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

Marta Gomez-Barrero, *Member, IEEE*, Pawel Drozdowski, Christian Rathgeb, Jose Patino, Massimiliano Todisco, Andreas Nautsch, Naser Damer, *Member, IEEE*, Jannier Priesnitz, Nicholas Evans, and Christoph Busch, *Senior Member, IEEE*

***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.**

***Index Terms*—COVID-19, biometrics, mask, hygiene, touchless biometrics, remote authentication, mobile biometrics.**

I. 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 250 million confirmed infections while more than five 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

(a) Surgical mask [5]

(b) Cloth mask [5]

(c) Filter mask[1]

(d) Printed mask[2]

Fig. 1. Examples of typical protective face masks.

Manuscript received 1 December 2021; revised 11 July 2022; accepted 19 August 2022. Date of publication 1 September 2022; date of current version 15 December 2022. This work was supported 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 under Grant 406880674 and Grant ANR-18-CE92-0024. *(Corresponding author: Marta Gomez-Barrero.)*

Marta Gomez-Barrero is with Hochschule Ansbach, 91522 Ansbach, Germany (e-mail: marta.gomez-barrero@hs-ansbach.de).

Pawel Drozdowski, Christian Rathgeb, Jannier Priesnitz, and Christoph Busch are with the da/sec—Biometrics and Internet Security Research Group, Hochschule Darmstadt, 64295 Darmstadt, Germany.

Jose Patino, Massimiliano Todisco, and Nicholas Evans are with EURECOM, 06904 Sophia Antipolis, France.

Andreas Nautsch was with EURECOM, 06904 Sophia Antipolis, France. He is now with Avignon University, 84029 Avignon, France.

Naser Damer is with the Fraunhofer Institute for Computer Graphics Research IGD, 64283 Darmstadt, Germany.

Digital Object Identifier 10.1109/TTS.2022.3203571

[1] Source: www.ikatehouse.com.

[2] Source: www.thenationalnews.com.

TABLE I
OVERVIEW OF COMMONLY USED 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

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). 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].

Biometric technologies have come to play an integral role in society, e.g., for identity management, surveillance, access 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 [14]. It should be however noted that the new measures have a limited impact on other biometric characteristics such as ear [15]. Even though this fact will also lead to renewed efforts directed to such biometric characteristics in order to achieve accurate and deployable systems in the near future, we limit the scope of this article to those biometric characteristics affected by health-related measures.

Table I 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. This work represents a narrative/integrated review. It is meant to selectively assess relevant works in the field of biometrics that (in)directly tackle challenges caused by the COVID-19 pandemic. It is aiming at offering guidance about future research directions and enabling new perspectives to emerge.

The rest of the article is organised as follows. The impact of facial masks on biometrics technologies is discussed in Section II. Section III addresses impacts upon mobile and remote biometric authentication. Section IV describes new opportunities and applications that have emerged as a result of the COVID-19 pandemic. The societal impact of these changes is discussed in Section V and concluding remarks are presented in Section VI.

II. 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.

A. 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 [16]. 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 [17], [18]. Relevant to the study presented here is a large body of research on occluded face detection [19] and recognition [20], though occlusion-invariant face recognition remains challenging [21]. 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) [22], [23]. The evaluation was performed using a large dataset of facial images with superimposed, digitally generated masks of varying size, shape, 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 [22], 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 [23], 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 [24].

Results from the related DHS Biometric Rally show similar trends [25]. 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 [25] tested with unmasked face images.

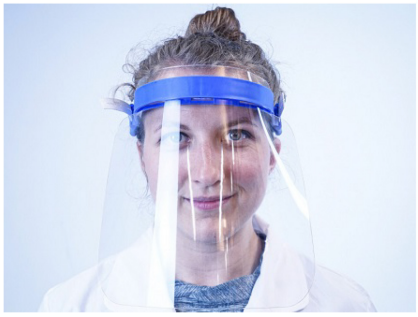
These U.S.-based studies are complemented by a number of academic studies. Two datasets [5], [26] of masked face images have been collected in Europe and China to support research efforts. While [26] provides data, however, it does not provide a formal evaluation of the effect of masks on face recognition performance. Moreover, this study did not address a specific usecase scenario, e.g., collaborative face verification. Damer *et al.* [5], [27], [28] 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 [22]: 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 [29], [30]. A recent study by Mathai *et al.* [31] 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 [32].

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 [33]. This quality estimation indicates the suitability of the image for recognition purposes [34], [35]. For

(a) Transparent mask[3]



(b) Face shield[4]

Fig. 2. Examples of alternative protective masks.

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 [36], 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.* [37] 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 numerous 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 [38], unconstrained data acquisition in general, as well as effects on the accuracy of human examiners [23], [28]. In addition, new areas of research have been opened, such as the automatic detection of whether a subject is wearing the mask correctly (i.e., covering mouth and nose) [39].

To foster research on the aforementioned issues, the Masked Face Recognition Competition (MFR) [40] was organised in 2021. The main goals of this competition were not only the enhancement of recognition performance in the presence of masks, but also the analysis of the deployability of the proposed solutions. A private dataset representing a collaborative multi-session real masked capture scenario was used to evaluate the submitted solutions. In comparison to one of the top performing academic face recognition solutions, 10 out of the 18 submitted solutions did achieve a higher masked face verification accuracy, thereby showing the way for future face recognition approaches. This was followed by a series of works that targeted enhancing the accuracy of masked face recognition, either by training task-specific models [41] or processing face templates extracted by existing models [42].

[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.

B. 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 [43]. 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 at a distance even from only reasonably cooperative data subjects on the move (e.g., while walking) [44], [45].

Solutions to iris recognition which use mobile devices and which operate using only visible wavelength illumination have been proposed in recent years [46], [47], [48]. 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 [49]. 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 [17], [18]. 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 [50] in addition to other biometric data. Due to their high computational efficiency and reliability [51], iris recognition systems are used successful within the Aadhaar programme for intensive identification (1-*N* search) and de-duplication (*N*-*N* search) [11].

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.

Fig. 3. IrisGuard Inc. UAE enrolment station.[5]

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., [52]). 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 recognition [53]. 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.

C. Periocular Recognition and Soft-Biometrics

Periocular recognition, namely recognition observing biometric characteristics from the area surrounding the eye [54], 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 [55], [56] 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 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 [56]. Similarly, Park *et al.* showed in [57] 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. Some newer works have also explored the fair of these methods across gender [58], reporting an equivalent performance of males and females for ocular-based mobile user-authentication at lower false match rates.

In addition to the aforementioned works, some multimodal approaches combining face, iris, and the periocular region have been proposed for mobile devices [59], also incorporating template protection in order to comply with the newest data privacy regulations such as the European GDPR [60].

As pointed out in Section II-B, 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 [49], [61], 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 purpose, 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 [62] or deep learning [63].

D. Voice Recognition

Progress in voice recognition has been rapid in recent years [64], [65], [66], [67], [68]. Being among the most convenient of all biometrics technologies, voice recognition

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

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 [69]. 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 [70], [71], 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 [72]: a bonafide user emits pop noise which naturally incurred while speaking close to the microphone. This 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 [73].

Related to these aforementioned issues, a study of the impact of face coverings upon the voice biometrics is reported in [74]. 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.

