Egyptian Journal of Forensic Sciences

LETTER TO THE EDITOR Open Access

The need for novel biometric-based systems such as tongue identification

Hannan Latif

The term biometrics is derived from two ancient Greek words 'bios' and 'metron,' which mean 'life' and 'measure' respectively. It involves the recognition of humans based on intrinsic physical or behavioral traits that are unique to individuals. Physical characteristics most used as modes of identification include fingerprints, dental records, the iris, and facial recognition amongst others. On the other hand, behavioral characteristics used for identification purposes include voice recognition, handwriting, keystroke patterns, and there is even ongoing research into gait patterns as a form of recognition. However, identifying people via biometrics is never a 100% accurate. There have been a myriad of studies suggesting this very notion. One study concluded that fake fingerprints extracted from paper or even those made from gelatin could potentially 'fool' fingerprint sensors (Matsumoto et al. 2002). This false acceptance, or even false rejection in some cases, is not unique to fingerprints and is seen across several biometrics. Thus, it is imperative to have a multi-modal system that can take in several biometrics at a time to identify a person. This will not only minimize chances of false or missed identifications and fraud but will also enhance the accuracy of correct identifications. Due to its uniqueness between individuals, there is a potential for the tongue to be used in such multi-factorial systems of identification.

Due to the growing need for new ways to identify people, some researchers have looked towards the uniqueness of the tongue and preliminary results suggest that it could be as unique as fingerprints and that tongue prints vary even in identical twins (Musa et al. 2014). The tongue is the only internal organ that can be protruded for inspection and it is well protected in the mouth cavity, making it less prone to being reverse engineered. The shape of the tongue along with the pattern of the ridges on the tongue and its texture are unique to individuals. Furthermore, these characteristics of the tongue are thought to remain stable over time (Liu et al. 2007). All these characteristics of the tongue make it a good candidate as a biometric tool. Jain et al. mentioned various parameters that need to be fulfilled for a trait to be considered a biometric (Jain et al. 2005):

1. Universality: every person should possess the trait.
2. Distinctiveness: each person should be unique for the trait.
3. Permanence: the trait should remain relatively stable over time.
4. Collectability: the trait should be easily measurable.
5. Circumvention: the trait should not be prone to easy forgery or reverse engineering.

The tongue can be deemed a good model as a biometric since it fulfills all these parameters, particularly the one regarding circumvention which is a problem with existing biometrics such as fingerprints. The tongue is less prone to forgery due to its well protected nature and consent is needed for its inspection, which might not be the case for other biometrics such as fingerprints.

One of the main questions regarding this novel mode of identification is how to analyze it for such purposes. A group of researchers has reported a 97.05% accuracy rate in identifying people via their tongue by acquiring images of the patterns on the tongue and comparing pixel intensities of those images (Sivakumar et al. 2018). By taking images of the tongue and converting them into three-dimensional plots of the image's pixels, the researchers were able to obtain unique plots for each tongue that was imaged. Another group of researchers has suggested that the tongue might also exhibit sexual dimorphism, which can aid in identification. The same group of researchers also concluded that using alginate to make impressions of the tongue resulted in a 90% match rate when the alginate impressions

Correspondence: hlatif.work@gmail.com
Associate Member at the Chartered Society of Forensic Sciences, London, UK

were compared with the corresponding photographs (Jeddy et al. 2017).

All biometric-based identification systems essentially operate in the same manner. Firstly, they capture a biometric sample. Then, they tune the sample after digitalizing it and perform feature extraction or data set creation within the system. The final step involves searching and matching the input sample with known samples in the database (a one to many comparisons, which aims to identify the person) and providing a matching score which indicates the similarity between the samples. Alternatively, the input sample can also be compared with only one other sample (a one to one comparison, which verifies the identity of the person) to determine if the input sample and the other sample in question are the same (OECDiLibrary 2004).

However, as stated before, this system of identification is not always accurate. Many studies have reported false acceptance (FAR) and false rejection rates (FRR) of several biometrics. The FAR is a probability that the system incorrectly concludes a match between the input sample and one already in the database (a measure of the percent of incorrect matches from the total). Whereas the FRR is the probability that the system fails to match the input sample with one within the database (a measure of the percent of failed matches from the total). The lower these rates are, the more accurate the identification system is. However, these systems are not a 100% accurate (Conti 2017).

