Advances and Applications in Mathematical Sciences
Volume 21, Issue 8, June 2022, Pages 4747-4760

EVALUATING USE OF BIOMETRIC AUTHENTICATION FOR FACE AND VOICE RECOGNITION

RIZWAN ALAM and G. AKILARASU

Dept. of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab, India
E-mail: rizwan.12000834@lpu.in

Abstract

When it comes to identification, only fingerprints had been used in 20th century in the name of biometric authentication when only ink was used to get fingerprints before the evolution of signatures in the 1960s and 1970s. Back in modern days, smartphones not only have a large amount of personal data, but also have access to sensitive information stored in internet banking, email, and social networks. Passwords are traditionally used to prevent unauthorised access. But it is not easy to remember various passwords for each service and using the same password for every service is not feasible. It is also not worth storing the password because the device can be stolen or lost. Biometric authentication is a safer alternative for verification with physical characteristics like fingerprints, iris, voice, and facial features. Biometric authentication also has other use cases and scenarios. This article will focus mainly on facial and voice recognition as biometric authentication measures and discuss their pros and cons, and use cases in real world scenarios. In order to fulfil these research objectives, this study relies on secondary data collected from various online sources like articles, publications, research papers, studies, reports, and more.

1. Introduction

Biometrics is a technical term which consists of behavioural or physical patterns of humans. Data security relies heavily on biometric authentication. It creates a data-oriented model to identify an individual. With that biometric and model details, access to applications and various network resources can be authenticated with biometric information. It is instantly becoming an important element of multifactor authentication as it combines seamless user

2020 Mathematics Subject Classification: 68T01.

Keywords: biometric authentication, face recognition, voice recognition, fingerprints, identification, private data.

Received October 5, 2021; Accepted January 15, 2022

experience and robust authentication. This technology has been a major industry trend over the years, especially because of recent innovations in AI in the tech industry. Compromised credentials have become the weak link for 20% of breaches reported by IBM (2021). It takes around 287 days on an average to detect and take actions against the breach.

There is a rise in the usage of AI-based security and it will definitely be competitive in industry. According to IBM, 25% of businesses have deployed AI-based security measures and 40% of those businesses have done partial deployment in 2021. The Remaining 35% of businesses are yet to deploy AI, making their clients highly vulnerable to security breaches. A business can save around $3.81 million by investing in AI-based security [1].

1.1 Background. User ID and password has always been the first layer of security over the past few decades. But millions of those user/password combinations are available on the Dark Web for sale these days due to several high-profile data breaches at leading businesses and financial institutions. The level of vulnerability is even higher, considering human tendency to use the same passwords in several accounts. On the other hand, biometric authentication is far more secure from such a vulnerability due to the unique biometric data of the user. It is far more difficult to replicate facial or fingerprint scan for an attacker if there are robust solutions deployed with strong spoof/liveness detection. On the other hand, authorised users can authenticate the same with just a moment. Hence, biometrics are known to be more convenient and secure than passwords [2].

Initially, biometrics may seem to be just another way to access a smartphone securely, but there are several use cases. Biometric authentication is simply meant to secure data with parts of human bodies that are unique and cannot be replicated easily. Though quantum computing and machine learning techniques can guess the password, biometric data like facial structure, irises, and fingerprints cannot be emulated or determined so easily [3].

The biometric technology will cross around US$55.42 billion in the international market by 2027 (Statista, 2022). Global spending on biometrics authentication is forecasted to cross over US$13 billion mark, i.e. from US$4.93 billion in 2017 to whopping $18 billion in the year 2027. Identity

verification is vital for information security as it allows only authorised people to access data and prevents malicious or hazardous intrusion. The facial detection was forecasted to reach US$3.8 billion mark in the year 2020. The market is projected to cross US$8.5 billion by the year 2025.

Biometric authentication for facial detection has been a very promising security feature over the years as it is used in millions of Android and iOS devices. With advancements of machine learning and augmented reality in facial recognition, facial recognition has been more mature with time. Another major reason behind the advancement of facial recognition is the pandemic for authentication and identification [5]. Facial recognition was a challenge for facial recognition programs due to rising use of face masks. However, a lot of facial detection programs can now consider face coverings, glasses, beard and other obstacles.