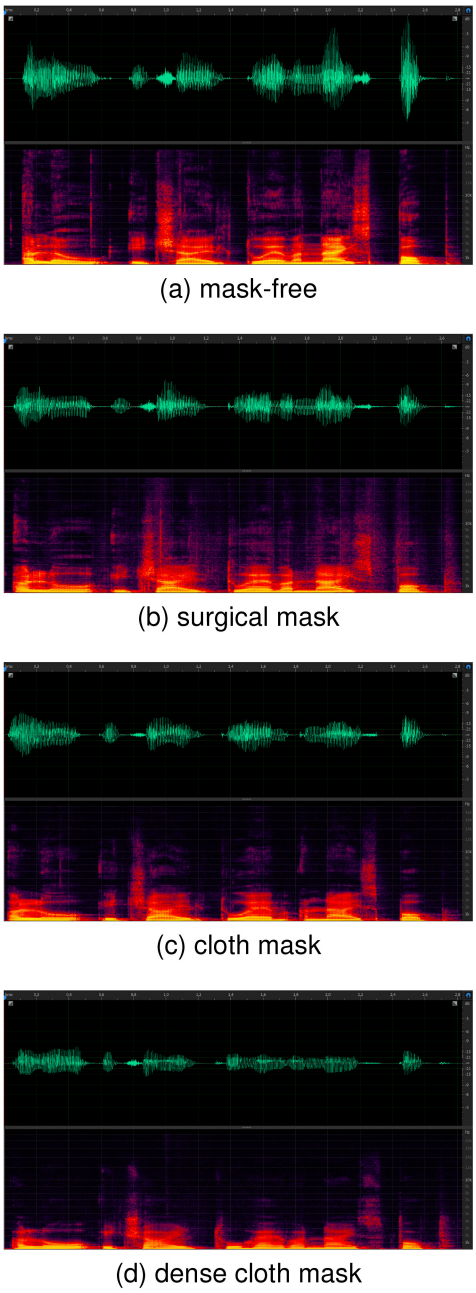


Fig. 4. Examples of four spectrograms of the utterance: *allow each child to have an ice pop*, pronounced by the same speaker wearing different types of masks: (a) mask-free, (b) surgical, (c) cloth and (d) dense cloth mask.

To reflect the current issues in the voice biometrics community, the 2020 findings of the 12th Computational Paralinguistics Challenge (COMPARE) considered a mask

detection sub-challenge. 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).

III. 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 [75]. Remote biometric authentication has already attracted significant attention [9], [76] 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 [77], [78]. 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.

A. Mobile Biometrics

The ever-increasing number of smartphones in use today has fueled research in mobile biometric recognition solutions, e.g., mobile face recognition [79] and mobile voice recognition [80], [81], [82]. Numerous biometric algorithms specifically designed or adapted to the mobile environment have been proposed in the literature [83]. 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 [84]. 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. These comparisons depend upon the secure transmission of biometric data (see Section III-C), 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 [85]. A number of different approaches to compress neural networks have been proposed, e.g., based on student-teacher networks [86] or pruning [87]. 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.

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.

B. 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 [88], [89].

In the eLearning arena, biometric technologies are used for user login, user monitoring, attention or 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 [90]. In order to minimise inconvenience, continuous biometric authentication calls for the use of biometric characteristics which require little

Fig. 5. BioID Identity Proofing for e-learning platforms [92].

to no user cooperation [88], e.g., text-independent keystroke dynamics [7], [91].

Presentation attacks can present a substantial threat to biometric technologies deployed in such scenarios (see Section III-C). This might be why, despite significant research interest, only few biometric recognition systems have been deployed in operational eLearning scenarios [88]. 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.

C. 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' [93], [94], [95]. 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 [96]. If PAD is implemented on the server side, then software-based attack detection mechanisms represent the only solution. Such software-based PAD for remote face and voice recognition were explored in the EU-H2020 TeSLA project [97]. It is expected that more research will be devoted to this topic in the future [98], [99].

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 biometric recognition in the form of template protection [100] overcome this vulnerability by enabling comparison of 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) [101] which supports the homomorphic encryption [102] 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.

IV. 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.

A. 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 [103]. 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 [104]. 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 [105], [106] such as those illustrated in Fig. 7. Touchless fingerprint sensors are generally either prototype hardware designs [107], [108] or are adapted from general purpose devices adapted to touchless fingerprint recognition [109], [110].

Both the capture and processing of fingerprints must usually be adapted to touchless acquisition [105]. The majority of touchless finger image acquisition sensors deliver colour

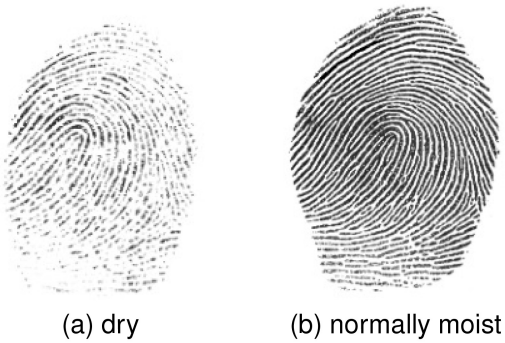


Fig. 6. Example of a dry fingerprint and the same fingerprint with normal moist (taken from [104]).

Fig. 7. Touchless capturing of fingerprints.

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 [111], [112]. While some differences between the two systems, e.g., mirroring, colour-to-grayscale conversion or inverted back- and foreground, can be readily compensated for without degrading accuracy, others, e.g., the aspect ratio or deformation estimation, prove more challenging [113], [114] 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 [115], [116], [117], 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 [115]. 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 [116] 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 [118]. 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[7] 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 [105], [106], [115]. 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 [105], [119].

B. 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 [120], [121], [122].

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 [123]. The data typically includes recordings of coughs [124], [125], [126], breathing sounds [127], [128] as well as speech excerpts [129].

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

[7]https://www.veinseek.com/

The database described in [129] contains recordings of five spoken sentences and in-the-wild speech, all recorded using 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 pre-processing, 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. Outcomes of these studies are very encouraging: the detection of COVID-19 through voice, but also through coughing or the sound of breathing, has an accuracy comparable to that of the antigen or saliva test [130], [131], [132], [133].

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 [134] and shopping centres [135]. Thermal face images can be used to detect individuals with fever [136], a possible symptom of COVID-19 infection. Similar face captures can also be used as an alternative capture spectrum for face recognition [137], [138], [139], however, with verification performances inferior to the visible [140], [141]. Despite the ease with which thermal monitoring can be deployed, it is argued in [142] 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 [143].

V. Societal Impact

As any other technology used by a large population, biometric recognition systems affect the society. So far, the positive aspects of such systems (e.g., faster authentication for border crossing or convenience for smartphone unlocking) have outweighed their disadvantages, mostly related to privacy and security issues [144], [145]. Such issues have been thoroughly analysed and (partially) dealt with, thereby increasing the acceptance of the users and boosting the deployment of biometric systems. Nevertheless, in the last years new, concerns have arisen related to the fairness of biometric recognition algorithms [146] and their trustworthiness [147], [148]. In addition, societal and ethical aspects of presentation attack detection methods have also been analysed [149].

