WIKIPEDIA

Biometrics

Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication)[note 1] is used in computer science as a form of identification and access control.[1][2] It is also used to identify individuals in groups that are under surveillance.

At Walt Disney World in Lake Buena Vista, Florida, biometric measurements are taken from the fingers of guests to ensure that a ticket is used by the same person from day to day

Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals.[3] Biometric identifiers are often categorized as physiological versus behavioral characteristics.[4] Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait,[5] and voice.[note 2] Some researchers have coined the term behaviometrics to describe the latter class of biometrics.[6]

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number.[3] Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.[3][7]

Contents

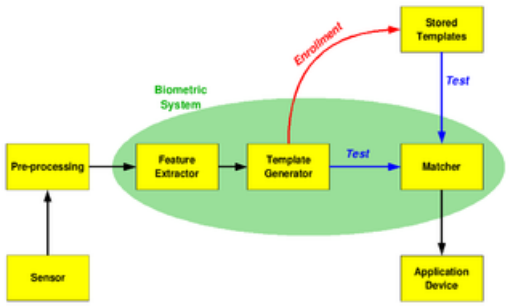
Biometric functionality

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain *et al.* (1999)[8] identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).
- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security.[9] No single biometric will meet all the requirements of every possible application.[8]

The block diagram illustrates the two basic modes of a biometric system.[4] First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person.[10] In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.[note 3] 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".[4]



Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be".[4] The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called *enrollment*. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a *template*. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the filesize and to protect the identity of the enrollee.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.[10] In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

Multimodal biometric system

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems.[11] For instance iris recognition systems can be compromised by aging irises[12] and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).[13][14]

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at different stages of a recognition system. In case of feature level fusion, the data itself or the features extracted from multiple biometrics are fused. Matching-score level fusion consolidates the scores generated by multiple classifiers pertaining to different modalities. Finally, in case of decision level fusion the final results of multiple classifiers are combined via techniques such as majority voting. Feature level fusion is believed to be more effective than the other levels of fusion because the feature set contains richer information about the input biometric data than the matching score or the output decision of a classifier. Therefore, fusion at the feature level is expected to provide better recognition results.[11]

Spoof attacks consist in submitting fake biometric traits to biometric systems, and are a major threat that can curtail their security. Multi-modal biometric systems are commonly believed to be intrinsically more robust to spoof attacks, but recent studies[15] have shown that they can be evaded by spoofing even a single biometric trait.

Performance

The following are used as performance metrics for biometric systems:[16]

- **False match rate** (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.[10]
- **False non-match rate** (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.
- **Receiver operating characteristic** or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- **Equal error rate** or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- **Failure to enroll rate** (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
- **Failure to capture rate** (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- **Template capacity**: the maximum number of sets of data that can be stored in the system.

History of biometrics

An early cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina. The History of Fingerprints (http://onin.com/fp/fphistory.html). Josh Ellenbogen and Nitzan Lebovic argued that Biometrics is originated in the identificatory systems of criminal activity developed by Alphonse Bertillon (1853–1914) and developed by Francis Galton's theory of fingerprints and physiognomy.[17] According to Lebovic, Galton's work "led to the application of mathematical models to fingerprints, phrenology, and facial characteristics", as part of "absolute identification" and "a key to both inclusion and exclusion" of populations.[18] Accordingly, "the biometric system is the absolute political weapon of our era" and a form of "soft control".[19] The theoretician David Lyon showed that during the past two decades biometric systems have penetrated the civilian market, and blurred the lines between governmental forms of control and private corporate control.[20] Kelly A. Gates identified 9/11 as the turning point for the cultural language of our present: "in the language of cultural studies, the aftermath of 9/11 was a moment of articulation, where objects or events that have no necessary connection come together and a new discourse formation is established: automated facial recognition as a homeland security technology." Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York, 2011), p. 100.

Adaptive biometric systems

Adaptive biometric systems aim to auto-update the templates or model to the intra-class variation of the operational data.[21] The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation. Recently, adaptive biometrics have received a significant attention from the research community. This research direction is expected to gain momentum because of their key promulgated advantages. First, with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to re-enroll or retrain the system from scratch in order to cope with the changing environment. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For mis-classification error (false acceptance) by the biometric system, cause adaptation using impostor sample.

