Biometrics: In Search of Identity and Security (Q & A)

Article *in* IEEE Multimedia · October 2018

DOI: 10.1109/MMUL.2018.2873494

CITATIONS
3

READS
70

6 authors, including:

Zahid Akhtar
University of Quebec, Montreal, Canada
56 PUBLICATIONS **398** CITATIONS
SEE PROFILE

Massimo Tistarelli
Università degli Studi di Sassari
192 PUBLICATIONS **2,629** CITATIONS
SEE PROFILE

Jean-Luc Dugelay
EURECOM
312 PUBLICATIONS **3,880** CITATIONS
SEE PROFILE

Biometrics: In Search of Identity and Security (Q & A)

Zahid Akhtar[1], Abdenour Hadid[2], Mark Nixon[3], Massimo Tistarelli[4], Jean-Luc Dugelay[5] and Sebastien Marcel[6]

[1]University of Quebec, Canada
[2]University of Oulu, Finland
[3]University of Southampton, UK
[4]University of Sassari, Italy
[5]EURECOM, France
[6]Idiap Research Institute, Switzerland

***Abstract*—To address the issues like identity theft and security threats, a continuously evolving technology known as biometrics is presently being deployed in a wide range of personal, government, and commercial applications. Despite the great progress in the field, several exigent problems have yet to be addressed to unleash biometrics full potential. This article aims to present an overview of biometric research and more importantly the significant progress that has been attained over the recent years. The paper is envisaged to further not only the understanding of general audiences and policy makers but also interdisciplinary research. Most importantly, this article is intended to complement earlier articles with updates on most recent topics and developments related to e.g. spoofing, evasion, obfuscation, face reconstruction from DNA, Big data issues in biometrics, etc.**

***Index Terms*—Biometrics, Face Recognition, Fingerprint Recognition, Iris Recognition, Security, Privacy, Forensics**

I. Introduction

Identity theft and security threats are growing concerns in our digital society. To address these issues, an emerging and continuously evolving technology known as *biometrics* has become widespread [1]. There is a reasonably permanent link between an individual and their biometric traits [2], biometrics thus can be employed in covert person recognition or in applications where an individual may attempt to conceal their true identity (e.g., using forged documents to cross borders). Although, biometrics has several advantages (e.g., nonrepudiation) over tokens or passwords, it suffers from false matches [11]. Thus, in several applications, a multi-factor authentication technique, which integrates biometrics with tokens and/or passwords, may be a better choice.

Despite great progress, several exigent problems have yet to be addressed to unleash biometrics' full potential. Various traits for biometrics have been investigated and published [5] as also can be seen in Fig. 1c. Though there exist several biometrics survey/review papers [4–6, 9, 10, 15] and books [2, 3, 11], their scopes are limited. For instance, [4] is focused mainly on physical biometric traits. [5, 6, 9, 10, 15] discuss only about mobile-, wearable-, behavioral-, and soft-biometrics, respectively. Similarly, [2, 3, 11] only provides description of fusion, spoofing, and fingerprint, respectively. Moreover, these publications do not give details of newly emergent topics. This paper significantly differs from previous articles in that it summarizes the evolution of biometrics including rising traits, research interests and applications. Specifically, this article aims to present an overview of biometric research and more importantly the significant progress that has been attained over the recent years. The paper is envisaged to further not only the understanding of general audiences and policy makers but also interdisciplinary research. Most importantly, this article is intended to complement earlier articles with updates on most recent topics and developments related to e.g. spoofing, evasion, obfuscation, face reconstruction from DNA, big data issues in biometrics, etc.

II. Fundamentals of Biometrics

Biometrics is attracting so much interest of people from all walks of life. This section thus discusses the basic issues of biometrics by answering the following questions:

What is biometrics?
Biometrics is the measurement and statistical analysis of people's biological (e.g., face) and behavioral (e.g., voice) characteristics (see Fig. 1a), which can be used to recognize or identify individuals [1]. The term biometrics is derived from the ancient Greek words 'bio' meaning life and 'metrikos' meaning to measure [2]. Biometrics is based on "who you are" rather than "what you have" (e.g., an ID card) or "what you know" (e.g., a password).

Does everyone have unique biometric traits?
In principle, each person has different biometric patterns [11]. However, the underlying scientific basis of biometric traits individuality (or uniqueness), i.e., quantitative information regarding the likelihood that another person could exhibit the same set of features, has not been formally established [1]. Thus, validity of biometric evidence is now being challenged in several court cases. A scientific basis for establishing such individuality is very important, which will lead to admissibility of biometrics identification in the courts of law as well as establishment of an upper bound on performance

