-19 era. Touchless, personal mobile biometrics solutions can help to deliver reliable authentication while also meeting strict hygiene requirements, even if the efficient integration of biometric recognition technologies into mobile device platforms remains challenging.

3.2. Biometrics in remote education

The use of learning management systems has increased dramatically in recent years, not least due to the promotion of home-schooling and eLearning during the COVID-19 pandemic. Learning management systems deliver remote education via electronic media. eLearning systems often require some form of identity management for the authentication of remote students. Biometrics solutions have proved extremely popular, with a number of strategies to integrate biometric recognition in eLearning environments having been proposed in recent years [77, 78].

In the eLearning arena, biometric technologies are used for user login, user monitoring, attention and emotion estimation and authorship verification. Fig. 5 shows an example for user login to an eLearning platform. Both one-time authentication (biometric verification at a single point in time) and continuous authentication (periodic over time) have utility in eLearning scenarios. Whereas one-time authentication might be suitable to authenticate students submitting homework, continuous authentication may be preferred to prevent students cheating while sitting remote examinations [79]. In order to minimise inconvenience, continuous biometric authentication calls for the use of biometric characteristics which require little to no user cooperation [77], e.g. text-independent keystroke dynamics [80, 81].

Presentation attacks can present a substantial threat to biometric technologies deployed in such scenarios (see Section 3.3). This might be why, despite significant research interest, only few biometric recognition systems have been deployed in operational eLearning scenarios [77]. Even so, eLearning systems will likely become more popular while the pandemic continues and, once operational, their use will likely be maintained in the future.

3.3. Security and privacy in remote biometrics

The remote collection of biometric information gives rise to obvious security and privacy concerns; the trustworthiness of the collection environment cannot be guaranteed. One of the

potentially gravest threats in this case, especially given the absence of any human supervision (e.g. in contrast to the automatic boarder control use case), is that of presentation attacks or 'spoofing' [83, 84, 85]. Presentation attacks involve the presentation of false, manipulated or synthesized samples to a biometric system made by an attacker to masquerade as another individual. Diverse presentation attack instruments, ranging from face masks to gummy fingers, have all been proved a threat. The detection of presentation attacks in a remote setting can be more challenging that in a local setting, depending on whether detection countermeasures are implemented on the client side or the server side. In case PAD is performed on the client side, hardware-based detection approaches can be employed, though these require specific, additional equipment beyond those used purely for recognition. Even these approach might still be vulnerable to presentation attacks, as demonstrated for Apple's Face ID system [86]. If PAD is implemented on the server side, then software-based attack detection mechanisms represent the only solution. Software-based PAD for face and voice were explored in the EU-H2020 TeSLA project [87] and is being currently researched in the DFG-ANR RESPECT project[6]. It is expected that more research will be devoted to this topic in the future.

In addition to the threat of direct attacks performed at the sensor level, there is also the possibility of indirect attacks performed at the system level. The storage of personal biometric information on mobile devices as well as the transmission of this information from the client to a cloud based server calls for strong data protection mechanisms. While traditional encryption and cryptographic protocols can obviously be applied to the protection of biometric data, any processing applied to the data required prior decryption, which still leaves biometric information vulnerable to interception. Encryption mechanisms designed specifically for biometrics recognition in the form of template protection [88] over come this vulnerability by enabling computation upon biometric data in the encrypted domain. Specific communication architectures that ensure privacy protection in remote biometric authentication scenarios where biometric data is transmitted between a client and a server have already been introduced, e.g. the Biometric Open Protocol Standard (BOPS) [89] which supports the homomorphic encryption [90] of biometric data.

As it has been described in this section, the use of remote biometric authentication in the times of COVID-19 provides many advantages. However, in order to achieve trustworthy identity management, it also requires appropriate mechanisms to protect privacy. Countermeasures to prevent or detect presentation attacks are also essential. The latter is usually more challenging in a remote authentication scenario, where means of detecting attacks may be more limited compared to conventional (accessible) biometric systems.

[6] http://www.respect-project.eu/

(a) dry (b) normally moist

Figure 6: Example of a dry fingerprint and the same fingerprint with normal moist (taken from [92]).

4. Emerging technologies

As discussed in the previous sections, the COVID-19 pandemic poses specific challenges to biometric technologies. However, it is also expected to foster research and development in emerging biometrics characteristics which stand to meet new requirements relating to the pandemic, as well as the use of biometric information directly for virus detection and monitoring e.g. of infected individuals. Such emerging biometric technologies are described in the following.

4.1. Touchless, hand-based biometrics

Hydro-alcoholic gel, strongly advocated as a convenient means to disinfection during the COVID era, can be used to protect the users of touch-based sensors such as those used for fingerprint recognition [91]. While they serve to reduce sensor contamination and pathogen transmission, hydro-alcoholic gels tend to dry the skin. The sensitivity of fingerprint sensors to variability in skin hydration is well known. It can degrade the quality of acquired fingerprints and hence also recognition reliability [92]. Severe dryness can even prevent successful acquisition as illustrated in Fig. 6, thereby resulting in failures to acquire.

Hygiene concerns have increased societal resistance to the use of touch-based sensors. These concerns have in turn fueled research efforts in 2D or 3D touchless fingerprint recognition systems [93, 94] such as those illustrated in Fig. 7. Touchless fingerprint sensors are generally either prototype hardware designs [95, 96] or are adapted from general purpose devices adapted to touchless fingerprint recognition [97, 98].