However, continuous research efforts are directed to resolve the open issues associated to the field of adaptive biometrics. More information about adaptive biometric systems can be found in the critical review by Rattani *et al.*

Recent advances in emerging biometrics

In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have emerged.[22][23] The research group at University of Kent led by Ramaswamy Palaniappan (http://sites.google.com/site/rpalanisenthi/) has shown that people have certain distinct brain and heart patterns that are specific for each individual. The advantage of such 'futuristic' technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time. This new generation of biometrical systems is called biometrics of intent (http://hir.harvard.edu/behavioral-profiling-politics-intent/) and it aims to scan *intent*. The technology will analyze physiological features such as eye movement, body temperature, breathing etc. and predict dangerous behaviour or hostile intent before it materializes into action.

On the portability side of biometric products, more and more vendors are embracing significantly-miniaturized Biometric Authentication Systems (BAS) thereby driving elaborate cost savings especially for large scale deployments.

Operator signatures

An operator signature is a biometric mode where the manner in which a person using a device or complex system is recorded as a verification template.[24] One potential use for this type of biometric signature is to distinguish among remote users of telerobotic surgery systems that utilize public networks for communication.[24]

Proposed requirement for certain public networks

John Michael (Mike) McConnell, a former vice admiral in the United States Navy, a former Director of U.S. National Intelligence, and Senior Vice President of Booz Allen Hamilton promoted the development of a future capability to require biometric authentication to access certain public networks in his keynote speech[25] at the 2009 Biometric Consortium Conference (https://web.archive.org/web/20100212102854/http://www.biometrics.org/bc2009/).

A basic premise in the above proposal is that the person that has uniquely authenticated themselves using biometrics with the computer is in fact also the agent performing potentially malicious actions from that computer. However, if control of the computer has been subverted, for example in which the computer is part of a botnet controlled by a hacker, then knowledge of the identity of the user at the terminal does not materially improve network security or aid law enforcement activities.[26]

Recently, another approach to biometric security was developed, this method scans the entire body of prospects to guarantee a better identification of this prospect. This method is not globally accepted because it is very complex and prospects are concerned about their privacy.

Issues and concerns

Human dignity

Biometrics have been considered also instrumental to the development of state authority[27] (to put it in Foucauldian terms, of discipline and biopower[28]). By turning the human subject into a collection of biometric parameters, biometrics would dehumanize the person,[29] infringe bodily integrity, and, ultimately, offend human dignity.[30]

In a well-known case,[31] Italian philosopher Giorgio Agamben refused to enter the United States in protest at the United States Visitor and Immigrant Status Indicator (US-VISIT) program's requirement for visitors to be fingerprinted and photographed. Agamben argued that gathering of biometric data is a form of bio-political tattooing, akin to the tattooing of Jews during the Holocaust. According to Agamben, biometrics turn the human persona into a bare body. Agamben refers to the two words used by Ancient Greeks for indicating "life", *zoe*, which is the life common to animals and humans, just life; and *bios*, which is life in the human context, with meanings and purposes. Agamben envisages the reduction to bare bodies for the whole humanity.[32] For him, a new bio-political relationship between citizens and the state is turning citizens into pure biological life (*zoe*) depriving them from their humanity (*bios*); and biometrics would herald this new world.

In Dark Matters: On the Surveillance of Blackness (https://www.dukeupress.edu/dark-matters), surveillance scholar Simone Browne formulates a similar critique as Agamben, citing a recent study[33] relating to biometrics R&D that found that the gender classification system being researched "is inclined to classify Africans as males and Mongoloids as females."[33] Consequently, Browne argues that the conception of an objective biometric technology is difficult if such systems are subjectively designed, and are vulnerable to cause errors as described in the study above. The stark expansion of biometric technologies in both the public and private sector magnifies this concern. The increasing commodification of biometrics by the private sector adds to this danger of loss of human value. Indeed, corporations value the biometric characteristics more than the individuals value them.[34] Browne goes on to suggest that modern society should incorporate a "biometric consciousness" that "entails informed public debate around these

technologies and their application, and accountability by the state and the private sector, where the ownership of and access to one's own body data and other intellectual property that is generated from one's body data must be understood as a right."[35]

