Journal of Indopacific Academy of Forensic Odontology (JINPAFO)

JINPAFO Vol.14, Issue 1, January - June 2025

REVIEWS AND OPINIONS

Digital Forensics Meets Dental Evidence: The Role of Forensic Dentistry in Combating Cybercrime

Rakesh K Gorea*

Professor Emeritus & Advisor, Medicolegal Institute Baba Farid University of Health Sciences, Faridkot, Punjab, India.

Abstract

In the age of rapidly advancing technology and rising digital threats, the field of forensic dentistry has begun to play a surprising yet significant role in cybercrime investigations. Traditionally linked to identifying human remains and bite mark analysis, forensic dentists now contribute valuable insights in cases involving identity fraud, digital impersonation, and facial recognition anomalies. Their expertise is crucial in authenticating biometric data, especially where dental imaging intersects with digital identity verification systems. This paper explores how forensic odontology is expanding its scope beyond the conventional, integrating with cyber forensics to tackle crimes like deepfake manipulations, illicit biometric data use, and cross-border identity theft. As cybercrime grows more sophisticated, so too must the interdisciplinary approaches to digital justice.

Keywords: Cybercrime, Digital crime, Digital evidence, Forensic dentistry, Forensic odontology, Identity fraud.

Introduction

Participation in social online communities should be respectful. They should use these platforms safely, both legally and ethically. But Dentists will come across cases when these things are being used that are not legal or are unethical, and their expertise in dentistry is needed to solve such problems, e.g., digital identity verification systems. Therefore, forensic dentists must have knowledge and skills in digital forensics to effectively deal with such cases.

Forensic odontology

Forensic Odontology is a branch of science that applies knowledge and skills of dentistry to help the investigation and judicial system of a country apprehend the criminals and solve the cases by determining the severity of injuries, and also helps in the identification process in various criminal and humanitarian issues.[1]

Digital literacy

It is the problem-solving capacity of having the skills to use data legally and ethically by using the technologies for communication in a responsible manner.[2]

Author for Correspondence:
Rakesh K Gorea, Professor Emeritus & Advisor, Medicolegal Institute Baba Farid University of Health Sciences, Faridkot, Punjab, India. Email id- rakeshgorea@gmail.com

How to cite: Gorea RK, Digital Forensics Meets Dental Evidence: The Role of Forensic Dentistry in Combating Cybercrime. J Indo Pacific Acad Forensic. Odontology. 2025 Jan-June 14 (1): 20-24.
DOI: 10.53275/jinpafo.v14.i1.05

Forensic dentists should know how to use social media responsibly. It is a necessary skill for dentists to avoid unnecessary litigation.[3]

Growth of digital crimes

Identity thefts in India in 2020 were 20,000; in 2021 were 18,000; in 2022 were 19,000 and in 2023 were 17,000; and in 2024 were 18,000, as per the National Crime Records Bureau of India. [4]

Digital literacy for forensic odontologists

Forensic odontologists can help in the identification scenarios, especially in those cases of cybercrimes where other methods of identification are of little help, especially in cases with digital evidence.

In mass disasters, antemortem records may be in digital form, which are utilised for identification in mass disasters.[5] Whenever dental records are recovered digitally, forensic dentists can help in analysing the same digital evidence and help in the investigative process of a cybercrime.[6]

Dentists can complement the digital evidence by providing physical identification parameters of the criminal involved in cybercrime.[7]

Different Types of Digital Crimes Involving Dentistry

Digital impersonation

It is the use of digital technologies to assume the identity of other people. It includes email impersonation and corporate impersonation, virtual and audio impersonation, and network and technological impersonation. In any such cases, dentists can be victims, and they should be awareness of it.

Identity fraud

For illicit gains, the personal information of someone is used fraudulently. It can be dental and medical identity theft, financial identity theft, or online identity theft.