Table 1 shows that a system relying on one biometric for identification is prone to errors. For example, it is interesting to note that for fingerprints, which are regarded as very good primary identifiers, systems relying on them could make about 1 false identification (the FAR) for every 1000 fingerprints that are used for identification purposes. Hence, reliance on more than one biometric decreases these error rates significantly (Ross and Poh 2009). Conversely, the use of a multi-modal biometric system, which incorporates more than one biometric for identification, helps in decreasing the FAR and FRR rates significantly. Using multiple biometric identifiers in such a system would result in a synergistic effect in decreasing the FAR and FRR error rates.

Table 1 Evaluation of the accuracy of various biometric techniques (Conti 2017)

Biometric	FAR range (%)	FRR range (%)
Face geometry	0.001–1	10–20
Fingerprint	0.0001–0.001	3–7
Hand geometry	1	1–10
Iris scan	~ 0	1–10
Retina scan	0.01	1
Keystrokes	1	1–10
Voice	2–5	1–10

Biometric verification systems, which make use of biometrics such as fingerprints, are highly reliable as compared to other methods of identification such as passwords or security codes because the former is harder to forge while the latter might be prone to duplication or forgetfulness. However, biometric-based systems are prone to error and in recent times, there has been a growing need to enhance security and privacy and hence, there is need for further research into novel identification techniques that are characteristic of individuals. The problem with biometric identification systems and the comparisons they make to identify and verify an individual's identity is that the matching score between samples implies a probability that the two samples are the same. This probability is never a 100%. Hence, using additional systems like identification via the tongue can add to the confidence of correctly identifying an individual. Furthermore, a multi-modal system, which combines several biometric technologies to find a match, will also result in a decrease to system costs (Yun n.d.). In the interest of enhancing security and privacy, the way forward would be to build identification systems that rely on multi-factor authentication. The use of the tongue in such a multi-factorial system holds promise due to its potential biometric nature. Additionally, if the tongue is introduced as a biometric identifier in formal settings, its potential use could also be introduced in forensic casework. As stated before, the tongue is relatively protected within the mouth cavity and the unique characteristics of the tongue tend to remain stable over time. This means that it is possible to use the tongue for identification in forensic case work where all other measures of identification are not available, such as in cases of decapitations. However, before incorporating the tongue as a mode of identification in such systems, further research is needed in the uniqueness of the tongue and its use in identification systems.

Abbreviations

FAR: False acceptance rate; FRR: False rejection rate

Author's contributions

The primary and corresponding author, Mr. Hannan Latif, is the sole author who fulfills the criteria for authorship for this manuscript. The author(s) read and approved the final manuscript.

Funding

The author declares that there is no funding information to provide.

Availability of data and materials

Not applicable

Ethics approval and consent to participate

Not applicable

Consent for publication
Dr. Vincenzo Conti has consented to the use of their table within this manuscript.

Competing interests
The author declares that no competing interests exist.

Received: 15 September 2020 Accepted: 26 November 2020
Published online: 04 December 2020

References

Conti V (2017) Biometric authentication overview: a fingerprint recognition sensor description. Int J Biosens Bioelectron 2(1):26–31
Jain A, Bolle R, Pankanti S (2005) Biometrics. Kluwer Academic Publishers, New York
Jeddy N, Radhika T, Nithya S (2017) Tongue prints in biometric authentication: a pilot study. J Oral Maxillofac Pathol 21(1):176–179
Liu, Z., Yan, J., Zhang, D. and Tang, Q. (2007). A tongue-print image database for recognition. [online] IEEE Xplore Digital Library. Available at: https://ieeexplore.ieee.org/abstract/document/4370517 [Accessed 6 Mar 2019].
Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S. (2002). Impact of artificial "gummy" fingers on fingerprint systems. [online] Cryptome. Available at: http://cryptome.org/gummy.htm [Accessed 9 Mar 2019].
Musa O, Elsheikh T, Hassona M (2014) Tongues: could they also be another fingerprint? Indian J Forensic Med Toxicol 8(1):171–175
OECDiLibrary. (2004). Biometric based technologies. Available at: https://www.oecd-ilibrary.org/science-and-technology/biometric-based-technologies_232075642747 [Accessed 6 Mar 2019].
Ross A, Poh N (2009) Multibiometric systems: overview, case studies, and open issues. Advances in Pattern Recognition, pp 273–292
Sivakumar T, Nair S, Zacharias G, Nair M, Joseph A (2018) Identification of tongue print images for forensic science and biometric authentication. J Intelligent Fuzzy Syst 34(3):1421–1426
Yun, Y. (n.d.). The '123' of biometric technology. [online] CiteSeerX. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.9348&rep=rep1&type=pdf [Accessed 5 Mar 2019].

Publisher's Note