Other scholars[36] have emphasized, however, that the globalized world is confronted with a huge mass of people with weak or absent civil identities. Most developing countries have weak and unreliable documents and the poorer people in these countries do not have even those unreliable documents.[37] Without certified personal identities, there is no certainty of right, no civil liberty.[38] One can claim her rights, including the right to refuse to be identified, only if she is an identifiable subject, if she has a public identity. In such a sense, biometrics could play a pivotal role in supporting and promoting respect for human dignity and fundamental rights.[39]

The biometrics of intent poses further risks. In his paper (http://hir.harvard.edu/behavioral-profiling-politics-intent/) in Harvard International Review, Prof Nayef Al-Rodhan cautions about the high risks of miscalculations, wrongful accusations and infringements of civil liberties. Critics in the US have also signalled a conflict with the 4th Amendment.

Privacy and discrimination

It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. For example, most biometric features could disclose physiological and/or pathological medical conditions (e.g., some fingerprint patterns are related to chromosomal diseases, iris patterns could reveal genetic sex, hand vein patterns could reveal vascular diseases, most behavioral biometrics could reveal neurological diseases, etc.).[40] Moreover, second generation biometrics, notably behavioral and electro-physiologic biometrics (e.g., based on electrocardiography, electroencephalography, electromyography), could be also used for emotion detection.[41]

There are three categories of privacy concerns:[42]

1. Unintended functional scope: The authentication goes further than authentication, such as finding a tumor.
2. Unintended application scope: The authentication process correctly identifies the subject when the subject did not wish to be identified.
3. Covert identification: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd.

Danger to owners of secured items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.[43]

Cancelable biometrics

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. If the electronic biometric identifier is stolen, it is nearly impossible to change a biometric feature. This renders the person’s biometric feature questionable for future use in authentication, such as the case with the hacking of security-clearance-related background information from the Office of Personnel Management (OPM) in the United States.

Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics to create a more secure system. It was first proposed by Ratha *et al.*[44]

"Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancelable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancelable biometrics is one of the major categories for biometric template protection purpose besides biometric cryptosystem."[45] In biometric cryptosystem, "the error-correcting coding techniques are employed to handle intraclass variations."[46] This ensures a high level of security but has limitations such as specific input format of only small intraclass variations.

Several methods for generating new exclusive biometrics have been proposed. The first fingerprint-based cancelable biometric system was designed and developed by Tulyakov *et al.*[47] Essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh *et al.*[48] and Savvides *et al.*,[49] whereas other methods, such as Dabbah *et al.*,[50] take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies

Soft biometrics

Soft biometrics traits are physical, behavioral or adhered human characteristics that have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). They are used to complement the identity information provided by the primary biometric identifiers . Although soft biometric characteristics lack the distinctiveness and permanence to recognize an individual uniquely and reliably, and can be easily faked, they provide some evidence about the users identity that could be beneficial. In other words, despite the fact they are unable to individualize a subject, they are effective in distinguishing between people. Combinations of personal attributes like gender, race, eye color, height and other visible identification marks can be used to improve the performance of traditional biometric systems.[51] Most soft biometrics can be easily collected and are actually collected during enrollment.Two main ethical issues are raised by soft biometrics.[52] First, some of soft biometric traits are strongly cultural based; e.g., skin colors for determining ethnicity risk to support racist approaches, biometric sex recognition at the best recognizes gender from tertiary sexual characters, being unable to determine genetic and chromosomal sexes; soft biometrics for aging recognition are often deeply influenced by ageist stereotypes, etc. Second, soft biometrics have strong potential for categorizing and profiling people, so risking of supporting processes of stigmatization and exclusion.[53]

International sharing of biometric data

Many countries, including the United States, are planning to share biometric data with other nations.

