Biometric Technology Today
ISSN (online): 1873-1880

Biometric Technologies in Dentistry: Applications, Advantages, and Ethical Safeguards

Chetnaya[1], Vipra*

[1] BDS, Desh Bahgat Dental College, Muktsar, Punjab, India

Email: sharma_2929@yahoo.com

* BDS, Genesis Institute of Dental Science and Research, Ferozepur, Punjab, India

Abstract

Biometric technologies are increasingly being integrated into dental practice, reflecting a wider trend in healthcare toward digital transformation and personalized care. Biometrics, defined as the automated recognition of individuals based on unique physiological or behavioral traits, encompass fingerprints, iris patterns, facial geometry, dental prints, palatal rugae, and oral activity monitoring. In dentistry, these modalities have diverse applications, ranging from secure patient identification and streamlined record management to forensic investigations, fraud prevention in insurance, and the customization of prosthodontic, orthodontic, and implant therapies. Biometric tools also support teledentistry by ensuring secure remote consultations and enable real-time monitoring of patient compliance with oral hygiene and appliance use. The benefits of such technologies include improved accuracy, enhanced data security, efficiency in clinical workflows, better patient adherence, and forensic reliability. Nevertheless, significant concerns remain regarding privacy, data security, legal and ethical safeguards, cost barriers, and patient acceptance. Unlike replaceable identifiers such as passwords, biometric data are permanent, raising particular concerns about breaches and misuse. The future of biometrics in dentistry lies in the integration of artificial intelligence, multimodal biometric systems, blockchain-secured databases, and smart oral devices, which together may foster precision and personalized dentistry. Overall, while biometrics hold substantial promise for transforming dental practice and research, their adoption must be carefully balanced with strong ethical, legal, and regulatory frameworks to ensure responsible and equitable use.

Keywords: Biometric Technologies, Dentistry, Ethical Safeguards

1. Introduction

Dentistry, like many other fields of healthcare, is undergoing rapid transformation as digital technologies become increasingly integrated into day-to-day practice. The shift toward digital record-keeping, advanced diagnostic imaging, and computer-assisted treatment planning has not only improved clinical accuracy but has also introduced new challenges regarding patient identification, data security, and personalization of care. Within this context, biometric technologies—the measurement and analysis of unique physiological and behavioral traits—are emerging as powerful tools with significant relevance to dental medicine. Biometrics refers to automated recognition systems based on distinct biological or behavioral characteristics such as fingerprints, iris patterns, facial geometry, or even voiceprints. In dentistry, biometric applications extend beyond general healthcare functions; they include identification through dental prints, palatal rugae, and occlusal patterns, as well as behavioral monitoring related to oral hygiene and appliance compliance[1-4]. Such integration offers a potential paradigm shift, wherein dental practitioners can leverage biometric identifiers not only to confirm patient identity but also to enhance treatment personalization and secure patient information.

The adoption of biometrics in dentistry has been motivated by several practical and ethical imperatives. First, traditional identifiers—such as personal documents or passwords—are susceptible to theft, duplication, and misuse. Second, dental professionals often encounter the challenge of working with patients who may not be able to communicate or identify themselves accurately, such as children, elderly individuals with cognitive impairment, or trauma victims[5]. Third, the rise of forensic odontology has highlighted the importance of dental traits as reliable postmortem identifiers, particularly in disaster victim identification (DVI) scenarios. Equally compelling is the movement toward personalized and precision dentistry, wherein treatments and prostheses are increasingly tailored to individual anatomical and functional characteristics. By integrating biometric data into computer-aided design and manufacturing (CAD/CAM) workflows, prosthodontic appliances, implants, and orthodontic devices can be created with unparalleled accuracy[6-7]. Biometric monitoring can also support behavioral interventions—for instance, smart toothbrushes and intraoral sensors may use biometric recognition to track whether patients adhere to prescribed oral hygiene regimens or orthodontic appliance usage.

However, despite these advantages, the adoption of biometrics in dentistry is accompanied by significant challenges and risks. Concerns regarding data privacy, cybersecurity breaches, and potential misuse of sensitive information are paramount. Unlike replaceable identifiers such as passwords, biometric traits are permanent and immutable; once compromised, they cannot be altered. Moreover, issues of cost, accessibility, and cultural acceptance may limit the universal adoption of biometric systems in dental practice[8-10]. This review aims to provide a comprehensive overview of the uses, benefits, and cautions associated with biometrics in dentistry. It will first classify and describe the principal types of biometric technologies relevant to dental care, before outlining their clinical, administrative, and forensic applications. Subsequent sections will analyze the benefits these systems offer to dental practice and research, followed by a critical discussion of the risks and ethical dilemmas they present. The review will conclude with an exploration of future directions, including the integration of artificial intelligence, multimodal biometrics, and secure blockchain-based systems for healthcare data management.