Both the capture and processing of fingerprints must usually be adapted to touchless acquisition [93]. The majority of touchless finger image acquisition sensors deliver colour images for which general image processing techniques are employed to improve contrast and sharpness. Traditional minutiae extractors and comparators may then be employed.

The interoperability of both touch-based and touchless devices is naturally desirable, e.g. to avoid the need for enrolment in two different systems. Interoperability has proven to be non-trivial [99, 100]. While some differences between the two systems, e.g. mirroring, colour-to-grayscale conversion or inverted

(a) Stationary touchless[7]

(b) Mobile touchless

Figure 7: Touchless capturing of fingerprints

back- and foreground, can be readily compensated for without degrading accuracy, others, e.g. the aspect ratio or deformation estimation, prove more challenging [101, 102] and can degrade reliability. Note that fingerprint images acquired using touchless sensors do not exhibit the deformations caused by pressing the finger onto a surface that characterise images acquired from touch-based sensors. Moreover, DPI alignment and ridge frequency estimation is required to enable a meaningful comparison of fingerprints acquired from touch-based and touchless sensors.

As an alternative to fingerprint recognition, some ATMs already incorporate fingervein-based recognition sensors which are robust to variability in skin hydration as well as presentation attacks. Images of the finger or hand are captured with NIR illumination, since light at NIR frequencies is absorbed differently by hemoglobin and the skin, thereby allowing for the detection of vein patterns. Touchless fingervein and palmvein sensors have been developed [103, 104, 105], though the lack of any control in the collection process typically causes significant rotation and translation variation. The quality of the capturing device as well as strategies to compensate for nuisance variation are hence key to the collection of high quality images and reliable performance. Touchless capturing device designs have been presented by various researchers, e.g. in [103]. This work showed that the degradation in recognition performance resulting from touchless acquisition can be addressed using finger misplacement corrections. On the other hand, the approach presented in [104] extracts a region of interest from captured samples and uses an oriented element feature extraction scheme to improve robustness.

The use of finger vein recognition for mobile devices is also emerging. Debiasi *et al.* developed an auxiliary NIR illumination device for smartphones which supports the capture of hand vascular patterns [106]. The device is connected and controlled via Bluetooth and can be adapted to different smartphones. The authors also presented a challenge response protocol in order to prevent replay and presentation attacks and showed that acceptable verification performance can be achieved using standard finger vein recognition algorithms. The VeinSeek Pro app[8] is able to capture vein images from the hand without the need for extra hardware. This approach is based on the fact that different colors of light penetrate different depths within the skin. By removing the signal from superficial layers of the skin, the authors argue that they can more easily see deeper structures. However, to the best of our knowledge there is no analysis so far of the feasibility of using these images for vein-based biometric recognition.

In summary, in the era of the COVID-19 pandemic, touchless hand-based biometric recognition seems to be a viable alternative to conventional touch-based systems. These technologies achieve similar levels of performance as touch-based technologies [93, 94, 103]. Some commercial products based on prototypical hardware design and general purpose devices, e.g. smartphones, are already available on the market. Nonetheless, touchless recognition remains an active field of research where several challenges need to be tackled, in particular recognition in challenging environmental conditions, e.g. uncontrolled background or varying illumination [107, 93].

4.2. COVID detection with biometric-related technologies

COVID-19 attacks the human body at many levels, but the damage to the respiratory system is what often proves fatal. The production of human speech starts with air in the lungs being forced through the vocal tract. Diminished lung capacity or disease hence impacts upon speech production and there have been attempts to characterise the effects of COVID-19 upon speech as means to detect and diagnose infection [108, 109, 110].

Initial efforts involved the collection and annotation of databases of speech as well as non-speech sounds recorded from healthy speakers and those infected with the COVID-19 virus [111]. The data typically includes recordings of coughs [112, 113, 114], breathing sounds [115, 116] as well as speech excerpts [117].

The database described in [117] contains recordings of five spoken sentences and in-the-wild speech, all recorded using

[7] Source: `https://pbs.twimg.com/media/DyCFi_AWsAMN8MK.jpg`

[8] `https://www.veinseek.com/`

the Wechat App from 52 COVID-confirmed and hospitalised patients in Wuhan, China, who also rated their sleep quality, fatigue, and anxiety (low, mid, and high). After data preprocessing, 260 audio samples were obtained. While these early works highlight the potential of biometrics and related technology to help in the fight against the COVID-19 pandemic, they also highlight the need for homogenised and balanced databases which can then be used to identify more reliable and consistent biomarkers indicative of COVID-19 infection.

Thermal face imaging has also come to play a major role during the pandemic, especially for the rapid surveillance of potential infections among groups of travellers on the move, e.g. in airports [118] and shopping centres [119]. Thermal face images can be used to detect individuals with fever [120], a possible symptom of COVID-19 infection. Similar face captures can also be used as an alternative capture spectrum for face recognition [121, 122, 123], however, with verification performances inferior to the visible [124, 125]. Despite the ease with which thermal monitoring can be deployed, it is argued in [126] that body temperature monitoring will be insufficient on its own to prevent the spread of COVID-19 into previously uninfected countries or regions and the seeding of local transmission. The European Union Aviation Safety Agency (EASA) concludes that thermal screening equipment, including thermal scanners will miss between 1% and 20% of passengers carrying a fever [127].

