Arun Ross et al., "Some Research Problems in Biometrics: The Future Beckons,"
Proc. of 12th IAPR International Conference on Biometrics (ICB), (Crete, Greece), June 2019.

Some Research Problems in Biometrics: The Future Beckons

Arun Ross*
Sudipta Banerjee, Cunjian Chen, Anurag Chowdhury, Vahid Mirjalili,
Renu Sharma, Thomas Swearingen, Shivangi Yadav
Michigan State University, East Lansing, MI 48824 USA

Abstract

The need for reliably determining the identity of a person is critical in a number of different domains ranging from personal smartphones to border security; from autonomous vehicles to e-voting; from tracking child vaccinations to preventing human trafficking; from crime scene investigation to personalization of customer service. Biometrics, which entails the use of biological attributes such as face, fingerprints and voice for recognizing a person, is being increasingly used in several such applications. While biometric technology has made rapid strides over the past decade, there are several fundamental issues that are yet to be satisfactorily resolved. In this article, we will discuss some of these issues and enumerate some of the exciting challenges in this field.

1. Introduction

Biometrics refers to the automated or semi-automated recognition of individuals based on their physical, behavioral or psychophysiological traits [13]. These traits include face, fingerprints, iris (physical); gait, keyboard typing pattern, signature (behavioral); ECG, EEG, and saccadic eye movement (psychophysiological). A classical biometric system may be viewed as a pattern recognition engine that extracts a set of discriminative features from the input biometric data and compares this against a set of stored "templates" in order to determine a match. Thus, a significant number of early papers in the biometric literature dealt with data acquisition, quality enhancement, feature extraction, and matching. However, the study of biometrics extends beyond pattern recognition and engages researchers from many different fields such as computer vision, signal processing, cognitive psychology, sensor design, forensics, information security, physiology, genetics, human factors, cryptography, jurisprudence, ethics, *etc*. Further, since a biometric system deals with the personal information of an individual, aspects related to data privacy are also being addressed. Thus, an operational biometric system has to contend with a broad gamut of problems ranging from robust pattern recognition to provable data security/privacy in diverse scenarios.

The past decade has witnessed significant technical progress in the field of biometrics [14]. This includes: (a) incorporation of compact biometric sensors in small personal devices like smartphones; (b) deployment of biometric systems in large-scale identification and de-duplication applications, such as India's Unique ID program that uses face, fingerprint and iris; (c) development of robust matching techniques for various biometric modalities based on Deep Learning; (d) investigation of previously under-explored biometric traits (such as ECG) for use in wearable devices; (e) methods for rapidly searching through large biometric databases; and (f) design of countermeasures for addressing various types of adversarial attacks against biometric systems. Notwithstanding this progress, there are a number of fundamental problems that are yet to be resolved in the field of biometrics. In this article, we highlight a few of these challenges and discuss the research opportunities in the field (Figure 1).

2. Fundamental Science

Biometric recognition is based on two central tenets: *distinctiveness* and *persistence* of the biometric trait of an individual. Distinctiveness is a measure of the uniqueness of a biometric trait to an individual and indicates how that biometric trait varies across the population. Persistence, on the other hand, is a measure of the temporal stability of the biometric trait pertaining to an individual. Surprisingly, our knowledge about the distinctiveness and persistence of even the four most extensively studied biometric traits (fingerprint, face, iris and voice) is incomplete [23, 7, 32] and often relegated to anecdotal interpretation of error rates rather than a systematic exploration of the biology of the trait [22].

Research problem 1: Designing robust models for quantifying the uniqueness and permanence of a bio-

