www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

Biometric Security: A Review to Future

Tushar Sharma[1]; Upinder Kaur[2]

[1]Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
[1]tushar.rk1990@gmail.com

[2]Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
[2]upinderkaur45@gmail.com

Abstract

This paper presents the different biometric with their limitations and introduces their alternative in form of brain biometric, Breath biometrics, and Tongue biometrics. Brain biometric uses brain wave while breath biometric uses one's breath and tongue biometric uses a tongue's shape and variation to distinguish them and present a good alternative for the presently used biometric like fingerprint, iris recognition, face recognition.

Key-words: Biometric Security, Authentication, Brain Biometric, Breath Biometric, Tongue Biometric, conventional Biometric.

1. Introduction

In today's modern world, where we are advancing as a modern civilization that benefits and assures a better and convenient lifestyle by contrived technology things and technology. It also brings new challenges and one of them is privacy and cybersecurity. There are numerous cyber-attacks or clickjacking throughout the internet and our gadgets like mobiles, tablets, laptops, etc. are in the ambit of these attackers. It always a challenge in front of security experts. To tackle these problems and increase security, results in the commencement of biometric security.

Biometric validation, a word derived from the ancient Greek word "bio" meaning life and "metric" meaning measurement. Everyone in the world has a different and contradictory character that we see in others. Biometric technology can detect a person based on different facial features or features of their face, fingerprints, signature, DNA, or iris pattern and transmit a secure and simple method for verification purposes.

Received: 17.06.2021 – Accepted: 18.07.2021

When we think of biometric security, we esteem three things: -

1. Difficult to break and steal.
2. It can be cancellable when a user wants.
3. Accessible by a user only.

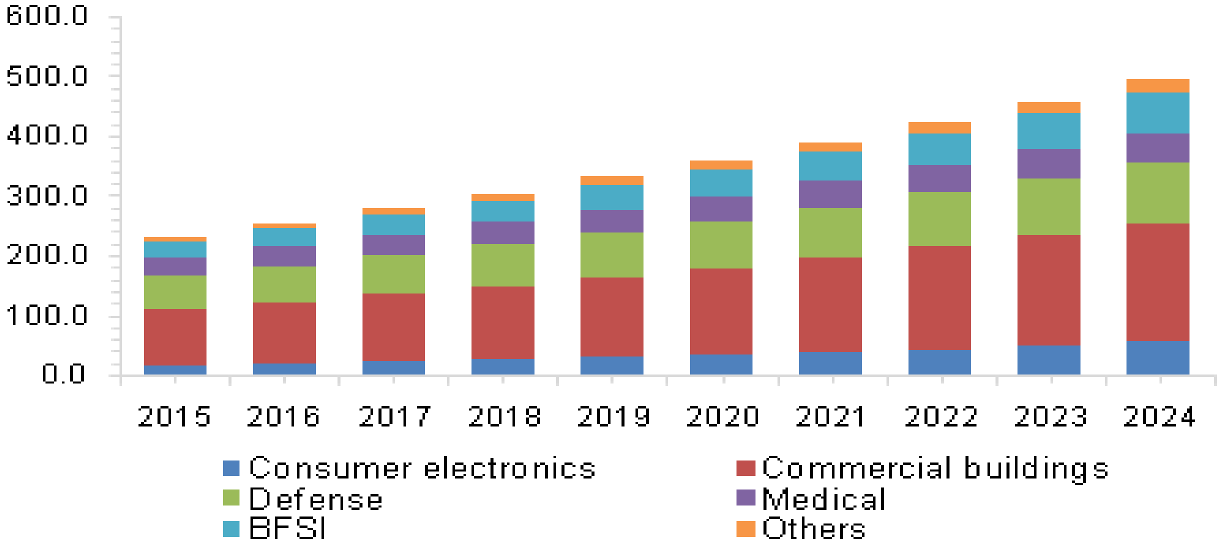
Currently, the most popular biometric technology is the fingerprint, face, and iris recognition. These are preferred by most of the organization and mobile and laptop manufacturers to protect their devices. These not only help them to protect their data but to keep a record of their employees and people entering their premises.