5. Conclusions

This article has summarised the main challenges posed by the pandemic to biometric recognition, as well as the new opportunities for existing biometrics to be harnessed or adapted to the COVID-19 era, or where biometrics technology itself has potential to help in the fight against the virus. The use of hygienic masks covering the nose and mouth, as well as the secondary impacts of strict hygiene measures implemented to control the spread of pathogens all have potential to impact upon biometrics technology, thereby calling for new research to maintain reliable recognition performance.

Facial biometrics are among the most impacted characteristic; masks occlude a considerable part of the face, leading to degraded recognition performance. This is the case not only for opaque masks but also for transparent face shields, since reflections caused variation that is non-trivial to model. Opportunities to overcome these difficulties are found by focusing parts of the face that remain uncovered, namely the iris and the wider periocular region.

Whereas solutions to iris recognition that use the NIR spectrum are well studied, numerous efforts in recent years have focused on less constrained approaches to iris recognition that use mobile devices and the visible spectrum. Given the lower quality of such images, image super-resolution techniques have been proposed to improve image quality. Such techniques can also be applied to the full periocular region. To date, the adoption of such systems is low, but likely to increase in the future.

Hand-based biometric systems are also affected by the new hygiene practices which typically result in drier skin, lower quality fingerprint images and degraded recognition performance. Both touch-based and touch-less systems are affected. Vein-based recognition systems are more robust to variations in skin condition. In contrast to traditional touched-based vein sensors, touch-less capture devices introduced in the last two years can reduce the risk of infection from contact with a contaminated surface. Further research is nonetheless needed to bridge the gap between the performance of less constrained, touchless systems and their better constrained touch-based counterparts.

Like facial biometrics, voice biometric systems are also impacted by the wearing of facial masks which can interfere with speech production. Like many other forms of illness, COVID-19 infections can also interfere with the human speech production system and also degrade recognition performance. These same effects upon the speech production mechanism, however, offer potential for the detection of pulmonary complications such as those associated with serious COVID-19 infections.

The challenges in ensuring reliable biometric recognition performance have grown considerably during the COVID-19 era and call for renewed research efforts. With many now working or receiving education at home, some of the greatest challenges relate to the use of biometric technology in remote, unsupervised verification scenarios. This in turn gives greater importance to continuous authentication, presentation attack detection, or biometric template protection to ensure security and privacy in such settings which have come to so define the COVID-19 era.

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 and the DFG-ANR RESPECT Project (406880674 / ANR-18-CE92-0024).

References

[1] World Health Organization, Coronavirus disease (COVID-19) pandemic, https://www.who.int/emergencies/diseases/novel-coronavirus-2019, last accessed: February 19, 2021.

[2] European Union, Re-open eu, https://reopen.europa.eu/, last accessed: February 19, 2021.

[3] #Masks4All, What countries require masks in public or recommend masks?, https://masks4all.co/what-countries-require-masks-in-public/, last accessed: February 19, 2021.

[4] L. Peeples, Face masks: what the data say, Nature 586 (7828) (2020) 186–189.

[5] N. Damer, J. H. Grebe, C. Chen, F. Boutros, F. Kirchbuchner, A. Kuijper, The effect of wearing a mask on face recognition performance: an exploratory study, in: International Conference of the Biometrics Special Interest Group (BIOSIG), Gesellschaft für Informatik e.V., 2020, pp. 1–10.

[6] V. M. Patel, R. Chellappa, D. Chandra, B. Barbello, Continuous user authentication on mobile devices: Recent progress and remaining challenges, IEEE Signal Processing Magazine 33 (4) (2016) 49–61.

[7] S. Mondal, P. Bours, A study on continuous authentication using a combination of keystroke and mouse biometrics, Neurocomputing 230 (2017) 1–22.

[8] M. Tistarelli, C. Champod, Handbook of biometrics for forensic science, Springer, 2017.

[9] M. Tistarelli, S. Z. Li, R. Chellappa, Handbook of Remote Biometrics, Springer, 2009.

[10] A. N. Al-Raisi, A. M. Al-Khouri, Iris recognition and the challenge of homeland and border control security in UAE, Telematics and Informatics 25 (2) (2008) 117–132.

[11] A. Dalwai, Aadhaar technology and architecture: principles, design, best practices and key lessons, Tech. rep., Unique Identification Authority of India (UIDAI) (March 2014).

[12] European Commission, Smart borders, https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en, last accessed: February 19, 2021(2018).

[13] Thales, Automated Fingerprint Identification System (AFIS) overview - a short history, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history, last accessed: February 19, 2021(April 2019).

[14] S. Z. Li, A. K. Jain, Handbook of face recognition, Springer, 2011.

[15] I. Masi, Y. Wu, T. Hassner, P. Natarajan, Deep face recognition: A survey, in: Conference on graphics, patterns and images (SIBGRAPI), IEEE, 2018, pp. 471–478.

[16] G. Guo, N. Zhang, A survey on deep learning based face recognition, Computer Vision and Image Understanding 189 (2019) 102805.

[17] M. Opitz, G. Waltner, G. Poier, H. Possegger, H. Bischof, Grid loss: Detecting occluded faces, in: European Conference on Computer Vision (ECCV), Springer, 2016, pp. 386–402.

[18] D. Zeng, R. N. J. Veldhuis, L. Spreeuwers, A survey of face recognition techniques under occlusion, arXiv preprint arXiv:2006.11366.