In testimony before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification" in 2009, Kathleen Kraninger and Robert A Mocny[54] commented on international cooperation and collaboration with respect to biometric data, as follows:

> *“To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provide a new way to bring terrorists’ true identities to light, stripping them of their greatest advantage—remaining unknown.”*

According to an article written in 2009 by S. Magnuson in the National Defense Magazine entitled "Defense Department Under Pressure to Share Biometric Data" the United States has bilateral agreements with other nations aimed at sharing biometric data.[55] To quote that article:

> *“Miller [a consultant to the Office of Homeland Defense and America's security affairs] said the United States has bilateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement.”*

Likelihood of full governmental disclosure

Certain members of the civilian community are worried about how biometric data is used but full disclosure may not be forthcoming. In particular, the Unclassified Report of the United States' Defense Science Board Task Force on Defense Biometrics states that it is wise to protect, and sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities.[56] This also potentially applies to Biometrics. It goes on to say that this is a classic feature of intelligence and military operations. In short, the goal is to preserve the security of 'sources and methods'.

Countries applying biometrics

Countries using biometrics include Australia, Brazil, Canada, Cyprus, Greece, China, Gambia, Germany, India, Iraq, Israel, Italy, Malaysia, Netherlands, New Zealand, Nigeria, Norway, Pakistan, South Africa, Saudi Arabia, Tanzania,[57] Ukraine, United Arab Emirates, United Kingdom, United States and Venezuela.

Among low to middle income countries, roughly 1.2 billion people have already received identification through a biometric identification program.[58]

There are also numerous countries applying biometrics for voter registration and similar electoral purposes. According to the International IDEA’s ICTs in Elections Database,[59] some of the countries using (2017) Biometric Voter Registration (BVR) are Armenia, Angola, Bangladesh, Bhutan, Bolivia, Brazil, Burkina Faso, Cambodia, Cameroon, Chad, Colombia, Comoros, Congo (Democratic Republic of), Costa Rica, Ivory Coast, Dominican Republic, Fiji, Gambia, Ghana, Guatemala, India, Iraq, Kenya, Lesotho, Liberia, Malawi, Mali, Mauritania, Mexico, Morocco, Mozambique, Namibia, Nepal, Nicaragua, Nigeria, Panama, Peru, The Philippines, Senegal, Sierra Leone, Solomon Islands, Somaliland, Swaziland, Tanzania, Uganda, Uruguay, Venezuela, Yemen, Zambia, and Zimbabwe.[60][61][62]

India's national ID program

India's national ID program called Aadhaar is the largest biometric database in the world. It is a biometrics-based digital identity assigned for a person's lifetime, verifiable online instantly in the public domain, at any time, from anywhere, in a paperless way. It is designed to enable government agencies to deliver a retail public service, securely based on biometric data (fingerprint, iris scan and face photo), along with demographic data (name, age, gender, address, parent/spouse name, mobile phone number) of a person. The data is transmitted in encrypted form over the internet for authentication, aiming to free it from the limitations of physical presence of a person at a given place.

About 550 million residents have been enrolled and assigned 480 million Aadhaar national identification numbers as of 7 November 2013.[63] It aims to cover the entire population of 1.2 billion in a few years.[64]

See also

- Aadhaar
- Access control
- AFIS
- AssureSign
- BioAPI
- Biometric passport
- Biometric voter registration
- Biometrics in schools
- BioSlimDisk
- Facial recognition system
- Fingerprint recognition
- Fuzzy extractor
- Gait analysis
- Government database
- Hand geometry
- Handwritten biometric recognition
- Identity Cards Act 2006
- International Identity Federation
- Iris recognition
- Keystroke dynamics
- Private biometrics
- Retinal scan
- Signature recognition
- Smart city
- Speaker recognition
- Surveillance
- Vein matching
- Voice analysis

Notes

1. As Jain and Ross (2008, footnote 4 on page 1) point out, "the term *biometric authentication* is perhaps more appropriate than *biometrics* since the latter has been historically used in the field of statistics to refer to the analysis of biological (particularly medical) data [36]" (wikilink added to original quote).
2. Strictly speaking, *voice* is also a physiological trait because every person has a different vocal tract, but voice recognition is classed as behavioural as it is affected by a person's mood. Biometric voice recognition is separate and distinct from speech recognition with the latter being concerned with accurate understanding of speech content rather than identification or recognition of the person speaking.
3. Systems can be designed to use a template stored on media like an e-Passport or smart card, rather than a remote database.