In the context of the COVID-19 pandemic, the use of contact-based biometric systems have similarly lead to health-related concerns. Systems where contact with the capture device is necessary could still be employed in a private scenario (e.g., for unlocking your own smartphone or for remote for authentication from your own laptop), but contact-less approaches will be preferred for global applications (e.g., building access control) in order to prevent the spread of viruses. In fact, it can be argued that the use of contact-less biometrics can even reduce the transmission of pathogens in some scenarios such as airport [150]. This trend will probably remain even after the COVID-19 pandemic can be considered to be over.

On the other hand, the need for further digitalisation in almost all societal levels, including sensitive applications such as online exams or eHealth systems, where subject identification is of the utmost importance, has increased the acceptance of biometric technologies as a convenient and reliable means of authentication. Thus, more research is being done in this area [151], [152], together with socioeconomic analysis of success and failure of big-scale implementations of such systems [153].

However, further digitalisation also brings some disadvantages. In general, and not only regarding biometric recognition, the tracking activities and health checks implemented worldwide in order to prevent the spread of COVID-19 have had deep implications on the privacy and freedom of the subjects. For instance, free travel within Schengen has been suspended for months, needing to fulfill certain criteria in terms of negative COVID-19 tests, vaccination status, or registration forms to enter a country.[8] In addition, facial recognition systems have been used in countries such as Poland, China, or Russia to ensure that individuals in quarantine remain at home. In spite of the benefits for the collective health, "*the use of biometrics (including facial recognition) in response to COVID-19 raises a number of privacy and security concerns, particularly when these technologies are being used in the absence of specific guidance or fully informed and explicit consent. Individuals may also have problems exercising a wide range of fundamental rights, including the right of access to their personal data, the right to erasure, and the right to be informed as to the purposes of processing and who that data is shared with*", as the Organisation for Economic Co-operation and Development (OECD) states in its policy response to Coronavirus (COVID-19) [154]. Thus, the OECD gives a number of recommendations including the use of privacy-by-design approaches, such as the ones described in Section III-C, and the limitation on the time sensitive data can be stored.

The added societal concerns due to the exploitation of sensitive biometric data have been also addressed by The British Academy [155]. As the Academy points out, "*Sharing data is crucial for furthering research and maximising its potential to help overcome the current pandemic and better prepare for future health crises*". However, bias or errors derived from the use of biometric technologies for authentication can result in negative impacts such as discrimination, and diminish the trust on COVID-19 related technologies. Therefore, the Academy recommends maintaining a human element in the loop. In addition, existing digital inequalities might also limit the potential benefits of health technologies and increase the social disadvantages of some groups. The report also includes some numbers: "*6 million people in the UK cannot turn on a device and up to 50% of those are aged under 65*". Furthermore, in order to minimise the potential discrimination caused by biometric technologies, several characteristics

[8] https://reopen.europa.eu/en/

should be considered: apps which rely on voice recognition software that may not work effectively for those with a speech impairment, can be beneficial for those with reduced sight.

In March 2022, the European Data Protection Supervisor (EDPS) published a report on COVID-19 related processing of the Union institutions, bodies, offices and agencies (EUIs) [156]. In this survey, the EDPS reviews body temperature checks, contact tracing, COVID testing and handling of results, monitoring presence within the premises, vaccination campaigns, access control, and the use of IT-tools in telework. Regarding access control, where biometric recognition systems can be in place, the EUIs correctly informed the individuals about the processing activities carried our and specified a time limit for data retention, as recommended by the OECD. However, as the report points out, the lawful grounds of this identification requirement may not be given, since "*staff members [· · ·] cannot provide freely given, specific, informed and unambiguous as well as explicit consent*". Similarly, "*consent would also not be appropriate for visitors, who are in most cases obliged to come to the EUI premises for work purposes*". Also, some EUIs had not indicated that they process health data even if they were doing so. In view of these negative impact on the privacy rights of the individuals, the EDPS recommends the EUIs to check the lawfulness and regularly reassess the necessity and proportionality of the existing COVID-related processing activities.

From those reports we can conclude that biometrics and other technologies have not only provided the subjects with additional advantages to access digital services, but have also had a negative impact on their right to privacy. Thus, we would like to urge the community to assess the necessity of identity checks before implementing them, and use all the available tools to minimise the negative impact of such a control: biometric template protection schemes to prevent sensitive data leakage, or presentation attack detection modules to minimise the success chances of identity theft.

VI. Conclusion

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.

Still, 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.

References

[1] "Coronavirus disease (COVID-19) pandemic." World Health Organization. Accessed: Aug. 23, 2022. [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019

[2] "Re-open EU." European Union. Accessed: Aug. 23, 2022. [Online]. Available: https://reopen.europa.eu/

[3] "What countries require masks in public or recommend masks?" #Masks4All. Accessed: Aug. 23, 2022. [Online]. Available: https://masks4all.co/what-countries-require-masks-in-public/

[4] L. Peeples, "Face masks: What the data say," *Nature*, vol. 586, no. 7828, pp. 186–189, Oct. 2020.

[5] N. Damer, J. H. Grebe, C. Chen, F. Boutros, F. Kirchbuchner, and A. Kuijper, "The effect of wearing a mask on face recognition performance: An exploratory study," in *Proc. Int. Conf. Biometrics Spec. Interest Group (BIOSIG)*, Darmstadt, Germany, Sep. 2020, pp. 1–10.

[6] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.

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

[8] M. Tistarelli and C. Champod, *Handbook of Biometrics for Forensic Science*. Cham, Switzerland: Springer, 2017. [Online]. Available: https://link.springer.com/book/10.1007/978-3-319-50673-9

[9] M. Tistarelli, S. Z. Li, and R. Chellappa, *Handbook of Remote Biometrics*. London, U.K.: Springer, 2009. [Online]. Available: https://link.springer.com/book/10.1007/978-1-84882-385-3

[10] A. N. Al-Raisi and A. M. Al-Khouri, "Iris recognition and the challenge of homeland and border control security in UAE," *Telematics Inform.*, vol. 25, no. 2, pp. 117–132, May 2008.

[11] A. Dalwai, "Aadhaar technology and architecture: Principles, design, best practices and key lessons," Unique Identif. Authority India (UIDAI), New Delhi, India, Rep., Mar. 2014.

[12] "Smart borders." European Commission. 2018. Accessed: Aug. 23, 2022. [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en

[13] "Automated fingerprint identification system (AFIS) overview—A short history." Thales. Apr. 2019. Accessed: Aug. 23, 2022. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history

[14] S. Carlaw, "Impact on biometrics of COVID-19," *Biometric Technol. Today*, vol. 2020, no. 4, pp. 8–9, 2020.

[15] Ž. Emeršič *et al.*, "The unconstrained ear recognition challenge 2019," in *Proc. Int. Conf. Biometrics (ICB)*, 2019, pp. 1–15.

[16] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*. London, U.K.: Springer, 2011.

[17] I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Deep face recognition: A survey," in *Proc. Conf. Graph. Patterns Images (SIBGRAPI)*, Oct. 2018, pp. 471–478.

[18] G. Guo and N. Zhang, "A survey on deep learning based face recognition," *Comput. Vis. Image Understanding*, vol. 189, Dec. 2019, Art. no. 102805.

