EEG Biometrics outside the Laboratory: A Review of Advances and Challenges in Real-World Secure Authentication

Bhaskarabhatla Akshay[1*], Pasula Nethra[2], Satya Kusi[3]

[1,2]B.Sc. Digital Forensics, Malla Reddy University, Hyderabad, India

[3]Assistant professor, Department of Digital Forensics, Malla Reddy University, Hyderabad, India

[1]bakshay4545@gmail.com*, [2]pnethra27@gmail.com[3]satyakusi06@gmail.com

Abstract

As more resources go virtually(online), we also need ways to prove that are safe, dependable and easy to use. Now-a-days normally passwords, cookies, PINs all the credentials are being hacked and stolen by the attackers not only this but biometrics such as fingerprints, face recognition which are being spoofed by the attackers and may misuse the personal data. To prevent from the attack's researchers used EEG biometrics which is used to get the brain signals which are used to identify the person and this brain signals is also known as "brain prints" which is preventing from attacks and which are hard to spoof and it is more secure than all other biometrics. This paper look for EEG based authentication which are used for identification of individual and it is done in good and controlled laboratory setup so that we can get the brain signals accurately. And there are variations in brain signals depending on the person how they behave or how they are while collecting the brain signals such as at resting state we can get different brain prints and movements while recording or any emotions, stress so that it will produce different brain signals but these EEG systems which are easy to use and produce accurate results and work good in noisy conditions or uncontrolled environment. Overall, by these studies this paper suggests to build EEG authentication that are secure, reliable and accurate and are suitable for the real-world usage.

Keywords: EEG biometrics; Brain prints; Secure authentication; Wearable EEG; Real-world environments; Cybersecurity; Machine learning; Privacy and ethics

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_23

1. Introduction

As There is more dependence on use of digital devices and services which has became integrated part of everyone's life so it's necessary to secured, quick and easy to use verification methods. Authentication traditional methods like entering passwords, PIN and authentication tokens are prone to attacks like brute force attack, dictionary attack, rainbow table attack so introduction of biometrics like fingerprint, iris, retina, and face helps to mitigate this attacks but vulnerable to coercion, spoofing, impersonation (Jain et al., 2011; Galbally et al., 2014; Li et al., 2021). so to protect from these attacks researchers moved to EEE signals which are stable, difficult to forge, unique to individual, these are brain wave patterns generated by electrical activity of neurons in brain by showing images or listening audio generates EEG graph (Palaniappan, 2013; Campisi & La Rocca, 2014; Ruiz-Blondet et al., 2016).

Unlike traditional biometrics EEG signals are cannot be easily copied this allows strong protection against spoofing attacks (Maiorana & Campisi, 2017; Yang & Deravi, 2013). Initial stages of experiments in Brainprints the results shown accuracy in controlled lab environments but these rigid setup cannot be applicable for real-time commerical purpose as scalability is required (Li et al., 2021; Abo-Zahhad et al., 2016; Cimatti et al., 2021; Sun et al., 2022; Dimitriadis et al., 2019).

There has been huge advancement development in recent years which are real world applicability by wearable EEG devices and advancements in machine learning techniques, and signal processing (Marín- Morales et al., 2021; Lopez et al., 2021; Liu et al., 2021; Alzu'bi & Deravi, 2021). Research scientist have searched various stimulus models like motor imagery, resting state patterns, Event-related potentials (ERPs), emotional responses, and functional connectivity to be more reliable and practical outside lab.

Because of these challenges, there is a clear need to step back and carefully review how close EEG-based authentication systems are to real-world use. This paper looks across recent studies to understand what progress has been made, what methods are working better, and what problems still stand in the way of practical deployment outside the lab environments.

2. Literature Review

2.1 Laboratory-Based EEG Biometrics

Early EEG biometric systems mainly focused on medical grade EEG machines which is used in the laboratory to see the brain signals which are unique to every individual. These studies show how good it was and it is giving the accurate 95% results to identify the person and which was done in the good environment without any noise or distractions. so which is proved that brain signals can work to identify the individuals (Khosla-Akino et al.2021; khosla et al.2016) (Palaniappan, 2013; Campisi & La Rocca, 2014; Ruiz-Blondet et al., 2016)

2.2 Stimulus Paradigms for EEG Authentication

As it is increasing day by day researchers started investigating multiple stimulus paradigms where in the resting state EEG which is easy for the individuals, but signals can change because of mood, stress or work pressure (Li et al.,2021; Marin-Morales et al., 2021).Motor imagery in EEG which is full secure and works good with the wearable devices, but

individuals need training and brain signals changes across the sessions (Abo-Zahhad et al. ,2016) .Emotion-elicted EEG which is unique patterns for every individual,if the emotional response is consistent then it works well and give accurate results and which is difficult in the real world (Cimatti et al. , 2016)

