EMBO reports

Biometrics' new identity—measuring more physical and biological traits

Research into the characteristics that are unique to an individual is addressing the need to correctly identify people in a variety of medical, social and security contexts

Andrea Rinaldi

There is no need to remember complex combinations of random numbers and characters. From now on, you are the password: your fingerprint, face, iris, gait or odour—any of your potentially unique attributes—can theoretically be used to identify you. This is the idea behind biometrics, which was once confined to the realm of spy movies and high-security facilities, but is now increasingly common in everyday security checks at borders, for secure payments and logging in to mobile devices. Beyond security, though, biometrics technology is also driving and enabling other applications that include forensic science, data sharing over networks and reducing identification errors in hospitals.

> *"Biometrics is essentially ready for mass application, as the success of the Indian Aadhaar programme demonstrates."*

While fingerprints and retina patterns are the most well-known biometric identifiers, they are not the only characteristics that can be used for biometric identification. Physical traits such as the shape of the face, hand or ear, the vasculature in the finger or DNA—so-called hard biometrics—as well as behavioural characteristics such as gait, signature, voice and typing patterns can all be used to identify individuals (Fig 1). Another large and rapidly expanding category—which includes characteristics such as skin or eye colour, height, weight and tattoos—is known as "soft biometrics" and provides less distinctive, less categorical information, but has the advantage that such traits can be measured from a distance without cooperation from the subject. Even body odour is being actively explored as a practicable biometric identifier (http://www.sciencedaily.com/releases/2014/02/140204073823.htm).

Biometrics is essentially ready for mass application, as the success of the Indian Aadhaar programme demonstrates. Launched in 2010 by the Unique Identification Authority of India (https://uidai.gov.in/), the goal of the programme is to provide all 1.2 billion Indian citizens with a unique 12-digit number linked to biometric features to serve as an identification system "devoid of any classification of caste, creed, religion and geography". In a country where hundreds of millions have no official ID and where the poor are often excluded from subsidies or social benefits—such as food coupons and cooking gas—because they cannot prove their identity, the initiative will both enable fairer access to government benefits and permit residents to access other services, like opening a bank account or applying for loans. The programme's biometric database includes two iris scans, ten digital fingerprints and a digital photo for every resident (Fig 2). An online platform will help service providers authenticate the identity of residents electronically, in a safe and quick manner. Although enrolment is voluntary, the response has been enthusiastic. So far, more than 900 million "Aadhaars" have been issued, and the number grows by one million every day.

> *"Conventional but trusted biometric techniques such as fingerprints and face recognition are vulnerable to attacks…"*

There is global interest in the Aadhaar scheme and the underlying biometrics technology from other governments and international organizations. "We've got to think about how we can integrate this technology into a massive effort to scale up access to financial services", said Jim Yong Kim, President of the World Bank (http://www.worldbank.org/en/news/feature/2013/05/02/India-8217-s-Massive-I-D-Program-Exemplifies-8216-Science-of-Delivery-8217). Kim described the programme as an excellent example of the integration of technology for social welfare use and a major driver in the effort of eradicating poverty by 2030.

The main challenge in the biometrics field is, needless to say, security. Conventional but trusted biometric techniques such as fingerprints and face recognition are vulnerable to attacks, for instance by presenting an artefact that imitates the unique biological trait of a person to a biometric scanner, thereby gaining illegal access to a protected device or service. Given the growing importance of biometrics, this practice, known as spoofing, is not a marginal issue and the EU-funded Tabula Rasa project has attempted to

Freelance science writer in Cagliari, Italy. E-mail: rinaldi.ac@gmail.com
DOI 10.15252/embr.201541677 | Published online 14 December 2015