To present one situation, let us say, you use RFID, nanochips, or some forged biometric hacked using some hacking device. An intruder can put a virus in the system of the organization or institution. As many add security frames as part of their mainframe network to reduce cost, so the intruder not only accesses the biometric details of the employee working there but also ingress to the mainframe network of the organization. Hence, he can bring down the whole system of the institution on their knee and they have no option other than being spectators. So, it is important to realize the seriousness of security. One possible way to do it by remote the security network without any connectivity to the mainframe network or the internet so we can prevent at least cyber-attacks. And if something happens, we can ensure minimum damage to the institution.

In addition, United States-based Homeland Security newswire has released a statistical study of the market claiming that billions of dollars are being invested in developing various biometric technologies that can identify anyone in any remote part of the world. The industry is now one of the fastest growing in the world. It is expected that there will be an increase in market share from USD 36.6 billion by 2020 to USD 68.6 billion by 2025. [2] It is estimated that it grows at a CAGR of 13.4% during the climate. Major driving factors in the market include increased biometric use on consumer electronic devices for verification and identification, a growing need for surveillance and protection by the increased threat of terrorist attacks, and increased adoption of biometric technology in automotive systems.

So far, we have come to understand how effective and efficient this technology is and how it occupies an important place in our lives and sometimes we do not know how often we use this technology. It evolves as a necessity for everyone, but this technology has a limit and some self-control.

Graph 1



Graph 1: above graph shows North America Biometric Sensor Market revenue by end-use, 2015 - 2024, (Revenue, USD Million)

When comes to their limitations. Fingerprints can be faked through plastic molds, wood glue. They can be inaccurate when some dirt is present on the finger or sensor, even a little moisture can hoax it. One may think that these fingerprints stay throughout life, but it is a myth, skin conditions like psoriasis (a condition in which skin cells build up and form scales and itchy, dry patches.) or other genetic problems can damage or distort the fingerprints. Another limitation is that they are easily available as they are leftover on surfaces and one can easily use a microscopic slide or fingerprint dust to collect fingerprints and mold them to use. And it is now impractical to use this technology in the age where we have advances in DNA, brain, and body science.

Table 1 - Comparison of different Biometric System

Biometric Features	Fingerprint	Face	Iris	Retina	Voice	Brain
Universality	Medium	High	High	High	Medium	High
Uniqueness	High	Low	High	High	Low	High
Permanence	High	Medium	High	Medium	Low	High
Collectability	Medium	High	Medium	Low	Medium	High
Performance	High	Low	High	High	Low	High
Acceptability	Medium	High	Low	Low	High	Medium
Circumvention	Medium	High	Low	Low	High	High

Received: 17.06.2021 – Accepted: 18.07.2021

Face scanners also have a limitation, even though a high-resolution camera sensor is used but sometimes they also get tricked. Face Scanner usually uses in mobile phones, tablets, iPads, laptops, or other electronic gadgets uses low-resolution cameras of 8 or 16 MP which sometimes fails to scan the face properly. Even a small variation or different angle can trick the system algorithm so one has to be stable to record their face to the sensor and adjust the camera according to it and we have always experienced it when we must adjust our smartphones to unlock the screen and sometimes irritates us after many failed attempts and few times set the maximum attempt timer.

If we talk about the iris scanner, it also has limitations like the face scanners do not have high-resolution scanners to scan the iris. One of the most common problems faced by this technology is the different eye shapes and sizes. Our genes decide the structure and sizes of our face and our eyes, so it is very difficult to capture the iris in case of very small eyes and at the same time we must keep our eyes very close to the scanner to scan properly. Iris may deform non-elastically as the pupil may change its size due to medical or other conditions. As this technology uses infrared light to scan so using it over a long and constant time, can harm our iris and cause a problem like inflame in the eyes. For those people who wear eyeglasses, lens it is very difficult to scan the iris. So, improvement and further research are needed to make it better.

Therefore, there is a need to find an alternative for these conventional biometric systems which is more reliable, secure, and accurate than these pre-existing technologies. The user can trust them blindly and can be used in day-to-day life.