[19] M. Opitz, G. Waltner, G. Poier, H. Possegger, and H. Bischof, "Grid loss: Detecting occluded faces," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Oct. 2016, pp. 386–402.

[20] D. Zeng, R. N. J. Veldhuis, and L. Spreeuwers, "A survey of face recognition techniques under occlusion," 2020, *arXiv:2006.11366*.

[21] L. Song, D. Gong, Z. Li, C. Liu, and W. Liu, "Occlusion robust face recognition based on mask learning with pairwise differential siamese network," in *Proc. Int. Conf. Comput. Vis. (ICCV)*, Oct. 2019, pp. 773–782.

[22] M. Ngan, P. Grother, and K. Hanaoka, "Ongoing face recognition vendor test (FRVT) part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8311, Jul. 2020.

[23] M. Ngan, P. Grother, and K. Hanaoka, "Ongoing face recognition vendor test (FRVT) part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8331, Nov. 2020.

[24] "FRVT face mask effects." National Institute of Standards and Technology. Nov. 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://pages.nist.gov/frvt/html/frvt_facemask.html

[25] "Biometric technology rally at MdTF." Department of Homeland Security. 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://mdtf.org/Rally2020

[26] Z. Wang *et al.*, "Masked face recognition dataset and application," 2020, *arXiv:2003.09093*.

[27] N. Damer, F. Boutros, M. Süßmilch, F. Kirchbuchner, and A. Kuijper, "Extended evaluation of the effect of real and simulated masks on face recognition performance," *IET Biom.*, vol. 10, no. 5, pp. 548–561, 2021. [Online]. Available: https://doi.org/10.1049/bme2.12044

[28] N. Damer, F. Boutros, M. Süßmilch, M. Fang, F. Kirchbuchner, and A. Kuijper, "Masked face recognition: Human versus machine," *IET Biometrics*, to be published. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/bme2.12077

[29] Y. Li, S. Liu, J. Yang, and M.-H. Yang, "Generative face completion," in *Proc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 5892–5900.

[30] J. Zhang, R. Zhan, D. Sun, and G. Pan, "Symmetry-aware face completion with generative adversarial networks," in *Proc. Asian Conf. Comput. Vis. (ACCV)*, Dec. 2018, pp. 289–304.

[31] J. Mathai, I. Masi, and W. AbdAlmageed, "Does generative face completion help face recognition?" in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2019, pp. 1–8.

[32] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition," in *Proc. Conf. Comput. Commun. Security*, Oct. 2016, pp. 1528–1540.

[33] T. Schlett, C. Rathgeb, O. Henniger, J. Galbally, J. Fiérrez, and C. Busch, "Face image quality assessment: A literature survey," 2020, *arXiv:2009.01103*.

[34] P. Terhörst, J. N. Kolf, N. Damer, F. Kirchbuchner, and A. Kuijper, "SER-FIQ: Unsupervised estimation of face image quality based on stochastic embedding robustness," in *Proc. CVPR*, 2020, pp. 5650–5659.

[35] F. Boutros, M. Fang, M. Klemt, B. Fu, and N. Damer, "CR-FIQA: Face image quality assessment by learning sample relative classifiability," 2021, *arXiv:2112.06592*.

[36] D. Lin and X. Tang, "Quality-driven face occlusion detection and recovery," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Minneapolis, MN, USA, Jun. 2007, pp. 1–7. [Online]. Available: https://doi.org/10.1109/CVPR.2007.383052

[37] L. Zhang, X. Shao, F. Yang, P. Deng, X. Zhou, and Y. Shi, "Multi-branch face quality assessment for face recognition," in *Proc. 19th IEEE Int. Conf. Commun. Technol. (ICCT)*, Xi'an, China, Oct. 2019, pp. 1659–1664. [Online]. Available: https://doi.org/10.1109/ICCT46805.2019.8947255

[38] B. Fu, N. Spiller, C. Chen, and N. Damer, "The effect of face morphing on face image quality," in *Proc. 20th Int. Conf. Biometrics Spec. Interest Group (BIOSIG)*, Sep. 2021, pp. 173–180. [Online]. Available: https://dl.gi.de/20.500.12116/37451

[39] B. Batagelj, P. Peer, V. Štruc, and S. Dobrišek, "How to correctly detect face-masks for COVID-19 from visual information?" *Appl. Sci.*, vol. 11, no. 5, p. 2070, 2021.

[40] F. Boutros *et al.*, "MFR 2021: Masked face recognition competition," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2021, pp. 1–10.

[41] M. Huber, F. Boutros, F. Kirchbuchner, and N. Damer, "Mask-invariant face recognition through template-level knowledge distillation," in *Proc. 16th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG)*, Jodhpur, India, Dec. 2021, pp. 1–8. [Online]. Available: https://doi.org/10.1109/FG52635.2021.9667081

[42] F. Boutros, N. Damer, F. Kirchbuchner, and A. Kuijper, "Self-restrained triplet loss for accurate masked face recognition," *Pattern Recognit.*, vol. 124, Apr. 2022, Art. no. 108473. [Online]. Available: https://doi.org/10.1016/j.patcog.2021.108473

[43] J. Daugman, "How iris recognition works," *Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[44] J. R. Matey, "Iris on the Move™," in *Encyclopedia of Biometrics*, S. Z. Li and A. K. Jain, Eds. Boston, MA, USA: Springer, 2009, pp. 805–810.

[45] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan, and A. Ross, "Long range iris recognition: A survey," *Pattern Recognit.*, vol. 72, pp. 123–143, Dec. 2017.

[46] H. Proença, "Iris recognition: On the segmentation of degraded images acquired in the visible wavelength," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 8, pp. 1502–1516, Aug. 2010.

[47] K. B. Raja, R. Raghavendra, V. K. Vemuri, and C. Busch, "Smartphone based visible iris recognition using deep sparse filtering," *Pattern Recognit. Lett.*, vol. 57, pp. 33–42, May 2015.

[48] A. Rattani and R. Derakhshani, "Ocular biometrics in the visible spectrum: A survey," *Image Vis. Comput.*, vol. 59, pp. 1–16, Mar. 2017.

[49] J. Tapia, M. Gomez-Barrero, and C. Busch, "An efficient super-resolution single image network using sharpness loss metrics for iris," in *Proc. Int. Workshop Inf. Forensics Security (WIFS)*, Dec. 2020, pp. 1–6.

[50] "Aadhaar dashboard." Unique Identification Authority of India. Accessed: Aug. 23, 2022. [Online]. Available: https://www.uidai.gov.in/aadhaar_dashboard/

[51] J. Daugman and C. Downing, "Searching for doppelgängers: Assessing the universality of the IrisCode impostors distribution," *IET Biometrics*, vol. 5, no. 2, pp. 65–75, Jun. 2016.

[52] S. M. Lajevardi, A. Arakala, S. A. Davis, and K. J. Horadam, "Retina verification system based on biometric graph matching," *IEEE Trans. Image Process.*, vol. 22, pp. 3625–3635, 2013.

[53] P. Rot, M. Vitek, K. Grm, Ž. Emeršič, P. Peer, and V. Štruc, *Deep Sclera Segmentation and Recognition*. Cham, Switzerland: Springer, 2020, ch. 13, pp. 395–432.