Facial recognition anomalies

Facial reconstruction is the domain of dentists. Facial recognition is a highly safe and dependable method, yet it can be exploited due to anomalies and vulnerabilities in the system. By spoofing and backdoor manipulations, unauthorised access can be made to a system.[8, 9, 10]

Deepfake manipulations

There can be a potential fraud where the dental images are being used for identification. It can use advanced artificial intelligence by manipulating dental radiographs and dental images. There can be mistreatment due to misdiagnosis, which may involve a huge expenditure. Misinformation about dental products can also be misused in dentistry. [11, 12]

Identification of human remains

Forensic odontologists are part of the team for the identification of human remains. It uses advanced databases and advanced technologies in addition to other methods, e.g., DNA profiling and dental records. Online manipulations of any of this data or databases can lead to misidentification and financial fraud. CODIS and NAMUS are important databases that are utilised for identification.[13]

Bite mark analysis

Bite mark analysis helps in the identification of the offenders by studying the pattern of the bite marks on the victim.[14, 15] especially in the sexual crimes.[16,17] .3D scanning has improved this method, and Cloud Compare Software is used to analyse. [18] Wherever networks and computers are used, there are chances of using them fraudulently and misidentification of the offender.

Cross-border identity theft

Digital technologies are helping cross-border transactions and facilitating business, but at the same time, cybercriminals are misusing them for financial fraud and other crimes. In one of the crimes, personal data of 147 million persons was stolen and misused, resulting in a lot of financial losses [19] and Interpol plays a crucial role in preventing such crimes, and forensic odontologists are part of Interpol. Terrorists are using air travel by producing false e-documents, and immigrants are being provided false documents to settle in other countries. Encrypted technology is being used by criminals to avoid being caught. [20] Forensic dentists must be aware of this.

Illicit biometric data use

Biometric data is used to give security so that there is no identification misuse**.** Cybercriminals misuse the biometric data to commit crimes, mostly financial fraud. Biometric data is traded on the dark web for criminal use. Prevention can be done by storing a biometric system in another biometric system through Steganography. [21]

Digital identification verification systems

Raise concerns regarding the privacy of individuals. Mass surveillance can be done by using this system, which is again a concern for the privacy of the users. [22]

Digital Evidence

Digital forensics involves computer forensics, mobile forensics, network forensics and cloud computing forensics and IoT forensics. The evidence must be convincing to the court; therefore, it must be complete. It must be accurate and authentic. [23]

Evidence in digital crime: this can be in the form of images, videos, audios and text messages, which can establish a link between the crime and the offender in the courts. This data is not visible and is very sensitive and fragile. If it is handled properly, only then will it be useful; otherwise, it will lose its integrity [24]. If any crime is committed using electronic media and computers, a digital trace is left on the machine, and this may be the incriminating evidence. [25]

Digital evidence has to be collected after finding its origin and preserved. After analysis, reconstruction is done, and finally, it is to be presented in the courts. It involves the recovery of data and IP address tracing to link the machine and the criminal to the crime. This also involves encryption and decryption of the data. There is a need to identify the files and their conversion and erasure. This evidence must be authentic. [26]

Collection of digital evidence

Chatlogs and screenshots are the useful parts of these protocols; time stamps also help in this process. Collection of data is very important as it will help in establishing the crime. This data is transmitted electronically. [24] See that the data, when collected, does not get adulterated. Different methods and tools can be utilised if the systems are compromised. [27]

Protocols of evidence collection in digital crimes should be followed meticulously.

Preservation

Data collected can be manipulated. To prevent it, Blockchain technology is used. There are two phases in a blockchain-based crime investigation system, which are hot and cold blockchains. Images and videos are stored in cold blockchains, and frequently changing data can be stored using by hot blockchain method. [28]

Maintaining the digital chain of custody of evidence is very crucial and involves a QR code to ensure that evidence remains tamper-proof by linking physical evidence with the digital evidence. [29]

Handling of victims of digital crimes

It is utmost desirable that forensic odontologists collaborate

with the cyber experts and law enforcement agencies. In this way, a better outcome can be expected as we will use the energy and resources properly.

Psychological help to the victims of cybercrime

Dentists must be educated on how to deal with the victims of trauma. They must have the psycho-education about the same, and this is especially important if the victim is a child. [30]

Never forget to refer the cases to the psychologist or psychiatrist, depending upon the condition of the victims, as this omission may sometimes lead to the loss of the life of the victim.

Forensic odontologists should advocate for the victims so that victims become useful and resilient members of society again.

Ethics in the collection of digital crimes

Admissibility of digital evidence and complying with privacy laws is a big challenge. There can be biases in the analysis of the digital evidence, so established methods should be used. There may be jurisdiction conflicts also. There is a need to comply with the search and laws of seizure of the evidence. A balance has to be maintained between human rights and legal requirements [31]

Technology advances rapidly compared to laws, so there will always be gaps in the technologies and legal framework, and there will always be challenges regarding the admissibility of digital evidence.