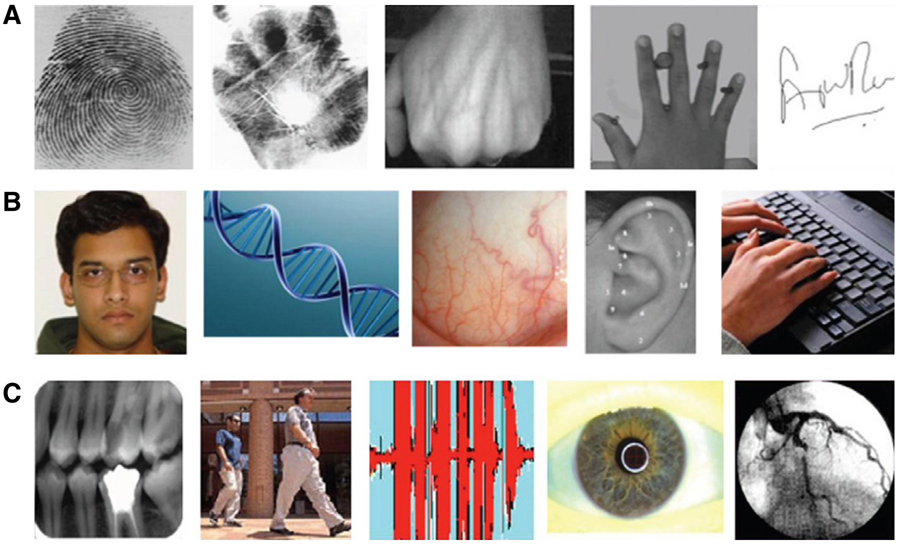


Figure 1. Examples of biometric traits.
(A) Fingerprints, palm prints, hand vasculature, hand shape and signature. (B) Face, DNA, sclera (on the eyeball), ear shape and typing patterns (keystroke dynamics). (C) Teeth (forensic odontology), gait, voice or speech, iris and retina. Some of these traits—fingerprints, palm prints, face, voice, teeth, ear shape and DNA—are also used in forensics. Reproduced with permission from: Jain AK, Ross A (2015) Bridging the gap: from biometrics to forensics. *Phil Trans R Soc B* 370: 20140254.

Figure 2. Recording personal features in rural India as part of the Aadhaar project.
"Aadhaar" means "foundation" or "base" in most Indian languages. See main text for more details. Credit: Unique Identification Authority of India.

tackle the problem in an innovative way (https://www.tabularasa-euproject.org/). Researchers involved in the project assessed the vulnerability of biometric systems to spoofing, revealing that many are susceptible to attack if they are not protected by adequate countermeasures and that the most accurate biometric systems, those with low false acceptance/false rejection rates, are also the most vulnerable ones. Among the various biometric characteristics the project investigated, gait was shown to be particularly robust to direct spoofing attacks [1].

"Through the project we have learned many important lessons, but also ended up with a new bunch of research questions that still remain unsolved", said Sébastien Marcel, leader of the biometrics group at the Idiap Research Institute in Martigny, Switzerland, and Tabula Rasa coordinator. "The project mostly focused on software-based countermeasures for anti-spoofing. Thanks to the work done, it's now clear that detection of more elaborated spoofing attacks will probably require a new generation of countermeasures combining hardware-based and software-based approaches".

Research into alternative systems is thus blooming, and novel avenues are being actively explored. Recent work has shown that electrophysiological signals—dependant on the electrical properties of tissues and cells—are distinctive enough for each individual person to be used for biometric applications, with the additional bonus of being inherently difficult, though not impossible, to forge. Bioelectrical signals recorded from the heart (electrocardiography, ECG) and the brain (electroencephalography, EEG) seem particularly well suited for these purposes [2].

Although no device based on electrophysiological biometry is on the market yet, the technology and the science underlying it have potential and unique features. First, electrophysiological signals are universal, meaning that while fingers can be cut off or retinas scarred, no living person can survive without a heart or brain—although the variability of individual ECG/EEG signals over time and surrounding context is still a matter of study. Second, unlike other biometric systems, both ECG and EEG signals can be monitored for prolonged periods—for example to continuously authenticate the user of a protected device after initial authentication. The Apple Watch applies the same principle of continuous monitoring, requiring the user to authenticate their identity with a password when the watch is strapped to the wrist, but then monitoring for a constant heartbeat to avoid the need for further authentication. As soon as there is an interruption in the heartbeat detected by the watch, the watch locks itself down again.