[54] F. Alonso-Fernandez and J. Bigun, "A survey on periocular biometrics research," *Pattern Recognit. Lett.*, vol. 82, pp. 92–105, Oct. 2016.

[55] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Smartphone authentication system using periocular biometrics," in *Proc. Int. Conf. Biometrics Spec. Interest Group (BIOSIG)*, 2014, pp. 1–8.

[56] T. de Freitas Pereira and S. Marcel, "Periocular biometrics in mobile environment," in *Proc. Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–7.

[57] U. Park, R. R. Jillela, A. Ross, and A. K. Jain, "Periocular biometrics in the visible spectrum," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 96–106, 2011.

[58] A. Krishnan, A. Almadan, and A. Rattani, "Probing fairness of mobile ocular biometrics methods across gender on VISOB 2.0 dataset," in *Proc. Int. Conf. Pattern Recognit.*, 2021, pp. 229–243.

[59] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 143–150.

[60] M. Stokkenes, R. Raghavendra, M. K. Sigaard, K. Raja, M. Gomez-Barrero, and C. Busch, "Multi-biometric template protection—A security analysis of binarized statistical features for bloom filters on smartphones," in *Proc. Int. Conf. Image Process. Theory Tools Appl. (IPTA)*, Dec. 2016, pp. 1–6.

[61] V. M. Ipe and T. Thomas, "Periocular recognition under unconstrained conditions using CNN-based super-resolution," in *Proc. Int. Conf. Adv. Commun. Netw. (ICACN)*, Dec. 2019, pp. 235–246.

[62] F. Alonso-Fernandez, J. Bigun, and C. Englund, "Expression recognition using the periocular region: A feasibility study," in *Proc. Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS)*, Nov. 2018, pp. 536–541.

[63] N. Reddy and R. Derakhshani, "Emotion detection using periocular region: A cross-dataset study," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2020, pp. 1–6.

[64] T. Kinnunen and H. Li, "An overview of text-independent speaker recognition: From features to supervectors," *Speech Commun.*, vol. 52, no. 1, pp. 12–40, 2010.

[65] J. H. L. Hansen and T. Hasan, "Speaker recognition by machines and humans: A tutorial review," *IEEE Signal Process. Mag.*, vol. 32, no. 6, pp. 74–99, Nov. 2015.

[66] M. Todisco, H. Delgado, and N. Evans, "Articulation rate filtering of CQCC features for automatic speaker verification," in *Proc. Interspeech*, 2016, pp. 1–5.

[67] A. Nagrani, J. S. Chung, and A. Zisserman, "VoxCeleb: A large-scale speaker identification dataset," 2017, *arXiv:1706.08612*.

[68] D. Snyder, D. Garcia-Romero, G. Sell, D. Povey, and S. Khudanpur, "X-vectors: Robust DNN embeddings for speaker recognition," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2018, pp. 5329–5333.

[69] A. Zent and J. T. Long, "Automotive sound absorbing material survey results," in *Proc. SAE Noise Vib. Conf. Exhibit.*, May 2007, pp. 1–7.

[70] H. S. Seddeq, N. M. Aly, A. A. Marwa, and M. H. Elshakankery, "Investigation on sound absorption properties for recycled fibrous materials," *J. Ind. Textiles*, vol. 43, no. 1, pp. 56–73, Jul. 2013.

[71] X. Tang and X. Yan, "Acoustic energy absorption properties of fibrous materials: A review," *Composites A, Appl. Sci. Manuf.*, vol. 101, pp. 360–380, Oct. 2017.

[72] Q. Wang *et al.*, "VoicePop: A pop noise based anti-spoofing system for voice authentication on smartphones," in *Proc. Conf. Comput. Commun.*, Apr. 2019, pp. 2062–2070.

[73] K.-N. C. Mac, X. Cui, W. Zhang, and M. Picheny, "Large-scale mixed-bandwidth deep neural network acoustic modeling for automatic speech recognition," in *Proc. Interspeech*, 2019, pp. 251–255.

[74] R. Saeidi, I. Huhtakallio, and P. Alku, "Analysis of face mask effect on speaker recognition," in *Proc. Interspeech*, Sep. 2016, pp. 1800–1804.

[75] C. Burt. "Remote authentication keeps the world working: A biometric update interview series." Accessed: Aug. 23, 2022. [Online]. Available: https://www.biometricupdate.com/202005/remote-authentication-keeps-the-world-working-a-biometric-update-interview-series

[76] G. Guo and H. Wechsler, *Mobile Biometrics* (Security. Institution of Engineering and Technology). London, U.K.: Inst. Eng. Technol., 2017.

[77] N. Kaur, P. W. C. Prasad, A. Alsadoon, L. Pham, and A. Elchouemi, "An enhanced model of biometric authentication in e-learning: Using a combination of biometric features to access e-learning environments," in *Proc. Int. Conf. Adv. Elect. Electron. Syst. Eng. (ICAEES)*, Nov. 2016, pp. 138–143.

[78] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognit. Lett.*, vol. 113, pp. 83–92, Oct. 2018.

[79] A. Rattani and R. Derakhshani, "A survey of mobile face biometrics," *Comput. Elect. Eng.*, vol. 72, pp. 39–52, Nov. 2018.

[80] E. Khoury *et al.*, "The 2013 speaker recognition evaluation in mobile environment," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[81] M. G. Gomar, "System and method for speaker recognition on mobile devices," U.S. Patent 9 042 867, May 2015.

[82] I. Bisio, C. Garibotto, A. Grattarola, F. Lavagetto, and A. Sciarrone, "Smart and robust speaker recognition for context-aware in-vehicle applications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8808–8821, Sep. 2018.

[83] A. Rattani, R. Derakhshani, and A. Ross, *Selfie Biometrics: Advances and Challenges* (Advances in Computer Vision and Pattern Recognition). Cham, Switzerland: Springer, 2019.

[84] "Fast IDentity online." FIDO Alliance. 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://fidoalliance.org/

[85] L. J. Ba and R. Caruana, "Do deep nets really need to be deep?" in *Proc. Int. Conf. Neural Inf. Process. Syst. Vol. 2*, Dec. 2014, pp. 2654–2662.

[86] P. Luo, Z. Zhu, Z. Liu, X. Wang, and X. Tang, "Face model compression by distilling knowledge from neurons," in *Proc. Conf. Artif. Intell. (AAAI)*, Feb. 2016, pp. 3560–3566.

[87] P. Molchanov, S. Tyree, T. Karras, T. Aila, and J. Kautz, "Pruning convolutional neural networks for resource efficient inference," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, Apr. 2017, pp. 1–17.

[88] C. Rathgeb, K. Pöppelmann, and E. Gonzalez-Sosa, "Biometric technologies for eLearning: State-of-the-art, issues and challenges," in *Proc. Int. Conf. Emerg. eLearn. Technol. Appl. (ICETA)*, 2020, pp. 1–6.

[89] P. S. Sanna and G. L. Marcialis, "Remote biometric verification for eLearning applications: Where we are," in *Proc. Int. Conf. Image Anal. Process. (ICIAP)*, Sep. 2017, pp. 373–383.