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

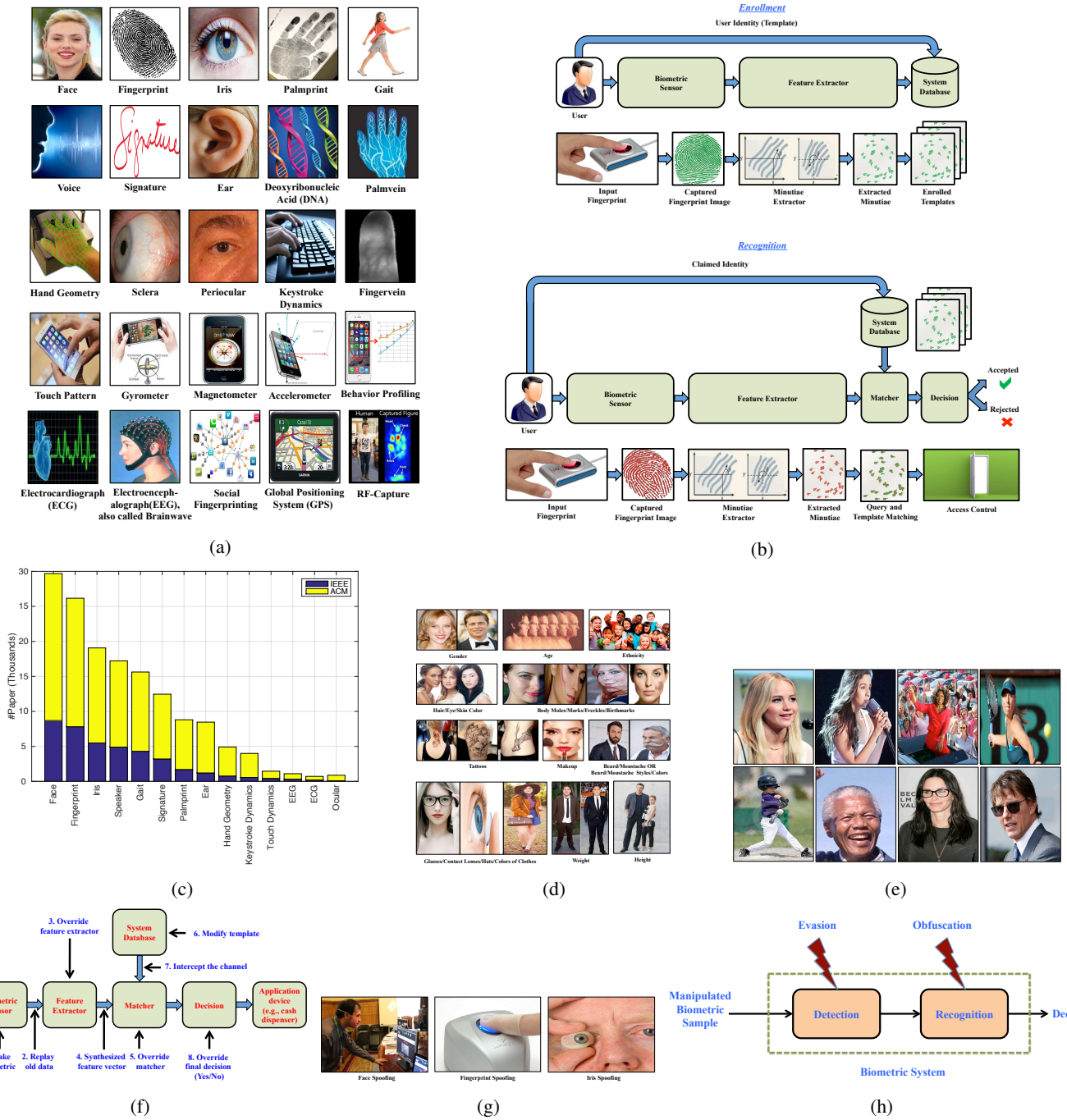

Fig. 1: (a) Plenty of body characteristics have been proposed and used for person recognition. Fingerprint, face, and iris modalities are the most adopted biometric traits. Novel traits in smartphone like touchscreen patterns, GPS data have been too proposed by researchers for biometric recognition, but are yet to attain sufficient level of technological maturity for deployment at mass level. (b) A generic biometric recognition system with an automated fingerprint identification system as an example. Each biometric verification system has two stages: enrollment and verification. The enrollment phase produces an association between a biometric characteristic and its identity. While, in the verification phase, an enrolled user claims an identity, which the system verifies on the basis of the user's biometric feature set. For fingerprint recognition, the sensor captures a digital image of a legitimate user's fingerprint. Its minutiae (salient features) are extracted and stored as a template in an enrolment database.These minutiae take the form of locations (x and y coordinates) and orientations (θ) of abrupt ends and junctions of fingerprint ridges. During identification, fingerprint minutiae are extracted from a query print in the same way and compared with the minutiae of the templates stored in the enrolment database. The number of minutiae that have similar x, y and θ coordinates forms a basis for determining the identity of the user. (c) The number of papers for specific biometric trait available via the IEEE-Xplore and the ACM Digital Library. (d) Examples of soft biometric traits. (e) Faces in the wild. (f) Points of attack in a generic biometric system. (g) Left: Face spoofing using a 3D mask. Middle: Fingerprint spoofing using a fake silicone fingerprint. Right: Iris spoofing using an artificial eyeball. (h) Scenarios for evasion and obfuscation.

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

of a biometric system. Existing individuality methods use feature representation or match score, but encounter lack of robust statistical models and entropy functions to accurately characterize intra- and inter-subject variations [4]. All in all, genotypic (genetically determined traits, e.g., DNA), phenotypic (traits determined through the interaction of genotype, development, and environment, e.g., fingerprint), and behavioral (traits determined by human activities, e.g., signature) biometric characteristics are high, medium and low in their uniqueness strength, respectively [2].

Is there any optimal biometric modality?

No biometric trait is optimal although a number of them are admissible. Indeed, no single biometric modality effectively meets all of the requirements (e.g., accuracy, size, cost, practicality, security, acceptability, and stability) of all the applications (e.g., border crossing, access control, mobile authentication, and welfare distribution) [2]. The choice of modality depends on the level of security required and other factors, such as culture (e.g., face modality would not be a good choice at places where most of the females use veils for religious convictions), environment (e.g., iris modality may be more suitable for workers in dark coal mines), and perception (e.g., people's fear regarding use of any specific modality). On the whole, though iris is regarded as most accurate form of phenotypic biometrics, there is no impeccable biometric characteristic [1]. For instance, the US National Institute of Standards and Technology (NIST) estimated 1 false match in 40 billion iris comparisons [4].

How can we establish any human features as a novel biometric?

Besides the existing biometric modalities, any human physiological, behavioral or adhered human characteristic can be defined as a novel biometric trait, if it satisfies certain basic criteria, such as universality (each person should possess the trait), distinctiveness (biometric patterns of two persons should be different), and permanence (invariant over a period of time) [2]. Moreover, it practically must meet speed, accuracy, safety (of the user), acceptance (by users), and hard to be forged requirements [9].