Another area where biometrics is bound to have a huge impact in the near future is in healthcare. Patient misidentification is a real problem, even in countries with advanced health systems. In the UK, more than 24,000 cases of patients being mismatched to their care were reported between February 2006 and January 2007 (http://www.nrls.npsa.nhs.uk/resources/?entryid45 = 59824). Obviously, the misidentification of patients can have dire consequences. These stretch from errors in drug administration and surgical interventions up to the discharge of infants to the wrong families. The UK's National Health Service (NHS) lists misidentification of patients as "never events": serious, largely preventable patient safety incidents that should not occur if the available preventative measures had been implemented (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215206/dh_132352.pdf).

The current identification systems in use in healthcare mostly rely on wristbands, which usually include the patient's name and an assigned number or code. However, there are instances were wristband use is not recommended—for example, in mental health units—or when the patient may refuse to wear a wristband. In other cases, such as in emergency care environments with high patient turnover, insufficient patient identity information or the need for rapid treatment can delay wristband use.

The most promising biometric identification system for medical use is vascular biometrics—the recognition of finger vein pattern using infrared light. Vein patterns differ for every individual and every finger and once developed during childhood are stable during adulthood. Light passes easily through the tissue in the finger and is absorbed by the haemoglobin in the blood, rendering an image from which vein pattern can be derived and matched to a patient profile in a database. Finger vein scanners are portable, the technology is safe and non-invasive, and several studies conducted in healthcare settings, including in emergency departments, have shown the high reliability of vascular biometrics [3].

"There has been only limited penetration [of biometric identification] into the health technology arena and one reason for this is the relative ignorance of biometric systems by healthcare professionals", wrote Max Jonas and colleagues at the University Hospital Southampton, UK, in a recent review on the topic [3]. "It is a certain prediction that with the accelerating development of health informatics in hospitals, biometric identification will have to become embedded within our clinical information systems".

Next-generation biometrics may well go beyond the human body. Several works point to the possibility of identifying individuals by looking at the bacteria that inhabit their bodies. Five years ago, when the study of the human microbiome was just beginning to flourish, researchers demonstrated that skin bacteria left on inanimate objects, such as computer keyboards, can be matched to the individual who used those objects with a high degree of certainty [4]. In other words, we leave unique bacterial "fingerprints" on the objects we touch.

The first foreseeable applications of such an approach could be in forensics, implementing the experience from other forensic evidence methods such as human DNA or fingerprint analysis, especially under certain conditions and in particular scenarios. For example, it might be easier in some cases to recover bacterial DNA than human DNA from surfaces, given the abundance of bacterial cells on the skin and on shed epidermal cells. "Furthermore, the technique might be useful for identifying objects from which clear fingerprints cannot be obtained, like fabrics, smudged surfaces, or highly textured surfaces", noted researchers [4].

More recently, Simon Lax and colleagues at the University of Chicago, USA, have looked at the pattern of microbes recovered from mobile phones and the soles of shoes of some 90 people attending three different scientific conferences. The bacterial profiles from the shoe samples clustered into distinct groups depending on the location, as there was a clear impact of the floor microbial community on the shoe microbiome [5]. This could help to trace the movements of both suspects and victims before reaching the crime scene.

Researchers could also infer the identity of individuals based on the microbes associated with their smart phone surface, even spotting significant differences between the front and the back of the phone owing to the fact that while the back is mainly in contact with the hands, the front comes into contact with the face and mouth. "Microbial communities show unique structure and composition based on surface type, the identity of the person interacting with the surface, and geographic location", the researchers concluded, stressing that delving into the personalized nature of the human microbiome and the microbial communities associated with urban environments could play a significant role in future forensic investigations [5].