*Email: rossarun@cse.msu.edu. Web: http://iprobe.cse.msu.edu

978-1-7281-3640-0/19/$31.00 ©2019 IEEE

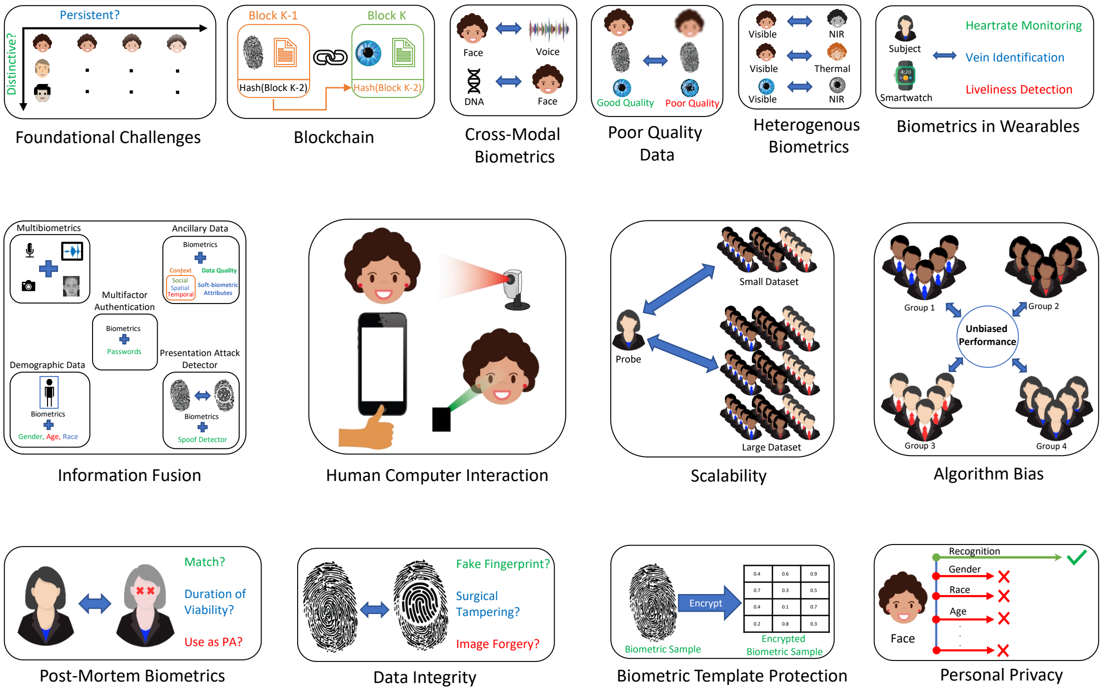

Figure 1: Illustration of some research problems in the field of biometrics.

metric trait.

3. Sensor and Human-Computer Interface

Almost every biometric system either implicitly or explicitly imposes some type of constraint on the user or the environment during data acquisition. As an example, an iris recognition system might expect the user to position their face in a certain way with respect to the camera; similarly, a speaker recognition system might require the environment to be reasonably quiet. For “ubiquitous biometric recognition” to gain traction, such constraints have to be surmounted in order to seamlessly recognize individuals, *i.e.*, the interaction between an individual and a biometric system should be transparent. This would necessitate the design of novel sensors, innovative human computer interfaces and robust data processing algorithms.

The Human-Computer Interface (HCI) – also known as the Human-Biometric System Interface (HBSI) – is perhaps the most significant component of the entire system (Figure 2). A poorly conceived HBSI can result in the acquisition of poor quality data which, in turn, can exacerbate the errors of the biometric matcher. It can also undermine the usability and security of the entire system. A thoughtfully designed HBSI, on the other hand, will not only enhance user adoption of the technology [8] but also significantly improve user throughput in high volume applications such as border control systems. The HBSI will also play a pivotal role in procuring useful information when dealing with non-cooperative subjects in law enforcement applications. Human factors (and ergonomics) is a relatively understudied problem in the biometrics literature.

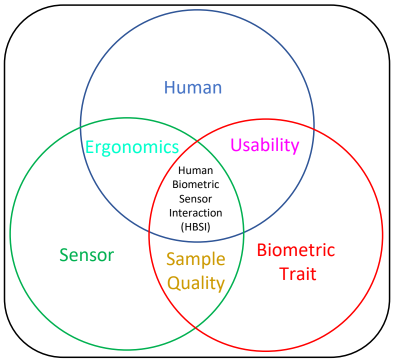

Figure 2: The design of the human-computer interface of a biometric system plays a crucial role in facilitating seamless interaction between a person and the biometric sensor in both cooperative and non-cooperative scenarios. Adapted from [16].

Research problem 2: Designing data-driven techniques for (a) modeling human behavior when interacting with a biometric system, and (b) using these models to redesign the human-computer interface for optimizing performance and enhancing usability.

Research problem 3: Developing energy-efficient multipurpose customizable biometric sensors that can not only acquire the biometric data of an individual but also rebuff adversarial attacks such as spoofing.

Research problem 4: Harnessing the principle of additive manufacturing for open-source physical production of innovative sensors and human-computer interfaces.

4. Smartphones and Wearable Devices

The explosive growth in the use of smartphones and wearable devices, such as smartwatches and activity trackers, presents an unprecedented opportunity for biometric researchers [3, 24]. Firstly, these devices store or transmit personal information (*e.g.*, financial or health data), thereby requiring an effective mechanism to restrict access to the legitimate owner. Secondly, these devices are outfitted with a large number of sensors that record various physical (*e.g.*, distance walked, posture) and biological (*e.g.*, heart rate, skin temperature) attributes of an individual; principled methods are needed to parse through this heterogeneous data and distill a compact representation that can be used as the biometric signature of that individual (Figure 3). A related challenge is to be able to generate a “portable” signature that can be used across devices belonging to the same individual.