It is especially true not just for convenience of consumers, but also for law enforcement agencies to detect criminals. Even if users have a face mask on, they can be verified with the database. 3D cameras can capture even more details on a human face than traditional 2D cameras. Facial recognition has never been so secure. Anyone could manipulate AI with a similar looking face or picture of someone else. The margin of error has been narrowed down by machine learning as a lot of anti-spoofing measures are used to keep hackers from manipulating facial recognition technology [6].

It was forecasted that the voice recognition market is expanding to $27.16 billion mark by 2026 from $10.7 billion in 2020 internationally [7]. Biometric authentication with voice recognition has greatly promoted hands-free communication. Voice recognition is widely used for identification. With proper training, Google Home and other smart home ecosystems can recognize the voice of family members and identify them. It is very useful to display relevant information to that person like their notifications and schedules.

In verification and authentication, voice recognition serves other purposes. A smart device can save a lot of time by accurately identifying someone and verifying as per their voice. However, there are several instances when deep learning is used to mimic a voice realistically 3 using "vocal synthesis" technique. In a case, a fraudulent activity took place using

"deep fake" voices at a UK-based energy firm which cost a whopping $250,000 in the year 2019 [8].

Vocal synthesis can be more realistic with the improvement of deep learning [9]. However, non-security applications are ideal for using voice recognition, especially identification, unless this technology improves enough to differentiate fake vs real voices properly. Autonomous transcriptions of recordings of conferences or classes and consumer-based smart home solutions can be better suited for voice recognition.

1.2 Literature Reviews. Chetty and Wagner (2006) proposed the "multilevel liveness verification (MLLV)" framework to realise safe and secure biometric authentication for face and voice recognition that can prevent several video and audio replay attacks. On the basis of novel "multimodal fusion" and "feature extraction" approaches, this framework reveals the dynamic and static relation between face and voice details from faces while speaking, adding several layers of security. Researchers tested 3 speaking corpora "AVOZES", "VidTIMIT" and "UCBN" and found great performance improvements in terms of "equal error rates (EER)" and DET curves against various synthesis and replay attacks [10].

With the significant rise in cybercrimes, it has become even more important to deploy a trusted user authentication system for both private data security and access control. For both public and personal use, biometric characteristics of humans like fingerprint, face, voice, iris, signature, etc. provide reliable security for both public and personal use. Alsaadi (2015) briefly discusses "psychological biometric authentication" systems. In addition, the author also explores the pros, cons, and future scope of each technique.

Abozaid et al. (2019) have proposed an efficient "multimodal biometric identification" technique for designing biometric authentication systems on the basis of combination of voice and face recognition. They used "statistical coefficients" and "cepstral coefficients" to extract voice recognition features and compared them. They also used various "Principal Component Analysis (PCA)" and "Eigenface" extraction techniques for facial recognition and compared the results. They used ANN, SVM, and GMM machine learning models for face and voice identification modality. They found better results

with "statistical and cepstral coefficients" in voice recognition, and SVM and Eigenface tests in case of facial detection [12].

Bhattacharyya et al. (2009) have reviewed the biometric authentication frameworks and some possibilities in future. They have depicted the current status of biometrics in security. They have also given suggestions on the use of biometric security, compared various techniques and their pros and cons [13]. Tresadern et al. (2012) have proposed the "Mobile Biometrics (MoBio)" framework which combines voice and face detection in real-time to secure personal data better and provide better accessibility to data stored in mobile devices [14].

1.3 Research Gap. These days, a lot of developed and developing countries have adopted biometric authentication for theft prevention and national security. Hence, biometrics play a vital role in security-related use cases like forensic investigation, identity theft prevention, terrorist activity detection, physical and logical access control, and IT security. A lot of biometric authentication methods are proposed to identify users with hand gestures, fingerprint, signature, face, voice, etc. or by combining such patterns. Various researchers have proposed, deployed, reviewed, and tested novel biometric techniques and algorithms over the past few years. Hence, this paper is 4 aimed to evaluate the use of voice and face recognition along with their positive and negative points for biometric authentication [11].