A team at the Harvard School of Public Health in Boston, USA, provided further evidence that personal microbial fingerprints are sufficiently distinguishable to identify an

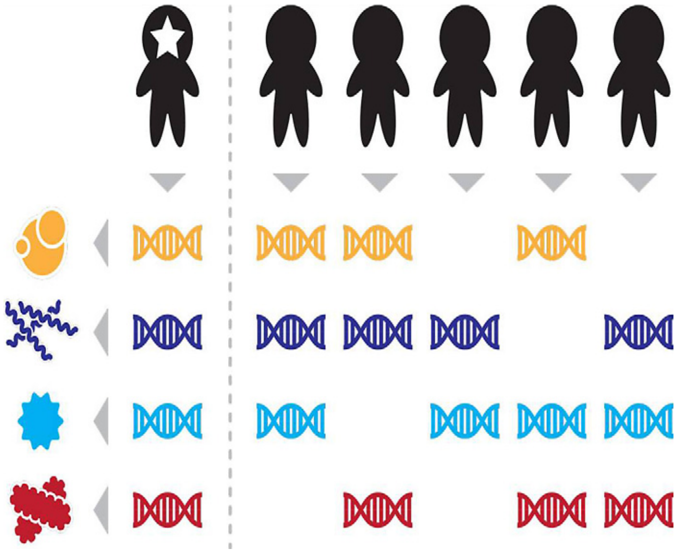
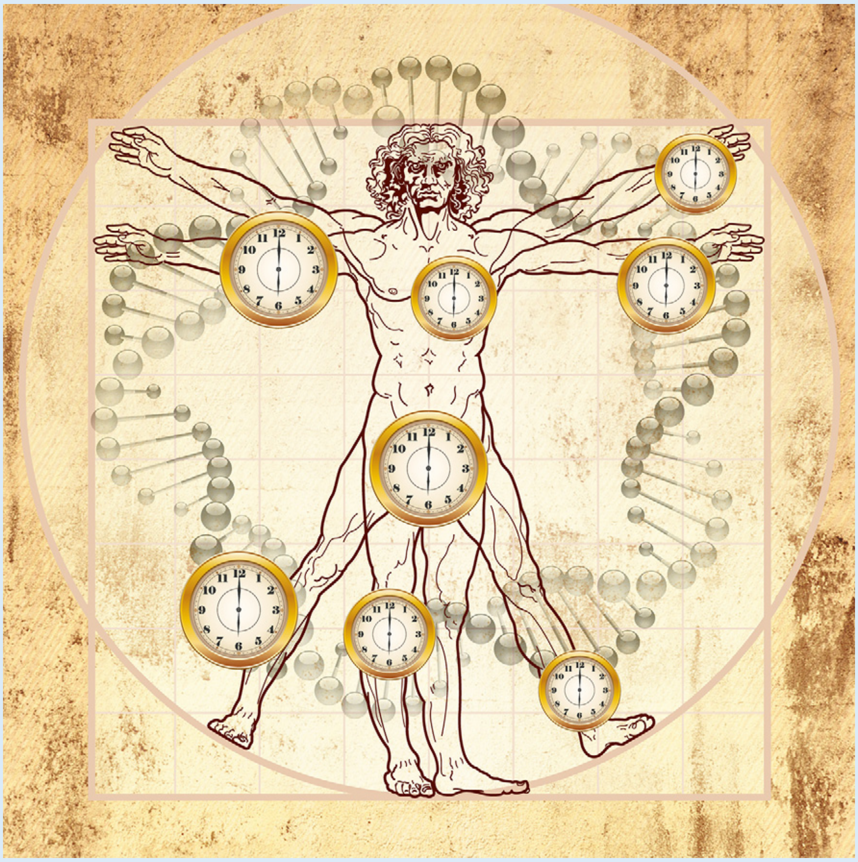


Figure 3. Microbial fingerprints.
Four microbial features inferred from metagenomic sequencing collectively distinguish the starred individual from the population (≥1 features are not detected in each other individual). Reproduced with permission from [6].

Sidebar A: Guess my age, if you can!