Research problem 5: Extracting a distinct and portable “signature” of a subject from the data generated by the built-in sensors present in smartphones and wearable devices.

Research problem 6: Designing inexpensive biometric sensors for integration with smartphones and wearable devices.

Research problem 7: Developing computationally simple methods for active user authentication in resource-constrained wearable devices that have limited battery power.

5. Presentation Attack Detection

A biometric system is vulnerable to presentation attacks where an adversary presents a fake (Figure 4) or altered (Figure 5) biometric trait to the sensor in order to fool the system [18]. Such an attack may be used to (a) enroll a fabricated trait in order to create a virtual identity that can be shared by a group of individuals; or (b) deliberately obfuscate one’s own trait in order to evade being identified; or (c) spoof the biometric trait of another person in order to masquerade as them. A number of hardware-based and software-based solutions have been developed for presentation attack detection (PAD), especially for the face, fingerprint and iris modalities. However, most of the current solutions do not generalize well across different sensors and environments.

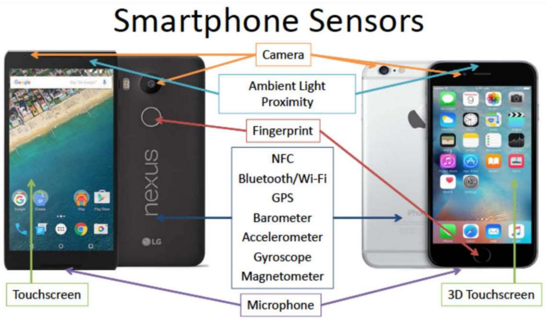

Figure 3: Smartphones are equipped with a number of built-in sensors. Data from these non-biometric sensors can be aggregated to construct a behavioral signature of its owner. © Debayan Deb

The challenge is to develop counter-measures that can deflect unseen and unknown attacks, *i.e.*, those attacks that have not been considered as yet, but which the system will encounter in the future. This is a formidable challenge that can evolve into a “cat-and-mouse” game between the adversary and the system designer. The advent of 3D printing and additive manufacturing will facilitate the generation of sophisticated presentation attack vectors. It is essential for PAD solutions to keep pace with these advanced technologies.

Research problem 8: Developing anti-spoofing methods that can generalize well across different types of attacks, sensors, environments, demographic groups and datasets.

Research problem 9: Designing presentation attack detectors for resource-constrained IoT devices such as smartphones and wearable devices.

Research problem 10: Automating the process of generating adversarial spoof artifacts for a specific biometric sensor by combining 3D printing technology with robotic process automation testing.

6. Poor Quality Data

As can be seen in Table 1, state-of-the-art biometric matchers exhibit very good performance when the quality of the input data is reasonably good. However, the performance sharply degrades when a matcher encounters poor quality data [2]. Examples of poor quality data include fingermarks lifted from a crime scene, audio data recorded in noisy environment, iris images awash with strong non-uniform illumination, or partially occluded low-resolution faces in surveillance videos (Figure 6). Reliably enhancing such data is a challenging problem since many data enhancement algorithms do not explicitly attempt to preserve

Table 1: Current state-of-the-art performance of four biometric modalities. Verification (V) performance is reported using the False Match Rate (FMR) and False Non-Match Rate (FNMR). Identification (I) performance is reported using the False Negative Identification Rate (FNIR) and False Positive Identification Rate (FPIR).

Modality	Mode	Report	Template Size	Performance	Dataset Size	Comments
Face	V	FRVT 1:1 [11]	1.4 KB	FNMR 2.71% @ FMR 0.01%	1K subjects, 100K images	"In-the-wild"
	I	FRVT 1:N [10]	2.05 KB	FNIR 2.0% @ FPIR 0.1%	485K Probe, 1.6M Gallery	Mugshots
Fingerprint	V	FVC-onGoing[1]	5.9 KB	FNMR 0.036% @ FMR 0.01%	115,710 comparisons	Operational conditions
	I	FpVTE [31]	6.1 KB	FNIR 1.9% @ FPIR 0.1%	30K Probe, 100K Gallery	Plain fingerprint
Iris	V	IREX IX [27]	12.33 KB	FNMR of 0.57% @ FMR 0.001%	260,809 subjects,	Both-eyes;
	I		12.33 KB	FNIR of 0.67% @ FPIR 0.1%	673,662 samples	High-quality
Voice	V	SRE 2016 [28]	not given	FNMR of 39% @ FMR 0.01%	201 speakers	Multi-lingual