Do biometric traits change over time?

Yes. Though fundamental premise of any biometric trait is its persistence, biometric trait undergoes aging [10]. Aging has profound negative effects on biometric systems, since it causes alterations (e.g., shape and texture changes in face as also depicted in Fig. 1d), which subsequently make the enrolled templates unrepresentative of the query after a certain time lapse [4]. The biometric aging issue is undertaken by either virtual template synthesis for aging and de-aging transformations or adaptive mechanisms that continuously adapt the enrolled templates to the aging variation of the input/query samples [1].

Why does not a biometric system output 100% perfect match decision?

To better understand the answer of this question, let us first revisit the five basic components (see Fig. 1b) of a biometric system. Foremost, there is the sensor to capture the biometric trait (e.g., a fingerprint) and convert the information to a digital format. Then, feature extraction module processes the trait to extract a set of salient features (e.g., fingerprint minutiae); during enrollment the extracted features known as templates (X_T) are stored in the database. The matcher module compares the input/query biometric sample (X_Q) with the templates (X_T) in the database to produce the match scores. Finally, the decision module makes final decision using a predetermined threshold [11]. The fundamental premise of a biometric system is that when a biometric sample is presented, it will produce correct decision. However, the biometric systems are never 100% accurate. Unlike password or token-based systems, biometric systems—being inherently probabilistic endeavor—do not produce perfect match decision [6]. The imperfect accuracy of biometric systems occurs mainly because two samples of the same biometric trait belonging to the same person are not exactly same owing to change in user's trait (e.g., bruises and ageing), user's interaction with the sensor (e.g., pose), imperfect imaging condition (e.g., sensor noise), ambient conditions (e.g., illumination), feature representation limitation (i.e., failing to retain invariances and discriminatory information in different patterns from the same class), and poor matching ability [4]. Thus, a biometric system makes two types of errors: (i) False Match or False Accept Rate (FMR or FAR) – mistaking biometric samples from two different persons to be from the same person; (ii) False Non-Match or False Reject Rate (FNMR or FRR) – mistaking two biometric samples from the same person to be from two different persons. Both FMR and FNMR are dependent on decision threshold and a trade-off between them is opted based on application and requirements [5, 9]. NIST benchmark evaluations attained false negative–false positive (%) pair as 0.6–0.01, 4–0.1, and 7–0.1 for fingerprint, face, and voice, respectively [4].

What are soft biometrics?

Soft biometrics can be expounded as characteristics that provide some information about the individual, but alone mainly lack the distinctiveness and permanence to sufficiently differentiate any two individuals [10]. Soft biometrics, also known as biometric ancillary information, include personal attributes such as gender, age, ethnicity, hair color, height, weight, etc. (see Fig. 1d), which can be extracted from primary biometric traits, namely face, fingerprint and iris. Soft biometrics are useful in either enhancing the matching accuracy of a primary biometric system in a fusion framework or pruning the search biometric databases [15].

III. Current Status of Biometrics

Though biometrics is continuously advancing, it still has a long way to go. The following five questions, with example evidence, highlight the current state of biometrics.

Have we already arrived in the future of biometric authentication?

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

The future is almost here. Across the globe biometric technology has virtually arrived in our daily lives ranging from border crossing, surveillance to mobile devices. Biometric engineering is already good enough that governments, business institutions and individuals are exploiting it to curb security threats, frauds and identity thefts. Governments are employing biometrics to keep track of who is entering and departing from their borders, and receiving welfare payments [4], e.g., the Office of Biometric Identity Management (formerly known as 'US-VISIT') program, i.e., visitors to the US provide fingerprint and face images at their port of entry that are matched against various watch-lists [7]. Business institutions are securing their facilities, websites and proprietary databases via biometric techniques, e.g., HSBC is providing 15 million customers its biometric banking software to access online and phone accounts using their fingerprint or voice[1]. Likewise, the masses are accepting and willing to utilize biometric systems more and more for accessing laptops, mobile phones, cars, homes, and mobile payments, e.g., Apple iPhone 5s, Samsung Galaxy S4, and Fujitsu NX F-04G smartphones that can be automatically unlocked using fingerprint, face, and iris, respectively. Thanks to the new generation of compact and cheap sensors, the current biometrics are affordable, user friendly, fully automatic, real-time, and incorporable into any everyday used security system.

How are biometric technologies being updated?

Typical biometric systems still use traditional data acquisition techniques, i.e., either touch-based (e.g., fingerprint), requirement of user's co-operation (e.g., face) or very close encounter with the scanning device (e.g., iris). Nevertheless, biometric software and hardware are getting ever more sophisticated. In terms of hardware, novel sensors based on thermal, ultrasound, multispectral, 3D, mobile and smart mechanisms are now available, which are capable of recording biometric samples in difficult conditions as well [5]. Indeed, touchless sensors, including ones which scan a biometric pattern directly from just below the skin's surface, are presently being incorporated in commercial products [4]. In terms of software, biometrics is demonstrably progressing not only to handle heterogeneous or interoperability but also to increase data-quality, data reliability, speed, privacy, and security against attacks [3]. The perfect marriage of hardware and software advancement has made 'on-the-fly' high-throughput biometric systems possible. These systems can successfully capture and identify biometric patterns from individuals in motion even from large distances [4]. Moreover, offbeat authentication systems based on novel traits or inter-biometric traits are actively being studied to bring the systems to individual level [14].

Are computer better than human for biometric recognition in terms of accuracy?

The answer isn't so straightforward and not yet settled. This is largely because of the challenging covariates, such as modality type, application, ethnicity, and quality of the input samples. Few studies compared the performance of automated biometric systems and humans for face recognition, latent fingerprint identification and demographic information estimation; the humans outperformed automated algorithms under difficult samples (e.g., when very small portion of the biometric trait sample is available) [1]. However, algorithms based on deep learning, year by year, tend to reach or even to outperform humans. Familiarity of the users greatly helped the humans for better performance in face recognition. Incorporating such information and human cognition into automated biometric systems will greatly improve the accuracy; which is still an open issue [11].

