Chapter 11
Biometric-Driven Encryption and Blockchain-Based Audit Trail for Secure Forensic Evidence Management

Yacine Belhocine
https://orcid.org/0009-0002-1747-6008
Laboratory of Mathematics, Informatics, and Systems, University of Echahid Cheikh Laarbi Tbessi, Tebessa, Algeria

Abdallah Meraoumia
Laboratory of Signals and Smart Systems, Echahid Cheikh Larbi Tebessi University, Algeria

Salim Chitroub
https://orcid.org/0009-0001-1814-3304
Laboratory of Intelligent and Communicating Systems Engineering, USTHB, Algiers, Algeria

Hakim Bendjenna
Laboratory of Mathematics, Informatics, and Systems, University of Echahid Cheikh Laarbi Tbessi, Tebessa, Algeria

ABSTRACT

The secure management of biometric evidence is essential in modern forensic investigations, requiring data integrity, confidentiality, and accountability throughout the evidence lifecycle. This chapter presents a framework combining homomorphic

DOI: 10.4018/979-8-3373-4972-5.ch011

encryption with blockchain-based audit trails to enhance security and transparency in biometric systems. Biometric features, such as palmprints, are encrypted using homomorphic schemes, allowing computations on encrypted data without compromising privacy. Encrypted feature vectors are stored in a decentralized environment via the InterPlanetary File System (IPFS), while all interactions are logged through blockchain smart contracts for tamper-proof auditability. Experiments show the system maintains high recognition accuracy with acceptable computational overhead and low transaction costs. This approach provides a scalable, privacy-preserving, and forensically sound solution for managing biometric evidence in digital investigations and legal proceedings.

INTRODUCTION

The intersection of biometric technology and digital forensics is increasingly critical for securing identity verification, preserving evidence integrity, and enabling lawful investigative access. In the digital era, forensic procedures extend beyond physical evidence collection and manual analysis, with digital systems, especially those handling biometric data, playing a central role in identification and authentication. Biometric modalities such as fingerprints, palmprints, iris patterns, and facial features provide distinctive, hard-to-forge identifiers, making them valuable in forensic investigations (Klasén et al., 2024).

Despite these advantages, widespread biometric adoption introduces challenges in security, privacy, and evidence management. Traditional systems rely on centralized databases, creating single points of failure and exposing evidence to insider threats, unauthorized access, and data breaches. Centralized storage also limits transparency, making verifiable chain-of-custody enforcement difficult (Moussa, 2021). Forensic environments demand reproducibility, integrity preservation, and procedural accountability. Biometric data is inherently irrevocable, so strong protection mechanisms are essential both at rest and during processing, while still allowing analysis for identification or evidentiary correlation. This tension between confidentiality and operational usability is further complicated in multi-agency or cross-jurisdictional investigations (Baig & Eskeland, 2021).

Privacy-preserving computation techniques, particularly homomorphic encryption (HE), have gained attention for enabling secure operations on encrypted biometric feature vectors. HE allows comparisons and classification while preserving confidentiality, providing practical protection without undermining forensic utility (Krishna Prakasha & Sumalatha, 2025). However, confidentiality alone is insufficient: forensic admissibility requires immutable audit trails. Blockchain technology addresses this by recording evidence-handling events as decentralized,

EEG-based Classification of Epileptic and Non-Epileptic Events using Multi-Array Decomposition

Evangelia Pippa, Vasileios G. Kanas, Evangelia I. Zacharaki, Vasiliki Tsirka, Michael Koutroumanidisand Vasileios Megalooikonomou (2016). *International Journal of Monitoring and Surveillance Technologies Research (pp. 1-15).*
www.irma-international.org/article/eeg-based-classification-of-epileptic-and-non-epileptic-events-using-multi-array-decomposition/167691