[19] L. Song, D. Gong, Z. Li, C. Liu, W. Liu, Occlusion robust face recognition based on mask learning with pairwise differential siamese network, in: International Conference on Computer Vision (ICCV), IEEE/CVF, 2019, pp. 773–782.

[20] M. Ngan, P. Grother, K. Hanaoka, Ongoing face recognition vendor test (FRVT) part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms, Tech. Rep. NISTIR 8311, National Institute of Standards and Technology (July 2020).

[21] M. Ngan, P. Grother, K. Hanaoka, Ongoing face recognition vendor test (FRVT) part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms, Tech. Rep. NISTIR 8331, National Institute of Standards and Technology (November 2020).

[22] National Institute of Standards and Technology, FRVT face mask effects, https://pages.nist.gov/frvt/html/frvt_facemask.html, last accessed: February 19, 2021(November 2020).

[23] Department of Homeland Security, Biometric Technology Rally at MdTF, https://mdtf.org/Rally2020, last accessed: February 19, 2021(2020).

[24] Z. Wang, G. Wang, B. Huang, Z. Xiong, Q. Hong, H. Wu, P. Yi, K. Jiang, N. Wang, Y. Pei, H. Chen, Y. Miao, Z. Huang, J. Liang, Masked face recognition dataset and application, arXiv preprint arXiv:2003.09093.

[25] Y. Li, S. Liu, J. Yang, M.-H. Yang, Generative face completion, in: Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, 2017, pp. 5892–5900.

[26] J. Zhang, R. Zhan, D. Sun, G. Pan, Symmetry-aware face completion with generative adversarial networks, in: Asian Conference on Computer Vision (ACCV), Vol. 11364, Springer, 2018, pp. 289–304.

[27] J. Mathai, I. Masi, W. AbdAlmageed, Does generative face completion help face recognition?, in: International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–8.

[28] M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter, Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition, in: Conference on Computer and Communications Security, ACM, 2016, pp. 1528–1540.

[29] T. Schlett, C. Rathgeb, O. Henniger, J. Galbally, J. Fiérrez, C. Busch, Face image quality assessment: A literature survey, CoRR abs/2009.01103.

[30] P. Terhörst, J. N. Kolf, N. Damer, F. Kirchbuchner, A. Kuijper, SER-FIQ: unsupervised estimation of face image quality based on stochastic embedding robustness, in: CVPR, IEEE, 2020, pp. 5650–5659.

[31] D. Lin, X. Tang, Quality-driven face occlusion detection and recovery, in: 2007 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2007), 18-23 June 2007, Minneapolis, Minnesota, USA, IEEE Computer Society, 2007. doi:10.1109/CVPR.2007.383052.
URL https://doi.org/10.1109/CVPR.2007.383052

[32] L. Zhang, X. Shao, F. Yang, P. Deng, X. Zhou, Y. Shi, Multi-branch face quality assessment for face recognition, in: 19th IEEE International Conference on Communication Technology, ICCT 2019, Xi'an, China, October 16-19, 2019, IEEE, 2019, pp. 1659–1664. doi:10.1109/ICCT46805.2019.8947255.
URL https://doi.org/10.1109/ICCT46805.2019.8947255

[33] J. Daugman, How iris recognition works, Transactions on Circuits and Systems for Video Technology (TCSVT) 14 (1) (2004) 21–30.

[34] J. R. Matey, Iris on the move™, in: S. Z. Li, A. K. Jain (Eds.), Encyclopedia of Biometrics, Springer US, 2009, pp. 805–810.

[35] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan, A. Ross, Long range iris recognition: A survey, Pattern Recognition 72 (2017) 123–143.

[36] H. Proença, Iris recognition: On the segmentation of degraded images acquired in the visible wavelength, Transactions on Pattern Analysis and Machine Intelligence (TPAMI) 32 (8) (2009) 1502–1516.

[37] K. B. Raja, R. Raghavendra, V. K. Vemuri, C. Busch, Smartphone based visible iris recognition using deep sparse filtering, Pattern Recognition Letters 57 (2015) 33–42.

[38] A. Rattani, R. Derakhshani, Ocular biometrics in the visible spectrum: A survey, Image and Vision Computing 59 (2017) 1–16.

[39] J. Tapia, M. Gomez-Barrero, C. Busch, An efficient super-resolution single image network using sharpness loss metrics for iris, in: Proc. Int. Workshop on Information Forensics and Security (WIFS), IEEE, 2020.

[40] Unique Identification Authority of India, Aadhaar dashboard, https://www.uidai.gov.in/aadhaar_dashboard/, last accessed: February 19, 2021.

[41] J. Daugman, C. Downing, Searching for doppelgängers: assessing the universality of the IrisCode impostors distribution, IET Biometrics 5 (2) (2016) 65–75.

[42] S. M. Lajevardi, A. Arakala, S. A. Davis, K. J. Horadam, Retina verification system based on biometric graph matching, Transactions on Image Processing 22 (9) (2013) 3625–3635.

[43] P. Rot, M. Vitek, K. Grm, Ž. Emeršič, P. Peer, V. Štruc, Deep Sclera Segmentation and Recognition, Springer, 2020, Ch. 13, pp. 395–432.

[44] F. Alonso-Fernandez, J. Bigun, A survey on periocular biometrics research, Pattern Recognition Letters 82 (2016) 92–105.

