Biometrics and its use: Viewpoint

Dipankar Dasgupta*

Department of Computer Science, The University of Memphis, USA

*****Corresponding author:** Dipankar Dasgupta, Department of Computer Science, The University of Memphis, Memphis, TN 38152, USA;
Email: dasgupta@memphis.edu

Opinion

Biometric is a combination of two Greek words, namely Bio (life) and Metric (to measure). Biometrics has been used for many purposes including identification of human, in particular, recognition of an individual through physiological and behavioral traits or attributes.

Physical biometrics

It includes physical characteristics of human such as the appearance, body structures, and other aspects. Computational algorithms are used to extract various biometric characteristics such as 2D ridge-valley maps in fingerprints, face image, audio recordings of the voice, near-infrared images of the iris, video of gait motion, etc.

Behavioral biometrics

Are those which are related to the behavior (in certain aspects) of an individual. Hence, such biometrics verification can prevent a person from authenticating/accessing if his behavior is different from the stored behavioral pattern/profile. The examples of this type of biometrics are-voice, keystroke analysis, mouse dynamics, signature, etc.

While biometrics applications are widespread [1-3], these mainly fall in three different categories: law enforcement, governments, and commercial.

Law enforcement

Police departments use fingerprint identification systems to identify criminals or fugitives; forensic applications also use biometric to expedite or validate the investigation process.

Governments

Different branches of the government or federal agencies use biometrics to identify citizens and foreign nationals. Some of the examples are driving license, national ID card, social security card, border control, passport, visitor-visa program, etc.

Business

Commercial sectors increasingly using biometrics to secure their authentication process, and verified transactions. Some example applications include ATM booths, credit cards, facility access, network login, online service and data access. Healthcare and medical science extensively use various forms of biometrics (external and internal) for blood transfusion, organ matching, identification of biological parents, ancestry, etc.

Different biometrics is used primarily in two spaces: real-world physical verification of human and increasingly used for cyber-identity, authentication and authorization of legitimate access to the computing systems and services. In cyber space, identity verification is always challenging, since in many instances, it is not possible to know who is on the other side of a virtual communication. Specifically, it is difficult to verify legitimate user identity (from Spoofed) with cent percent accuracy in both biometric or none biometric authentication processes. To alleviate the situation, multi-factor authentication is becoming essential for important transactions and services on the Internet [4,5].

Similarly, in our real-world, physical biometric verifications are also facing major challenges due to many reasons such as:

I.   Physical biometrics may change over time due to natural, accidental or advertent changes (e.g. in fingerprints)

II.   Some type of physical biometrics such as appearances may change because of fashion or makeover (e.g. color contact lenses, hair color and cosmetics, etc.)

III.   Physical biometrics may get changed due to surgery, skin drafting, nose implant, face lifting, anti-aging skin repair, amputation, botox, etc.

IV.   With the development of sophisticated skin-like facemasks for use in movies and other recreational purposes, such masks can also be used to defeat the face or fingerprint recognition system for illegal access

Due to the above-mentioned factors and technological advancements of appearance and shape shifting, it is quite difficult to accurately identify human by physical attributes as these can be easily altered now.

Furthermore, if we consider the above-mentioned factors as external biometrics, internal biometrics is also emerging for human identity verification. Forensic science is now going deeper inside human body to identify a person using internal characteristics, such as body pressure, blood type, pulse rate, assuming that these are inert and hard to change, though these require intrusive measurements and can undergo changes during stress and sickness [3]. In addition, organ transplant, blood transfusion, immunotherapy and hormone therapy may influence the internal biometrics of the body; also recently reported that 7% percent of DNA has changed to an astronaut after spending a year-long in the space shuttle [6,7].

Searching for true identity

If the purpose of biometric use are to check the human behavior (good, bad, harmful, harmless, authentic, non-authentic facts) then the focus should be on the brain, which is irreplaceable and controls human behavior [6]. Accordingly, human identity is reflected through expressions of human mind that can be seen by how the person behaves in different contexts and situations. If we can precisely capture, the manifestation of brain activities or mind change (if it is the expression of brain function), we may reach a more accurate representation of a human's identification. A mind reader can interpret the state of mind from the changes in brain's electrochemical signals and can determine the true identity of a human and his actions.

Researchers developed a biometric Brainprint system [4] to identify individuals with 100% accuracy measuring their EEG signals that represent their brain activities. In general, every individual's brain react in a different manner to a same set of images. Hence, the brain activities through EEG signals are able to identify every brainprint (in other words, individuals) with absolute accuracy. A brainprint of an individual is recorded by having a user look at an image while hooked up to an electroencephalograph that captures his/her brain activity in response to the stimulus. This step basically the registration phase for the biometric modality. During authentication phase, the user's identity would be verified by exposing her to the stimulus again, recording her current response and using different pattern recognition algorithms to compare the registered EEG data with authentication EEG data. This biometric based system has the great potential to be deployed in high security based system, where 100% accuracy is an absolute need.

Use of biometric beyond identity science

Biometric analytics refers to the discovery of useful patterns within biometric signals to ascertain potentially interesting information about a person other than identity, such as emotional state or longevity [6]. For example, voice recognition is used to better understand a speaker's emotional state, honesty, concentration level, and other attributes to define a person's character and personality. Monitoring audience facial reactions such as detecting smiles, confusion, boredom or distress while watching video can help editing movies, or developing higher impact advertising. Also face analytics software, developed to digitize emotion, age estimation in determining longevity which will have implications in the cosmetics and rejuvenation industries. To conclude, with further understanding of how brain works, technological advances may come to help human using augmented artificial brain (robot) in making decisions for or on behalf of them. It will be interesting to envision the type of biometrics to be used in future for human identity.

References

1. Zhang David D (2013) Automated biometrics: Technologies and systems. Springer Science & Business Media, UK, Pp.6.

2. Ruiz Blondet, Maria V, Zhanpeng Jin, Sarah Laszlo (2016) CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification. IEEE Transactions on Information Forensics and Security 11(7): 1618-1629.

3. Ricanek Karl (2013) The Next Biometric Challenge: Medical Alterations. Computer 46: 94-96.

4. Ashbourn Julian (2014) Biometrics: Advanced identity verification: the complete guide. Springer, UK.

5. Dasgupta D, Roy A, Nag Abhijit (2017) Advances in User Authentication. Springer International Publishing, UK.

6. Ricanek Karl (2014) Beyond Recognition: The Promise of Biometric Analytics. IEEE.

7. Raven Benjamin (News reporter) (2018) NASA study reveals 7% percent of DNA has changed to an astronaut after spending a year-long in the space shuttle. US & World News from MLIVE.com).

Your next submission with Juniper Publishers will reach you the below assets
• Quality Editorial service
• Swift Peer Review
• Reprints availability
• E-prints Service
• Manuscript Podcast for convenient understanding
• Global attainment for your research
• Manuscript accessibility in different formats **(Pdf, E-pub, Full Text, Audio)**
• Unceasing customer service
Track the below URL for one-step submission **https://juniperpublishers.com/online-submission.php**