1.4 Research Question

- What are the use cases and pros and cons of facial recognition for biometric authentication?

- What are the use cases and pros and cons of voice recognition for biometric authentication?

1.5 Research Objectives

- To explore the use cases and pros and cons of voice recognition for biometric authentication.

- To explore the use cases and pros and cons of face recognition for biometric authentication.

2. Research Methodology

To fulfil above research objectives, this study is based on secondary data collected from various sources like research papers, journals, articles, and other relevant online sources.

3. Analysis of Study

Biometrics are helpful to authenticate and identify an individual with a set of verifiable, recognizable, specific and unique data of an individual. Biometric identification answers "who are you?" and authentication proves "you are really who you say you are." A face is captured by 2D/3D scanner for facial biometrics. It is then transformed into digital data with an algorithm before comparing the captured image to the images in the database.

These automated systems can check or identify the identity of a person within seconds on the basis of their facial geometry. Such as bridge of the nose, spacing of eyes, contour of ears, lips, and chin, etc. It can be made possible even on the ground in unstable and dynamic environments. Facial recognition was first introduced in the iPhone X in the smartphone industry. There are also other signatures used for authentication via the human body, such as iris scans, fingerprints, digitization of veins in the palm, voice recognition, etc. This article is focused on facial and voice recognition.

3.1. What are the use cases and pros and cons of facial recognition for biometric authentication?

Facial recognition refers to verification and identification of a person with facial structure. It can detect and locate faces in videos and images. It transforms analog details of a face into digital data or vectors as per facial features of an individual. It is known to be the most natural form of all biometric measurements. A lot of tech giants are looking for the top spot in biometric innovation like Apple, Google, Microsoft, and Amazon. They constantly publish their discoveries in AI, face detection, and image recognition. Here are some of the emerging facial recognition technologies.

- **Academia** The Chinese University based in Hong Kong developed the "GaussianFace" algorithm in 2014 with 98.52% accuracy in facial identification, while humans achieved 97.53%.

● **Google and Facebook.** Facebook introduced its official "DeepFace" algorithm in 2014 to determine whether faces in two photographs belong to the same person and scored 97.25% in accuracy. On the other hand, humans are merely 0.28% better than this program. Google also introduced the FaceNet program in June 2015 and it achieved 99.63% accuracy in the "Labelled Faces in the Wild (LFW)" dataset [15].

● **IBM, Microsoft and Megvii.** According to a study by researchers in the Massachusetts Institute of Technology on February 2018, error rates were higher in "FACE++" tools developed by IBM, Microsoft, and Chinese giant Megvii to identify darker-skin women in comparison to men with lighter skin [16].

● **Amazon.** Amazon is promoting its cloud-based service for facial recognition "Rekognition" to law enforcement, according to a report in May 2018 [17]. It could recognize up to 100 people in an image and match faces against databases with tens of millions of facial records.

3.1.1. Facial Recognition Use Cases. Facial recognition is widely used in different industries in this day and age. But it plays a vital role in these segments.

● **Law Enforcement.** Facial recognition is widely used by law enforcement agencies, given increasing crime rate and terrorism. Prevention and detection of crime are some of the major benefits of facial recognition systems.

Source – Thales (2021) [18].

Figure 1. An Illustration of Automated Biometric Identification Systems (ABIS) used by Forensic experts to analyse several biometrics.

Facial recognition is very helpful in issuing identity credentials, border checks, police check posts, and improving public security missions like finding disoriented adults and missing children, finding and identification of abused children, tracking and identifying criminals, and supporting investigations.

● **Healthcare.** Thanks to deep learning, various advancements have been made in this industry. It is now possible to use face recognition in detecting genetic diseases with 96.6% of success rate like DiGeorge syndrome, and track the use of medication by patients more accurately [19].