A few alternatives we can look upon are: -

A. Brain biometric
B. Breath biometric
C. Tongue biometric

Let discuss each of them in brief below:-

A. Brain Biometric

Brain biometric includes brain signals or electrical activity through the scalp using electroencephalogram devices. Electroencephalograms are a more secure way of security as the brain wave dies with the human death and hence are unique trait wipe out with human death and on the other side, it is difficult to imprint them and provide a high level of security. Brain, as we all know, is an internal organ and hence is a proof of life or death, means it will work only when a person is alive and stop with his death, so it will satisfy all three condition which we stated above for a biometric i.e., difficult to break, cancellable by a user and accessible by a user.

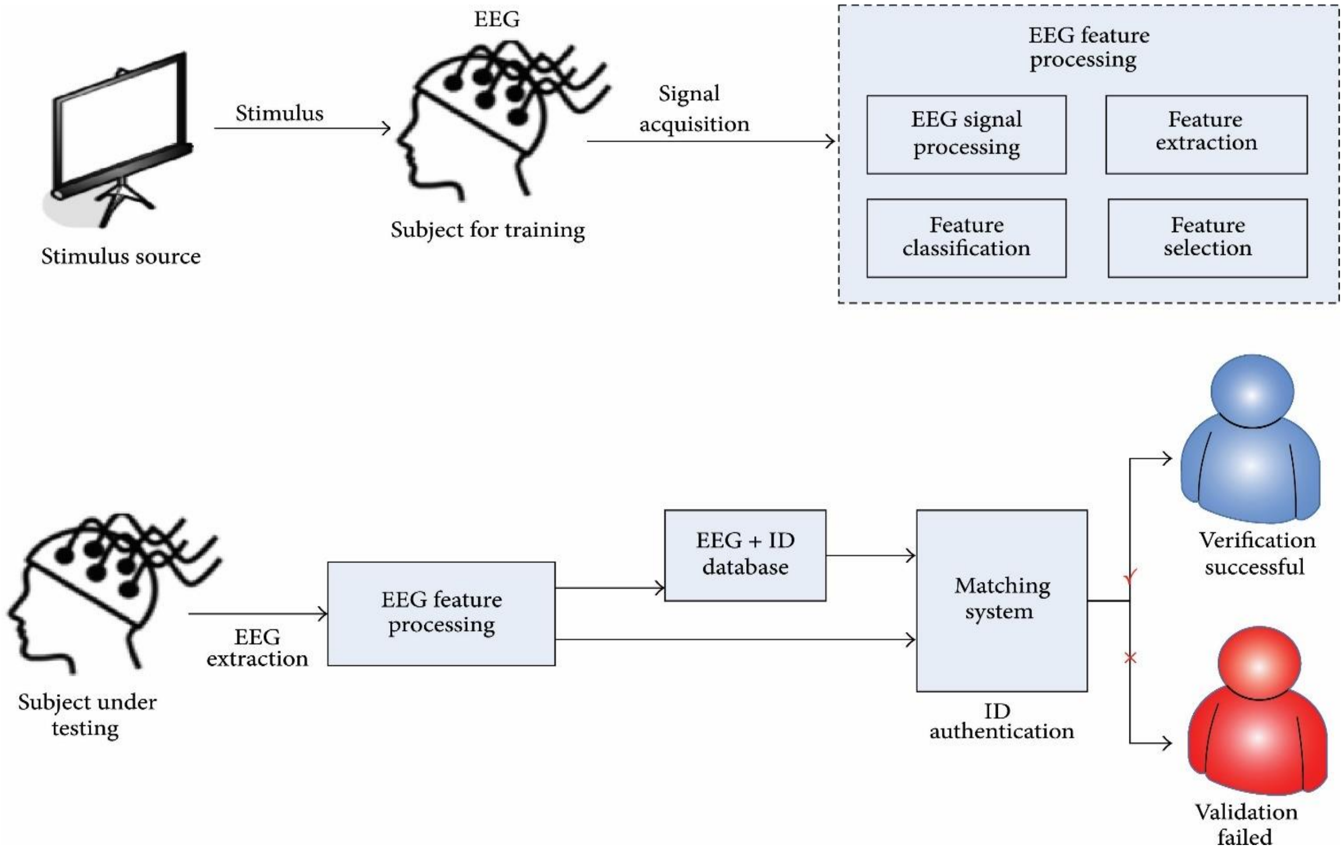
This biometric identification is based on the principle that our brain reacts differently to different words, pictures, or situations which is enough to have a different identity. These signals are strong and more accurate.

