


# Chapter 2


## Forensic Audit Trails and Biometric–Based Authentication

**Deepak Gupta**

 <https://orcid.org/0000-0003-3929-1362>


*Institute of Technology and  
Management, Gwalior, India*

**Pratish Rawat**

 <https://orcid.org/0000-0003-3230-7464>


*Poornima University, India*

**Raghu Nangunuri**

 <https://orcid.org/0009-0001-2372-1324>

*Kamala Institute of Technology and  
Science, India*

**C. Umarani**


 <https://orcid.org/0000-0002-9008-3350>

*Christ Academy Institute for Advanced  
Studies, India*

**Srinivasan Nagaraj**

*CBIT, Proddatur, India*

**Someshwar Siddi**

 <https://orcid.org/0000-0002-6045-5408>

*St. Martin's Engineering College, India*

**S. Keerthi**

*Dayananda Sagar College of  
Engineering, Karnataka, India*

### ABSTRACT

*Forensic audit trails combined with biometric-based authentication represent a critical convergence in modern cybersecurity infrastructure. This chapter examines the technical implementation, forensic methodologies, and investigative frameworks for biometric authentication systems. The integration of immutable audit trails with biometric verification creates comprehensive forensic evidence chains essential for digital investigations. We analyze forensic challenges including spoofing attacks, presentation attacks, and biometric template security. The chapter explores multimodal biometric systems, liveness detection mechanisms, and blockchain-based audit trail*

DOI: 10.4018/979-8-3373-4972-5.ch002

*implementations. Critical examination of privacy-preserving forensic techniques, GDPR compliance, and admissibility of biometric evidence in legal proceedings provides practical guidance. Real-world case studies demonstrate forensic analysis of compromised biometric systems.*

## **1. INTRODUCTION**

The proliferation of biometric authentication systems across financial institutions, healthcare facilities, government agencies, and consumer applications has fundamentally transformed identity verification paradigms (Jain et al., 2024). Biometric authentication leverages unique physiological and behavioral characteristics—including fingerprints, facial features, iris patterns, voice prints, and behavioral dynamics—to establish user identity with unprecedented accuracy. However, this technological advancement introduces complex forensic challenges requiring specialized investigative methodologies and comprehensive audit trail architectures.

Forensic audit trails in biometric systems serve dual purposes: operational security monitoring and post-incident investigation (Kaur & Khanna, 2024). These immutable logs capture authentication attempts, template matching scores, system access patterns, and anomalous behaviors, creating evidentiary foundations for digital forensics. The integration of biometric authentication with robust audit mechanisms enables forensic investigators to reconstruct security incidents, identify attack vectors, and establish chains of custody for digital evidence.

Contemporary biometric systems face sophisticated adversarial threats including presentation attacks (spoofing), deep learning-based forgeries, template reconstruction attacks, and privacy violations (Hadid et al., 2021). Forensic investigators must understand both the technical architecture of biometric authentication systems and the methodologies for detecting, analyzing, and prosecuting biometric-related cyber-crimes. This chapter provides comprehensive coverage of forensic audit trail design, biometric security vulnerabilities, investigative techniques, and legal considerations.

The convergence of biometrics and forensics occurs within increasingly complex regulatory environments. The European Union's General Data Protection Regulation (GDPR) classifies biometric data as sensitive personal information requiring enhanced protection. Similarly, the California Consumer Privacy Act (CCPA), Illinois Biometric Information Privacy Act (BIPA), and emerging international frameworks impose strict requirements on biometric data collection, storage, and forensic examination. Forensic investigators must navigate these regulatory constraints while maintaining investigative effectiveness.

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/forensic-audit-trails-and-biometric-based-authentication/402964](http://www.igi-global.com/chapter/forensic-audit-trails-and-biometric-based-authentication/402964)

## Related Content

---

### IAM Risks during Organizational Change and Other Forms of Major Upheaval

C. Warren Axelrod (2012). *Digital Identity and Access Management: Technologies and Frameworks* (pp. 1-18).

[www.irma-international.org/chapter/iam-risks-during-organizational-change/61527](http://www.irma-international.org/chapter/iam-risks-during-organizational-change/61527)

### Improving In-Flight Learning in a Flapping Wing Micro Air Vehicle

Monica Sam, Sanjay Boddhu, Kayleigh Duncan, Hermanus Botha and John Gallagher (2016). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 62-75).

[www.irma-international.org/article/improving-in-flight-learning-in-a-flapping-wing-micro-air-vehicle/158005](http://www.irma-international.org/article/improving-in-flight-learning-in-a-flapping-wing-micro-air-vehicle/158005)

### Fully Homomorphic Encryption Without Noise

Yacine Ichibane, Youssef Gahi, Mouhcine Guennoun and Zouhair Guennoun (2019). *International Journal of Smart Security Technologies* (pp. 33-51).

[www.irma-international.org/article/fully-homomorphic-encryption-without-noise/249208](http://www.irma-international.org/article/fully-homomorphic-encryption-without-noise/249208)

### Solutions of LDA for Small Sample Size Problems

David Zhang, Xiao-Yuan Jing and Jian Yang (2006). *Biometric Image Discrimination Technologies: Computational Intelligence and its Applications Series* (pp. 156-186).

[www.irma-international.org/chapter/solutions-lda-small-sample-size/5922](http://www.irma-international.org/chapter/solutions-lda-small-sample-size/5922)

### Skin Detection with Small Unmanned Aerial Systems by Integration of Area Scan Multispectral Imagers and Factors Affecting their Design and Operation

Stephen R. Sweetnich and David R. Jacques (2014). *International Journal of Monitoring and Surveillance Technologies Research* (pp. 67-84).

[www.irma-international.org/article/skin-detection-with-small-unmanned-aerial-systems-by-integration-of-area-scan-multispectral-imagers-and-factors-affecting-their-design-and-operation/130621](http://www.irma-international.org/article/skin-detection-with-small-unmanned-aerial-systems-by-integration-of-area-scan-multispectral-imagers-and-factors-affecting-their-design-and-operation/130621)