References

1. "Biometrics: Overview" (https://web.archive.org/web/20120107071003/http://biometrics.cse.msu.edu/info.html). Biometrics.cse.msu.edu. 6 September 2007. Archived from the original (http://biometrics.cse.msu.edu/info.html) on 7 January 2012. Retrieved 2012-06-10.
2. "What is Biometrics?" (http://biometrics.cse.msu.edu/info/index.html). *Biometrics Research Group*. Michigan State University. Retrieved 10 November 2017.

3. Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification" (http://helios.et.put.poznan.pl/~dgajew/download/PUT/SEMESTR_10/IO/FACE_RECOGNITION/BiometricsACM.pdf). *Communications of the ACM*, 43(2), p. 91–98. doi:10.1145/328236.328110 (https://doi.org/10.1145%2F328236.328110)
4. Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. *Handbook of Biometrics* (https://www.springer.com/computer/image+processing/book/978-1-4419-4375-0). Springer. pp. 1–22. ISBN 978-0-387-71040-2.
5. Damaševičius, R.; Maskeliūnas, R.; Venčkauskas, A.; Woźniak, M. Smartphone User Identity Verification Using Gait Characteristics (https://www.researchgate.net/publication/308753210_Smartphone_User_Identity_Verification_Using_Gait_Characteristics), Symmetry 2016, 8, 100.
6. "Biometrics for Secure Authentication" (https://web.archive.org/web/20120325163848/http://biosecure.it-sudparis.eu/public_html/biosecure1/public_docs_deli/BioSecure_Deliverable_D10-2-3_b3.pdf) (PDF). Archived from the original (http://biosecure.it-sudparis.eu/public_html/biosecure1/public_docs_deli/BioSecure_Deliverable_D10-2-3_b3.pdf) (PDF) on 25 March 2012. Retrieved 29 July 2012.
7. Weaver, A. C. (2006). "Biometric Authentication". *Computer*, 39 (2), p. 96–97. DOI 10.1109/MC.2006.47
8. Jain, A. K.; Bolle, R.; Pankanti, S., eds. (1999). *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.
9. Bleicher, Paul (2005). "Biometrics comes of age: despite accuracy and security concerns, biometrics are gaining in popularity". *Applied Clinical Trials*.
10. Sahoo, SoyujKumar; Mahadeva Prasanna, SR (1 January 2012). Mahadeva Prasanna, SR, Choubisa, Tarun. "Multimodal Biometric Person Authentication : A Review" (https://web.archive.org/web/20130917130654/http://tr.ietejournals.org/text.asp?2012%2F29%2F1%2F54%2F93139). *IETE Technical Review*. **29** (1): 54. doi:10.4103/0256-4602.93139 (//doi.org/10.4103%2F0256-4602.93139). Archived from the original (http://tr.ietejournals.org/text.asp?2012/29/1/54/93139) on 17 September 2013. Retrieved 23 February 2012. Missing `|last2=` in Authors list (help)
11. M. Haghighat, M. Abdel-Mottaleb, & W. Alhalabi (2016). Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition (https://dx.doi.org/10.1109/TIFS.2016.2569061). IEEE Transactions on Information Forensics and Security, 11(9), 1984–1996.
12. "Questions Raised About Iris Recognition Systems" (http://sciencedaily.com/releases/2012/07/120712141938.htm). *Science Daily*. 12 July 2012.
13. Saylor, Michael (2012). *The Mobile Wave: How Mobile Intelligence Will Change Everything*. Perseus Books/Vanguard Press. p. 99.
14. Bill Flook (3 October 2013). "This is the 'biometric war' Michael Saylor was talking about" (http://www.bizjournals.com/washington/blog/techflash/2013/10/this-is-the-biometric-war-michael.html). *Washington Business Journal*.
15. Zahid Akhtar, "Security of Multimodal Biometric Systems against Spoof Attacks" (http://pralab.diee.unica.it/sites/default/files/Akhtar_PhD2012.pdf), Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6 March 2012.
16. "Characteristics of Biometric Systems" (https://web.archive.org/web/20081017165633/http://www.ccert.edu.cn/education/cissp/hism/039-041.html). Cernet. Archived from the original (http://www.ccert.edu.cn/education/cissp/hism/039-041.html) on 17 October 2008.
17. Josh Ellenbogen, *Reasoned and Unreasoned Images: The Photography of Bertillon, Galton, and Marey* (University Park, PA, 2012)
18. Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in *Critical Inquiry* 41:4 (Summer, 2015), 841–868.
19. Nitzan Lebovic, "Biometrics or the Power of the Radical Center", in *Critical Inquiry* 41:4 (Summer, 2015), p. 853.
20. David Lyon, *Surveillance Society: Monitoring Everyday Life* (Philadelphia, 2001).
21. A. Rattani, "Adaptive Biometric System based on Template Update Procedures", PhD thesis, University of Cagliari, Italy, 2010
22. [R. Palaniappan, "Electroencephalogram signals from imagined activities: A novel biometric identifier for a small population", published in E. Corchado *et al.* (eds): *Intelligent Data Engineering and Automated Learning – IDEAL 2006*, Lecture Notes in Computer Science, vol. 4224, pp. 604–611, Springer-Verlag, Berlin Heidelberg, 2006. DOI:10.1007/11875581_73]
23. R. Palaniappan, and S. M. Krishnan, "Identifying individuals using ECG signals", *Proceedings of International Conference on Signal Processing and Communications*, Bangalore, India, pp. 569–572, 11–14 December 2004. DOI:10.1109/SPCOM.2004.1458524]
24. Langston, Jennifer (8 May 2015). "Researchers hack Teleoperated Surgical Robot to Reveal Security Flaws" (http://www.scientificcomputing.com/news/2015/05/researchers-hack-teleoperated-surgical-robot-reveal-security-flaws). *Scientific Computing*. New Jersey. Retrieved 17 May 2015.
25. McConnell, Mike (January 2009). *KeyNote Address* (http://www.boozallen.com/consulting-services/services_article/42861927). Biometric Consortium Conference. Tampa Convention Center, Tampa, Florida. Retrieved 20 February 2010.