Dr. Blair C. Armstrong, a lead researcher for the Basque Center project, comes with a unique idea that proposes a technique based on semantic memory (it is a portion of long-term memory that processes ideas and concepts that are not drawn from personal experience) of a person is more reliable and harder to forged identification security.[3]

Brain wave is a unique biological trait of being which is hard to forget. Electroencephalogram devices record brain waves along the scalp. Brain waves are generated by the ever-changing bioelectrical field in the human brain. Our brain behaves differently in different situations and different brain waves are produced. We can record the change of the bioelectric fields by inserting electrode(s) into the brain or using an electrode cap on the scalp to collect electroencephalogram data. These electroencephalogram features are then processed in the system and compare with the electroencephalogram database and decide where to give access or not to the respective person. But at the same time, we must remember that the brain wave of twins is nearly identical, and we required a good level of sensors to differentiate them.

Electroencephalogram devices must have sensors to capture all these brain signals through the scalp and include a bio amplifier, an A/D converter, and a computer set up to control and process the data. To further increase this security, we must make the above setup independent means it should not be connected to any other device in the mainframe so that they can be left alone without connectivity with any network which helps in protecting from the cyber-attack, which is the main reason we need new technology to counter this.

Figure 1 - Block Diagram of Brain Biometric System



Electroencephalogram is sensitive to emotional and mental state. This means that during the verification it depends on our mood if the biometric got accepted or rejected. During enrollment, data is recorded at only a calm state because a calm state has better EER (Extreme Energy Ratio) as compared to other states. So, during verification states like stress, calm or excitement can be used.

By combining various biometric systems (like face, fingerprint, iris) with brain biometric we can increase the security and hence develop a system difficult to break-in. Given that brain print is difficult to forge as we cannot copy another person's thought process, this technology always has an advantage over others.

B. Breath Biometric

Many people have not heard of this biometric as it is not used anywhere but, in the future, we can have this one of the biometric identities. This is full-proof security that is under the control of the respective person and nearly impossible to forge.

Recently, Researchers Pablo Martinex-Lozano Sinues, Renato Zenobi from ETH Zurich, the Department of Chemistry and Applied Biosciences, and Malcolm Kohler from the Pulmonary

Division of University Zurich conducted a study in which they asked their participants to breathe through a warm pipe. connected to the gas port of the quadrupole time-of-flight mass spectrometer (a machine commonly used in chemistry to distinguish different chemical components of different samples). [6]

The result of this is their respiration as the spectrometer separates air into its chemical components. They conclude that there is a slight change in the sample that can help identify people.

The fact that everyone has a unique breath print is due to all microbes that inhabit our bodies. The advantage of this biometric is that every individual a metabolism and different body process which result in a change in the breath pattern. One more advantage of this biometric is that these breakpoints not only vary between individuals but also change throughout the day within individuals in a reflection of shifting chemical reactions within the body. So, this biometric guarantee you that you always have a different password at different daytime just like the highly confidential things are protected by changing the password every day or every specific time to prevent any attack on them and now you also got that protection through your breath print.

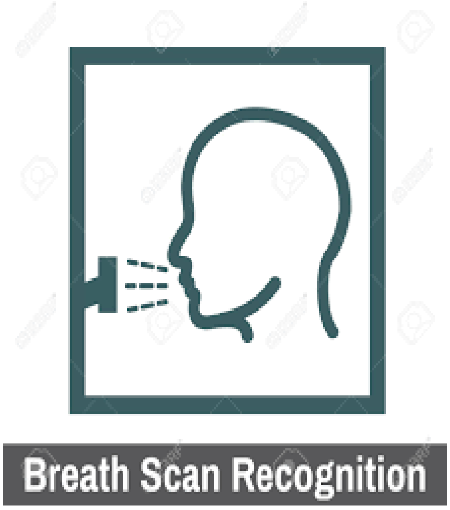
Table 2 - Features of Biometric Technology