[90] E. Flior and K. Kowalski, "Continuous biometric user authentication in online examinations," in *Proc. Int. Conf. Inf. Technol. New Gener. (ITNG)*, Apr. 2010, pp. 488–492.

[91] A. Morales and J. Fierrez, "Keystroke biometrics for student authentication: A case study," in *Proc. Conf. Innov. Technol. Comput. Sci. Educ. (ITiCSE)*, Jun. 2015, p. 337.

[92] "Identity assured online exams & personalized e-learning." BioID, GmbH. 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://www.bioid.com/online-exams-e-learning/

[93] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Mar. 2001.

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

[95] R. Raghavendra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Comput. Surveys*, vol. 50, no. 1, pp. 1–37, 2017.

[96] Bkav Corp. *How Bkav Tricked iPhone X's Face ID With a Mask*. (2017). Accessed: Aug. 23, 2022. [Online Video]. Available: https://www.youtube.com/watch?v=i4YQRLQVixM

[97] S. Bhattacharjee, M. Ivanova, A. Rozeva, M. Durcheva, and S. Marcel, "Enhancing trust in eAssessment—The TeSLA system solution," in *Proc. Int. Technol. Enhanced Assessment Conf. (TEA)*, 2018, pp. 1–18.

[98] M. Fang, F. Boutros, A. Kuijper, and N. Damer, "Partial attack supervision and regional weighted inference for masked face presentation attack detection," in *Proc. 16th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG)*, Jodhpur, India, Dec. 2021, pp. 1–8. [Online]. Available: https://doi.org/10.1109/FG52635.2021.9667051

[99] M. Fang, N. Damer, F. Kirchbuchner, and A. Kuijper, "Real masks and spoof faces: On the masked face presentation attack detection," *Pattern Recognit.*, vol. 123, Mar. 2022, Art. no. 108398. [Online]. Available: https://doi.org/10.1016/j.patcog.2021.108398

[100] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Security*, vol. 2011, p. 3, Sep. 2011.

[101] *IEEE Standard for Biometric Open Protocol*, IEEE Standard 2410-2019, Jun. 2019.

[102] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doroz, and B. Sunar, "Practical homomorphic encryption: A survey," in *Proc. Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 2792–2795.

[103] K. Okereafor, I. Ekong, I. O. Markson, and K. Enwere, "Fingerprint biometric system hygiene and the risk of COVID-19 transmission," *Biomed. Eng.*, vol. 5, no. 1, Apr. 2020, Art. no. e19623.

[104] M. A. Olsen, M. Dusio, and C. Busch, "Fingerprint skin moisture impact on biometric performance," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Mar. 2015, pp. 1–6.

[105] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *EURASIP J. Image Video Process.*, vol. 2021, p. 8, Feb. 2021.

[106] A. Kumar, *Contactless 3D Fingerprint Identification* (Advances in Computer Vision and Pattern Recognition). Cham, Switzerland: Springer, 2018.

[107] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch, "A low-cost multimodal biometric sensor to capture finger vein and fingerprint," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Sep. 2014, pp. 1–7.

[108] J. Galbally, G. Bostrom, and L. Beslay, "Full 3D touchless fingerprint recognition: Sensor, database and baseline performance," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 225–233.

[109] A. Kumar and Y. Zhou, "Contactless fingerprint identification using level zero features," in *Proc. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2011, pp. 114–119.

[110] C. Stein, C. Nickel, and C. Busch, "Fingerphoto recognition with smartphone cameras," in *Proc. Int. Conf. Biometrics Spec. Interest Group (BIOSIG)*, Sep. 2012, pp. 1–12.

[111] J. M. Libert, J. D. Grantham, B. Bandini, K. Ko, S. Orandi, and C. I. Watson, "Interoperability assessment 2019: Contactless-to-contact fingerprint capture," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8307, May 2020.

[112] S. Orandi, J. M. Libert, B. Bandini, K. Ko, J. D. Grantham, and C. I. Watson, "Evaluating the operational impact of contactless fingerprint imagery on matcher performance," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. NISTIR 8315, Sep. 2020.

[113] P. Salum, D. Sandoval, A. Zaghetto, B. Macchiavello, and C. Zaghetto, "Touchless-to-touch fingerprint systems compatibility method," in *Proc. Int. Conf. Image Process. (ICIP)*, Sep. 2017, pp. 3550–3554.

[114] C. Lin and A. Kumar, "Matching contactless and contact-based conventional fingerprint images for biometrics identification," *IEEE Trans. Image Process.*, vol. 27, pp. 2008–2021, 2018.

[115] C. Kauba, B. Prommegger, and A. Uhl, "Combined fully contactless finger and hand vein capturing device with a corresponding dataset," *Sensors*, vol. 19, no. 22, pp. 5014–5039, Nov. 2019.

[116] H. Ma and S. Y. Zhang, "Contactless finger-vein verification based on oriented elements feature," *Infrared Phys. Technol.*, vol. 97, pp. 149–155, Mar. 2019.

[117] F. Marattukalam and W. H. Abdulla, "On palm vein as a contactless identification technology," in *Proc. Aust. New Zealand Control Conf. (ANZCC)*, Nov. 2019, pp. 270–275.

[118] L. Debiasi, C. Kauba, B. Prommegger, and A. Uhl, "Near-infrared illumination add-on for mobile hand-vein acquisition," in *Proc. Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Oct. 2018, pp. 1–9.

[119] A. Malhotra, A. Sankaran, A. Mittal, M. Vatsa, and R. Singh, "Chapter 6—Fingerphoto authentication using smartphone camera captured under varying environmental conditions," in *Human Recognition in Unconstrained Environments*. London, U.K.: Academic, 2017, pp. 119–144.

[120] B. W. Schuller, D. M. Schuller, K. Qian, J. Liu, H. Zheng, and X. Li, "COVID-19 and computer audition: An overview on what speech & sound analysis could contribute in the SARS-CoV-2 corona crisis," 2020, *arXiv:2003.11117*.

[121] G. Deshpande and B. W. Schuller, "Audio, speech, language, & signal processing for COVID-19: A comprehensive overview," 2020, *arXiv:2011.14445*.

[122] K. D. Bartl-Pokorny *et al.*, "The voice of COVID-19: Acoustic correlates of infection," 2020, *arXiv:2012.09478*.

[123] J. Shuja, E. Alanazi, W. Alasmary, and A. Alashaikh, "COVID-19 open source data sets: A comprehensive survey," *Appl. Intell.*, vol. 51, pp. 1296–1325, Sep. 2020.

[124] A. Imran *et al.*, "AI4COVID-19: AI enabled preliminary diagnosis for COVID-19 from cough samples via an app," 2020, *arXiv:2004.01275*.

[125] C. Brown *et al.*, "Exploring automatic diagnosis of COVID-19 from crowdsourced respiratory sound data," 2020, *arXiv:2006.05919*.

[126] N. Sharma *et al.*, "Coswara—A database of breathing, cough, and voice sounds for COVID-19 diagnosis," 2020, *arXiv:2005.10548*.

[127] M. Faezipour and A. Abuzneid, "Smartphone-based self-testing of COVID-19 using breathing sounds," *Telemed. e-Health*, vol. 26, no. 10, pp. 1202–1205, Oct. 2020.

