03-SRJ-486-149

SIAZGA RESEARCH JOURNAL, 2025
Vol. 04 | No. 04 | December - 2025 | 222 – 230
DOI: https://doi.org/10.5281/zenodo.18380777

Original Article

A Comparative Analysis of Biometric Security Techniques: Evaluating Contact Touch-Based and Touch Less Biometric Techniques

Hina Ali* & Dr. Din Muhammad Sangrasi

[1] *Department of Software Engineering, Mehran University of Engineering and Technology, Hyderabad, Pakistan*

Abstract

The increasing rise in electronic crimes has underlined the critical need for strong authentication techniques that enforce strict access control and data protection. Biometric authentication is a potential method that uses distinct physiological (like palm, eye retina, fingerprints etc.) and behavioral (like signature, keystroke etc.) traits for identity verification. This research compares touch based versus touch less biometric systems, focusing on performance, accuracy, and user acceptability. Addressing a gap in existing security standards, the study investigates the rising move towards touch less biometric driven by the desire to avoid physical contact and disease transmission. The research findings provide light on the potential of touch less technology to provide a more sanitary and dependable alternative to traditional procedures, with implications for wider adoption across a variety of sectors.

Keywords: *Touch based and touches less biometric, biometric techniques, Physiological bio-metrics, Behavioral bio-metrics, Biometric Security, Identifiers Covid-19*

How to cite:
Ali, H., & Sangrasi, D. M. (2025). A Comparative Analysis of Biometric Security Techniques: Evaluating Contact Touch-Based and Touch Less Biometric Techniques. *Siazga Research Journal, 4*(4), 222–230.
https://doi.org/10.5281/zenodo.18380777

INTRODUCTION

Now a day's biometric systems are gradually gaining recognition as a technical tool for a variety of applications, including organizational security, data protection, and attendance tracking, among others [1,2]. It is also clear that securing data, information, and organizations is critical across all four generations [3-5]. Initially, security approaches were significantly different from those utilized when technology is incorporated in the security process. Passwords, patterns, and biometric access are some of the technical security mechanisms now in use [6, 7]. Biometrics is the practice of examining and comparing an individual's unique physiological patterns in a way to correctly identify the human . Not all physical traits are important to this goal [8–9]. The intrinsic desired in biometrics relies on the application and includes uniqueness, measurability, acceptability, universality, stability, efficiency, and imperviousness [10, 11].

Biometric technology is among latest rapid growing technology in which human traits such as faces, fingerprints, palms, retina, and iris scans are employed for data collection, security, data access etc [12, 13]. Biometrics, despite its vast scope, is not a new topic, and technological advancements have aided in its use. For example, early identification was done using thumb imprints, which were inked and recognized using a magnifying lens [14, 15]. Biometric technology is classified into two categories: behavioral and physiological biometrics [16, 17]. Figure 1 depicts many kinds of biometric technology.

*Corresponding Author: Hina Ali | Mehran University of Engineering and Technology, Jamshoro, Pakistan
Hinaabdullah04@gmail.com