Biometrics is increasingly able to measure the most intimate features of the human body, but, oddly enough, it still cannot say for sure how old a person is. Indeed, objective and precise estimation of chronological age in living individuals remains a real challenge, and no unequivocal and reliable method exists. The need for age assessment involves various disparate cases. War and poverty are bringing thousands of refugees to Europe who cannot present evidence for their date of birth. If age is disputed, the process for accessing asylum, or the way one is treated in criminal proceedings, may differ substantially depending on the assigned status of "adult" or "child". To assess a child's nutritional status, it is necessary to know his or her age. In fact, the most common indicators of undernutrition are based on height (stunting) or weight (underweight) with respect to standard values for children of the same sex and age. However, while rich countries can rely on accurate demographic information from civil registration systems, more than 230 million children under five are not registered at birth in the world most of them in Asia and sub-Saharan Africa. "In these regions, children without a certain date of birth—month and year—have zero probability of selection in large epidemiological studies on nutritional status", said anthropologist Elisabetta Marini from the University of Cagliari, Italy. "We have shown that in sub-Saharan Africa a selection bias favouring registered children is present in demographic and health surveys, and can lead to underrate undernutrition prevalence" [9]. Guessing the age of unregistered children by asking parents is prone to inaccuracies, often ending up with an undervaluation of the age of these children, especially if they are stunted. The effect of this bias is, again, the underestimation of malnutrition. "We have calculated that systematic incorrect estimation of age of 3 months can lead to a significant difference in the prevalence of malnutrition and that 6 months of bias can lead to an error up to 28%", said Ornella Comandini, a PhD student in the Marini laboratory. In practice, age is estimated through a range of medical (X-rays of the hand and wrist, dental examination, X-rays of clavicles) and physical (height, weight, constitutional type) assessments. However, the accuracy of any of these methods has been questioned, as they are subject to influence by a number of variables, including nutritional status. Molecular approaches have also been put forward, although their application is less common. The most accredited one is racemization of aspartic acid from dentin, whereas the length of telomeres is now considered a better predictor of life span, rather than chronological age. The new kid on the block is the biological clock proposed by Steve Horvath, a geneticist and bioinformatician at the University of California at Los Angeles, USA. The method is based on the finding that DNA methylation levels across a broad spectrum of human tissues and cell types correlate with age; a median error of 3.6 years was found, but accuracy improves to 18 months for some types of cells, like those from brain cortex [10].



Sidebar A Figure: A biological clock based on epigenetic signatures able to estimate the age of human tissues and cells has been recently described. Reproduced with permission from [10].

individual over time among hundreds of people. Researchers tapped into microbiome data collected from 242 individuals enrolled in the Human Microbiome Project (http://hmpdacc.org/) and derived metagenomic codes from sets of microbial taxa or genes from different body sites (skin, mouth, gut and vagina) and individuals [6]. The codes were not only found to be unique between individuals, but were also largely stable over time: the gut habitat, in particular, produced the most stable codes, with more than 80% of individuals still identifiable a year after the initial sampling (Fig 3). "Linking a human DNA sample to a database of human DNA 'fingerprints' is the basis for forensic genetics, which is now a decades-old field. We've shown that the same sort of linking is possible using DNA sequences from microbes inhabiting the human body—no human DNA required", said lead author Eric Franzosa in a statement (http://www.hsph.harvard.edu/news/press-releases/personal-microbiomes-contain-unique-fingerprints/).

While it might be a while before microbiome-based biometric approaches enter the courtroom, profiling bacteria attached to pubic hairs could lead to a more straightforward forensic application. In the case of rape and sexual assaults, pubic hairs are often shed by offenders, but DNA analysis—which could pin down the perpetrator—is often hampered by the lack of sufficient genetic material from the hair. A recent study suggests that instead, the analysis of the bacterial communities living on pubic hairs could be used as a "microbial signature" for sexual crimes [7].