26. Schneier, Bruce. "The Internet: Anonymous Forever" (http://www.schneier.com/essay-308.html). Retrieved 1 October 2011.
27. Breckenridge K. (2005). "The Biometric State: The Promise and Peril of Digital Government in the New South Africa". *Journal of Southern African Studies*, 31:2, 267–82
28. Epstein C. (2007), "Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders". *International Political Sociology*, 1:2, 149–64
29. Pugliese J. (2010), *Biometrics: Bodies, Technologies, Biopolitics.* New York: Routledge
30. French National Consultative Ethics Committee for Health and Life Sciences (2007), Opinion N° 98, "Biometrics, identifying data and human rights" (http://www.ccne-ethique.fr/en/publications/biometrics-identifying-data-and-human-rights#.VenJ87TDU5E)
31. Agamben, G. (2008). "No to bio-political tattooing". *Communication and Critical/Cultural Studies*, 5(2), 201–202. Reproduced from Le Monde (10 January 2004).
32. Agamben G.(1998), *Homo Sacer: Sovereign Power and Bare Life*. Trans. Daniel Heller-Roazen. Stanford: Stanford University Press
33. Gao, Wei; Ai, Haizhou. *Face Gender Classification on Consumer Images in a Multiethnic Environment* (https://www.researchgate.net/publication/221383488_Face_Gender_Classification_on_Consumer_Images_in_a_Multiethnic_Environment). pp. 169–178. doi:10.1007/978-3-642-01793-3_18 (//doi.org/10.1007%2F978-3-642-01793-3_18).
34. Walker, Elizabeth (2015). "Biometric Boom: How the private sector Commodifies Human characteristics" (https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=25+Fordham+Intell.+Prop.+Media+%26+Ent.+L.J.+831&srctype=smi&srcid=3B15&key=a4b55d68b2513a0c985a62bb9064501d). *Fordham Intellectual Property, Media & Entertainment Law Journal*.
35. Browne, Simone (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press. p. 116.
36. Mordini, E; Massari, S. (2008), "Body, Biometrics and Identity" *Bioethics*, 22, 9:488
37. UNICEF, Birth Registration (http://www.unicef.org/protection/57929_58010.html)
38. Dahan M., Gelb A. (2015) "The Role of Identification in the Post-2015 Development Agenda" (http://documents.worldbank.org/curated/en/2015/07/24849193/role-identification-post-2015-development-agenda) – World Bank Working Paper No. 98294 08/2015;
39. Mordini E, Rebera A (2011) "No Identification Without Representation: Constraints on the Use of Biometric Identification Systems". *Review of Policy Research*, 29, 1: 5–20
40. Mordini E, Ashton H,(2012), "The Transparent Body – Medical Information, Physical Privacy and Respect for Body Integrity", in Mordini E, Tzovaras D (eds), *Second Generation Biometrics: the Ethical and Social Context*. Springer-Verlag: Berlin
41. Mordini E, Tzovaras D,(2012), *Second Generation Biometrics: the Ethical and Social Context*. Springer-Verlag: Berlin
42. Pfleeger, Charles; Pfleeger, Shari (2007). *Security in Computing* (4th ed.). Boston: Pearson Education. p. 220. ISBN 978-0-13-239077-4.
43. Kent, Jonathan (31 March 2005). "Malaysia car thieves steal finger" (http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm). *BBC Online*. Kuala Lumpur. Retrieved 11 December 2010.
44. N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, vol. 40, pp. 614–634, 2001.
45. "Cancelable biometrics – Scholarpedia" (http://www.scholarpedia.org/article/Cancelable_biometrics). *www.scholarpedia.org*. Retrieved 2015-11-05.
46. Feng, Y. C.; Yuen, P. C.; Jain, A. K. (2010-03-01). "A Hybrid Approach for Generating Secure and Discriminating Face Template" (http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5371831). *IEEE Transactions on Information Forensics and Security*. **5** (1): 103–117. doi:10.1109/TIFS.2009.2038760 (//doi.org/10.1109%2FTIFS.2009.2038760). ISSN 1556-6013 (//www.worldcat.org/issn/1556-6013).
47. S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric Hash Functions for Fingerprint Minutiae", *Proc. Int'l Workshop Pattern Recognition for Crime Prevention, Security, and Surveillance*, pp. 30–38, 2005
48. A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs", *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 28, pp. 1892–1901, 2006.
49. M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "'Corefaces' – Robust Shift-Invariant PCA based Correlation Filter for Illumination Tolerant Face Recognition", presented at IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), 2004.
50. M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition", presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.
51. Ratha, N. K., J. H. Connell, and R. M. Bolle. (2001). "Enhancing security and privacy in biometrics based authentication systems". *IBM Systems Journal* 40(3): 614–634.