2. Classification of Biometric Technologies in Dentistry

Biometric technologies can be broadly classified into physiological biometrics and behavioral biometrics, with dentistry encompassing both categories. In addition, dentistry contributes unique identifiers specific to the oral cavity, such as palatal rugae and occlusal morphology.

2.1 Physiological Biometrics

Fingerprints remain the most widely used biometric trait globally. In dentistry, fingerprint-based systems can be implemented for clinic access control, staff attendance, and patient verification. While practical, their use in dental-specific applications is limited, since fingerprints provide no direct link to oral health or treatment[11].

Iris recognition offers one of the highest levels of accuracy among biometric technologies. It relies on the unique patterns of the iris, which remain stable throughout life. In dental practice, iris recognition can be deployed in secure electronic health record (EHR) systems or as a verification method in teledentistry platforms[12-13].

Facial recognition has grown rapidly due to advances in machine learning and computer vision. Dental applications include patient identification during appointments, automatic matching of radiographic

images with correct patient profiles, and even real-time monitoring of facial movements during orthodontic therapy. Additionally, three-dimensional facial scans are increasingly used in aesthetic dentistry to guide smile design and reconstructive procedures.

Dental prints are highly distinctive. The morphology of teeth, dental restorations, and occlusal patterns has long been used in forensic odontology for human identification. With the digitization of intraoral scans, dental prints can be stored and used not only for legal purposes but also for patient re-identification across different institutions[5-10].

Palatal rugae, the ridges located on the anterior third of the hard palate, are unique to each individual and remain relatively stable even after orthodontic treatment or trauma. Digital imaging of palatal rugae has been proposed as a biometric modality, particularly in forensic contexts where dental records may be available.

2.2 Behavioral Biometrics

Behavioral biometrics rely on patterns of human activity that can be measured and analyzed[14-17].

Voice recognition can authenticate patients in teledentistry consultations or helpline communications. Its integration with artificial intelligence also allows real-time monitoring of stress, anxiety, or discomfort during dental procedures.

Handwriting and signature recognition may be less relevant clinically but remain useful for secure consent documentation in dental clinics.

Keystroke dynamics, though rarely applied in dentistry, could theoretically be integrated into secure access systems for dental staff using digital health platforms.

Oral activity recognition—a novel category—includes monitoring of chewing, swallowing, and brushing patterns through intraoral sensors or smart devices. Such data provide insights into patient compliance, dietary habits, and oral hygiene effectiveness.

2.3 Comparative Overview

Physiological biometrics generally provide higher accuracy and stability than behavioral biometrics, making them suitable for secure patient identification and forensic use. Behavioral biometrics, however, offer the advantage of continuous authentication and provide insights into patient behaviors relevant to oral health. Dentistry's unique identifiers—such as dental prints and palatal rugae—combine the strengths of both categories, offering permanence and uniqueness tied directly to oral structures[18].

3. Applications of Biometrics in Dentistry

Biometrics in dentistry serve a wide range of applications, spanning clinical practice, patient management, research, forensic science, and healthcare administration.

3.1 Patient Identification and Record Management

Dental clinics increasingly rely on electronic health records. Biometric authentication ensures that the correct patient record is accessed and updated. Unlike traditional identifiers (ID cards, passwords), biometrics reduce risks of record mismatching, a particularly relevant issue when treating vulnerable populations or during emergency interventions. In multi-specialty hospitals, biometric systems also

prevent duplication of patient records and improve interoperability between dental and medical databases[10-12].

3.2 Fraud Prevention in Dental Insurance

Insurance fraud—such as claims submitted under false identities or duplication of services—remains a persistent problem. Biometric verification of patients at the time of treatment provides a safeguard against fraudulent claims. This not only reduces financial loss for insurers but also protects patients from identity misuse.

3.3 Forensic Dentistry and Legal Identification

Forensic odontology has long recognized dental features as highly reliable identifiers. In mass disasters, accidents, or criminal investigations, biometric dental traits such as dental prints, restorations, and palatal rugae assist in victim identification. Digital storage of dental biometric data can significantly accelerate disaster victim identification processes, particularly when combined with centralized national databases[14-18].