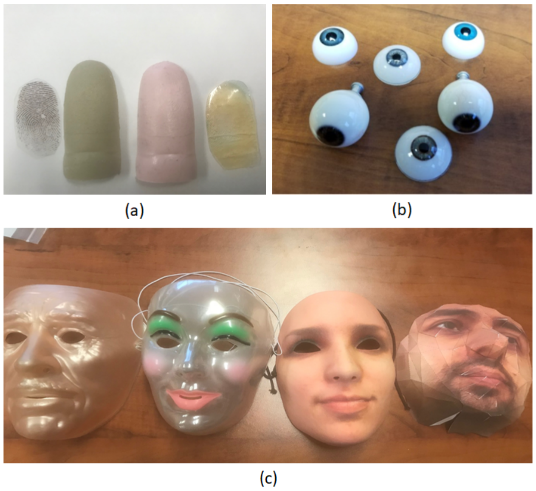
(a)
(b)
(c)

Figure 4: Examples of different types of spoof artifacts for (a) fingerprint, (b) iris and (c) face.

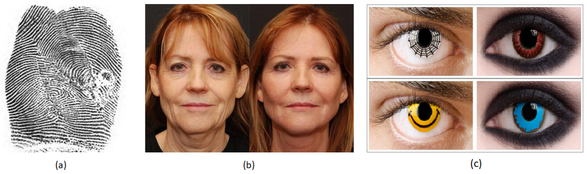
(a)
(b)
(c)

Figure 5: Examples of altered/obfuscated biometric traits. (a) A surgically altered fingerprint depicting transplantation with Z-cut. (b) A face image before and after plastic surgery.[2] (c) Cosmetic contact lenses can obfuscate the underlying iris texture pattern.[3]

the *biometric content* of the input data; this can potentially alter the biometric cue in the data resulting in its inadvertent match with an incorrect identity. This can have serious consequences in law enforcement applications. Further, when using poor quality biometric data as evidence in a court-of-law, it is necessary to first compute its *evidential value*, *i.e.*, its utility for reliably identifying an individual.

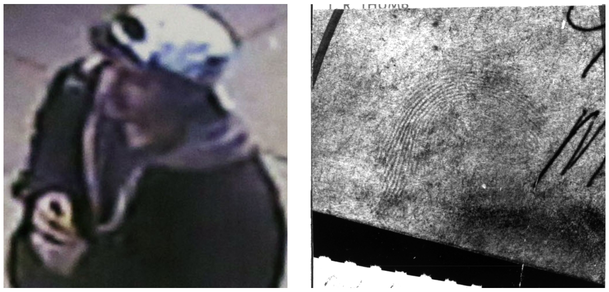

Figure 6: Examples of poor quality data: face image of the Boston bomber captured using a surveillance camera (left) and a latent fingerprint on the surface of an object (right).

Research problem 11: Developing methods for enhancing poor quality data such that the biometric content is not unduly perturbed.

Research problem 12: Designing robust feature extraction and matching algorithms that can successfully operate on poor quality data.

Research problem 13: Computing the evidential value of poor quality biometric data, especially in forensic applications.

7. Data Integrity

The *integrity* of the raw biometric data (*e.g.*, face image) is of paramount importance, especially when it is used as evidence in a court of law. However, the raw biometric data of a person can be maliciously modified for nefarious purposes. For example, digital images and videos of a person's face may be subtly modified using an editing tool such as Adobe Photoshop with the intention of creating a false match. The problem is compounded when strategically altered images and videos are displayed on the Web, particularly on image sharing platforms. This leads to a proliferation of doctored images and their duplicates on the Web,

[1] https://biolab.csr.unibo.it/fvcongoing/

[2] https://www.cincyfacialplastics.com/before-and-after/luxe-lift-pictures-5859

[3] https://hoovervisioncenter.com/2015/10/21/halloween-hazard-the-dangers-of-cosmetic-contact-lenses/

making it difficult to identify the original (pre-modified) image. Recently, Generative Adversarial Networks (GANs) have been used to synthesize *realistic* looking images and videos known as *DeepFakes* (Figure 7).

When images posted on the Web are used for determining the identity of a person, an erroneous match due to perturbations in the images can have serious consequences. Therefore, it is essential for a biometric system to validate the integrity of the input digital media prior to processing it (Figure 8). The principle of digital image forensics [9] can be used for this purpose.

Research problem 14: Designing algorithms for detecting *DeepFakes* as well as maliciously modified images/videos of a person.

Research problem 15: Developing methods to identify the original unmodified image from a given set of near-duplicate biometric images and to infer the trail of photometric and geometric modifications that produced the other images.