Is biometrics a threat to health?

No. Biometrics has been in use for over 30 years, with no reported health menaces [1]. There are many evaluation reports on the health safety of biometrics, which are also used by governments and institutes to attest to their health hazards, e.g., ISO/IEC TR 24714-1:2008 report. There do exist health concerns with touching a sensor (e.g., fingerprint) used by countless individuals that may transmit infections, which is identical to those encountered in daily life (e.g., touching a doorknob). Likewise, iris readers using near-infrared light have been suspected to damage eyes; this is not true because they use 750-760nm IR light not lasers/UV lights, and the amount of this light is no more than would be received by walking outside on a sunny day. Exciting researches and products are in progress to counteract this fear; for example development of contactless/visible spectrum sensors. All in all, biometric systems including commercial ones pose no health threat, since they are safety certified by standardizing bodies (e.g., RoHS, EC) [11].

Are there any biometric standards?

Biometric standards are general rules for collecting, evaluating, storing, and sharing biometrics [18]. There are several national and international organizations developing biometric standards:

i Standards development organizations (SDO): including ISO/IEC, ITU-T, CEN, ANSI
ii Industry consortia: including BioAPI Consortium, Biometric Consortium, OASIS, FIDO Alliance (UAF)
iii Other organizations: including ICAO, ILO

SDO, industry consortia and other organizations develop standards in accordance with their legislative mandates, objectives of members (e.g., UAF/U2F in Fido alliance; adopted in many products e.g., Samsung S5 fingerprint scanner), and particular applications within domain, respectively. Among all, the ISO/IEC Joint Technical Committee 1 is more active and till date has published more than 30 international standards related to biometric acquisition, evaluation, security, etc.

IV. Current Issues and Challenges of Biometrics

Despite the progress, a number of key challenging issues are being faced by biometrics, which are detailed in this section.

What are the key challenges biometrics facing in recent years?

[1] http://www.bbc.com/news/business-35609833

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

Despite recent advances, biometrics still has to deal with many technical, societal, legal and standardization challenges. The key technical issue surrounding biometrics is the low performances in the wild (also know as unconstrained biometric recognition) [4]. In the wild, by definition, exhibit large range of disparity seen in everyday life, which includes variability in illumination, pose, imaging modalities, and occlusions to name a few (see Fig. 1e). Similarly, the biometric interoperability (cross-scenarios) between systems, datasets and sensors are negatively impacting the overall recognition performance. Also, majority of existing biometric algorithms fails to identify a person after or before the plastic surgery, since it greatly alters texture and global appearance of biometric traits [1]. The cultural and social backgrounds are affecting largely the efficacy of biometrics, too. For instance, some people avoids to provide their biometrics (e.g., full face image) due to customary adornments or privacy concerns over how their biometrics will be used, since there is a supposedly irrevocable link between biometric traits and personal records. Presently, biometrics is facing many legal complications such as acceptance of biometrics as digital signature and biometric trait's individuality. Furthermore, though there exists several biometric standards, a variety of challenges remain unsolved like patent ambush and application tensions when two standards have significant differences [18].

Is biometric negative identification an issue?
Biometrics can be categorized in 'positive' and 'negative' identification modes [1]. In positive identification, the user submits willingly their biometric trait with their identity to the system. The system affirms the match by comparing the submitted trait only against his/her traits in the template database. While, negative identification does not demand any identity claim by the user. Here, the user's biometric trait is compared generally against all the individuals' trait in the database to ascertain the identity [2]. The traditional person recognition techniques (e.g., passwords) work for positive recognition; only biometrics can be used for negative identification [4]. The prime aim of negative identification is to prevent an individual from using multiple identities (e.g., the passport issuing authority can check that the applicant does not already have a passport under different name). Perhaps, the well-known negative identification system is the 'US-VISIT'. However, negative identification carry several risks, such as use of biometric trait (e.g., fingerprint) either as a linking identifier across disparate databases without people's consent or for completely unrelated purposes, which lead thus to infringement on civil liberties and privacy [11]. Most importantly the result of a false match in negative identification may get wrong person either convicted or denied the access. The ongoing standardization (within and between industry and nations) plans to share and unify the databases, which would potentially put one's entire life history in interoperating databases that would be only a biometric trait away. Similarly, negative identification can also empower racist or ageist approaches of stigmatization and exclusion, since ancillary information, such as ethnicity, gender and age can be extracted from primary biometric traits viz., face, fingerprint and iris [15].

What about the missing data in multibiometric systems?
Since multibiometric systems (i.e., systems that consolidate the evidences from two or more biometric traits) provide several advantages (e.g., lower error rates), thus large-scale systems are increasingly becoming multimodal (e.g., US-VISIT) [2]. However, multimodal systems frequently encounter the missing data problem. For instance, an enrolled user of a face and fingerprint based system may have lost his/her fingers in an accident. Likewise, only subset of modalities was obtained from the crime scene. The missing data scenario may occur owing to missing modalities either in template, query or incomplete score information from the individual matchers. There exist solutions (e.g., extended likelihood ratio-based score fusion [4]) that are capable to tackle above outlined three kinds of missing data successfully without compromising the accuracy [2].

Can biometrics differentiate identical twins?
Identical twins have the closest genetics-based relationship; therefore maximum similarity between their biometric traits is expected to be found among them [1]. Recent advances have made it possible to successfully distinguish identical twins using their fingerprint, retina, iris, thermogram or face, when minute details (e.g., moles) or motion information are incorporated. Also, scientists have lately developed a DNA based genetic test that can distinguish between identical twins, and is currently being used in the courts. It is found that unimodal biometric systems exhibit a slightly lower accuracy for identifying twins than non-twins. However, multibiometric systems (e.g., fingerprint with iris) have shown remarkable improvement in identical twins verifications [4].