3.4 Customized Treatment Planning

In **prosthodontics**, biometric data from intraoral scanners and facial recognition systems enhance CAD/CAM workflows. Denture designs can be tailored to the unique morphology of a patient's oral cavity and facial proportions.

In **orthodontics**, biometric monitoring through intraoral sensors can detect whether patients wear aligners or retainers as prescribed. Compliance tracking helps clinicians evaluate treatment effectiveness and adjust plans accordingly.

In **implantology**, biometric integration allows for precise matching of implant dimensions to patient-specific bone morphology. Facial scans further support aesthetic considerations in smile restoration.

3.5 Remote Dentistry and Tele-Dentistry

Tele-dentistry platforms, particularly those used for rural or underserved populations, benefit from biometric patient authentication to prevent misidentification. Voice recognition and facial recognition systems allow secure remote consultations. Furthermore, wearable devices with oral sensors can transmit behavioral biometric data (such as brushing frequency) to dentists for remote monitoring[19].

3.6 Workforce Authentication and Access Control

In dental institutions, biometrics enhance administrative security. Fingerprint or iris recognition can regulate staff access to sensitive areas such as radiology suites, sterilization rooms, and digital record archives. This not only safeguards patient information but also ensures compliance with infection-control protocols[20].

4. Benefits of Biometric Use in Dentistry

The benefits of biometric integration in dentistry can be classified into **clinical, administrative, forensic, and patient-related advantages**.

1. **Accuracy and Reliability** – Biometrics reduce misidentification risks in clinical and forensic settings.

2. **Time Efficiency** – Automated recognition accelerates patient check-in and record retrieval.
3. **Enhanced Security** – Sensitive health data are better protected through biometric authentication compared with conventional passwords or cards.
4. **Patient Compliance Monitoring** – Behavioral biometrics encourage adherence to treatment regimens, thereby improving outcomes.
5. **Forensic Utility** – Stored dental biometrics aid in disaster victim identification and criminal investigations.
6. **Contribution to Precision Dentistry** – Personalized prostheses and implants improve both functionality and aesthetics.

5. Cautions, Risks, and Ethical Considerations

Despite these benefits, caution is warranted.

- **Data Privacy and Cybersecurity**: Biometric databases are attractive targets for hackers. A stolen biometric cannot be reissued like a password.
- **Legal and Consent Issues**: Collecting biometric data requires informed consent and compliance with laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).
- **Misidentification Risks**: Errors in recognition algorithms could lead to wrongful identification or denial of treatment.
- **Cost and Inequality**: Advanced systems may be unaffordable for smaller clinics, widening the gap between urban and rural practices.
- **Psychological Acceptance**: Patients may feel uncomfortable with facial scans or intraoral monitoring, raising concerns about surveillance.
- **Forensic Dilemmas**: Using biometric dental records in criminal investigations must balance public interest with individual rights.

6. Future Perspectives and Emerging Trends

The future of biometrics in dentistry is closely tied to advancements in **artificial intelligence, big data, and secure digital infrastructures**.

- **AI-Enhanced Biometrics**: Machine learning algorithms improve recognition accuracy and enable predictive analytics.
- **Multimodal Biometrics**: Combining multiple traits—such as facial scans, dental prints, and voice recognition—enhances robustness.
- **Blockchain Integration**: Decentralized storage of biometric data can strengthen security and transparency.

- **Smart Oral Devices**: Wearable or intraoral sensors may track chewing, swallowing, or hygiene behaviors in real time.
- **Global Databases for Forensic Use**: Standardized, ethically managed repositories could accelerate disaster victim identification while ensuring privacy.

7. Conclusion

Biometric technologies are poised to play a transformative role in dentistry, offering solutions for patient identification, forensic applications, personalized treatment, and administrative efficiency. Their integration into dental practice can enhance precision, security, and trust. However, the risks associated with privacy breaches, ethical dilemmas, and unequal access cannot be overlooked. For successful adoption, biometrics in dentistry must be accompanied by robust regulatory frameworks, informed consent protocols, and continuous engagement with patients and professionals.

Looking ahead, the combination of biometrics with artificial intelligence and secure data systems promises to revolutionize oral healthcare, aligning it with the broader movement toward precision and personalized medicine.