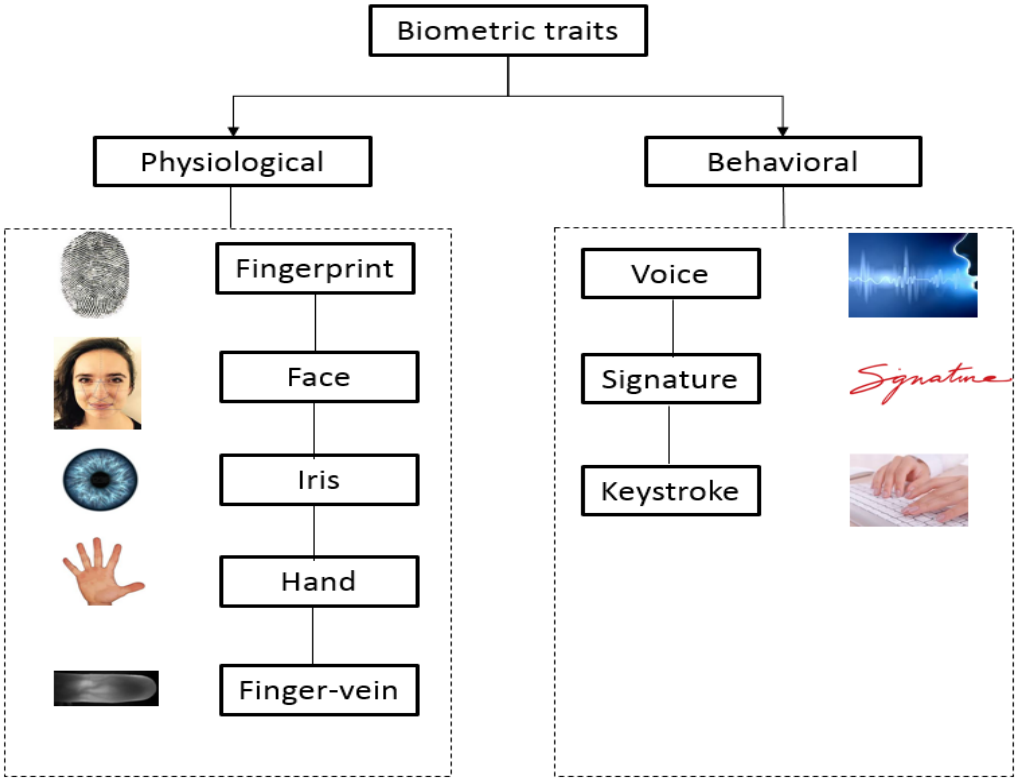

Fig.1 Categories of biometric security

2. LITERATURE REVIEW

Biometric securities have advanced significantly in recent years, notably in terms of touch based and touch less modality. Touched biometric systems, such as fingerprint and palm print identification, have been widely researched for their dependability and broad use [30-39]. However, issues remain in terms of sanitation and vulnerability to spoofing attacks. Recent research has looked into the integration of behavioral biometrics, such as touch dynamics, to improve security. For example, Dave et al. [51] suggested a touch-movement-based continuous authentication schema that uses machine learning techniques and showed promising results in user verification.

In contrast, touches less biometric systems have grown in popularity, particularly in light of the COVID-19 epidemic, which highlighted the necessity for contactless alternatives. Advances in deep learning have accelerated the development of contactless fingerprint identification technologies. Chowdhury and Imtiaz [52] performed a thorough evaluation to demonstrate the effectiveness of deep learning algorithms in improving the accuracy of contactless fingerprint recognition. Furthermore, the incorporation of face recognition technology into businesses such as the UAE oil and gas sector demonstrates the practical uses and advantages of touch less biometrics in improving security measures [1-5][40-45].

However, the uses of touch less technologies have raised questions about data security and privacy. The idea of inverse biometrics, where biometric templates might possibly be recreated, offers major privacy dangers, needing strong encryption and data security methods [45-55].

2. METHODOLOGY

This study adopts a systematic approach, beginning with a thorough literature review to gain insight into the current state of biometric technology, with an emphasis on both physiological and behavioral sent status of biometric technology, with an emphasis on both touch based and touch less biometrics. The evaluation draws on trustworthy sources to in–vestigate the effectiveness, accuracy, and user acceptance of various technologies. Following the literature study, a comparison analysis is performed, with particular qualities chosen from each area. Furthermore, the study examines how different health and hygeine factors impacts the adoption of biometric technology, specifically the shift of biometric security system from touch based to t touch less systems . This component entails recognizing new trends and evaluating the possibility of touch less biometrics to reduce

disease transmission while maintaining strong security for different purposes.

BEHAVIORAL BIOMETRIC

Behavioral biometrics may be characterized more specifically as the utilization of human actions such as how someone walks, types, and signs. The behavioral patterns of human are not fixed they can be change with time of condition [18]. Biometrics based on behaviors gained popularity with the emergence of the pandemic owing to the requirement for touch less systems [19, 20]. Since 2019, behavioral biometrics has gained popularity, and many academics are researching on these technologies. The fact that users do not need to make contact with the biometric device to use it, which prevents the spread of infectious illnesses, is the primary driver of this acceptance [21].