[45] K. B. Raja, R. Raghavendra, M. Stokkenes, C. Busch, Smartphone authentication system using periocular biometrics, in: Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG), 2014, pp. 1–8.

[46] T. de Freitas Pereira, S. Marcel, Periocular biometrics in mobile environment, in: International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2015, pp. 1–7.

[47] U. Park, R. R. Jillela, A. Ross, A. K. Jain, Periocular biometrics in the visible spectrum, Transactions on Information Forensics and Security (TIFS) 6 (1) (2011) 96–106.

[48] K. B. Raja, R. Raghavendra, M. Stokkenes, C. Busch, Multi-modal authentication system for smartphones using face, iris and periocular, in: International Conference on Biometrics (ICB), IEEE, 2015, pp. 143–150.

[49] M. Stokkenes, R. Raghavendra, M. K. Sigaard, K. Raja, M. Gomez-Barrero, C. Busch, Multi-biometric template protection - a security analysis of binarized statistical features for bloom filters on smartphones, in: International Conference on Image Processing Theory, Tools and Applications (IPTA), IEEE, 2016, pp. 1–6.

[50] V. M. Ipe, T. Thomas, Periocular recognition under unconstrained conditions using CNN-based super-resolution, in: International Conference on Advanced Communication and Networking (ICACN), Springer, 2019, pp. 235–246.

[51] F. Alonso-Fernandez, J. Bigun, C. Englund, Expression recognition using the periocular region: A feasibility study, in: International Conference on Signal-Image Technology Internet-Based Systems (SITIS), IEEE, 2018, pp. 536–541.

[52] N. Reddy, R. Derakhshani, Emotion detection using periocular region: A cross-dataset study, in: International Joint Conference on Neural Networks (IJCNN), IEEE, 2020, pp. 1–6.

[53] T. Kinnunen, H. Li, An overview of text-independent speaker recognition: From features to supervectors, Speech communication 52 (1) (2010) 12–40.

[54] J. H. L. Hansen, T. Hasan, Speaker recognition by machines and humans: A tutorial review, IEEE Signal Processing Magazine 32 (6) (2015) 74–99.

[55] M. Todisco, H. Delgado, N. Evans, Articulation rate filtering of CQCC features for automatic speaker verification, in: Proc. Interspeech, 2016.

[56] A. Nagrani, J. S. Chung, A. Zisserman, Voxceleb: a large-scale speaker identification dataset, arXiv preprint arXiv:1706.08612.

[57] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, S. Khudanpur, X-vectors: Robust dnn embeddings for speaker recognition, in: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2018, pp. 5329–5333.

[58] A. Zent, J. T. Long, Automotive sound absorbing material survey results, in: SAE 2007 Noise and Vibration Conference and Exhibition, SAE International, 2007, pp. 1–7.

[59] H. S. Seddeq, N. M. Aly, A. A. Marwa, M. H. Elshakankery, Investigation on sound absorption properties for recycled fibrous materials, Journal of Industrial Textiles 43 (1) (2013) 56–73.

[60] X. Tang, X. Yan, Acoustic energy absorption properties of fibrous materials: A review, Composites Part A: Applied Science and Manufacturing 101 (2017) 360–380.

[61] Q. Wang, X. Lin, M. Zhou, Y. Chen, C. Wang, Q. Li, X. Luo, VoicePop: A pop noise based anti-spoofing system for voice authentication on smartphones, in: Conference on Computer Communications, IEEE, 2019, pp. 2062–2070.

[62] K.-N. C. Mac, X. Cui, W. Zhang, M. Picheny, Large-Scale Mixed-Bandwidth Deep Neural Network Acoustic Modeling for Automatic Speech Recognition, in: Proc. Interspeech 2019, 2019, pp. 251–255.

[63] R. Saeidi, I. Huhtakallio, P. Alku, Analysis of face mask effect on speaker recognition, in: Interspeech, ISCA, 2016, pp. 1800–1804.

[64] C. Burt, Remote authentication keeps the world working: A biometric update interview series, `https://www.biometricupdate.com/202005/remote-authentication-keeps-the-world-working-a-biometric-update-interview-series`, last accessed: February 19, 2021.

[65] G. Guo, H. Wechsler, Mobile Biometrics, Security, Institution of Engineering and Technology, 2017.

[66] N. Kaur, P. W. C. Prasad, A. Alsadoon, L. Pham, A. Elchouemi, An enhanced model of biometric authentication in e-learning: Using a combination of biometric features to access e-learning environments, in: International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES), IEEE, 2016, pp. 138–143.

[67] G. Fenu, M. Marras, L. Boratto, A multi-biometric system for continuous student authentication in e-learning platforms, Pattern Recognition Letters 113 (2018) 83–92.

[68] A. Rattani, R. Derakhshani, A survey of mobile face biometrics, Computers & Electrical Engineering 72 (2018) 39–52.