Are there big data issues in biometrics as well?
Broadly speaking, big data in biometrics is the collection and analysis of millions biometrics-related data of many sorts for completely diverse purposes and with different properties, such as usability, availability, reliability, maintainability, privacy, security, performance, and so on [4]. For instance, UIDAI (Unique Identification Authority of India) is a system that provides identity to all persons (i.e., 1.25 billion) resident in India using biometrics. Like any other big data system, biometrics is also facing four main challenges: volume (database size), velocity (response/processing-time), veracity (robust to fraudulent), and variety (multiple biometric identifiers). It is a very active research field to devise big data techniques addressing these challenges in various biometrics scenarios, while eliminating risk, privacy and accuracy concerns.

V. Hot topics in biometrics

This section presents an overview of most noticeable recent topics (trends) that aim to make authentication more convenient and secure.

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

How are novel biometric traits in smartphones different from well-established modalities?

Smartphones are rapidly becoming data hubs and being used for storing e-mail, personal photos, online history, passwords, and online banking including payment information. Therefore, they require a high level of security. Consequently, traditional well-established biometric traits (such as face, fingerprint, and iris) are continuously being studied and incorporated in commercial mobile devices. The state-of-the-art in mobile fingerprint, face, iris, voice, keystroke-, and touch-dynamics recognition attain 2.0%, 3.58%, 0.05%, 0.47%, 3.6%, and 3.5% EER, respectively [5]. Nevertheless, most of the users do not either use biometrics or password to protect their device[2] because of time consumption for authentication[3] and/or demand of co-operation using traditional traits. But, mobile devices also possess other sensors, such as accelerometer, magnetometer, gyroscope, GPS, barometer, proximity sensors, and touchscreen (see Fig. 1a), which might also assist in user authentication by deriving novel mobile behavioral biometric traits, such as scrolling patterns, phone movement [5]. In fact, research on novel mobile biometrics using these sensors is progressively emerging. Contrary to traditional traits, novel mobile biometric traits are unobtrusive, user-friendly, fast, continuous, invisible, hard-to-spoof, and require minimal interaction for authentication. However, there are still several challenging problems in improving privacy, security, usability, and ergonomics of novel mobile biometrics [5].

Why are behavioral biometrics getting so much attention now?

Contrary to physical biometrics that involve innate human characteristics (e.g., fingerprint), behavioral biometrics identifies an individual using not what they are, but what/how they do certain activities [9]. Behavioral biometrics are immensely vital for surveillance, particularly towards identifying critical events before or as they happen. Examples of behavioral biometrics are gait, voice, mouse/keyboard use attributes, touch screen patterns on mobile devices, cognitive, and interaction with various websites/apps. Behavioral biometrics provide a higher level of accuracy and security, especially when they are fused with data from mobile/wearable device's in-built sensors (e.g., accelerometer and gyroscope), which are comparatively difficult to be mimicked, besides multibiometrics making it harder for an intruder to spoof several biometric traits simultaneously [2]. Moreover, since most of the behavioral biometrics are non-invasive, frictionless, unobtrusive, and hard to spoof (e.g., it is almost impossible spoofing the phone movements of users performing 'phone-hold signals and touchscreen' based multimodal authentication), they are therefore gaining now so much momentum.

How is biometric privacy concern being addressed?

The growth in use of biometrics has also escalated concerns about individual's privacy and data security. Biometrics can also be misused for unintended purposes against one's will, as biometric data also reveals additional information, such as age, race and certain genetic disorders[4] that can be extracted by automated schemes [10]. Efforts are afoot to design privacy-preservation (also known as de-identification or changeability) algorithms to reduce the likelihood of unauthorized disclosure of such personal attributes [4]. The implicit aim of de-identification is to protect privacy while preserving data utility. In privacy-preservation, biometric data content may be altered to remove or obfuscate personal information. Another track being pursued specially to decrease privacy concerns is legislation by governments (e.g., European Union constitution against sharing biometric identifiers and personal information) and assurance by biometric vendors to adhere to a set of ethical guidelines in their product design [18]. Nevertheless, it is worth mentioning that an individual can not be recognized from just a random photograph without associated metadata.

Besides DNA, can any other biometric trait be employed to verify the kinship?

Yes. Face biometrics can also be used for kin recognition. Kinship verification from facial images is a relatively new research arena in biometrics, which aims at training the machine to determine automatically whether there is a kin relation between a pair of given face images [4]. The kinship is defined as a relationship between two persons who are biologically related with overlapping genes. Potential applications for kinship verification are family album organization, genealogical research, missing family members search, assisting legitimate immigrants and victims of trafficking. Current kinship verification algorithms attain accuracy ranging from 70 to 80% [1].

Does 3D biometrics overcome the drawbacks of traditional 2D systems?

2D biometric systems use two-dimensional intensity images, and achieve good performance under constrained environments. They still however encounter difficulties in handling large amounts of variations owing to lighting conditions, poses, occlusion, etc. [4]. While, 3D biometric technology is an emerging trend that utilizes three-dimensional geometric information of biometric traits and holds great promise. 3D systems perform inherently robust and better than traditional 2D systems under these variations [14], besides taking us towards much demanded touchless biometrics. Nevertheless, 3D biometric technologies are yet not much robust to expression, facial hair, and large occlusions in face recognition. A lot of research is undergoing into 3D and 2D interplay, such as how to match one to the other (e.g., iterative closest point algorithm), how to obtain one from the other (e.g., polygonalmes), how to fuse 2D and 3D information (e.g., competitive fusion), and how to utilise one to constrain the other (e.g., serial fusion of modalities/features).

[2]This way, users leave their personal information accessible to malicious individuals (www.kpcb.com/insights/2013-internet-trends).