3.1 One Signature

It is worth noting that signatures are quite common as biometric signatures. Automated biographical signatures, that is, the signature can analyse numerous distinguishing factors such as strokes, pressure, and other writing characteristics. [22]

3. 2 Gait Recognition

It is noteworthy to note, however, that each individual has a unique walking style. Gait recognition is not actively used owing to issues such as the need for huge datasets, less convenient patterns, and so on; nonetheless, the research is still ongoing [23-25].

3.3 Keystroke Dynamics

Keystroke dynamics are primarily concerned with the behavior of a person using a keyboard. While this approach is new in biometric security, research is ongoing in this area [26].

3.4 Voice

Every person has a unique and distinct voice, which includes characteristics such as frequency, harmonic richness, and intensity [1, 3]. Other characteristics distinguish them, such as language, accent, method of speech, and even tempo. In speech recognition systems, for example, the human voice is often converted from analogue to digital form and then evaluated as a pattern or a piece of text with the goal of identifying [4]. Behavioral biometrics refers to human behavioral characteristics such as movement, walking, keyboard, signature, and so on [12]. Figure 2 illustrates the voice recognition method.

3.5 Handwriting

This is also known as behavioral biometrics, as it captures handwriting-related characteristics. Because we all write differently, handwriting may easily be utilized to authenticate persons.

4. PHYSIOLOGICAL BIOMETRIC

Physiological biometrics is the utilization of physical characteristics of the human body, such as vivid iris and retina, face recognition, fingerprints, and palm prints [26–27]. Physiological patterns of human are fixed and unique. In Physiological biometric category some features can be used as touched biometric like finger print and some can be used as touch less like eye retina, face recognition etc.

4.1 Eye Retina and iris of human eye

Biometrics uses nerve patterns in the back of the eye, known as the retina, where as the colored area of the eye is known as the iris. Figure 3 illustrates the anatomy of the human eye. Everyone has a unique arrangement of blood vessels in their eye retina, retinal identification is extremely accurate and impossible to falsify.

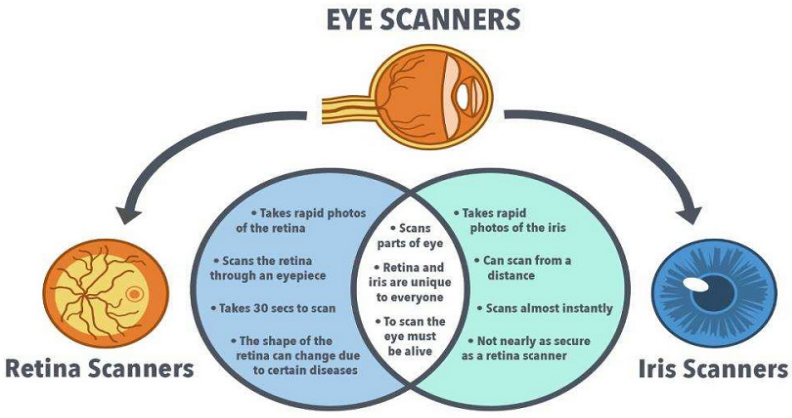

Fig. 2. Eye retina and iris scan of human eye

4.2 Fingerprint for Biometric

Finger print identification is one of oldest biometric authentication method, even this method was used before invention of technology. Fingerprint identification is one of the most widely utilized authentication systems today, with applications ranging from commercial, civil, and forensic [28]. Over the last decade, research on fingerprint-based identifying systems has gotten extremely accurate. In this method front part of the human finger is used for unique identification. Front part of human finger print is collectively referred to as minutiae include ridges, bridges, loops, and more. Figure 3 (a, b) explains the fingerprint minutiae.