Benefit	Brain Biometric	Breath Biometric	Tongue Biometric
Accuracy	High	Medium	High
Privacy	High	High	Medium
Speed	Medium	Low	High
Work with masks /gloves	Yes	No	No
Work with glasses /goggles	Yes	Yes	Yes
Collectability	Low	High	Medium
Long term stability	High	High	Medium

For reference, we heard that dogs are used in medicine to detect cancers, lung disease, and now only we heard that these dogs are also helping in the detection of coronavirus. So, what you think about how they do this? These dogs do not know any chemistry or biology of these diseases. They sniff them from our breath and if we can copy their unique talent, we can develop a system not only to identify each individual but also detect diseases or problems in our body.

Received: 17.06.2021 – Accepted: 18.07.2021

Figure 2 - Breath Biometric



This is new to everyone and needs some research but once we can channelize this, I can give you one surety that your identity and data are safe. And not only this but you have full control over it unlike those conventional methods of fingerprint or face which can be forged or can be accessible from the government or institutional database. So, do not be surprised if you heard a breath identification system installed everywhere in the future.

C. Tongue Biometric

The tongue is a vital organ that helps in various tasks like speech, tasting, eating. But now we are also considering it as a new biometric identity. As it is an internal organ like the brain it also offers the same advantage as we discuss above. With them, it has one more advantage that the tongue can be easily exposed for verification and at the same time are also protected in our mouth.

The features which we can observe in the tongue are not just the tongue print but also the shape, color, mobility, and variation in person to person. The dorsal surface of the tongue is also unique for each person. The characteristic features of the tongue exhibit remarkable differences even between identical twins.

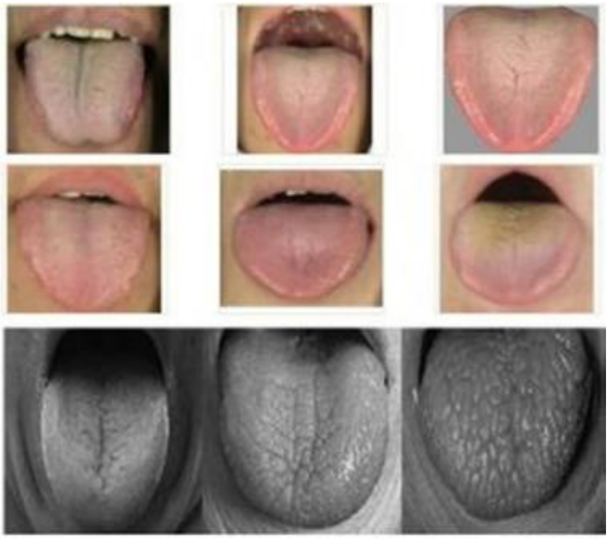
According to one research process in which they did their research for twenty participants. Participants were screened for visual cues that followed which digital images above language were taken. Moderate language visibility was performed, and simulations were performed using a toothpick. Images and broadcasts were analyzed by two viewers for a variety of top morphology including composition, presence or absence of debris, and pattern distribution. Three points of consideration were considered to determine the status of the language.

Received: 17.06.2021 – Accepted: 18.07.2021

They also found that the most common morphological factor in the dorsum of the tongue was the presence of medial holes. Most straight fissures were seen in men and one straight fissure was a common find in women. The language was predominantly U-shaped for both men and women. The V-shaped tongue was seen in 25% of women.[7]

A digital photograph of a tongue is taken and then match from the database and then evaluate if it is a match or not and to permit the person or not. The system matches the photograph by marking reference point and match the color shape and texture etc. of the tongue and give a result.

Figure 3 - Different Types of Tongue use in Tongue Biometric



We all know the potential of the tongue and need further research to develop. The method of identification is easy to develop and difficult to forged and provided the best alternative in the future.

2. Conclusion

In this paper, we have discussed the alternative for the conventional method of the biometric system. We have tried to identify the unique trait present in a human body like brain wave, breath print, tongue print which are more reliable and secure than those previously used systems like a fingerprint, face scan, iris scan. We have seen that those conventional technologies are quite accessible by the intruders and can be used to harm the host. So, the introduction of new biometric technology will help us to tackle the challenges faced by the usual systems. Brain waves are the new draft in this field. Imagine one day you can control the surrounding you with your brain. You can have a new identity in form of your breath, and you have your tongue in place of those RFIDs (Radio-frequency identification).