Material and Methods

Academic search engine Google Scholar has been used to find the relevant literature i.e. Journal articles, conference papers using the key words. YouTube and Google Search engine has been used to supplement the scholarly research for some reports and whitepapers from reputed organizations and government websites and academic institutions which have been used to review the current situation and their applicability for the forensic nurses. Only relevant material available in English has been used. Materials from non-credible sources and not in English have been excluded. A thematic analysis was conducted for recurring patterns, gaps and emerging trends.

Discussion

Dentists require digital literacy so that no offender takes advantage of digital illiteracy amongst dentists to circumvent the investigative system.

Challenges

Digital evidence is always challenging and becomes inadmissible in court many times if the legal process is not adhered to while collecting the evidence. [23]

Problems in the investigation of digital crimes include integrating digital and physical evidence, and this may require special techniques. There is also a need to maintain the authenticity and integrity of the digital data so that these remain admissible in the courts.

Advanced computational methods are required because digital data, in most cases, is of huge volume and it requires Optical Character Recognition and Text Comparison Algorithms. [32]

Ethical dilemmas

Privacy of the persons with whom dentists are dealing is a big issue, and they should always try to ensure that the privacy of the individual is not interfered with. Information about the patients should only be given according to the law of the country, and the same holds true for the digital evidence.

Ethical dilemmas are always there before dentists when they come across criminal cases. According to the ethics of their profession, they have to be loyal to the persons with whom they are dealing, but simultaneously, they have to take care of the legal process and obligations. Sometimes these may be just opposing each other.

Sometimes, due to heinous crimes and their publicity in the press, a person may become biased. Dentists should avoid bias when they are dealing with such cases, and they should always remain unbiased.

How to overcome the challenges?

Informed consent, wherever applicable, should always be taken first before proceeding with the collection of the evidence. Biases and personal beliefs should be avoided while performing these medicolegal duties, and we must not forget the truth. [33]

Principles of ethics are very important; principles of autonomy, beneficence, non-maleficence and justice must be followed. Evidence-based decisions in previous such cases should be followed in cases of doubt. [34] If unable to conclude how to handle the ethical dilemma, it is always better to consult Hospital ethics committees and legal advisors.

Secure storage and secure transfer of the data should always be taken care of, and a chain of digital evidence of transfer should always be maintained. It is better to protect the files with passwords while transferring the data.

Login ID, pasword, personal identiofaction number (PIN), Personal Identification Number (PIN) and two-factor authentication systems have been used, but these are becoming insufficient to protect the systems. To overcome the privacy challenges, techniques such as steganography and behavioural biometrics can be utilised. A two-layered e-biometric system can also be used. [21] [35]

Prolonged or first-time exposure to forensic digital evidence may lead to burnout amongst the doctors, and this impact should be taken care of by peers and superiors. Professional help should always be sought and provided promptly.

15 cybercrime forensic labs have been established in India, and a Digital Personal Data Protection Act was enacted in

2023 to reduce and curb cybercrimes. [4]

It is very pertinent to have a framework for the collection of digital evidence so that it can be admissible in court. [23]

Awareness

Awareness of cybercrimes is needed amongst dentists and forensic dentists so that hackers may not be able to get personal information by sending fake emails and messages or while using websites. There is always under-reporting because of the shame involved in these frauds. By using personal information of someone, they may take the dental services and dental prescriptions and raise fraudulent dental bills. This involves complicating dental records and insurance claims.

Academic Courses

Most forensic dentists do not study the digital evidence collection and preservation, so specialised small courses can be started for forensic dentists to learn these different aspects of digital and cybercrime should be initiated so that forensic dentists can handle such cases when they have to deal with them.

Team work

A forensic odontologist can be an important member of the team to build a strong case against the offender and provide justice to the victims. They can help in thwarting digital crimes, especially against young people.

Conclusion

A time is coming when digital crimes will not be uncommon. In some cases, the help of the forensic odontologist will be required. Forensic odontologists should be fully aware of the issue and should be equipped with the knowledge and skills to handle such cases. While handling such cases, they should also be aware of the challenges, including ethical challenges, so that they can become an important member of the team investigating digital crimes. Online crimes sometimes leave an invisible trauma on the victims. Forensic odontologists should know how to deal with the victims and offenders of digital crimes. They should know how to identify, collect, preserve, and analyse the data. Validation and justice should be their aim and can provide healing in some cases. They should also understand how they have to present the dental evidence in cybercrimes to the courts. Dental educators should take the lead to empower their dental students to deal with cases of digital crimes.