Fig. 3(a). Fingerprint detailed minutiae

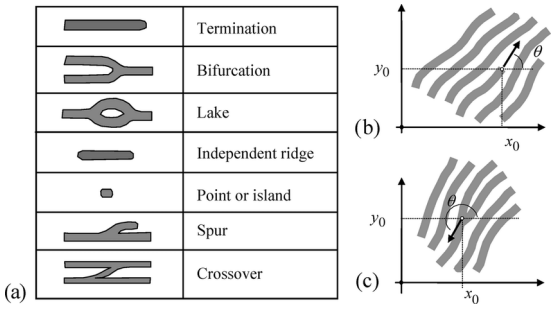

Fig. 3(b). Fingerprint detailed minutiae

4.3 Face recognition

The face recognition technique is a popular biometric approach that uses facial traits to identify people. This procedure is rather affordable [29].In this method face geometry is captured for identification and authentication purpose. This method is touch less biometric security method

4.4 Palm recognition

Palm recognition is touched and a physiological kind of biometrics. This approach detects a person by focusing on their palm. Aside from the four principal applications of the palm listed above, other areas include pores, lines, and ridges [3]. Figure 7 depicts several parts of the palm.

- i. Interdigital: The upper limb's extremity, also known as the hand's outermost or terminal limb.
- ii. Hypothenar: This is by far the largest portion of the palm and is found where the fingers are arranged.
- iii. Thenar: This is the region near the thumb of the palm but on the rim.
- iv. Principle. Lines: These are the palm's prominent or big lines. Palm recognition is a physiological approach of biometric security.

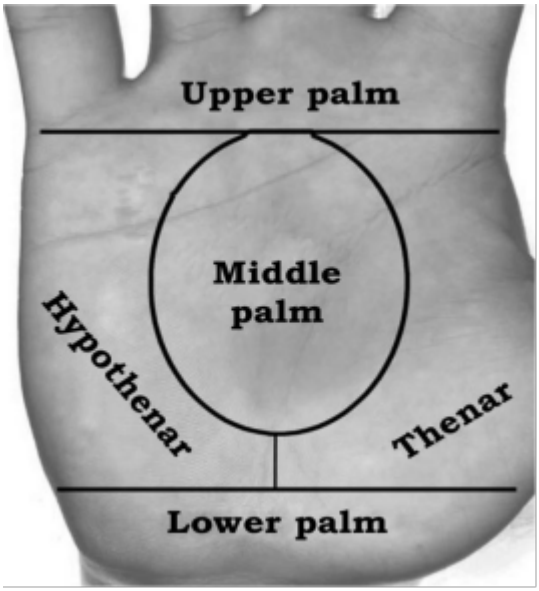

Fig. 4. Human Hand Palm

TOUCH BASED BIOMETRIC TECHNIQUES

Touch based biometric systems needs physical touch with the sensor/device like finger print, palm scanner etc. These systems are bit slower due to physical contact process. By using these systems user can feel intrusive or inconvenient [13][44]. Although its performance and accuracy is high but may degrade with dirt, moisture, wear, latent prints or spoofing. Touch based systems can be easily installed in Offices, ATMs, door access, smart phones etc[1][2][46].

TOUCH LESS BIOMETRIC TECHNIQUES

These systems don't need any physical touch with sensors like Face recognition, iris scanning, voice recognition, and touch less fingerprinting .these systems are also good in accuracy but can be affected by environment factors like light etc [40-45].

COMPARISON BETWEEN TOUCH BASED AND TOUCH LESS BIOMETRIC TECHNIQUES

Touch based biometric like finger print, palm are still very old and widely used biometrics. According to many polls and estimates, fingerprints are the oldest and most widely used biometric technology. They are commonly utilized for a variety of purposes, including employer access to cash registers, ATMs, and purchase confirmation at many campus retailers [30, 31]. Figure 8 depicts a percentage-wise comparison of physiological biometrics.

Use of touch based biometrics like face recognition, speech recognition, eye retina etc is also increasing because of hygiene and health problems especially after pandemics of COVID 19. Face recognition is the most widely recognized type of biometric security technology, since it is used to open mobile applications and search the FBI database [32]. Corporations and government now regularly utilize pale and durable biometrics. For example, Wells Fargo has incorporated both iris scanning and face recognition into mobile banking. It is also used in healthcare to identify patients and their medical histories. Air travelers at major airports in the United States United Arab emirate also use speech recognition, eye retina, iris, and heartbeat readers. However, they are less commonly used due to features such as user friendliness, reduced cost, and simple installation [33].According to different survey reports and studies, the most commonly used type of touched biometrics is signature biometrics [34, 35]. For ages, signatures were used to authenticate papers, even in banking before technology was introduced. Some other touch less biometrics like vocal recognition and vocal pattern analysis are also on the rise [36–37].