● **Retail and Banking.** It is definitely the most important and underrated domain for using facial recognition. Facial recognition has made KYC easier for banking in 2021 (Thales). In Q2 2020, 64% of "primary checking accounts" were opened online and 36% of those accounts were opened in US branches of Bank of America and Chase, probably because a lot of branches were temporarily closed due to pandemic [20].

3.1.2. Pros and Cons. Considering the above arguments, here are some of the pros and cons of facial recognition

Pros

● It is one of the most convenient technologies for biometric authentication. It takes less friction in the device's camera as compared to authentication code or fingerprint scan.

● A lot of mobile devices have facial recognition as default features. So, it takes very little setup.

● Facial recognition is widely used in various industries like retail, banking, law enforcement, and healthcare for its several benefits.

Cons

● Default solutions are not at all effective as proprietary or third-party solutions.

● All facial recognition systems are not foolproof as hackers can easily spoof some of them.

● Users have to blink, move their head, or perform certain actions for verification due to "active liveness detection" in facial recognition. An

attacker can circumvent and analyse this process.

P. S. Liveness detection is a process to combat spoofed biometric information, i.e., to ensure that biometric data is obtained from a live human instead of an algorithm or machine (like deep fakes), and it also needs liveness test.

3.2. What are the use cases and pros and cons of voice recognition for biometric authentication?

Voice biometrics are more accurate and faster than ever thanks to significant advances in neural networks. These systems can access larger use cases and identify a person with less speech samples. Biometric voice recognition is expected to grow up to US$3.9 billion mark by 2026 from $1.1 billion in the year 2020 at a CAGR of 22.8%, according to a 279 pages' report by Voice Biometrics Market (2021). According to a four years' forecast by Mordor Intelligence, device interactions have been limited in the finance sector because of poor security features and there is a 269% rise in fraud attacks against them, which is significantly higher than other industries. Hence, financial institutions might use voice recognition along with other speech recognition options in a few years to come. Voice biometric recognition inputs individuals' voices to store in the database. It is stored as a print for verification. The software can split voice into several frequencies to make input print. At this stage, behavioural attributes are recognized which work together to create voice print.

3.2.1. Use Cases of voice recognition. There are multiple use cases of voice recognition for biometric authentication.

- **Fraud Detection.** Voice recognition is a very powerful tool for fraud detection. Multi-factor authentication is widely used to avoid unauthorised access to financial resources or client data with the prevalence of identity theft. Voice biometrics provide spoof-resistant, safe authentication.

- **Contact centre.** It is probably the most widespread application of speech recognition. It bypasses the most tiresome questions at the beginning of every interaction from the customer. Voice is used to authenticate and verify callers to save effort and time for both the agent and consumers.

- **Financial services.** The financial services market across the world

has witnessed great changes over the years. Fintech and mobile banking has made consumers' lives easier. But security risks are also on the rise. Voice biometrics are processing thousands of verifications every day in several languages.

● **Digital signatures.** Voice biometrics can create voice signatures which make life insurance and other underwriting documents the legally binding contracts. Voice signatures are also used to authorise financial transactions.

● **Team Management.** Voice biometrics is used in workforce management, which is very common. Speech verification is a safe alternative to badge systems for large workforce in an organisation.

3.2.2. Pros and Cons of Voice Recognition

Pros

● **Minimal operation costs.** Banks and call centres can use voice recognition to save money. They can save millions of dollars by saving a lot of steps needed in previous verification methods. It can detect a consumer's voice to verify their identity in end-to-end chat without any inquiries.

● **Better user experience.** It is another major benefit of voice recognition which is usually overlooked. There is no need to offer PINs, passwords, or answer tedious questions for verification. This way, speech recognition is ideal for multichannel and omnichannel strategies.

● **Accuracy.** Voice recognition is more trusted and accurate as compared to passwords, which are easy to modify, forget, or guess. One cannot reproduce or forget voice. It is a lot more convenient and reliable.

● **Easy implementation.** It is easy to implement in businesses without additional systems or equipment as they have small requirements.