Conflict of Interest

None.

Source of Funding

None.

References

1. Gorea RK, FORENSIC ODONTOLOGY AND ITS FUTURE IN INDIA. [cited 2025 Jul 25]; Available from: https://www.researchgate.net/profile/Rakesh-Gorea/publication/236624809_Forensic_odontology_and_its_future_in_India/links/551bbf650cf251c35b50a5a9/Forensic-odontology-and-its-future-in-India.pdf
2. Program Planning [Internet]. [cited 2025 Jul 15]. Available from: https://www.dcp.edu.gov.on.ca/en/program-planning/transferable-skills/digital-literacy
3. Gorea RK. Social media and the medical profession. Int J ETHICS TRAUMA Vict. 2017;3(01):6–11.
4. India's Cybercrime Crackdown in 2024: Key Arrests, Trends, and Technological Advances [Internet]. [cited 2025 Jul 15]. Available from: https://www.daanik.com/blog/why-cybercrime-had-no-safe-haven-in-india-in-2024
5. Role of forensic odontology in human identification: A review. Int J Appl Dent Sci. 2020 Jan 1;6(1):109–11.
6. Tobio R. Association between Forensic DNA in Odontology and the Identification of Humans of Mass Disasters: A Systematic Review. Судебная Медицина [Internet]. 2024 Sep 17 [cited 2025 Jul 25]; Available from: https://scispace.com/papers/association-between-forensic-dna-in-odontology-and-the-1tsdjko6bswp
7. The role of forensic odontology and dental anthropology: An approach to forensic issues. J Dent Spec [Internet]. 2024 Apr 15 [cited 2025 Jul 25]; Available from: https://scispace.com/papers/the-role-of-forensic-odontology-and-dental-anthropology-an-wqfisxdpik
8. Ibsen M. Differential Anomaly Detection for Facial Images. ArXiv Comput Vis Pattern Recognit [Internet]. 2021 Oct 7 [cited 2025 Jul 25]; Available from: https://scispace.com/papers/differential-anomaly-detection-for-facial-images-4vlg6krcgb
9. Ptucha. SciSpace - Paper. IGI Global; 2015 [cited 2025 Jul 25]. p. 536–47 Facial Expression Recognition. Available from: https://scispace.com/papers/facial-expression-recognition-55ry6sa921
10. Kremic E. SciSpace - Paper. رشن للن فيان ةعماج راد; 2017 [cited 2025 Jul 25]. The Biometric Model as a Method of Protection from Cyber Frauds. Available from: https://scispace.com/papers/the-biometric-model-as-method-of-protection-from-cyber-26a6v28dvc
11. Singbal K. Digital imagery: reality or fakery. Int J Contemp Dent [Internet]. 2011 Oct 1 [cited 2025 Jul 25];1(3). Available from: https://scispace.com/papers/digital-imagery-reality-or-fakery-42k8cvnmfl
12. Dias de Silva, M. Fake news and dental education. Br Dent J. 2019 Mar 1;226(6):397–9.
13. SciSpace - Paper [Internet]. Manchester University Press eBooks; 2022 [cited 2025 Jul 25]. Series editors' preface. Available from: https://scispace.com/papers/series-editors-preface-2uoa55g8
14. Gorea RK, Jasuja OP, Abuderman AA, Gorea A. Bite marks on skin and clay: A comparative analysis. Egypt J Forensic Sci. 2014;4(4):124–8.
15. Gorea RK, Jha M, Jasuja OP, Vasudeva K, Aggarwal AD. Marvellous tools of identification–bite marks. Med Leg Update. 2005;5(2):61–4.
16. Gorea RK, Jasuja OP, Aggarwal AD, Narula R. Revenge by the Bites. J Indian Acad Forensic Med. 2007 Mar;29(1):17–20.
17. Gorea RK. Bite marks utility in sexual offences. Indian J Dent. 2011;2(2):37–9.
18. Beltrame. Bitemarks and 3D scanner: An objective comparison