Biometric security systems have quickly emerged as an essential component of modern identity verification processes, particularly in light of rising need for robust, user-friendly, and scalable authentication techniques. Touched biometric systems—such as fingerprint identification, palm vein scanning, and hand geometry—have long been regarded as the gold standard in many industries because to their maturity, cost-effectiveness, and consistent performance under controlled settings [41], [42]. Fingerprint identification, in particular, is one of

the most widely used modalities worldwide due to its simplicity of acquisition and uniqueness [43]. However, research has discovered several downsides. Physical contact not only creates hygiene problems, particularly after COVID-19 [44], but also causes sensor wear and impaired effectiveness in the presence of dirt, dampness, or injuries [45]. Furthermore, many commercial systems face unsolved issues with attackers or hackers such latent fingerprint recovery and spoofing [46].

On other hand touch less biometric technologies, have grown in popularity due to their non-contact and more sanitary nature. Facial recognition, iris scanning, and speech recognition are becoming increasingly used in high-security situations such as airports, hospitals, and cell phones [47], [48]. Recent improvements in machine learning and computer vision have considerably increased the accuracy and resilience of these systems, even in uncontrolled environments [49]. Nonetheless, touch less systems encounter environmental obstacles such as illumination sensitivity (for facial and iris detection), occlusions (e.g., masks or sunglasses), and background noise (for speech recognition) [50]. Following is detailed features based comparison between touch less and touch based biometrics systems [58].

Table:1

Features based comparison between touch less and touch based biometric systems.

Features	Touch based Biometric	Touch less Biometric
Definition	Needs physical touch with the sensor/device. Physical touch is not required; instead	Proximity or picture capture is used. [55]
Examples	Fingerprint scanners, palm reader	Face recognition, iris scanning, voice recognition, and touchless fingerprinting.[51]
Hygiene	Less hygienic – germ transmission is easy.	More hygienic – no contact needed.[23,33]
Speed	Slightly slower due to physical contact process.	Generally faster, especially in high-throughput environments.[54][45]
User Experience	Can feel intrusive or inconvenient.	More convenient and user-friendly.[39]
Environmental Limitations	Performance can be reduced because of dirt, moisture.	Affected by lighting (for face/iris), ambient noise (voice).[40]
Accuracy	High accuracy under controlled conditions.	High accuracy, but may suffer under poor conditions (e.g., lighting).[43]
Security	Vulnerable to latent prints or spoofing (if not aliveness-aware).	latest systems may include aliveness detection (e.g., blinking in face ID).[47]
Finance	Installation cost is low , generally.	Its installation cost is higher because of advanced sensors/cameras.[42]
Use Cases	Offices, ATMs, door access, smart phones.	Airports, smart phones (Face ID), healthcare, border control.[41,42]

Still usage of touch based is higher than usage of touch less biometric systems. Here is a pie chart showing the estimated global usage distribution of touched (60%) vs. touch less (40%) biometric technologies, based on industry trends and recent research insights[56][55].