52. Mordini E, Ashton H (2012), "The Transparent Body – Medical Information, Physical Privacy and Respect for Body Integrity'". In Mordini E, Tzovaras D (eds), *Second Generation Biometrics: the Ethical and Social Context*. Berlin: Springer-Verlag (https://www.springer.com/us/book/9789400738911), 2057–83
53. Mordini E (2013) *Biometrics*. In Henk A. M. J. ten Have, Bert Gordijn (eds) *Handbook of Global Bioethics* Berlin: Springer, 341–356
54. "Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger, Screening Coordination, and Director Robert A. Mocny, US-VISIT, National Protection and Programs Directorate, before the House Appropriations Committee, Subcommittee on Homeland Security, 'Biometric Identification' " (https://www.dhs.gov/ynews/testimony/testimony_1237563811984.shtm). US Department of Homeland Security. March 2009. Retrieved 20 February 2010.
55. Magnuson, S (January 2009). "Defense department under pressure to share biometric data" (http://www.nationaldefensemagazine.org/ARCHIVE/2009/JANUARY/Pages/DefenseDepartmentUnderPressuretoShareBiometricData.aspx). *NationalDefenseMagazine.org*. Retrieved 20 February 2010.
56. Defense Science Board (DSB) (September 2006). "On Defense Biometrics" (http://www.acq.osd.mil/dsb/reports/ADA465930.pdf) (PDF). Unclassified Report of the Defense Science Board Task Force. Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics: 84. Retrieved 20 February 2010. |chapter= ignored (help)
57. web article dated 24 February 2015 (http://www.planetbiometrics.com/article-details/i/2740/) in *planet biometrics* entitled "Biometric voter registration launches in Tanzania" accessed 21 January 2016
58. Gelb, Alan; Julia Clark (2013). *Identification for Development: The Biometrics Revolution* (http://www.cgdev.org/content/publications/detail/1426862/). The Center for Global Development.
59. "ICTs in Elections Database | International IDEA" (http://www.idea.int/data-tools/data/icts-elections). *www.idea.int*. Retrieved 2017-07-19.
60. "If the EMB uses technology to collect voter registration data, is biometric data captured and used during registration? | International IDEA" (http://www.idea.int/data-tools/question-view/738). *www.idea.int*. Retrieved 2017-07-19.
61. "The Biometric ID Grid: A Country-by-Country Guide : The Corbett Report" (https://www.corbettreport.com/the-biometric-id-grid-a-country-by-country-guide/). *www.corbettreport.com*. Retrieved 2017-07-19.
62. "Biometric Voter Registration and Voter Identification —" (http://aceproject.org/electoral-advice/archive/questions/replies/916219364). *aceproject.org*. Retrieved 2017-07-19.
63. "Aadhaar scheme does not violate fundamental rights, says UIDAI" (http://zeenews.india.com/news/nation/aadhaar-scheme-does-not-violate-fundamental-rights-says-uidai_884850.html). Zee News. October 22, 2013.
64. "Building a Biometric National ID: Lessons for Developing Countries from India's Universal ID Program", Alan Gelb and Julia Clark, The Center for Global Development, October 2012, http://www.cgdev.org/doc/full_text/GelbClarkUID/1426583.html