for bitemarks. A pilot study. J Forensic Leg Med. 2024 Jan 1;102:102639–102639.
19. Diana B, Mariia I, Ann D. The impact of cross-border cybercrime on global security [Internet]. Закарпатський угорський інститут імені Ференца Ракоці II; 2024 [cited 2025 Jul 25]. Available from: https://dspace.kmf.uz.ua/jspui/handle/123456789/4773
20. Smith RG. Travelling in cyberspace on a false passport: controlling transnational identity-related crime. 2001 [cited 2025 Jul 25]; Available from: http://britsoccrim.org/new/volume5/004.pdf
21. Vallabhu S. Vol. 1, SciSpace - Paper. 2021 [cited 2025 Jul 25]. Biometric Steganography Using MPV Technique. Available from: https://scispace.com/papers/biometric-steganography-using-mpv-technique-7f9nh19yrb
22. Nnamoco N. A behaviour biometrics dataset for user identification and authentication. Data Brief. 2022 Nov 1;45:108728–108728.
23. Digital Forensic and Distributed Evidence. Adv Multidiscip Sci Res J. 2022 Jul 26;1(1):357–62.
24. Digital Crime Evidence (2019) | R. Parkavi [Internet]. [cited 2025 Jul 18]. Available from: https://scispace.com/papers/digital-crime-evidence-3gr4ub4y3z?utm_source=scholar.google.com&utm_content=insights_citation
25. SciSpace - Paper [Internet]. Springer, Cham; 2018 [cited 2025 Jul 24]. p. 9–12 Cybercrime, Cyber Aided Crime and Digital Evidence. Available from: https://scispace.com/papers/cybercrime-cyber-aided-crime-and-digital-evidence-4ff4ucfmme
26. Cybercrime Unmasked: Investigating Cases and Digital Evidence. Int J Emerg Multidiscip Comput Sci Artif Intell [Internet]. 2023 Nov 25 [cited 2025 Jul 24];2(1). Available from: https://scispace.com/papers/cybercrime-unmasked-investigating-cases-and-digital-evidence-1g58tsruwq
27. A survey on digital evidence collection and analysis. In: SciSpace - Paper [Internet]. IEEE; 2017 [cited 2025 Jul 25]. p. 247–53. Available from: https://scispace.com/papers/a-survey-on-digital-evidence-collection-and-analysis-3lwx6sua4m
28. Blockchain-Based Digital Forensics Investigation. Int J Sci Res [Internet]. 2023 Jan 5 [cited 2025 Jul 25]; Available from: https://scispace.com/papers/blockchain-based-digital-forensics-investigation-14yanjvh9g
29. Hildevrandt. Digitised forensics: retaining a link between physical and digital crime scene traces using QR-codes. Proc SPIE. 2013 Mar 7;8667:213–23.
30. Forkey H, Szilagyi M, Kelly ET, Duffee J, THE COUNCIL ON FOSTER CARE AND KINSHIP CARE, COUNCIL ON COMMUNITY PEDIATRICS, COUNCIL ON CHILD ABUSE AND NEGLECT, COMMITTEE ON PSYCHOSOCIAL ASPECTS OF CHILD AND FAMILY HEALTH. Trauma-Informed Care. Pediatrics. 2021 Aug 1;148(2):e2021052580.
31. Aleke N. Legal and Ethical Challenges in Digital Forensics Investigations. Adv Digit Crime Forensics Cyber Terror Book Ser. 2024 Dec 30;147–76.
32. Rekdal J. SciSpace - Paper. 2014 [cited 2025 Jul 25]. Cross-comparison of Digital and Digitized Physical Evidence. Available from: https://scispace.com/papers/cross-comparison-of-digital-and-digitized-physical-evidence-1eqty7a4qy
33. Gorea R. Beyond the Screen: The Expanding Role of Forensic Nursing in Managing Cybercrime Victimisation. Int J Ethics Trauma Vict. 1925;11(1):1–8.
34. Gorea RK. Evidence based medical ethics: A critical evaluation. Int J Ethics Trauma Vict. 2015;1(01):5–7.
35. Prabha. SciSpace - Paper. NISCAIR-CSIR, India; 2017 [cited 2025 Jul 25]. Intruder Detection System Based on Behavioral Biometric Security. Available from: https://scispace.com/papers/intruder-detection-system-based-on-behavioral-biometric-2dm42m1j14