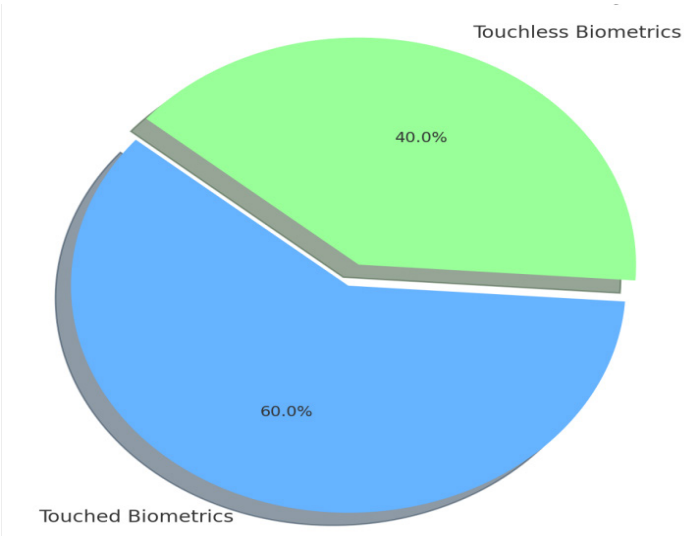

Fig.5. pie chart of touch based and touch less

CONCLUSION

Biometric authentication systems may be classified into physiological and behavioral categories, as well as touch-based and touch-less biometric techniques. Physiological biometric features, like iris, palm, finger print, facial features etc, are based on stable and distinct bodily characteristics that provide high accuracy and long-term dependability. Whereas behavioral biometrics, such as speech patterns, keyboard dynamics, and gait, analyses behaviors that may change over time yet nonetheless allow for ongoing and adaptive verification. Touch-based systems need physical contact with a sensor, which might be impractical in terms of hygiene and convenience, particularly in public or hospital environments. Touch less biometric techniques, like face or iris recognition; improve the user experience by allowing for quick, contact-free interaction, making them more popular in current security situations. The decision to choose between these biometric techniques is determined by application requirements, environmental conditions, and acceptance among users, with new trends leading to the integration of various biometric modalities for increased robustness and usability.

Competing Interests

The authors did not declare any competing interest.

References

[1] S. Anthony, "No Title Berkeley researchers replace passwords with past thoughts by reading your mind," 2013. [Online]. Available: www.extremetech.com/computing/152827-berkeley-researchers-authenticate-your-identity-with-just-your-brainwaves-replace-passwords-with-passthoughts.

[10] S. H. Halili, "Technological advancements in education 4.0," Online J. Distance Educ. E-Learn., vol. 7, no. 1, pp. 63–69, 2019.

[11] M. Hampson, "The bioacoustic signatures of our bodies can reveal our identities," 2019. [Online]. Available: spectrum.ieee.org/the-human-os/telecom/security/the-bioacoustic-signatures-of-our-bodies-can-reveal-our-identities.

[12] C. Burt, "New technologies for finger vein, voice, and facial biometrics unveiled," 2019. [Online]. Available: www.biometricupdate.com/201908/new-technologies-for-finger-vein-voice-and-facial-biometrics-unveiled.

[13] C. Buttle, "The problem of biometrics in education," Biometric Technol. Today, vol. 2013, no. 6, pp. 5–7. [Online]. Available: www.sciencedirect.com/science/article/abs/pii/S0969476513701115.

[14] T. Arakawa, "Ear acoustic authentication technology: using sound to identify the distinctive shape of the ear canal," 2018. [Online]. Available: www.nec.com/en/global/techrep/journal/g18/n02/180219.html.

[15] J. Aron, "Your heartbeat could keep your data safe," 2012. [Online]. Available: www.newscientist.com/article/mg21328516.500-your-heartbeat-could-keep-your-%0Adata-safe/%0A.

[16] S. A. Abdulrahman and B. Alhayani, "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics," Mater. Today: Proc., vol. 80, pp. 2642–2646, 2023.

[17] P. Martinez-Lozano, M. Kohler, and R. Zenobi, "Human breath analysis may support the existence of individual metabolic phenotypes," PLoS ONE, vol. 8, no. 4, p. e59909, 2018.

[18] G. A. Dafoulas, C. C. Maia, J. S. Clarke, A. Ali, and J. Augusto, "Investigating the role of biometrics in education—the use of sensor data in collaborative learning," in Int. Conf. e-Learning, pp. 115–123, 2018.

[19] Y. Gao, W. Wang, V. Phoha, W. Sun, and Z. Jin, "EarEcho," in ACM Interact., Mobile, Wearable Ubiquitous Technol., p. 1, 2019.