Further reading

- Biometrics Glossary – Glossary of Biometric Terms (http://www.fulcrumbiometrics.com/Articles.asp?ID=268) based on information derived from the National Science and Technology Council (NSTC) Subcommittee on Biometrics. Published by Fulcrum Biometrics, LLC, July 2013
- Biomtrics Institute Privacy Code (https://web.archive.org/web/20070705211205/http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8), September 2006
- Biometric Vulnerability Assessment Framework (http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=48), Published by the Biometrics Institute, 2007–2011
- Delac, K., Grgic, M. (2004). A Survey of Biometric Recognition Methods (http://www.vcl.fer.hr/papers_pdf/A%20Survey%20of%20Biometric%20Recognition%20Methods.pdf).
- Biometric Technology Application Manual (http://www.biometricscatalog.org/ApprovedDocuments/evaluation/ceeb3a01-801e-4d2c-b447-bc79d13d2d62.pdf). Published by the National Biometric Security Project (NBSP), the BTAM is a comprehensive reference manual on biometric technology applications.
- "Fingerprints Pay For School Lunch". (2001). Retrieved 2008-03-02. [1] (http://www.cbsnews.com/stories/2001/01/24/national/main266789.shtml)
- "Germany to phase-in biometric passports from November 2005". (2005). E-Government News. Retrieved 2006-06-11. [2] (http://ec.europa.eu/idabc/en/document/4338/194)
- Oezcan, V. (2003). "Germany Weighs Biometric Registration Options for Visa Applicants", Humboldt University Berlin. Retrieved 2006-06-11.
- Ulrich Hottelet: Hidden champion – Biometrics between boom and big brother (https://web.archive.org/web/20120401144536/http://www.german-times.com/index.php?option=com_content&task=view&id=91&Itemid=12), German Times (https://web.archive.org/web/20111213222947/http://www.german-times.com/), January 2007.
- Paul Benjamin Lowry, Jackson Stephens, Aaron Moyes, Sean Wilson, and Mark Mitchell (2005). "Biometrics, a critical consideration in information security management", in Margherita Pagani, ed. *Encyclopedia of Multimedia Technology and Networks*, Idea Group Inc., pp. 69–75.

External links

- The dictionary definition of biometrics at Wiktionary