[128] S. Trivedy, M. Goyal, P. R. Mohapatra, and A. Mukherjee, "Design and development of smartphone-enabled spirometer with a disease classification system using convolutional neural network," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 9, pp. 7125–7135, Sep. 2020.

[129] J. Han *et al.*, "An early study on intelligent analysis of speech under COVID-19: Severity, sleep quality, fatigue, and anxiety," in *Proc. Interspeech*, Oct. 2020, pp. 4946–4950.

[130] M. R. Kamble *et al.*, "PANACEA cough sound-based diagnosis of COVID-19 for the DiCOVA 2021 challenge," in *Proc. Interspeech*, 2021, pp. 906–910.

[131] M. R. Kamble, J. Patino, M. A. Zuluaga, and M. Todisco, "Exploring auditory acoustic features for the diagnosis of COVID-19," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2022, pp. 566–570.

[132] R. K. Das, M. Madhavi, and H. Li, "Diagnosis of COVID-19 using auditory acoustic cues," in *Proc. Interspeech*, 2021, pp. 921–925.

[133] F. Avila *et al.*, "Investigating feature selection and explainability for COVID-19 diagnostics from cough sounds," in *Proc. Interspeech*, 2021, pp. 951–955.

[134] B. Goodwin and L. M. Alvarez. "Airports deploy thermal cameras to control COVID-19, science suggests it's merely 'safety theatre"' 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://www.computerweekly.com/news/252485233/Airports-deploy-thermal-cameras-to-control-Covid-19-science-suggests-its-merely-safety-theatre

[135] "Thermal screening, masks, hand hygiene mandatory in malls under new guidelines." NDTV. 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://www.ndtv.com/india-news/24-30-degrees-ac-temperature-social-distancing-detailed-guidelines-for-malls-2240889

[136] J.-W. Lin, M.-H. Lu, and Y.-H. Lin, "A thermal camera based continuous body temperature measurement system," in *Proc. Int. Conf. Comput. Vis. Workshops (ICCVW)*, Oct. 2019, pp. 1681–1687.

[137] K. Mallat, N. Damer, F. Boutros, A. Kuijper, and J.-L. Dugelay, "Cross-spectrum thermal to visible face recognition based on cascaded image synthesis," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2019, pp. 1–8.

[138] S. M. Iranmanesh and N. M. Nasrabadi, "Attribute-guided deep polarimetric thermal-to-visible face recognition," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2019, pp. 1–8.

[139] N. Damer, F. Boutros, K. Mallat, F. Kirchbuchner, J. Dugelay, and A. Kuijper, "Cascaded generation of high-quality color visible face images from thermal captures," 2019, *arXiv:1910.09524*.

[140] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2019, pp. 4690–4699.

[141] S. Farokhi, J. Flusser, and U. U. Sheikh, "Near infrared face recognition: A literature survey," *Comput. Sci. Rev.*, vol. 21, pp. 1–17, Aug. 2016.

[142] B. J. Quilty, S. Clifford, S. Flasche, and R. M. Eggo, "Effectiveness of airport screening at detecting travellers infected with novel coronavirus (2019-nCoV)," *Euro Surveill.*, vol. 25, no. 5, Feb. 2020, Art. no. 2000080.

[143] "EASA ECDC COVID-19 aviation health safety protocol." European Union Aviation Safety Agency (EASA). 2020. Accessed: Aug. 23, 2022. [Online]. Available: https://www.easa.europa.eu/document-library/general-publications/covid-19-aviation-health-safety-protocol

[144] E. J. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, vol. 1. Dordrecht, The Netherlands: Springer, 2016.

[145] S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "Ethical, legal, and social implications of biometric technologies," in *Biometric-Based Physical and Cybersecurity Systems*. Cham, Switzerland: Springer, 2019, pp. 535–569.

[146] T. de Freitas Pereira and S. Marcel, "Fairness in biometrics: A figure of merit to assess biometric verification systems," 2021, *arXiv:2011.02395*.

[147] A. K. Jain, D. Deb, and J. J. Engelsma, "Biometrics: Trust, but verify," 2021, *arXiv:2105.06625*.

[148] C. Rathgeb, P. Drozdowski, N. Damer, D. C. Frings, and C. Busch, "Demographic fairness in biometric systems: What do the experts say?" 2021, *arXiv:2105.14844*.

[149] A. P. Rebera, M. E. Bonfanti, and S. Venier, "Societal and ethical implications of anti-spoofing technologies in biometrics," *Sci. Eng. Ethics*, vol. 20, no. 1, pp. 155–169, 2014.

[150] "COVID-19: Effective and responsible biometric solutions and concepts in a time of pandemic—Building a resilient response," Biometrics Inst., London, U.K., Rep., 2020.

[151] M. Faúndez-Zanuy, J. Fiérrez, M. A. Ferrer, M. D. Cabrera, R. Tolosana, and R. Plamondon, "Handwriting biometrics: Applications and future trends in e-Security and e-Health," *Cogn. Comput.*, vol. 12, no. 5, pp. 940–953, 2020. [Online]. Available: https://doi.org/10.1007/s12559-020-09755-z

[152] C. Vizitiu, C. Bîră, A. Dinculescu, A. Nistorescu, and M. Marin, "Exhaustive description of the system architecture and prototype implementation of an IoT-based eHealth biometric monitoring system for elders in independent living," *MDPI Sens.*, vol. 21, no. 5, p. 1837, 2021.

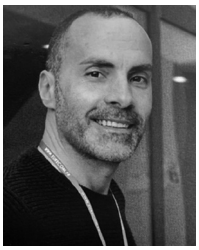
[153] J. Effah, E. Owusu-Oware, and R. Boateng, "Biometric identification for socioeconomic development in Ghana," *Inf. Syst. Manag.*, vol. 37, no. 2, pp. 136–149, 2020.
[154] "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics," Org. Econ. Co-Oper. Develop. (OECD), Paris, France, Rep., 2020.
[155] "The COVID decade: Understanding the long-term societal impacts of COVID-19," British Acad., London, U.K., Rep., 2021.
[156] "Survey on COVID-19 related processing activities by EUIs," Eur. Data Prot. Supervisor (EPDS), Brussels, Belgium, Rep., 2022.

Marta Gomez-Barrero (Member, IEEE) is a Research Professor for IT-Security with a focus on biometric recognition with Hochschule Ansbach, Germany. She currently coordinates the ANR-DFG Project RESPECT and was actively involved in the EU projects SOTAMD, BATL, and TABULA RASA. She has coauthored more than 90 technical publications in the field of biometrics, and her current research focuses on security and privacy evaluations of biometric systems (PAD and BTP). She has also received a number of distinctions, including the EAB European Biometric Industry Award 2015, the Best Ph.D. Thesis Award by the Universidad Autonoma de Madrid 2015/16, the Archimedes Award for young researches from Spanish MECD, the Best Paper Award at WIFS 2021, Odyssey 2018, and ICB 2015, and the Best Poster Award at ICB 2013. She is the General Chair of the BIOSIG conference and has served for several conferences, such as IJCB, IWBF, and EUSIPCO, and journals, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE, *IET Biometrics*, and *Pattern Recognition* (Elsevier). Further, she is the Co-Chair of the European Association for Biometrics Academic SIG, an Associate Editor for the *EURASIP Journal on Information Security* and *EURASIP Journal on Image and Video Processing*, a member of the IARP TC4 Conference Committee and the IEEE Biometrics Council Security and Privacy Technical Committee, and represents the German Institute for Standardisation (DIN) in ISO/IEC SC37 JTC1 SC37 on biometrics.