[69] E. Khoury, B. Vesnicer, J. Franco-Pedroso, R. Violato, Z. Boulkcnafet, L. M. Mazaira Fernández, M. Diez, J. Kosmala, H. Khemiri, T. Cipr, R. Saeidi, M. Günther, J. Žganec-Gros, R. Z. Candil, F. Simões, M. Bengherabi, A. Álvarez Marquina, M. Penagarikano, A. Abad, M. Boulayemen, P. Schwarz, D. Van Leeuwen, J. González-Domínguez, M. U. Neto, E. Boutellaa, P. G. Vilda, A. Varona, D. Petrovska-Delacrétaz, P. Matějka, J. González-Rodríguez, T. Pereira, F. Harizi, L. J. Rodriguez-Fuentes, L. E. Shafey, M. Angeloni, G. Bordel, G. Chollet, S. Marcel, The 2013 speaker recognition evaluation in mobile environment, in: International Conference on Biometrics (ICB), IEEE, 2013, pp. 1–8.

[70] M. G. Gomar, System and method for speaker recognition on mobile devices, uS Patent 9,042,867 (May 2015).

[71] I. Bisio, C. Garibotto, A. Grattarola, F. Lavagetto, A. Sciarrone, Smart and robust speaker recognition for context-aware in-vehicle applications, Transactions on Vehicular Technology (TVT) 67 (9) (2018) 8808–8821.

[72] A. Rattani, R. Derakhshani, A. Ross, Selfie Biometrics, Advances and Challenges, Springer, 2019.

[73] FIDO Alliance, Fast identity online, `https://fidoalliance.org/`, last accessed: February 19, 2021(2020).

[74] L. J. Ba, R. Caruana, Do deep nets really need to be deep?, in: International Conference on Neural Information Processing Systems - Volume 2, MIT Press, 2014, pp. 2654–2662.

[75] P. Luo, Z. Zhu, Z. Liu, X. Wang, X. Tang, Face model compression by distilling knowledge from neurons, in: Conference on Artificial Intelligence (AAAI), ACM, 2016, pp. 3560–3566.

[76] P. Molchanov, S. Tyree, T. Karras, T. Aila, J. Kautz, Pruning convolutional neural networks for resource efficient inference, in: International Conference on Learning Representations (ICLR), OpenReview.net, 2017, pp. 1–17.

[77] C. Rathgeb, K. Pöppelmann, E. Gonzalez-Sosa, Biometric technologies for elearning: State-of-the-art, issues and challenges, in: International Conference on Emerging eLearning Technologies and Applications (ICETA), 2020, pp. 1–6.

[78] P. S. Sanna, G. L. Marcialis, Remote biometric verification for elearning applications: Where we are, in: International Conference Image Analysis and Processing (ICIAP), Springer, 2017, pp. 373–383.

[79] E. Flior, K. Kowalski, Continuous biometric user authentication in online examinations, in: International Conference on Information Technology: New Generations (ITNG), IEEE, 2010, pp. 488–492.

[80] A. Morales, J. Fierrez, Keystroke biometrics for student authentication: A case study, in: Conference on Innovation and Technology in Computer Science Education (ITiCSE), ACM, 2015, p. 337.

[81] S. Mondal, P. Bours, A study on continuous authentication using a combination of keystroke and mouse biometrics, Neurocomputing 230 (2017) 1 – 22.

[82] BioID, GmbH, Identity assured online exams & personalized e-learning, `https://www.bioid.com/online-exams-e-learning/`, last accessed: February 19, 2021(2020).

[83] N. Ratha, J. Connell, R. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Systems Journal 40 (3) (2001) 614–634.

[84] S. Marcel, M. S. Nixon, J. Fierrez, N. Evans, Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, Springer, 2019.

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

[86] Bkav Corp, How Bkav tricked iPhone X's Face ID with a mask, `https://www.youtube.com/watch?v=i4YQRLQVixM`, last accessed: February 19, 2021(2017).

[87] S. Bhattacharjee, M. Ivanova, A. Rozeva, M. Durcheva, S. Marcel, Enhancing trust in eAssessment - the TeSLA system solution, in: International Technology Enhanced Assessment Conference (TEA), 2018, pp. 1–18.

[88] C. Rathgeb, A. Uhl, A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security 3.

[89] Institute of Electrical and Electronics Engineers, IEEE 2410-2019 - IEEE Standard for Biometric Open Protocol (June 2019).

[90] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doroz, B. Sunar, Practical homomorphic encryption: A survey, in: International. Symposium on Circuits and Systems (ISCAS), IEEE, 2014, pp. 2792–2795.

[91] K. Okereafor, I. Ekong, I. O. Markson, K. Enwere, Fingerprint biometric system hygiene and the risk of COVID-19 transmission, Biomedical Engineering 5 (1) (2020) e19623.

[92] M. A. Olsen, M. Dusio, C. Busch, Fingerprint skin moisture impact on biometric performance, in: International Workshop on Biometrics and Forensics (IWBF), IEEE, 2015, pp. 1–6.

[93] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, M. Margraf, An overview of touchless 2D fingerprint recognition, EURASIP Journal on Image and Video Processing.

[94] A. Kumar, Contactless 3D Fingerprint Identification, Advances in Computer Vision and Pattern Recognition, Springer, 2018.

[95] R. Raghavendra, K. B. Raja, J. Surbiryala, C. Busch, A low-cost multimodal biometric sensor to capture finger vein and fingerprint, in: International Joint Conference on Biometrics (IJCB), IEEE, 2014, pp. 1–7.

[96] J. Galbally, G. Bostrom, L. Beslay, Full 3D touchless fingerprint recognition: Sensor, database and baseline performance, in: International Joint Conference on Biometrics (IJCB), IEEE, 2017, pp. 225–233.