> *"In the absence of human biological trace evidence, bacterial DNA has the potential to provide the link between victim and offender in sexual assaults"*

In the study, researchers sampled seven individuals, three male and four female, at the start of the study and after two and five months. Metagenomic analysis of microbial DNA extracted from the samples revealed that each individual's pubic hairs harboured distinct communities of microbes and that pubic hair microbiota was stable over time. Furthermore, it was possible to clearly distinguish between pubic hairs from the sexes, largely because of the prevalence of *Lactobacillus* in the female pubic hair samples and the absence of these bacteria in the male samples [7].

"In the absence of human biological trace evidence, bacterial DNA has the potential to provide the link between victim and offender in sexual assaults", said lead author Silvana Tridico, from Murdoch University, Australia, pointing to the fact that the advent of DNA profiling has resulted in an increase of sexual offenders using condoms, which they take away, post-assault. "Microbial DNA profiling of human hair may provide independent data to augment other, more traditional, forensic data", Tridico said. "Like all novel forensic techniques, bacterial DNA profiling of hairs will require robust evaluation and validation prior to its introduction into casework".

A significant extension of these microbiome studies for biometric forensics comes from what happens when we die. Because microbes play a key role in the decomposition of cadavers, analysis of this "necrobiome" might hold important clues for estimating the time since death, and much more. For example, as measurable changes occur in the soil bacterial community during the decomposition process when a body is buried, analysis of bacteria not indigenous to the soil could be used as an indicator for locating clandestine graves. So far, results from model studies—not conducted on human remains—are promising, showing that the microbial clock that ticks in a decomposing body can be fine-tuned by characterizing microbial succession after death, ultimately permitting investigators to estimate post-mortem intervals [8].

As the requirements for personal recognition become more important, biometrics finds itself at an intriguing intersection of a range of rapidly advancing disciplines. With biometric technologies creeping further into everyday life, there will be a growing impact on society, security and privacy, as well as the ethical discussions that those impacts will entail.

References

1. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Process Mag* 32: 20 – 30
2. Riera A, Dunne S, Cester I, Ruffini G (2012) Electrophysiological biometrics: opportunities and risks. In *Second Generation Biometrics: The Ethical, Legal and Social Context*, Mordini E, Tzovaras D (eds), pp 149 – 176. Dordrecht, Germany: Springer
3. Jonas M, Solangasenathirajan S, Hett D (2014) Patient identification, a review of the use of biometrics in the ICU. In *Annual Update in Intensive Care and Emergency Medicine 2014*, Vincent J-L (ed), pp 679 – 688. Cham, Switzerland: Springer
4. Fierer N, Lauber CL, Zhou N, McDonald D, Costello EK, Knight R (2010) Forensic identification using skin bacterial communities. *Proc Natl Acad Sci USA* 107: 6477 – 6481
5. Lax S, Hampton-Marcell JT, Gibbons SM, Barguil Colares G, Smith D, Eisen JA, Gilbert JA (2015) Forensic analysis of the microbiome of phones and shoes. *Microbiome* 3: 21
6. Franzosa EA, Huang K, Meadow JF, Gevers D, Lemon KP, Bohannan BJ, Huttenhower C (2015) Identifying personal microbiomes using metagenomic codes. *Proc Natl Acad Sci USA* 112: E2930 – E2938
7. Tridico SR, Murray DC, Addison J, Kirkbride KP, Bunce M (2014) Metagenomic analyses of bacteria on human hairs: a qualitative assessment for applications in forensic science. *Investig Genet* 5: 16
8. Metcalf JL, Wegener Parfrey L, Gonzalez A, Lauber CL, Knights D, Ackermann G, Humphrey GC, Gebert MJ, Van Treuren W, Berg-Lyons D *et al* (2013) A microbial clock provides an accurate estimate of the postmortem interval in a mouse model system. *eLife* 2: e01104
9. Comandini O, Cabras S, Marini E (2015) Birth registration and child undernutrition in sub-Saharan Africa. *Public Health Nutr* doi:10.1017/S136898001500333X
10. Horvath S (2013) DNA methylation age of human tissues and cell types. *Genome Biol* 14: R115