[3]The average smartphone user checks their device 150 times per day. If unlocking the device takes 2 seconds, the typical user spends 5 minutes unlocking their device every day (www.kpcb.com/insights/2013-internet-trends).

[4]For example, certain malformed fingers might be statistically correlated with certain genetic disorders [11].

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

VI. Security of Biometric Systems

Like any conventional security system, biometrics can suffer malicious adversaries, who may manipulate data to compromise its integrity. Here are few most commonly asked security questions.

What are the points where a biometric system can be compromised?

The security of biometric systems can be compromised at eight possible different points [3, 11] as shown in Fig. 1f. Attacks from point 1 are carried out at the sensor using fake biometric traits, also known as presentation or spoofing attacks [3]. Attacks from points 2, 4 and 7 exploits possible weak points in the communication channels and try to intercept or insert information into the channel. Points 3, 5, 6 and 8 may be performed as Trojan Horse attacks to bypass the feature extractor, the matcher, the system database and decision modules. These vulnerabilities may cause denial-of-service, intrusion, and privacy erosion due to function creep [5]. Numerous techniques to mitigate biometric security risks have been developed, which we will discuss below in consequent questions.

Anyway, biometrics has various security advantages over traditional 'what you know' and 'what you have' authentications. For instance, most passwords are simple (e.g., nickname) or regular dictionary words (e.g., university) that can be easily guessed, hacked, borrowed, or stolen. Token are prone to loss, duplication, sharing, or theft. Moreover, passwords/tokens are unable to provide nonrepudiation. While, biometrics offers the property of nonrepudiation and de-duplication, and cannot be lost, forgotten, shared or distributed [9]. Though, many biometrics are not secret leading thus to spoofing, biometric forging requires more time, experience, and access privileges. Additionally, behavioral biometrics (particularly mobile traits, e.g., touchscreen) provide normally stronger security than physical traits (e.g., face), since they demand advanced technical skills to be spoofed [3].

Is spoofing another serious concern to biometrics?

Biometric spoofing is a procedure in which a biometric system may be subverted by masquerading as registered user, and thereby gaining illegitimate access and advantages [7]. For example, presenting a face mask to the system (see Fig. 1g). Spoofing attacks are still a major concern (e.g., just two days after the iPhone5s hit the market, it was fooled by a fingerprint spoof), but several countermeasures have been developed. For instance, the liveness detection methods that exploit physiological signs (e.g., eye blinking) to determine whether there is a live person or an artificial replica in front of the biometric sensor [3]. Similarly, novel sensors are also available that can detect spoofing attacks themselves [3].

What are the biometric 'hill-climbing' and 'brute-force' attacks?

The hill-climbing attacks on biometrics consist of submitting *synthetic* biometric representations iteratively to the system and, according to the output match score, modifying such data randomly until the acceptance threshold is exceeded. While, brute-force attacks are performed by submitting *real* biometric samples to the systems until the system wrongly accepts one as of the genuine user [3]. These two attacks can be perpetrated both at feature extraction module (type 2 in Fig. 1f), where input image is modified till successful recognition is achieved, and at matcher module (type 4 in Fig. 1f), where synthetic random templates are perturbed until the decision threshold is surpassed. To crack the system successfully, the hill-climbing attacks require less resources and efforts than brute-force attacks. In fact, the attacker in brute-force must have a data set containing thousands of real biometric samples in order to efficiently fool the system, whereas no real biometric samples are needed in hill-climbing attacks. Further, if we compare the robustness of biometrics and password-based security systems, then passwords are easy to be cracked by brute-force dictionary attacks or by simple guessing [6, 9]. For instance, suppose that a biometric verification system is operating at 0.001% FAR. A 0.001% FAR also indicates that 1 out of 100,000 brute force attacks on an average will be successful. While, if we consider this as an equivalent to the robustness offered by a randomly chosen five-digit PIN, then a brute-force attack against a five-digit PIN will require only 50,000 attempts on an average to intrude the system.

What does biometric evasion and obfuscation mean?

Surveillance and forensic applications include the detection task, e.g., detecting known speakers in intercepted conversations. The threat here involves evasion and obfuscation, whereby the person of interest may seek to provoke a missed detection. When a person intentionally alters their own biometric trait to target detection module is known as evasion. When recognition module is targeted, it is called obfuscation [3]. Contrary to spoofing, the aim of evasion and obfuscation is not being falsely accepted, but to avoid being either detected or identified by one's true identity mainly in the case of surveillance and forensics. For instance, use of face occlusion/make-up/plastic-surgery or fingerprint alternation. The evasion or obfuscation attacks target two distinctly different components of a typical biometric systems as illustrated in Fig. 1h. In recent years, methods (e.g., biometric alternation detection [4]) to detect such attacks have been developed.

Is it possible to reverse-engineer a biometric trait sample from a biometric template?

Yes. Template is a compact description of original data, and it is not contemplated, by definition, to disclose crucial information about original biometric sample. Therefore, it was traditionally believed that template does not contain enough information to allow reconstruction of original sample [5]. In other words, template generation techniques have been presumed to be "one-way" schemes. But, recent studies on inverse biometrics have questioned this common belief, and designed techniques to regenerate original samples from its templates [1]. However, inverse biometrics can be thwarted by cancelable biometrics or biometric cryptosystem that generates cryptographic keys based on biometric samples to protect not

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

only templates but also user's privacy [4].

Can biometrics be reissued like passwords when compromised?

Biometrics is permanent corporeal attribute of a person, and cannot be physically replaced when compromised. To address this problem, a novel technique called '*cancelable biometrics*' has been lately developed [11]. The basic idea of this approach is that instead of storing the original template, it is the mathematically transformed template that is stored in the enrolment database. In particular, a transformation function (F) is applied to the biometric template (X_T), and only the transformed template ($F(X_T;K)$) is stored in the database; where K is the parameter that characterizes the F. Like passwords, these transformed templates when compromised can be revoked and reissued, since whenever the transformation function/parameter is changed new revocable or cancelable templates are produced [3].