Research problem 16: Designing robust sensor-fingerprinting algorithms that can link a biometric image to the specific sensor unit that produced it.

Figure 7: Examples of realistic-looking digital face images generated using GANs. Taken from *thispersondoesnotexist.com*.

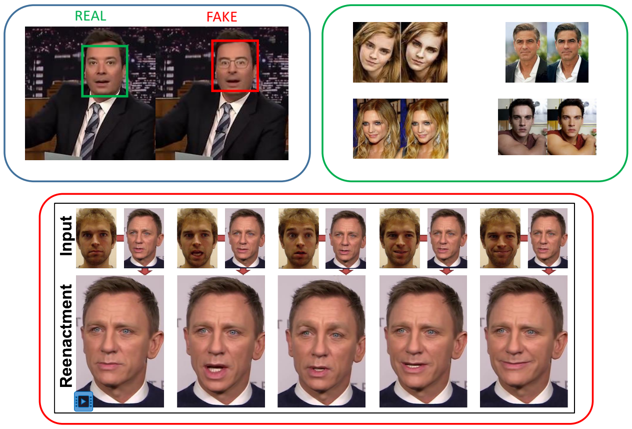

Figure 8: Examples of digitally modified media. Top left: A GAN-generated face image.[4] Top right: Near duplicate face images of four subjects created using Photoshop.[5] Bottom: Rendering of a "fake" video by transferring the facial expressions of one individual (source) to another individual (target).[6]

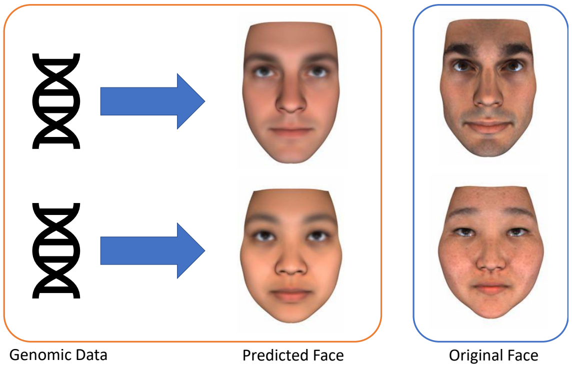

Figure 9: Illustration of cross-modal biometrics where a face image is generated from the DNA sample of a subject. Adapted from Lippert *et al.* [17].

8. Cross-modal Biometrics

Cross-modal matching involves associating the data pertaining to one biometric modality with that of another modality. There is limited work on this topic. One application where cross-modal association can be beneficial is in the mapping of genomic data to phenotypic traits [17]. For example, generating the face image of a person from their DNA sample can be useful in criminal investigations (Figure 9). Cross-modal matching can also be useful in applications where a specific biometric trait may not be consistently available. For example, in the case of an indoor surveillance video, the face image of a subject may not be available in every frame due to low image-resolution, poor illumination, non-frontal pose or occlusions. However, the audio of the subject's voice may be available in such frames. The ability to associate the voice samples of a subject with their face images for cross-modal identity matching can be valuable. The matching itself can be accomplished by the extraction of common soft biometric cues from the two modalities (*e.g.*, age, gender, height, weight) or by modeling the correlation between the morphological aspects of a subject's face and the acoustic characteristics of their voice [21]. Another example of cross-modal matching would be linking RGB face images in a face database with near-infrared (NIR) iris images in an iris database [15].

A related problem is *heterogeneous* matching that involves comparing data originating from two distinctly different sensors but pertaining to the same modality, *e.g.*, cross-spectral matching of RGB face images with thermal

[4] https://www.deeptracelabs.com/

[5] https://www.buzzfeed.com/jessicamisener/23-celebrities-before-after-photoshop

[6] https://web.stanford.edu/~zollhoef/papers/CVPR2016_Face2Face/page.html

face images (Figure 10). While it may not be as challenging as cross-modal biometrics, it nevertheless is an unsolved problem notwithstanding the large number of papers on the topic.

Research problem 17: Developing methods for establishing the degree of correlation, at the biological level, between two or more biometric traits.

Research problem 18: Developing techniques to deduce phenotypic attributes from genomic data for cross-modal biometric matching.

Research problem 19: Designing methods for generating a canonical representation of one biometric trait from another trait.

Research problem 20: Developing models to assess the upper bound on the recognition accuracy of cross-spectral biometric recognition.