Pawel Drozdowski worked as a Senior Researcher with the Faculty of Computer Science, Hochschule Darmstadt, Germany. He coauthored over 35 technical publications in the field of biometrics. His research interests include biometrics, information security and privacy, pattern recognition, and algorithmic fairness. He won the European Biometric Industry Award of the European Association for Biometrics in 2021, the Best Student Paper Runner-Up Award (WIFS'18), the Best Poster Award (BIOSIG'19), and the Best Paper Award (WIFS'21).

Christian Rathgeb is a Senior Researcher with the Faculty of Computer Science, Hochschule Darmstadt, Germany. He is a Principal Investigator with the National Research Center for Applied Cybersecurity ATHENE. His research interests include pattern recognition, iris and face recognition, security aspects of biometric systems, secure process design, and privacy enhancing technologies for biometric systems. He coauthored over 100 technical papers in the field of biometrics. He is a winner of the EAB—European Biometrics Research Award 2012, the Austrian Award of Excellence 2012, the Best Poster Paper Awards (IJCB'11, IJCB'14, and ICB'15), the Best Paper Award Bronze (ICB'18), and the Best Paper Award (WIFS'21). He is a member of the European Association for Biometrics (EAB), a Program Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG), and an Editorial Board Member of *IET Biometrics*. He has served for various program committees and conferences, such as ICB, IJCB, BIOSIG, and IWBF, and journals as a Reviewer, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE, and *IET Biometrics*.

Jose Patino received the Ph.D. degree in computer science and electrical engineering from Sorbonne University, France, in 2019. He is a Researcher in speech technologies and machine learning, with an interest in topics related to voice biometrics, such as speaker recognition, anti-spoofing, or speaker diarization. He was a Research Assistant and then a Postdoctoral Researcher with EURECOM's Audio Security and Privacy Group from 2016 to 2021, where he contributed to numerous research projects both at the French and international levels. He co-organized the inaugural edition of the Voice Privacy Challenge and the 2021 edition of the ASVspoof series, community-led initiatives that homogenize and promote research in speaker anonymization, and speaker anti-spoofing, respectively. Since late 2021, he has been with Cerence Inc. He has coauthored more than 30 publications.



Massimiliano Todisco received the Ph.D. degree in sensorial and learning systems engineering from the University of Rome Tor Vergata in 2012. He is an Assistant Professor with the Digital Security Department, EURECOM, France. He is currently serving as a Principal Investigator and the Coordinator for TReSPAsS-ETN, an H2020 Marie Skłodowska-Curie Innovative Training Network and RESPECT, a PRCI project funded by the French ANR and the German DFG. He co-organizes the ASVspoof challenge series, which is community-led challenges which promote the development of countermeasures to protect automatic speaker verification (ASV) from the threat of spoofing. He has coauthored more than 100 publications. His current interests are in developing explainable DNN architectures for speech processing and speaker recognition, fake audio detection and anti-spoofing, and the development of privacy preservation algorithms to prevent disclosure of sensitive data.

Andreas Nautsch received the B.Sc. and M.Sc. degrees from Hochschule Darmstadt (dual studies with atip GmbH) in 2012 and 2014, respectively, and the Doctoral degree from Technische Universitat Darmstadt in 2019. From 2014 to 2018, he was with the da/sec Biometrics and Internet Security Research Group, Hochschule Darmstadt, German National Research Center for Applied Cybersecurity. He served as an Expert Delegate to ISO/IEC and a Project Editor of the ISO/IEC 19794-13:2018 Standard, and is a Coinitiator and the Secretary of the ISCA Special Interest Group on Security and Privacy in Speech Communication.

Naser Damer (Member, IEEE) received the Ph.D. degree in computer science from TU Darmstadt in 2018. He is a Senior Researcher with Fraunhofer IGD, performing research management, applied research, scientific consulting, and system evaluation. His main research interests lie in the fields of biometrics, machine learning, and information fusion. He is a Research Area Coordinator and a Principal Investigator with the National Research Center for Applied Cybersecurity ATHENE, Germany. He lectures on human and identity-centric machine learning, as well as on ambient intelligence with TU Darmstadt. He is a member of the organizing teams of several conferences, workshops, and special sessions, including being a Program Co-Chair of BIOSIG. He serves as an Associate Editor for *Pattern Recognition* (Elsevier) and the *Visual Computer* (Springer). He represents the German Institute for Standardization (DIN) in the ISO/IEC SC37 International Biometrics Standardization Committee. He is a member of the IEEE Biometrics Council serving on its Technical Activities Committee.

Jannier Priesnitz received the B.Sc. degree in computer science and the M.Sc. degree from Hochschule Darmstadt in 2015 and 2018, respectively, where he is currently pursuing the Ph.D. degree with da/sec, ATHENE, National Research Center for Applied Cybersecurity. His current research focuses on mobile touchless fingerprint recognition.

Nicholas Evans is a Professor with EURECOM, France, where he heads research in Audio Security and Privacy. He is a Co-Founder of the community-led, ASVspoof Challenge series and has lead or co-lead a number of special issues and sessions with an anti-spooing theme. He participated in the EU FP7 Tabula Rasa and EU H2020 OCTAVE projects, both involving antispoofing. Today, his team is leading the EU H2020 TReSPAsS-ETN Project, a training initiative in security and privacy for multiple biometric characteristics. He co-edited the second edition of the *Handbook of Biometric Anti-Spoofing*, served previously on the IEEE Speech and Language Technical Committee and serves currently as an Associate Editor for the IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE.

Christoph Busch (Senior Member, IEEE) is a member of the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway. He holds a joint appointment with the Computer Science Faculty, Hochschule Darmstadt, Germany. Further, he lectures the course Biometric Systems with DTU, Denmark, since 2007. On behalf of the German BSI, he has been the Coordinator for the project series BioIS, BioFace, BioFinger, BioKeyS Pilot-DB, KBEinweg, and NFIQ2.0. In the European Research Program, he was an Initiator of the Integrated Project 3D-Face, FIDELITY, and iMARS. Further, he was/is a partner in the projects TURBINE, BEST Network, ORIGINS, INGRESS, PIDaaS, SOTAMD, RESPECT, and TReSPAsS. He is also a Principal Investigator with the German National Research Center for Applied Cybersecurity (ATHENE). He coauthored more than 500 technical papers and has been a speaker at international conferences. Moreover, he is the Co-Founder and a Member of Board of the European Association for Biometrics that was established in 2011 and assembles in the meantime more than 200 institutional members. He is a member of the editorial board of the *IET Biometrics* and formerly of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. Furthermore, he chairs the TeleTrusT Biometrics Working Group as well as the German Standardization Body on Biometrics and is a Convenor of WG3 in ISO/IEC JTC1 SC37.