Above and beyond, we have presented the practical consideration with a theoretical advantage over the other biometric technology. Brain Biometric cannot be collected without the user's consent. Breath biometric frequency can be controlled, and tongue print is inaccessible by others. With great benefit and security, we must work together to develop this technology to introduce in the market. We have numerous resources to improve our privacy and security. Many new technologies are under development and many are waiting to be developed. Many biometric systems are used in the judiciary as forensic evidence, but they are not always accurate. So, we must look for an alternative that is 100% accurate. Contrarily, there are numerous biometric technologies developed into technology platforms which take over the world soon.

Acknowledgement

The author is grateful for the support provided by the Assistant Professor Upinder Kaur, faculty of computer science, school of computer science and engineering, Lovely Professional University, Punjab, India.

References

Ross, A., Banerjee, S., Chen, C., Chowdhury, A., Mirjalili, V., Sharma, R., & Yadav, S. (2019). Some research problems in biometrics: The future beckons. In *2019 International Conference on Biometrics (ICB),* 1-8. IEEE.

Mehra, A. (2020). Biometric System Market with COVID-19 Impact by Authentication Type (Single-Factor: Fingerprint, Iris, Face, Voice; Multi-Factor), Offering (Hardware, Software), Type (Contact-based, Contactless, Hybrid), Vertical, and Region - Global Forecast to 2025. (2020). Markets and Markets. https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

Gui, Q., Ruiz-Blondet, M. V., Laszlo, S., & Jin, Z. (2019). A survey on brain biometrics. *ACM Computing Surveys (CSUR), 51*(6), 1-38.

Reshmi, K. C., Muhammed, P. I., Priya, V. V., & Akhila, V. A. (2016). A novel approach to brain biometric user recognition. *Procedia Technology, 25,* 240-247.

Liang, W., Cheng, L., & Tang, M. (2016). Identity recognition using biological electroencephalogram sensors. *Journal of Sensors, 2016.*

Vrankulj, A. (2013, April 5). *Swiss researchers investigate unique breath prints*. biometric update. https://www.biometricupdate.com/201304/swiss-researchers-investigate-unique-breathprints

Jeddy, N., Radhika, T., & Nithya, S. (2017). Tongue prints in biometric authentication: A pilot study. *Journal of oral and maxillofacial pathology: JOMFP*, *21*(1), 176.

Nuwer, R. (2013, April 5). *Swiss researchers investigate unique breath prints*. Smithsonianmag.com. https://www.smithsonianmag.com/smart-news/your-breath-is-as-unique-as-your-fingerprint-16068566/

Radhika, T., Jeddy, N., & Nithya, S. (2016). Tongue prints: A novel biometric and potential forensic tool. *Journal of forensic dental sciences*, *8*(3), 117.

Godbole, M., Narang, B., Palaskar, S., Patil, S., & Bartake, A.R. *Tongue Scanning as a Biometric* Tool: A Review.

Fierrez, J., Morales, A., & Ortega-Garcia, J. (2021). *Biometrics Security.*

Alrahawe, E.A., Humbe, V.T., & Shinde, G.N. *An Analysis on Biometric Traits Recognition.*

Godbole, M., Narang, B., Palaskar, S., Patil, S., & Bartake, A.R. Tongue Scanning as a Biometric Tool: A Review.

Mishra, A.D. *Biometric Authentication System.*

Petrova, K. (2002). *Biometric security systems: finally, a friend?*

Bearsky23. “Biometric Scanning Graphic Breath Scan Recognition.” 123RF, bearsky23, www.123rf.com/photo_85635134_stock-vector-biometric-scanning-graphic-breath-scan recognition.html.

Mainguet, J. F. (2020, October 10). Biometrics: tongue [Digital image]. Retrieved November 20, 2020, from https://biometrics.mainguet.org/types/tongue.htm

Liang, W., Cheng, L., & Tang, M. (2016). Brain wave-based identity recognition system. [Photograph]. Identity recognition using biological electroencephalogram sensors. *Journal of Sensors,* 2016.