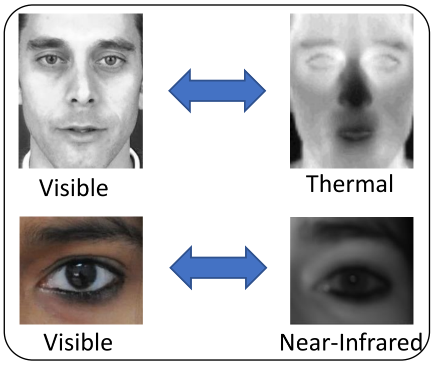

Figure 10: Heterogeneous biometric recognition in the context of face (top) and iris (bottom).

9. Postmortem Biometrics

In some scenarios, it may be necessary to identify a deceased person by comparing their postmortem (PM) biometric data with the corresponding antemortem (AM) data. For example, police officers have sought to unlock the smartphone of a deceased suspect by using the suspect’s postmortem fingerprint.[7] Another application is victim identification using postmortem data in the wake of mass fatalities due to tsunamis, terrorist attacks, wars, earthquakes or nuclear explosions. While dental radiographs have been traditionally used for postmortem biometric identification (especially in the context of mass disasters), there is increasing interest in utilizing other biometric modalities, such as face, fingerprints and iris, for this purpose [30]. However, postmortem biometric identification is beset with a number of challenges due to reduced data quality and natural decomposition of body parts. Furthermore, in many cases, the feature extraction and matching algorithms developed for antemortem data may not be able to successfully process postmortem data. Factors such as cause of death, subject’s age, environmental conditions, *etc*., can also impact the biometric utility of certain traits.

Research problem 21: Designing novel quality enhancement, segmentation and feature extraction algorithms for processing postmortem biometric data.

Research problem 22: Developing methods to effectively match postmortem data of a subject with the corresponding antemortem data.

Research problem 23: Modeling the temporal degradation in postmortem biometric data and determining the factors that impact the biometric utility of postmortem data.

Research problem 24: Investigating the feasibility of using postmortem biometric traits to launch a presentation attack against a biometric system.

10. Soft Biometrics

While biometric data is typically used for *recognizing* an individual, it is possible to deduce or extract additional information, such as age, gender, ethnicity, height, weight, hair color, eye color, clothing style, tattoos, *etc*., from the same data [6]. These attributes, sometimes referred to as soft biometric attributes, can be used independently or in conjunction with primary biometric traits to improve the recognition accuracy of a biometric system. Further, they provide a human-interpretable description of the underlying biometric data (*e.g*., “Young Asian Male” or “Iris With a Dilated Pupil”). They can also be used to restrict the search space in a gallery database to only those identities that share similar soft biometric attributes as the input probe data. In spite of their potential benefits, there are a number of open research problems in this area.

Research problem 25: Designing methods to deduce soft biometric information from poor quality biometric data.

Research problem 26: Extracting soft biometric information from behavioral traits.

Research problem 27: Estimating upper bounds on the uniqueness and persistence of soft biometric attributes.

11. Personal Privacy

As stated in the previous section, recent advances in machine learning has made it possible to extract ancillary information, such as a person’s age, gender, ancestral origin and health, from their biometric data using sophisticated classifiers [6]. The possibility of eliciting genetic information from facial images has also been studied [19]. When such information is extracted without the subject’s consent, then issues of *function creep* and *privacy infringement* are

[7] https://www.livescience.com/62393-dead-fingerprint-unlock-phone.html

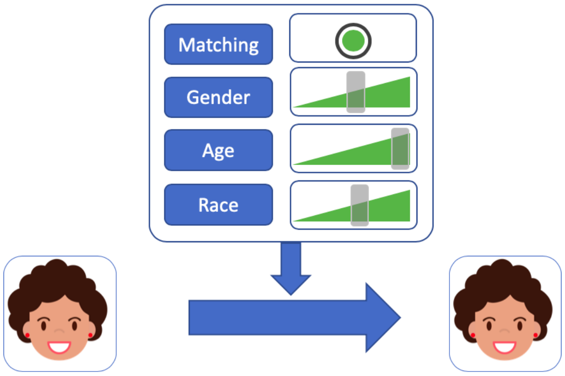

Figure 11: Illustration of controllable biometric privacy, where users can determine which information to keep and which to conceal.

brought to the fore. Similarly, when biometric data is used to unmask the identity of a person by *linking* information from seemingly disparate sources, it can represent a privacy breach. For example, matching an *unidentified* face image from a pseudonymized dating website with an *identified* face image in a social network website can expose sensitive details about a person through data accretion [1].

Recent research has explored the notion of controllable privacy [29] where specific ancillary cues are suppressed in the raw image (Figure 11). For example, semi-adversarial neural networks have been designed to remove gender cues from a face image, through a series of perturbations, such that the performance of automated gender classifiers is confounded but the performance of face matchers is retained [20]. Introduction of the EU General Data Protection Regulation (GDPR) has reinforced the importance of designing privacy-preserving methods in the context of biometric systems.