[2] C. Burt, "Biometric ear canal geometry recognition developed by University of Buffalo researchers," 2019. [Online]. Available: www.biometricupdate.com/201909/biometric-ear-canal-geometry-recognition-developed-by-university-of-buffalo-researchers.

[20] F. Jan, S. Alrashed, and N. Min-Allah, "Iris segmentation for non-ideal iris biometric systems," Multimedia Tools Appl., vol. 83, no. 5, pp. 15223–15251, 2024.

[21] S. Baird, "Biometrics 'security technology': it is important for students to understand that technology can be used as part of a solution to a problem," Technol. Teach., vol. 61, no. 5, pp. 18–23, 2002.

[22] J. Lee, "Researcher says brainwaves could be a way for security systems to verify identity," 2015. [Online]. Available: http://www.biometricupdate.com/201505/researcher-

says-brainwaves-could-be-a-way-for-security-systems-to-verify-identity.

[23] S. J. Elliott, J. L. Peters, and T. J. Rishel, "An introduction to biometrics technology: its place in technology education," J. Ind. Teach. Educ., vol. 41, no. 4, pp. 1–8, 2004.

[24] R. Ferguson, "Learning analytics: drivers, developments and challenges," Int. J. Technol. Enhanced Learn., vol. 4, no. 5/6, pp. 304–317, 2012.

[25] K. Yang, Y. Dou, S. Lv, F. Zhang, and Q. Lv, "Relative distance features for gait recognition with Kinect," J. Vis. Commun. Image Represent., vol. 39, pp. 209–217, 2016.

[26] "Ears: the new fingerprints?," Yale Scientific, 2011. [Online]. Available: www.yalescientific.org/2011/05/ears-the-new-fingerprints.

[27] K. H. Kim, S. W. Bang, and S. R. Kim, "Emotion recognition system using short-term monitoring of physiological signals," Med. Biol. Eng. Comput., vol. 42, no. 3, pp. 419–427, 2004.

[28] T. D. Jager, "Application of biometric fingerprinting to encourage the active involvement of student teachers in lectures on differentiated instruction," South Afr. J. Educ., vol. 39, no. 2, pp. 1–11, 2019.

[29] R. King, "Explainer: Facial thermography," 2013. [Online]. Available: www.biometricupdate.com/201308/explainer-facial-thermography.

[3] J. Sim, H. Noh, W. Goo, N. Kim, S. Chae, and C. Ahn, "Identity recognition based on bioacoustics of the human body," IEEE Trans. Cybern., pp. 1–12, 2019.

[30] S. L. Gray, "Biometrics in schools: the role of authentic and inauthentic social transactions," UCL Inst. Educ. [Online]. Available: discovery.ucl.ac.uk/id/eprint/1545213/3/Leaton_Gray_Biometrics_BSA_conference.pdf.

[31] M. Mufandaidza, T. Ramotsoela, and G. Hancke, "Continuous user authentication in smartphones using gait analysis," in 44th Annu. Conf. IEEE Ind. Electron. Soc., 2018.

[32] Z. Korotkaya, "Biometric person authentication: odor," Dept. Inf. Technol., Lab. Appl. Math., Lappeenranta Univ. Technol., 2003.

[33] M. O. Krucoff, S. Rahimpour, M. W. Slutzky, E. V. Reggie, and D. A. Turner, "Enhancing nervous system recovery through neurobiologics, neural interface training, and neurorehabilitation, neuroprosthetics," Front. Neurosci., vol. 10, p. 584, 2016.

[34] B. Hond, "Your brain's unique response to words can reveal your identity," 2015. [Online]. Available: www.newscientist.com/article/dn27555-your-brains-unique-response-to-words-can-reveal-your-identity.

[35] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen, "A robust and reusable ECG-based authentication and data encryption scheme for eHealth systems," in 2016 IEEE Glob. Comm. Conf., pp. 1–6.

[36] B. Grawemeyer, M. Mavrikis, W. Holmes, W. Gutierrez-Santos, M. Wiedmann, and N. Rummel, "Affecting O-task behavior: how affect-aware feedback can improve student learning," in LAK, pp. 104–113, 2016.