VII. Future of Biometrics

Interdisciplinary researchers are leaping into the world of biometrics to develop novel unobtrusive future biometric traits. Some questions related to future are examined here.

Wearable biometrics: Fad or the Future?

Wearable biometrics refers to person identification technology incorporated into items of garments and/or accessories that can read, record, and compare individual's biometric traits such as heart rate, respiratory rate, or any type of physical activity [6]. Examples of wearable devices are smart watches, bands, ear-pods, jewelry, eyeglasses, contact lenses and clothing. Wearable biometrics has tendency to provide seamlessly continuous authentication without user's interaction, efforts and cooperation [5]. Slowly but surely, wearable biometric devices will become crucial physical extensions of our lives to digitally unlock our every day physical and virtual lives–from car to communications, home security to banking, healthcare to other services. Soon, a more sophisticated insights of Electroencephalography (EEG), electrocardiogram (ECG) and Electromyography (EMG) patterns in wearables would help gauging our likes and dislikes for entertainment, smart home controlling, and interactive gaming beside the identification [6]. Wearable biometrics will only continue to grow becoming sooner or later a universal authenticator that intuitively knows who we are, where we are, what we want to do. In fact, latest analysis report has forecast that by 2019 globally there will be 604 million users of wearable biometrics[5].

Is it possible to identify individuals based on their brainwaves?

Yes. Researchers have devised a technique to identify people by their brain activities or brainwaves (formally known as EEG). The system recognizes individuals by monitoring the unique patterns of electrical activities within the brain in response to certain words [8]. Such neurological responses are known as 'Brainprint', which are recorded using an established method called electroencephalogram (EEG). This novel biometrics is like a fingerprint for your brain signal, but its usability and acceptability hitherto is rather limited owing to requirement of user wearing an EEG cap and a medium level accuracy of current recognition algorithms [8].

Can wi-fi signals identify and track people even through walls?

Very lately, researchers have developed a system named RF-capture, which can identify and track people even through walls using just wi-fi signals [12]. The RF-capture uses radio frequency signals—which can traverse walls and reflect off the human body—to capture 'reflections patterns' (i.e., the representative silhouette human figure) in order to detect, track or identify the person even if he/she is fully occluded. Nevertheless, RF-capture's accuracy decreases with increase in number of users to be identified, e.g., accuracy deceases to 88% for 15 subjects [12].

Can GPS (Global Positioning System) information be used to identify individuals?

Yes. With the advent of portable devices (e.g., smartphones, tablets) equipped with GPS, Bluetooth and WiFi sensors, the location and mobility data could be easily collected. Pattern of movements and locations, when traced on a map, creates something akin to a fingerprint that is unique to each individual; known as 'GPS fingerprint' or 'digital footprint'. One can identify 'who you are' by tracing your mobile device's location data [14]. The study showed that only four spatio-temporal points are enough to uniquely identify 95% of the individuals [14]. Other publicly available information (e.g., a person's home or work address and geo-localized tweet) together with GPS fingerprint may also be used to re-identify the person with enhanced accuracy. This raises the individuals' privacy and security issues. Since, the 'de-anonymization' attack[6] can be used not only for identification but also linking back to their personal data. For instance, burglars can plan house breaking according to digital fingerprint when successfully linked to the home address. Likewise, insurance companies can track frequent hospital visits; interpreting it as indicator for bad health. GPS based identification has to go a long way since it is very prone to misclassification when two or more individuals' paths cross or GPS precisions are coarsened, besides devising techniques to anonymize GPS data while maximizing utility [14].

Can we identify users of social networks by their data footprint?

It is possible to uniquely identify the users of social networks over the time, since the data generated by a social network user leaves a viable trail of data that can serve as a unique identifier just like the human fingerprint, which is named as 'social fingerprinting' [17]. A social fingerprint mainly contains three

[5]http://www.planetbiometrics.com/article-details/i/2341/desc/wearables-to-drive-second-wave-of-biometric-adoption-report/

[6]When an adversary tries to infer the identity of a particular individual behind a set of location and mobility traces.

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

overarching types of information: the initiator, the selected activity, and the recipient. On any given social network, a user chooses how to engage with the network and a specific recipient of the action. For instance, on Twitter, users can reply to, favorite, or re-tweet the information of other users. It is worth emphasizing that large-scale evaluation study has yet to be conducted to substantiate the findings of existing researches. Moreover, current social fingerprinting techniques are applicable to single social networking data and struggle to handle missing/incorrect profile attributes [17].

Is it true that face can be reconstructed from DNA?
Of late, researchers have studied the ways genes influence facial development, and devised mathematically a computer program that can construct facial features of a person using genetic markers from their DNA. This technique is known as 'DNA phenotyping' or 'molecular photo fitting' [14]. The recreated face includes fairly accurate everything from skin tone to eye color, hair color, ancestry, and freckling. Yet, age, baldness and hair curliness are tough parameters to predict and to reconstruct in the face. Nevertheless, the technique is expected, in the near future, to recreate faces of extinct human relatives. Though, the developed technique is in its infancy, it is still quite useful for law enforcement agencies to hunt down the suspects. The prospect of widespread DNA phenotyping has unnerved many experts. Some scientists are questioning the accuracy of the techniques, while others are cynical about the technique being used for racial profiling among law enforcement agencies, besides infringing on privacy and taking civil liberties into uncharted waters.

What will biometrics do in the next twenty years?
Though biometrics is not new, day by day it is becoming increasingly mainstream thanks to the growth of mobile and wearable devices [6]. We can see glimpses of what biometric future will look like. Advances in existing and novel biometric traits are providing better security and more accurate ways to identify people. Arrival of this trend, within the next ten years, promises to revolutionize aspects of life using synergistic multiple biometrics for eGoverment, eHealth, eBanking, eBanking and Smart Homes, etc. [9]. In other words, biometrics in the future will matter more than ever. Though it is too early to predict the exact essence of biometrics in the future, it is undeniable that there will be no way around biometrics-based recognition.