We have different methods, event-related potentials (ERP) especially P300 and visual responses which are easy, strong and can detect the brain signals which is of low-cost EEG devices and have portable authentication (Maiorana & Campisi, 2017; Sun et al., 2022). Additionally, "Functional connectivity" research stated that network level neural associations has been established over a constant stretch enhancing to equipment-related and ecological variability (Fraschini et al., 2018; Diimitriadis et al., 2019)

2.3 Wearable EEG Devices

The growth of consumer EEG wearable has become EEG biometrics are closer to real world (Casson, 2019; Zhang et al., 2021). These dry electrode devices supports login authentication and quick to setup or continously monitoring identity. However because of few electrodes the signals can become weaker and easily distracted by noise or any issues(Liu et al. , 2021).

2.4 Machine Learning and Deep Learning Approaches

To prevent accuracy from dropping when condition change, recent studies use AI method such as deep learning and transfer learning and domain adaptation these techniques will enhance the system to learn better from the old data adapt to new sessions and will work good when EEG device or recording conditions are different (Gao et al., 2020;Berkovsky et al., 2021; Xu et al. ,2022).

Even though the technology is increasing there are some concerns whether EEG biometrics will stay accurate over the long time and people will be comfortable using EEG devices and it helps to how to protect the individuals brain signal information(Lopez et al. ,2021; Alzu'bi &Deravi,2021).Current study or literature show good progress in making EEG based authentication as practical to use in real world and EEG device which is smaller and having good hardware and algorithms that can be used in different situations.

3. Analysis

This study show good progress towards EEG based authentication which helps in consumer grade hardware,machine learning efficiency and signals can handle noise in the signals.But EEG biometrics that is good to do in the laboratory outside the laboratory it will become difficult. In real world the brain signals may become poor or behaviors may change from one to another and devices are not easy everytime (Marin-Morales et al.,2021; Lopez et al. ,2021; Alzu'bi & Deravi, 2021)

Mainly in this type stimulus paradigm selection was used while recording the EEG that will know how good the authentication was in the real world. Methods we use are event related potentials which are having good performance than in the resting stage . This is because of ERPs will have clear and good brain responses that are easier to detect and use accurately even with limited settings (Maiorana & Campisi, 2017; Sun et al.
,2021).Using visual and sound prompt which can make EEG signals less convinient for real world for

example when we unlock a mobile device or continous authentication will be there. Additionally, when we use in the resting state then the brain signals may be natural or user friendly . But brain signals are not correct everytime they may change according to the situation the individual behave such as mood,stress etc.(Li et al. , 2021; Marin-Morales et al. , 2021)

Another thing that is moving from many EEG signals to less and more good ones. Using reducing channels ,dry electrode which make the EEG devices easier and user friendly . However these devices collect less data about brain the authentication may change from different studies(Zhang et al. , 2021; liu et al
. , 2021). Older methods that used are manual or traditional machine learning models which is difficult in handling EEG signals. Deep neural networks will work good because it may automatically adapt and extract the accurate brain patterns even if there is any noise while recording(**Gao et al. ,2020; Berkovsky et al., 2021).**Deep learning model can easily overfit when there is a some training data or any changes that occur while capturing the EEG signals. To keep it correct for everytime researchers used some techniques such as trasfer learning, domain adaptation and personalized calibration. Which helps to understand the new conditions and behave properly (**Xu et al. ,2022;Lopez et al. ,2021**)

The problem that occurred in all the studies are there is no Exact way to test EEG authenticatiion. Many experiments that was done is collected data in only short period of time which are results looks good compared to correct (it will almost similar).This will not show how system works in real with long term usage(Koike-Akino et al. , 2021; loppez et al. , 2021).In real world the authentication system must test multiple times under different conditions and test must be done with time gaps and in uncontrolled envinorments we need to perform . But some are open EEG datasets which looks difficult to compare with different systems and we measure how they will work correctly .

Finally,even there are improvements ,user related comforts such as private information and the setup takes long and see people feel comfortable using the device in public.these are important for making the autentication as practical (Alzu'bi & Deravi, 2021). Dry electrodes that can feel uncomrtable to the individuals and some individuals think that device can read the thoughts that are going in mind which can feel uncomfortable to the users who are using it or they can fear or they will not trust the device. But EEG authentication that are accepted everywhere and it is easy to use and comfortable to use and individual feels that they can trust this EEG authentication.