Cons

Though there are some benefits, voice recognition has some disadvantages which can pose limitations or security risks for user experience.

● Any change in voice may deny access. Users who used face recognition to unlock devices may have learned that simple methods like wearing masks

during the pandemic may affect their access. In addition, authentication may be affected when there is loud music or noise in the background. Minor changes in speech patterns, accent or voice, sore throats, colds, and other common incidents may affect authentication.

- There are several new tools that can mimic voices and manipulate biometric data. Voice deep fakes are a more important concern and it is subject to more advancements to stay ahead of such practices.

- Voice recognition is quite easier to spoof than other methods for biometric authentication. So, liveness detection is needed to verify the actual user and ensure that it is not a spoof.

4. Results

This article has discussed facial and voice recognition as physical biometric authentication technologies. Face, fingerprints, voice, DNA, etc. are unique features of humans. These characteristics can become the data which AI can analyse and compare for authentication against the database. Facial recognition is one of the most popular use cases where researchers can make the most out of machine learning and AI. AI can be used widely with AR solutions for facial recognition by analysing facial geometry and matching the same against a database. Human programming cannot always improve efficiency and accuracy of biometric authentication, which are the major security concerns these days. These systems can be made more efficient and secure only with machine learning and artificial intelligence.

Behavioural biometric security is another interesting AI trend which uses unique characteristics of human behaviour on the way people interact with the environments, things that they may not even realise on themselves. It is another great layer of security against deep fake attempts. Keystroke movement, mouse activity, motion of mobile devices, and touch screen pressure, area, and press size are some of the most common ways for behavioural biometrics measurement.

BeCAPTCHA is one of the best examples of behavioural biometrics for bot detection, developed by the "Biometrics and Data Pattern Analytics Lab" at the "Autonomous University of Madrid" [21]. Behavioural biometrics can be used widely without letting the user know and save them from annoying tests

to prove that they are human, for example CAPTCHA tests, which have been prevalent for decades. Users may never need to click on palm trees, crosswalks, taxis, traffic lights, etc. to prove again and again that they are not a robot while browsing the web in a few years to come.

Behavioural biometrics can make such tasks a history and secure the entire session. Currently, if a user signs in and leaves the room suddenly out of some work, they unknowingly leave an unauthorised user with full access to their computer. It poses a serious risk to security. With behavioural biometrics, it cannot be possible. Computers could detect irregular usage patterns of another user and dynamically limit their access.

5. Conclusion

Though a high amount of security is provided with biometric authentication, there is still a long road to go. There are pros and cons of every form of biometrics technology. All of them are not effective across the world. Security is something which shouldn't be taken lightly. When private and sensitive data is at stake like institutional data, user data, and patient health records, it is very vital to take strict measures against security breaches. Failure in keeping security around that data can cause fraud which can cost hundreds or tens of millions to the businesses. Emerging biometric authentication technologies must be powered by machine learning and AI to stay ahead of time. They usually need experts to integrate the same with current systems.

References

[1] IBM Security Cost of a Data Breach Report, Available at (2021), https://www.ibm.com/downloads/cas/OJDVQGRY.

[2] What is Biometric Authentication? Use Cases, Pros and Cons | OneSpan. Retrieved 19 April (2022), from https://www.onespan.com/topics/biometric-authentication.

[3] J. Gregory, The Post-Quantum Cryptography World Is Coming: Here's How to Prepare, Security Intelligence, Retrieved 19 April (2021), from https://securityintelligence.com/articles/post-quantum-cryptography-how-to-prepare/.

[4] J. A. Sava, Global biometrics system market revenue 2025 | Statista, Retrieved 19 April (2022) from https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/.

[5] S. Maksymenko, Face Recognition App Development Using Deep Learning - MobiDev. Retrieved 19 April (2021), from https://mobidev.biz/blog/custom-face-detection-recognition-software-development.

[6] S. Maksymenko, Face anti-spoofing techniques for liveness detection in security systems, Retrieved 19 April (2022), from https://mobidev.biz/blog/face-anti-spoofing-prevent-fake-biometric-detection.