[97] A. Kumar, Y. Zhou, Contactless fingerprint identification using level zero features, in: Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE, 2011, pp. 114–119.

[98] C. Stein, C. Nickel, C. Busch, Fingerphoto recognition with smartphone cameras, in: International Conference of Biometrics Special Interest Group (BIOSIG), IEEE, 2012, pp. 1–12.

[99] J. M. Libert, J. D. Grantham, B. Bandini, K. Ko, S. Orandi, C. I. Wat-

son, Interoperability assessment 2019: Contactless-to-contact fingerprint capture, Tech. Rep. NISTIR 8307, National Institute of Standards and Technology (May 2020).

[100] S. Orandi, J. M. Libert, B. Bandini, K. Ko, J. D. Grantham, C. I. Watson, Evaluating the operational impact of contactless fingerprint imagery on matcher performance, Tech. Rep. NISTIR 8315, National Institute of Standards and Technology (September 2020).

[101] P. Salum, D. Sandoval, A. Zaghetto, B. Macchiavello, C. Zaghetto, Touchless-to-touch fingerprint systems compatibility method, in: International Conference on Image Processing (ICIP), IEEE, 2017, pp. 3550–3554.

[102] C. Lin, A. Kumar, Matching contactless and contact-based conventional fingerprint images for biometrics identification, Transactions on Image Processing 27 (4) (2018) 2008–2021.

[103] C. Kauba, B. Prommegger, A. Uhl, Combined fully contactless finger and hand vein capturing device with a corresponding dataset, Sensors 19 (22) (2019) 5014–5039.

[104] H. Ma, S. Y. Zhang, Contactless finger-vein verification based on oriented elements feature, Infrared Physics & Technology 97 (2019) 149–155.

[105] F. Marattukalam, W. H. Abdulla, On palm vein as a contactless identification technology, in: Australian & New Zealand Control Conference (ANZCC), IEEE, 2019, pp. 270–275.

[106] L. Debiasi, C. Kauba, B. Prommegger, A. Uhl, Near-infrared illumination add-on for mobile hand-vein acquisition, in: International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2018, pp. 1–9.

[107] A. Malhotra, A. Sankaran, A. Mittal, M. Vatsa, R. Singh, Chapter 6 - fingerphoto authentication using smartphone camera captured under varying environmental conditions, in: Human Recognition in Unconstrained Environments, Academic Press, 2017, pp. 119–144.

[108] B. W. Schuller, D. M. Schuller, K. Qian, J. Liu, H. Zheng, X. Li, COVID-19 and computer audition: An overview on what speech & sound analysis could contribute in the SARS-CoV-2 corona crisis, arXiv preprint arXiv:2003.11117.

[109] G. Deshpande, B. W. Schuller, Audio, speech, language, & signal processing for COVID-19: A comprehensive overview, arXiv preprint arXiv:2011.14445.

[110] K. D. Bartl-Pokorny, F. B. Pokorny, A. Batliner, S. Amiriparian, A. Semertzidou, F. Eyben, E. Kramer, F. Schmidt, R. Schönweiler, M. Wehler, B. W. Schuller, The voice of COVID-19: Acoustic correlates of infection, arXiv preprint arXiv:2012.09478.

[111] J. Shuja, E. Alanazi, W. Alasmary, A. Alashaikh, COVID-19 open source data sets: A comprehensive survey, Applied Intelligence (2020) 1–30.

[112] A. Imran, I. Posokhova, H. N. Qureshi, U. Masood, S. Riaz, K. Ali, C. N. John, M. Nabeel, AI4COVID-19: AI enabled preliminary diagnosis for COVID-19 from cough samples via an app, arXiv preprint arXiv:2004.01275.

[113] C. Brown, J. Chauhan, A. Grammenos, J. Han, A. Hasthanasombat, D. Spathis, T. Xia, P. Cicuta, C. Mascolo, Exploring automatic diagnosis of COVID-19 from crowdsourced respiratory sound data, arXiv preprint arXiv:2006.05919.

[114] N. Sharma, P. Krishnan, R. Kumar, S. Ramoji, S. R. Chetupalli, P. K. Ghosh, S. Ganapathy, Coswara–a database of breathing, cough, and voice sounds for COVID-19 diagnosis, arXiv preprint arXiv:2005.10548.

[115] M. Faezipour, A. Abuzneid, Smartphone-based self-testing of COVID-19 using breathing sounds, Telemedicine and e-Health 26 (10) (2020) 1202–1205.

[116] S. Trivedy, M. Goyal, P. R. Mohapatra, A. Mukherjee, Design and development of smartphone-enabled spirometer with a disease classification system using convolutional neural network, Transactions on Instrumentation and Measurement (2020) 7125–7135.

[117] J. Han, K. Qian, M. Song, Z. Yang, Z. Ren, S. Liu, J. Liu, H. Zheng, W. Ji, T. Koike, X. Li, Z. Zhang, Y. Yamamoto, B. W. Schuller, An early study on intelligent analysis of speech under COVID-19: Severity, sleep quality, fatigue, and anxiety, in: Interspeech, ISCA, 2020, pp. 4946–4950.

[118] B. Goodwin, L. M. Alvarez, Airports deploy thermal cameras to control covid-19, science suggests it's merely 'safety theatre', `https://www.computerweekly.com/news/252485233/Airports-deploy-thermal-cameras-to-control-Covid-19-science-suggests-its-merely-safety-theatre`, last accessed: February 19, 2021(2020).