By this Overall field that is improving, but we are doing trasition of research ideas into real commercial products which requires in every area better device, smart algorithms and stronger testing methods that are designed that focus the user neeeds.

Experts from Neuroscience, cybersecurity, wearable technology must work similarly to make EEG biometrics more reliable and secure the privacy and which can help the user daily for authentication.

4. Proposal Approaches

4.1 Progress in Wearable EEG Device Design

Future development in EEG Brain prints will depends on how advanced they evolve of wearable hardware. Despite today's consumer-grade EEG devices which are easier to set up, portable, but still

need to improve their performance incase of outside controlled environments especially shifting electrodes, everyday movements, prolonged use can introduce noise and weaken signal quality of EEG signal is still a challenge in real time usage outside lab (Casson, 2019; Zhang et al., 2021; Liu et al., 2021). Instead of heavy headset , research scientists need to develop more comfortable and easier to use like every day gadgets which look and feel like earbuds, or AR/VR headsets so that user feels more comfortable And also need to improve dry electrodes they often lose connection when used prolong or sweating which effects EEG signal quality. Need of more betterment of advanced electrode material and skin- electrode interfaces which can help to maintain stable connection even when users are talking, walking or working. By these improvements in EEG wearable headsets will make users more comfortable touse and more reliable, practical to use in real- time environments (Alzu'bi & Deravi, 2021).

4.2 Handling Changes in Brain Signals Over Time

The huge weak point of present EEG Brainprints biometric system is that Brain signals are not always the same they change according to factors like person's mood, stress, or mental effort can alter the EEG pattern even for the same person due to this problem genuine authentic user also fails to recognize (Li et al., 2021; Marín-Morales et al., 2021). Till now the research is on single-session datasets and short duration which is not reliable to real-time usage (Lopez et al., 2021). So there need to be conduct new research with large, variety of datasets along with increasing duration of months to years so that EEG biometric will be more reliable to use.

4.3 Reliable Models for Noisy Environments

Traditional methods don't work properly in noisy real time environments, they have low accuracy in outside lab. Deep learning methods can solve this problem but not completely as they still have weaknesses as data available for training is too small that it cannot learn in depth so it performance is low (Gao et al., 2020; Berkovsky et al., 2021). So the research in future should improve on methods such as self-supervised learning, transfer learning, domain adaptation to make models more reliable (Xu et al., 2022). There is also a need for energy-efficient and light weight models that can directly used on edge devices by these models can

reduce the need of sending sensitive information to external

servers and can enable real time authentication by keeping user data private.

4.4 Multimodal Biometric Authentication

Dependence on only EEG brainprints for authentication have less reliability when it is combined with other psychological or behavioural biometrics like face scan, fingerprints or keystroke pattern can make more robust and difficult to spoof (Maiorana & Campisi, 2017; Dimitriadis et al., 2019). So further researchers should work on multimodal and context-aware frameworks where EEG authentication only needed when other biometric methods are not enough to be reliable, with this helps in high security and adaptive use of EEG signals.

4.5 Need for Standard EEG Benchmarks

One of the biggest problem in EEG signals there is no common stranded framework and protocols for real-time environments usage as till date research is done on controlled lab environments, short session and less duration period the results are accurate but performance is decreased incase of real-

time environments usage (Koike-Akino et al., 2021; Lopez et al., 2021). So research further should more focus on creating open and publicly present EEG brainprints datasets taken in real-time environments and also need of performance measuring tests like EER, accuracy, FAR/FRR and handling noise in real-time usage so that results can be verified accross multiple studies and technology can be properly validated.

4.6 Ethical and Privacy Challenges

EEG signal has sensitive and cognitive information about a person like emotions,focus levels, mental status and personal thoughts which are private to individual and has ethical value that obstructive incase of EEG based biometrics so researchers need to create a template that must be preserving privacy, need to store the EEG data securely by using encryption techniques (Alzu'bi & Deravi, 2021). And also need to develop strong countermeasures and requirement of careful threat analysis for replay attacks where attacker use previously recorded EEG data or create fake EEG signals.

5. Conclusion

EEG based biometrics which are secure,reliable and having good authentication and providing individuals a trust. This review tells that there has been a lot of data that how the signals are collected and how they are classified. And the field is tranfered from lab setup to the the real world environment which is an wearable device that can work in real life. These studies show that correct and accurate identification is possible even with the low level EEG devices and also have strong feature extraction which can show the accurate results of the brain signals.