Research problem 28: Designing methods for imparting controllable and quantifiable soft-biometric privacy to biometric data without compromising recognition accuracy.

12. Biases in Biometrics

Biometric systems, especially those based on face recognition, have exhibited demographic *bias* in which certain population groups have experienced significantly higher error rates than others. For example, face detection methods have been observed to fail more often on subjects with darker skin-tone than those with lighter skin-tone [5]. In another study, researchers found that automated face recognition systems developed in Western countries performed better on Caucasian faces than East Asian faces and, conversely, automated face recognition systems developed in East Asian countries performed better on East Asian faces than Caucasian faces [26]. While such biases could be attributed to the lack of sufficiently diverse training data, it nevertheless brings into question the fairness and integrity of AI-based systems. Indeed, data-driven approaches seem to be vulnerable to such biases and it remains to be seen how this can be mitigated in the context of biometric systems that are increasingly being deployed in heterogeneous populations worldwide (Figure 12).

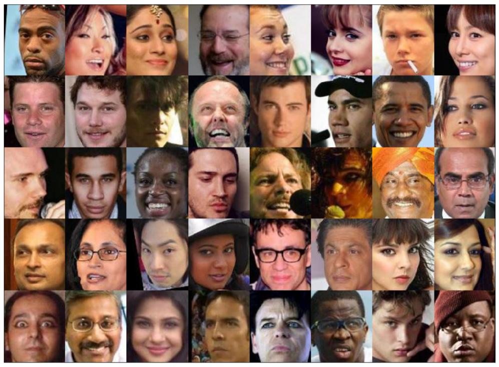

Figure 12: It is essential for biometric systems to be unbiased and perform well across diverse demographic groups (images are from the CelebA dataset).

Research problem 29: Determining the underlying cause for race and gender bias in biometrics and to design methods that alleviate this problem.

Research problem 30: Assembling large multimodal biometric datasets exhibiting demographic diversity in order to effectively train biometric matchers.

13. Other Research Problems

Besides the aforementioned topics, there are a number of other active research problems in the field. These include: (a) designing novel sensors for acquiring biometric data from infants and toddlers; (b) performing biometric recognition based on bacterial colonies on the human skin; (c) reliable human recognition from low-quality contaminated DNA samples; (d) homomorphic encryption methods for biometric template security; (e) integration of biometrics in the blockchain protocol for implementing self-sovereign identity; (f) information fusion techniques for combining biometrics with demographic data, quality measures, social information, and presentation attack detectors; (g) studying the impact of age and disease on the performance of individual biometric traits; (h) discovering and mitigating the impact of adversarial samples that can destabilize Deep Learning based biometric matchers; (i) harnessing explainable AI techniques for semantically interpreting trained neural network models; and (j) models for predicting biometric performance of large-scale systems having billions of identities.

14. Summary

Biometrics is a fascinating pattern recognition problem with several societal benefits [25]. The past decade has seen a surge in the use of biometric technology for diverse applications. Advancements in other domains have opened up new opportunities for biometric researchers. At the same time, a number of fundamental issues remain unsolved in the field even after several years [12]. In this paper, we highlighted some of the research opportunities in biometrics and discussed its intersection with adjacent fields including forensics, genomics, anthropology and psychology.

The definition of *identity* itself is continually evolving [4]. In an increasingly connected world,[8] the distinction between *social identity*, *online identity* and *device identity* has blurred. Individuals are increasingly leaving their “digital fingerprints” on the Web and in personal electronic devices such as smartphones and wearables. This, coupled with the widespread availability of inexpensive digital sensors and storage units, has led to the realization of *exo-self*, where the physical identity of a person overlaps significantly with their digital and device identities. This has further enhanced the scope of biometrics thereby bringing together evidence at the molecular level, biological level, behavioral level and digital level for human recognition.

References

[1] A. Acquisti, *et al.* Face Recognition and Privacy in the Age of Augmented Reality. *Journal of Privacy and Confidentiality*, 6(2):1–20, 2014. 7

[2] S. Bharadwaj, *et al.* Biometric Quality: A Review of Fingerprint, Iris, and Face. *EURASIP Journal on Image and Video Processing*, 2014(1):34, July 2014. 3

[3] J. Blasco, *et al.* A Survey of Wearable Biometric Recognition Systems. *ACM Computing Surveys*, 49(3):43:1–43:35, Sept. 2016. 3

[4] N. Bostrom and A. Sandberg. The Future of Identity. *Report Commissioned by the United Kingdom Government Office for Science*, 2011. 8