[119] NDTV, Thermal screening, masks, hand hygiene mandatory in malls under new guidelines, `https://www.ndtv.com/india-news/24-30-degrees-ac-temperature-social-distancing-detailed-guidelines-for-malls-2240889`, last accessed: February 19, 2021(2020).

[120] J.-W. Lin, M.-H. Lu, Y.-H. Lin, A thermal camera based continuous body temperature measurement system, in: International Conference on Computer Vision Workshops (ICCVW), IEEE/CVF, 2019, pp. 1681–1687.

[121] K. Mallat, N. Damer, F. Boutros, A. Kuijper, J.-L. Dugelay, Cross-spectrum thermal to visible face recognition based on cascaded image synthesis, in: International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–8.

[122] S. M. Iranmanesh, N. M. Nasrabadi, Attribute-guided deep polarimetric thermal-to-visible face recognition, in: International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–8.

[123] N. Damer, F. Boutros, K. Mallat, F. Kirchbuchner, J. Dugelay, A. Kuijper, Cascaded generation of high-quality color visible face images from thermal captures, CoRR abs/1910.09524. `arXiv:1910.09524`. URL `http://arxiv.org/abs/1910.09524`

[124] J. Deng, J. Guo, N. Xue, S. Zafeiriou, ArcFace: Additive angular margin loss for deep face recognition, in: Conference on Computer Vision and Pattern Recognition, Computer Vision Foundation / IEEE, 2019, pp. 4690–4699.

[125] S. Farokhi, J. Flusser, U. U. Sheikh, Near infrared face recognition: A literature survey, Computer Science Review 21 (2016) 1–17.

[126] B. J. Quilty, S. Clifford, S. Flasche, R. M. Eggo, Effectiveness of airport screening at detecting travellers infected with novel coronavirus (2019-nCoV), Eurosurveillance 25 (5) (2020) 2000080.

[127] European Union Aviation Safety Agency (EASA), EASA ECDC COVID-19 aviation health safety protocol, `https://www.easa.europa.eu/document-library/general-publications/covid-19-aviation-health-safety-protocol`, last accessed: February 19, 2021(2020).

Marta Gomez-Barrero is a Professor for IT-Security and technical data privacy at the Hochschule Ansbach, Germany. She serves as General Co-Chair of the BIOSIG conference and is PI of RESPECT (ANR-DFG Project). Her research interests include security and privacy evaluations of biometric systems, presentation attack detection methodologies, and biometric template protection schemes.

Dr. Christian Rathgeb is a Senior Researcher with the Faculty of Computer Science, Hochschule Darmstadt (HDA), Germany. He is a Principal Investigator in the National Research Center for Applied Cybersecurity ATHENE. He is a consultant at the secunet Security Networks.

Dr. Pawel Drozdowski is a Senior Researcher with the Faculty of Computer Science, Hochschule Darmstadt, Germany. He researches biometrics, information security and privacy, pattern recognition, and algorithmic fairness. He co-authored over 25 technical publications in those fields and represents the German Institute for Standardization in ISO/IEC JTC 1/SC 37.

Jose Patino (PhD, Sorbonne University, 2019) is a post-doctoral researcher at Audio Security and Privacy group at EURECOM, France. He co-organised the inaugural VoicePrivacy challenge and is currently involved in the ASVspoof consortium. His research interests include topics in voice biometrics and privacy preservation in speech processing.

Massimiliano Todisco (Member, IEEE) is an Assistant Professor within the Digital Security Department at EURECOM, France. He is serving as PI for the projects: TReSPAsS-ETN (H2020 MSCA), and RESPECT (French-German collaborative programme). He has more than 100 publications. His current interests are privacy-preserving DNN architectures for speech processing and fake audio detection.

Andreas Nautsch is with the Audio Security and Privacy group (EURECOM). He received the doctorate from TU Darmstadt (2019); served as project editor of the ISO/IEC 19794-13:2018 standard; is associate editor of the EURASIP JASMP, is co-initiator and co-chair of the ISCA SIG on Security & Privacy in Speech Communication.

Naser Damer is a senior researcher at Fraunhofer IGD. He received his PhD from TU Darmstadt (2018). He is a principal investigator at the ATHENE Center, serves as an AE for the Visual Computer journal, and represents the German Institute for Standardization (DIN) in ISO/IEC SC37 standardization committee.

Jannis Priesnitz received his B.Sc. degree of Computer Science in 2015 and his M.Sc. degree in 2018 from the Hochschule Darmstadt. Since 2018 he is a Ph.D. Student Member of da/sec at the ATHENE – National Research Center for Applied Cybersecurity. His current research focuses on mobile touchless fingerprint recognition.

Nicholas Evans is a Professor at EURECOM, France, where he heads the Audio Security and Privacy Group. His research interests include automatic speaker verification, presentation attack detection and privacy preservation. He serves as associate editor for IEEE TBIOM and is a co-founder of the community-led ASVspoof and VoicePrivacy initiatives.

Christoph Busch is member of NTNU-Gjøvik, Norway and HDA, Germany. Further he lectures at Denmark's DTU. He was initiator and participated in multiple projects on biometrics (e.g. 3D-Face, FIDELITY, iMARS), is PI in ATHENE, co-founder of the European Association for Biometrics (EAB) and convenor of WG3 in ISO/IEC JTC1 SC37.