[7] L. S. Vailshery, Global voice recognition market 2026 | Statista, Retrieved 19 April (2022), from https://www.statista.com/statistics/1133875/global-voice-recognition-market-size/.

[8] J. Vincent, This is what a deep fake voice clone used in a failed fraud attempt sounds like, The Verge. Retrieved 19 April (2020), from https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos.

[9] E. Krasnokutsky, TOP 9 Machine Learning Technology Trends To Impact Business in Retrieved 19 April (2022), from https://mobidev.biz/blog/future-machine-learning-trends-impact-business.

[10] G. Chetty and M. Wagner, Multi-level liveness verification for face-voice biometric authentication, In 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference IEEE (2006, September), (pp. 1-6).

[11] I. M. Alsaadi, Physiological biometric authentication systems, advantages, disadvantages and future development: A review, International Journal of Scientific and Technology Research 4(12) (2015), 285-289.

[12] A. Abozaid, A. Haggag, H. Kasban and M. Eltokhy, Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion, Multimedia Tools and Applications 78(12) (2019), 16345-16361.

[13] D. Bhattacharyya, R. Ranjan, F. Alisherov and M. Choi, Biometric authentication: A review, International Journal of *u*-and e-Service, Science and Technology 2(3) (2009), 13-28.

[14] P. Tresadern, C. McCool, N. Poh, P. Matejka, A. Hadid, C. Levy and S. Marcel, Mobile biometrics (mobio): Joint face and voice verification for a mobile platform, IEEE pervasive computing 99 (2012).

[15] F. Schroff, D. Kalenichenko and J. Philbin, Facenet: A unified embedding for face recognition and clustering, In Proceedings of the IEEE conference on computer vision and pattern recognition (2015), 815-823.

[16] L. Hardesty, Study finds gender and skin-type bias in commercial artificial-intelligence systems, Retrieved April 3 (2018), 2019.

[17] D. Goodin, Police use of Amazon's face-recognition service draws privacy warnings. Retrieved 23 (2018) April 2022, from https://arstechnica.com/tech-policy/2018/05/police-use-of-amazons-face-recognition-service-draws-privacy-warnings/

[18] Thales, Facial recognition: top 7 trends (tech, vendors, use cases), Retrieved 23 (2021). April 2022, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

[19] P. Kruszka, Y. A. Addissie, D. E. McGinn, A. R. Porras, E. Biggs, M. Share and M. Muenke, 22q11. 2 deletion syndrome in diverse populations, American Journal of Medical Genetics Part A, 173(4) (2017), 879-888.

[20] R. Shevlin, Digital Account Openings Surged Long Before The Pandemic [Thanks To Bank of America and Chase], (2020) Retrieved 23 April 2022, from https://www.forbes.com/sites/ronshevlin/2020/09/21/new-consumer-research-finds-consumers-open-more-checking-accounts-digitally-than-in-branches/?sh=280dba5222af.

[21] A. Acien, A. Morales, J. Fierrez and R. Vera-Rodriguez, BeCAPTCHA-Mouse: Synthetic mouse trajectories and improved bot detection, Pattern Recognition 127 (2022), 108643.

[22] Prateek Agrawal, Ranjit Kaur, Vishu Madaan, Sunil Babu Mukkelli and Dimple Sethi, Moving object detection and recognition using optical flow and eigen face using low resolution video, Recent Advances in Computer Science and Communications 13(6) (2020), 1180-1187. doi:10.2174/2213275911666181119112315

[23] Tiyasa Chakraborty, Sanjay Kumar Singh, Prateek Agrawal and Saruchi, An Efficient ANN based Human-Machine Interaction through Voice Command Recognition using Bengali Language, IEMCONGRESS, KolKata, India (2013), 23-25.

[24] D. Virmani, C. Gupta, P. Bamdev and P. Jain iSeePlus: A cost effective smart assistance archetype based on deep learning model for visually impaired, Journal of Information and Optimization Sciences 41(7) (2020), 1741-56.