However when we use EEG biometrics in real life which is still difficult because of noise, changes in the mood or any stress or changing the body movements while recording the brain signals. And there is no correct method to test and there are only some real world datasets which makes hard to compare the results.Finally individual accepts the challenge and pepole may feel it uncomfortable and they think that privacy loss and they worry wearing a EEG device becomes inconvinient for the individuals. These issues that are there need to be discussed in futhur works. EEG biometrics to use widely the field is compared across many areas better wearble devices,and understanding the brain signals how they often change, and we use smart algorithms that can work and handle the changes for long term in neural activity.Clear guidelines and transparent data which will improve the trust of the individual.If these challenges were focused then EEG biometrics which can grow and are having secure, reliable and scalable and it can be easy to use authentication method for the cybersecurity.

References

1. Li, F., Zhao, Q., et al. (2021). Password vulnerabilities in modern digital environments. *Computers & Security*, **112**, 102528.
2. Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer, New York.
3. Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric anti-spoofing: A review. *IEEE Access*, **2**, 1530–1554.
4. Palaniappan,R.(2013). Electroencephalogram-based biometrics: Challenges and practical implementation. *IEEE Systems Journal*, **7**, 832–845.
5. Campisi, P., & La Rocca, D. (2014). Brain waves for automatic biometric- based user recognition. *IEEE Transactions on Information Forensics and Security*, **9**, 782–800.
6. Ruiz-Blondet, M. V., Jin, Z., & Laszlo, S. (2016). CEREBRE: A new EEG-based biometric. *IEEE Transactions on Information Forensics and Security*, **11**, 1618– 1629.
7. Fraschini, M., et al. (2018). Functional connectivity analysis and biometrics. *Frontiers in Human Neuroscience*, **12**, 201.
8. Maiorana, E., & Campisi, P. (2017). EEG biometric recognition using visual stimuli. *Pattern Recognition*, **72**, 1–14.
9. Yang, S., & Deravi, F. (2013). On the usability of EEG signals for biometric recognition. *IEEE Transactions on Information Forensics and Security*, **8**, 1998–2008.
10. Khosla, A., et al. (2016). User authentication using task-evoked EEG. *Pattern Analysis and Applications*, **19**, 101–116.
11. Del Pozo-Barragán, A., et al. (2020). ERP-based identification in controlled environments. *Biomedical Signal Processing and Control*, **58**, 101843.
12. Koike-Akino, T., et al. (2021). High- accuracy EEG biometric systems in laboratory conditions. *Frontiers in Human Neuroscience*, **15**, 659142.
13. Casson, A. J. (2019). Wearable EEG: Advances and technologies. *Sensors*, **19**, 233.
14. Gao, Y., et al. (2020). Lightweight deep learning for EEG biometrics. *IEEE Access*, **8**, 217709–217720.
15. Zhang, C., et al. (2021). Real-time authentication with consumer-grade headsets. *Computational Intelligence and Neuroscience*, **2021**, 8876548.
16. Berkovsky, S., et al. (2021). Cloud- assisted EEG authentication. *Future Generation Computer Systems*, **125**, 265–276.
17. Xu, H., et al. (2022). Edge-computing solutions for neural biometrics. *IEEE Internet of Things Journal*, **9**, 11592–
    11603.
18. Li, J., et al. (2021). Resting-state EEG user identification: A comprehensive study. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, **29**, 1058–1069.
19. Abo-Zahhad, M., et al. (2016). Motor imagery for person recognition. *Computer Methods and Programs in Biomedicine*, **131**, 207–218.

20. Cimatti, D., et al. (2021). Emotion- based brain biometrics. *Sensors*, **21**, 1123.
21. Sun, H., et al. (2022). ERP-based secure authentication in wearable environments. *IEEE Access*, **10**, 25744–25755.
22. Dimitriadis, S. I., et al. (2019). Connectivity profiles as biometric signatures. *IEEE Transactions on Biomedical Engineering*, **66**, 1103–
1113.
23. Naseem, M. T., et al. (2023). Motion artifacts in wearable EEG: Mitigation techniques. *Biomedical Signal Processing and Control*, **79**, 104209.Marín-Morales, J., et al. (2021). Mental-state variability in authentication performance. *Computers in Biology and Medicine*, **130**, 104207.
24. Lopez, J., et al. (2021). Long-term EEG variability analysis. *Brain Sciences*, **11**, 1624.
25. Liu, Z., et al. (2021). Reduced- channel EEG authentication. *Electronics*, **10**, 294.
26. Alzu'bi, A., & Deravi, F. (2021). Usability and user acceptance of EEG biometrics. *IET Biometrics*, **10**, 685–
693.