Acknowledgment

This research work has been partially supported by a grant from the European Commission (H2020 MSCA RISE 690907 "IDENTITY").

References

[1] S. Z. Li, A. K. Jain, *Encyclopedia of Biometrics*, Springer, 2015.

[2] A. Ross, K. Nandakumar, A. K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[3] S. Marcel, M. S. Nixon, S. Z. Li, *Handbook of Biometric Anti-Spoofing*, Springer, 2014.

[4] A. K. Jain, K. Nandakumar, A. Ross, *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*, Pattern Recognition Letters, 2016.

[5] W. Meng, D. Wong, S. Furnell, J. Zhou, *Surveying the Development of Biometric User Authentication on Mobile Phones*, IEEE Communications Surveys and Tutorials, (17):3, pp. 1268-1293, 2015.

[6] C. Cornelius, C. Gutierrez, *A Survey of Biometrics for Wearable Devices*, Intel Technology Journal, (18):4, 2014.

[7] Z. Akhtar, *Security of Multimodal Biometric Systems against Spoof Attacks*, PhD thesis, University of Cagliari, Italy, 2012.

[8] B. C. Armstrong et al., *Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics*, Neurocomputing, 2015.

[9] R. V. Yampolskiy, V. Govindaraju, *Behavioural Biometrics: a Survey and Classification*, International Journal of Biometrics, (1):1, pp. 81–113, 2008.

[10] A. Dantcheva, P. Elia, A. Ross, *What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics*, IEEE Transactions on Information Forensics and Security, (11):3, pp. 441-467, 2016.

[11] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2009.

[12] F. Adib et al., *RF-Capture: Capturing a Coarse Human Figure Through a Wall*, ACM Trans. Graphics, 2015.

[13] Luquetti et al. *Modeling 3D Facial Shape from DNA*, PLoS, 2014.

[14] L. Rossi et al., *Spatio-temporal techniques for user identification by means of GPS mobility data*, EPJ Data Science, 2015.

[15] M S. Nixon, P. L. Correia, K. Nasrollahi, T. B. Moeslund, A. Hadid, M. Tistarelli, *On soft biometrics*, Pattern Recognition Letters, 68(2):218–230, 2015.

[16] J. Lu et al., *Neighborhood Repulsed Metric Learning for Kinship Verification*, IEEE TPAMI, 2014.

[17] A. Malhotra et al., *Studying User Footprints in Different Online Social Networks*, International Conference on Advances in Social Networks Analysis and Mining, 2012.

[18] F. Deravi, *Biometrics standards*, Advances in biometrics, Springer, 2008.

Biography

Dr. Zahid Akhtar: Dr. Akhtar is a postdoctoral researcher in the INRS-EMT center at the University of Quebec, Canada. His research interests include computer vision, pattern recognition, and image processing with applications in biometrics, affective computing, and security systems. Dr. Akhtar received a PhD in electronic and computer engineering from the University of Cagliari (Italy) in 2012. He is a member of the Italian Association for Pattern Recognition. Contact him at zahid.eltc@gmail.com, zahid.akhtar.momin@emt.inrs.ca.

Prof. Abdenour Hadid: Prof. Hadid is an adjunct professor and senior researcher in the center for machine vision

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE

research at the university of Oulu, Finland. His research interests include computer vision, machine learning, and pattern recognition with a particular focus on biometrics. He received a D.Sc. degree in electrical and information engineering from the University of Oulu in 2005. He is a member of the Pattern Recognition Society of Finland and the International Association for Pattern recognition (IAPR). Contact him at hadid@ee.oulu.fi.

Prof. Mark S. Nixon: Prof. Nixon is a professor of computer vision with the University of Southampton, U.K. His research interests are image processing and computer vision. His team were early workers in face recognition, later came to pioneer gait recognition and more recently joined the pioneers of ear biometrics. He received a PhD degree in Applied Estimation Theory from the University of Reading in 1983. He is a Fellow of IET, IAPR, and BMVA. Contact him at msn@ecs.soton.ac.uk.

Prof. Massimo Tistarelli: Prof. Tistarelli is a professor of computer science and the director of the computer vision laboratory with the University of Sassari, Italy. His main research interests cover biological and artificial vision, pattern recognition, biometrics, visual sensors, robotic navigation, and visuomotor coordination. He received a Ph.D. degree in computer science and robotics from the University of Genoa, Italy, in 1991. He is a member of the conference committee of the IEEE Biometrics Council, and a Fellow Member of IAPR. Contact him at tista@uniss.it.

Prof. Jean-Luc Dugelay: Prof. Dugelay is a professor with the department of digital security at EURECOM in Sophia Antipolis, France. His current research interests include domain of multimedia image processing, in particular activities in security (image forensics, biometrics and video surveillance, mini drones), and facial image processing. Prof. Dugelay received a PhD degree from France Tlcom Research (CCETT) at Rennes, France, in 1992. He is fellow member of IEEE and IAPR. Contact him at dugelay@eurecom.fr.

Dr. Sbastien Marcel: Dr. Marcel is a lecturer at the Ecole Polytechnique Fdrale de Lausanne and Senior Research Scientist with the Idiap Research Institute, Switzerland, where he leads the Biometrics Group and conducts research on multimodal biometrics, including face recognition, speaker recognition, vein recognition, and spoofing and anti-spoofing. He received a Ph.D. degree in signal processing from Universit de Rennes I, France, in 2000. He is member of IEEE and IAPR. Contact him at marcel@idiap.ch.

Digital Object Identifier 10.1109/MMUL.2017.265090754 1070-986X/$26.00 2017 IEEE