References:

1. Permata N.A., Setiawardhana, Sigit R. Forensic identification system using dental panoramic radiograph; Proceedings of the 2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC); Surabaya, Indonesia. 26–27 September 2017; pp. 281–287.
2. Gurses A., Oktay A.B. Human Identification with Panoramic Dental Images using Mask R-CNN and SURF; Proceedings of the 2020 5th International Conference on Computer Science and Engineering (UBMK); Diyarbakir, Turkey. 9–11 September 2020; pp. 232–237.
3. Fan F., Ke W., Wu W., Tian X., Lyu T., Liu Y., Liao P., Dai X., Chen H. Automatic human identification from panoramic dental radiographs using the convolutional neural network. Forensic Sci. Int. 2020;314:110416.
4. Lai Y.C., Fan F., Wu Q., Ke W., Liao P., Deng Z., Chen H., Zhang Y. LCANet: Learnable connected attention network for human identification using dental images. IEEE Trans. Med Imaging. 2020;40:905–915.
5. Zhong X., Yu D., Foong K.W.C., Sim T., Wong Y.S., Cheng H.L. Towards automated pose invariant 3D dental biometrics; Proceedings of the 2011 International Joint Conference on Biometrics (IJCB); Washington, DC, USA. 11–13 October 2011; pp. 1–7.
6. Zhong X., Zhang Z. 3D Dental Biometrics: Automatic Pose-invariant Dental Arch Extraction and Matching; Proceedings of the 2020 25th International Conference on Pattern Recognition (ICPR); Milan, Italy. 10–15 January 2021; pp. 6524–6530.
7. Reesu G.V., Woodsend B., Mânica S., Revie G.F., Brown N.L., Mossey P.A. Automated Identification from Dental Data (AutoIDD): A new development in digital forensics. Forensic Sci. Int. 2020;309:110218.

8. Gibelli D., Angelis D.D., Riboli F., Dolci C., Cattaneo C., Sforza C. Quantification of odontological differences of the upper first and second molar by 3D-3D superimposition: A novel method to assess anatomical matches. Forensic Sci. Med. Pathol. 2019;15:570–573
9. Mou Q., Ji L., Liu Y., Zhou P., Han M., Zhao J., Cui W., Chen T., Du S., Hou Y., et al. Three-dimensional superimposition of digital models for individual identification. Forensic Sci. Int. 2021;318:110597.
10. .Yu H., Li F., Saleh M., Busam B., Ilic S. Cofinet: Reliable coarse-to-fine correspondences for robust pointcloud registration; Proceedings of the 35th International Conference on Neural Information Processing System; Online Conference, Canada. 6–14 December 2021; pp. 23872–23884.
11. Rusu R.B., Blodow N., Beetz M. Fast Point Feature Histograms (FPFH) for 3D registration; Proceedings of the 2009 IEEE International Conference on Robotics and Automation; Kobe, Japan. 12–17 May 2009; pp. 3212–3217.
12. Rusu R.B., Blodow N., Marton Z.C., Beetz M. Aligning point cloud views using persistent feature histograms; Proceedings of the 2008 IEEE/RSJ International Conference on Intelligent Robots and Systems; Nice, France. 22–26 September 2008; pp. 3384–3391.
13. Zheng L., Li Z. Virtual Namesake Point Multi-Source Point Cloud Data Fusion Based on FPFH Feature Difference. Sensors. 2021;21:5441
14. Sun R., Zhang E., Mu D., Ji S., Zhang Z., Liu H., Fu Z. Optimization of the 3D Point Cloud Registration Algorithm Based on FPFH Features. Appl. Sci. 2023;13:3096.
15. Shi X., Peng J., Li J., Yan P., Gong H. The Iterative Closest Point Registration Algorithm Based on the Normal Distribution Transformation. Procedia Comput. Sci. 2019;147:181–190.
16. Li S., Wang J., Liang Z., Su L. Tree point clouds registration using an improved ICP algorithm based on kd-tree; Proceedings of the 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS); Beijing, China. 10–15 July 2016; pp. 4545–4548.
17. Pinkham R., Zeng S., Zhang Z. QuickNN: Memory and Performance Optimization of k-d Tree Based Nearest Neighbor Search for 3D Point Clouds; Proceedings of the 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA); San Diego, CA, USA. 22–26 February 2020; pp. 180–192.
18. Besl P.J., McKay N.D. A method for registration of 3-D shapes. IEEE Trans. Pattern Anal. Mach. Intell. 1992;14:239–256.
19. Lee C.J., Wang S.D. Fingerprint feature extraction using Gabor filters. Electron. Lett. 1999;35:288–290.
20. Alvarez-Cubero M.J., Saiz M., Martinez-Gonzalez L.J., Alvarez J.C., Eisenberg A.J., Budowle B., Lorente J.A. Genetic Identification of Missing Persons: DNA Analysis of Human Remains and Compromised Samples. Pathobiology. 2012;79:228–238.