[5] J. A. Buolamwini. *Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*. PhD thesis, Massachusetts Institute of Technology, 2017. 7

[6] A. Dantcheva, *et al.* What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE Transactions on Information Forensics and Security*, 11(3):441–467, 2016. 6

[7] J. G. Daugman. Probing the Uniqueness and Randomness of IrisCodes: Results from 200 Billion Iris Pair Comparisons. In *Proceedings of the IEEE*, volume 94, pages 1927–1935, 2006. 1

[8] A. De Luca, *et al.* I Feel Like I’m Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1411–1414, 2015. 2

[9] H. Farid. *Photo Forensics*. The MIT Press, 2016. 5

[10] P. Grother, *et al.* Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification. Technical Report 8238, National Institute of Standards and Technology (NIST), November 2018. 4

[11] P. Grother, *et al.* Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification. Technical report, National Institute of Standards and Technology (NIST), April 2019. (Draft version). 4

[12] A. K. Jain, *et al.* Biometrics: A Grand Challenge. In *Proceedings of the International Conference on Pattern Recognition (ICPR)*, volume 2, pages 935–942, August 2004. 8

[13] A. K. Jain, *et al.* *Introduction to Biometrics*. Springer Publishers, 2011. 1

[14] A. K. Jain, *et al.* 50 years of Biometric Research: Accomplishments, Challenges, and Opportunities. *Pattern Recognition Letters*, 79:80–105, August 2016. 1

[15] R. Jillela and A. Ross. Matching Face Against Iris Images Using Periocular Information. In *IEEE International Conference on Image Processing*, pages 4997–5001, 2014. 5

[16] E. P. Kukula, *et al.* The Human–Biometric–Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements. *IEEE Transactions on Instrumentation and Measurement*, 59(4):784–791, April 2010. 2

[17] C. Lippert, *et al.* Identification of Individuals by Trait Prediction Using Whole-Genome Sequencing Data. *Proceedings of the National Academy of Sciences*, 114(38):10166–10171, 2017. 5

[18] S. Marcel, *et al.*, editors. *Handbook of Biometric Anti-Spoofing - Presentation Attack Detection*. Springer, Second edition, 2019. 3

[19] A. Martinez-Monseny, *et al.* From Gestalt to Gene: Early Predictive Dysmorphic Features of PMM2-CDG. *Journal of Medical Genetics*, 2018. 6

[20] V. Mirjalili, *et al.* Gender Privacy: An Ensemble of Semi Adversarial Networks for Confounding Arbitrary Gender Classifiers. In *International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Los Angeles, CA, 2018. 7

[21] A. Nagrani, *et al.* Seeing Voices and Hearing Faces: Cross-Modal Biometric Matching. In *IEEE Computer Vision and Pattern Recognition (CVPR)*, pages 8427–8436, 2018. 5

[22] National Research Council. *Strengthening Forensic Science in the United States: A Path Forward*. The National Academies Press, Washington, DC, 2009. 1

[23] S. Pankanti, *et al.* On the Individuality of Fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(8):1010–1025, 2002. 1

[24] V. M. Patel, *et al.* Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, July 2016. 3

[25] J. N. Pato and L. I. Millett, editors. *Biometric Recognition: Challenges and Opportunities*. The National Academies Press, 2010. 8

[26] P. J. Phillips, *et al.* An Other-Race Effect for Face Recognition Algorithms. *ACM Transactions on Applied Perception (TAP)*, 8(2):14, 2011. 7

[27] G. Quinn, *et al.* IREX IX Part One: Performance of Iris Recognition Algorithms. Technical Report 8207, National Institute of Standards and Technology (NIST), April 2018. 4

[28] S. O. Sadjadi, *et al.* The 2016 NIST Speaker Recognition Evaluation. In *Interspeech*, pages 1353–1357, 2017. 4

[29] T. Sim and L. Zhang. Controllable Face Privacy. In *International Conference on Automatic Face and Gesture Recognition (FG)*, volume 4, pages 1–8, 2015. 7

[30] M. Trokielewicz, *et al.* Iris Recognition After Death. *IEEE Transactions on Information Forensics and Security*, 14(6):1501–1514, June 2019. 6

[31] C. I. Watson, *et al.* Fingerprint Vendor Technology Evaluation. Technical Report 8034, National Institute of Standards and Technology (NIST), January 2014. 4

[32] S. Yoon and A. K. Jain. Longitudinal Study of Fingerprint Recognition. *Proceedings of the National Academy of Sciences*, 112(28):8555–8560, 2015. 1

[8] As of April 2019, ∼55% of the world’s population has internet access and there are ∼25 billion IoT devices.