[37] Dell Technologies Inc., "Gen Z is here. Are you ready?," 2020.

[38] B. Vincent, "The space agency announced several health and biotech technology transfer opportunities," 2020. [Online]. Available: https://www.nextgov.com/emerging-tech/2020/02/nasa-tech-could-replace-passwords-your-heartbeat/163292/.

[39] D. Thakkar, "Five unconventional biometrics that surprisingly exist!," 2018. [Online]. Available: https://www.bayometric.com/5-unconventional-biometrics/.

[4] "NEC develops biometrics technology that uses sound to distinguish individually unique ear cavity shape," 2016. [Online]. Available: www.nec.com/en/press/201603/global_20160307_01.html.

[40] Thales, "Biometrics: authentication and identification (definition, trends, use cases, laws and latest news)—2020 review," 2020. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[41] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition,* Springer, 2009.

[42] R. Cappelli, D. Maio, and D. Maltoni, "Performance evaluation of fingerprint verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 28, no. 1, pp. 3–18, Jan. 2006.

[43] A. K. Jain, Y. Chen, and M. Demirkus, "Pores

and ridges: High-resolution fingerprint matching using level 3 features," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 29, no. 1, pp. 15–27, Jan. 2007.

[44] T. Matsumoto et al., "Impact of artificial 'gummy' fingers on fingerprint systems," in *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275–289, 2002.

[45] Y. Wang, J. Liu, and H. Wang, "Touchless biometric systems: A review," *IEEE Access*, vol. 8, pp. 170350–170369, 2020.

[46] D. M. Gragnaniello et al., "Face anti-spoofing based on color texture analysis," in *Proc. IEEE Intl. Conf. Image Processing (ICIP)*, 2013, pp. 1952–1956.

[47] S. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2014, pp. 1701–1708.

[48] S. Furui, "50 years of progress in speech and speaker recognition research," *Ecti Transactions on Computer and Information Technology*, vol. 1, no. 2, pp. 64–74, Nov. 2005.

[49] C. Garvie, A. Bedoya, and A. Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology, 2016.

[5] U. Šošević, I. Milenković, M. Milovanović, and M. Minović, "Support platform for learning about multimodal biometrics," J. Univers. Comput. Sci., vol. 19, no. 11, pp. 1684–1700, 2013.

[50] A. Ross and A. Jain, "Multimodal biometrics: An overview," in *Proc. 12th European Signal Processing Conference*, Vienna, Austria, 2007

[51] R. Dave, N. Seliya, L. Pryor, M. Vanamala, E. Sowells, and J. Mallet, "Hold On and Swipe: A Touch-Movement Based Continuous Authentication Schema based on Machine Learning," arXiv preprint arXiv:2201.08564, Jan. 2022.arXiv

[52] A. M. M. Chowdhury and M. H. Imtiaz, "Contactless Fingerprint Recognition Using Deep Learning—A Systematic Review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 714–730, Sep. 2022.MDPI

[53] S. H. Al Zaabi and R. Zamri, "Managing Security Threats through Touchless Security Technologies: An Overview of the Integration of Facial Recognition Technology in the UAE Oil and Gas Industry," *Sustainability,* vol. 14, no. 22, p. 14915, Nov. 2022.MDPI

[54] M. Gomez-Barrero and J. Galbally, "Reversing the Irreversible: A Survey on Inverse Biometrics," arXiv preprint arXiv:2401.02861, Jan. 2024

[55] A. K. Jain et al., "An introduction to biometric recognition," *IEEE Trans. on Circuits and Systems for Video Technology,* 2004.

[56] Y. Wang et al., "Touchless biometric systems: A review," *IEEE Access*, vol. 8, pp. 170350–170369, 2020.

[57] A. M. Chowdhury and M. H. Imtiaz, "Contactless Fingerprint Recognition Using Deep Learning—A Systematic Review," *Journal of Cybersecurity and Privacy,* 2022.

[58] S. H. Al Zaabi and R. Zamri, "Managing Security with Face Recognition in the UAE Oil Sector," 2023.