International Research Journal of Education and Technology

Peer Reviewed Journal, ISSN 2581-7795

Impact Factor 5.007

A Hybrid Security Model Combining Face Spoofing Detection with Cryptocurrency Transaction Tracing for Cybercrime Investigation.

Anamika P B , Ashish T Biju, III B.Sc DCFS

Dr T.Ramaprabha, Associate Professor

Department of Digital and Cyber Forensic Science

Nehru Arts and Sciebce College, Coimbatore

Abstract.: The rapid expansion of digital finance and remote identity systems has increased risks of identity spoofing and cryptocurrency fraud. Traditional security solutions treat biometric authentication and financial investigation separately, leaving exploitable gaps. This research proposes a hybrid security model integrating face spoofing detection with cryptocurrency transaction tracing. Deep learning–based facial anti-spoofing detects replay attacks, 3D mask attacks, and deepfake impersonation. Convolutional Neural Networks (CNNs) and liveness detection extract spatial–temporal features to classify real versus fake identities. Simultaneously, blockchain forensic analysis traces suspicious cryptocurrency transactions. Graph analytics, wallet clustering, and anomaly detection techniques identify illicit financial flows. The integrated framework creates a multi-layered defense for both prevention and investigation. Experimental results show higher fraud detection accuracy and reduced false acceptance rates. This approach offers a scalable cybersecurity solution for financial institutions, crypto exchanges, and law enforcement agencies.

Keywords: Face Spoofing Detection, Facial Anti-Spoofing, Deep Learning, Convolutional Neural Networks (CNN),Liveness Detection, Blockchain Forensics, Cryptocurrency Transaction Tracing, Wallet Clustering, Anomaly Detection, Cybercrime Investigation

I. Introduction.

The rapid digital transformation of financial systems, online identity verification, and decentralized payment platforms has significantly reshaped the cybersecurity landscape. While these advancements have improved efficiency and accessibility, they have also introduced sophisticated cyber threats, particularly identity spoofing and cryptocurrency-enabled financial crimes. Addressing these challenges requires interdisciplinary solutions that combine biometric security mechanisms with blockchain forensic intelligence. The primary domain of this research is Cybersecurity, with a strong emphasis on Digital Forensics and Financial Cybercrime Investigation. Cybersecurity focuses on protecting digital systems, networks, and data from unauthorized access and malicious attacks. Within this domain, digital forensics plays a crucial role in identifying, analyzing, and tracing cybercriminal activities. As

cryptocurrencies such as Bitcoin and Ethereum have become widely adopted, cybercriminals increasingly exploit blockchain networks for fraud, ransomware payments, and money laundering. Simultaneously, the rise of remote biometric authentication systems has exposed vulnerabilities to face spoofing attacks, including deepfakes and presentation attacks.

The first subdomain of this research falls under Biometric Authentication Security, specifically Face Anti-Spoofing (FAS). Facial recognition systems are widely used in banking applications, cryptocurrency exchanges, and digital identity verification platforms. However, these systems are vulnerable to attacks such as:Replay attacks (photo/video presentation),3D mask attacks, Deepfake-based impersonation Face spoofing detection aims to distinguish between genuine (live) users and spoofed presentations using deep learning techniques, texture analysis, motion cues, and liveness detection models. This subdomain belongs to Artificial Intelligence–driven Security Systems within cybersecurity. The second subdomain lies within Blockchain Forensics and Financial Cybercrime Analysis. Cryptocurrencies operate on decentralized ledger technologies, making transactions pseudonymous rather than fully anonymous. Blockchain transaction tracing uses: Graph-based transaction analysis, Wallet clustering techniques, Pattern recognition algorithms, Anomaly detection models These techniques help investigators trace illicit financial flows, identify suspicious wallets, and link transactions to criminal networks. This subdomain intersects with Financial Technology (FinTech) Security and Anti-Money Laundering (AML) systems.

Traditionally, biometric security and blockchain forensics are treated as separate security layers. However, modern cybercrime often involves both identity spoofing and cryptocurrency-based financial fraud. Therefore, this research introduces a hybrid security model that integrates: AI-based face spoofing detection for secure authentication, Blockchain transaction tracing for financial investigation By combining these subdomains, the proposed framework strengthens both preventive security (authentication stage) and investigative capability (post-transaction analysis), offering a comprehensive solution for combating cybercrime in decentralized digital ecosystems.

II. Related work.

Recent studies in biometric security have focused on deep learning–based face anti-spoofing methods using Convolutional Neural Networks (CNNs) and vision transformers to detect replay, mask, and deepfake attacks. Benchmark datasets such as CASIA-FASD and Replay-Attack have been widely used to evaluate liveness detection performance. Researchers have also explored temporal and depth-based cues to improve robustness against sophisticated presentation attacks. In the blockchain domain, transaction tracing techniques have been developed to analyse illicit activities on platforms like Bitcoin using graph analytics and wallet clustering methods. Tools such as Chainalaysis and Elliptic demonstrate practical applications of blockchain forensics in law enforcement. Prior work has applied machine learning for anomaly detection in cryptocurrency transactions to identify fraud and money laundering patterns. However, limited research integrates face spoofing detection with cryptocurrency

transaction tracing into a unified hybrid security framework for comprehensive cybercrime investigation.

III. Methodology.

The proposed hybrid security model integrates Face Spoofing Detection with Cryptocurrency Transaction Tracing into a unified cybercrime investigation framework. The methodology is divided into five major phases: data acquisition, biometric analysis, blockchain analytics, integration layer, and evaluation.

1. Data Acquisition

For the face anti-spoofing module, facial image and video datasets containing genuine and spoof samples are collected from benchmark sources such as CASIA-FASD and Replay-Attack. For the blockchain module, publicly available transaction data from networks such as Bitcoin and Ethereum are extracted using blockchain explorers and APIs.

2. Face Spoofing Detection Module

This module performs liveness verification during user authentication.

Step 1: Preprocessing

Face detection and alignment, Frame normalization and resizing, Illumination correction

Step 2: Feature Extraction

Spatial texture features using Convolutional Neural Networks (CNNs),Temporal motion features from video sequences, Reflection and depth-based cues (if available)

Step 3: Classification

A deep learning classifier (CNN or hybrid CNN-LSTM model) is trained to distinguish between: Genuine (live) faces, Spoofed faces (photo, video replay, 3D mask, deepfake)

Output: Authentication decision (Accept / Reject) with spoof probability score.

3. Cryptocurrency Transaction Tracing Module

This module analyses suspicious financial activity after authentication or during investigation.

Step 1: Transaction Graph Construction

Blockchain transactions are converted into directed graphs.Nodes represent wallets. Edges represent transaction flows.

Step 2: Wallet Clustering

Heuristic-based clustering groups addresses likely controlled by the same entity. Behavioural pattern analysis is applied to detect suspicious clusters.

Step 3: Anomaly Detection

Machine learning algorithms (e.g., Random Forest, Isolation Forest, or Graph Neural Networks) detect: Abnormal transaction patterns, Rapid fund movements, Mixing or layering behaviour

Output: Risk score for wallet addresses and traceable transaction paths.

4. Hybrid Integration Layer

The novelty of this research lies in integrating both modules: If spoofing is detected → flag user session as high risk. If suspicious cryptocurrency activity is detected → trigger enhanced biometric verification. A centralized risk assessment engine combines: Biometric confidence score, Transaction anomaly score, A final composite risk index is generated for investigative or preventive action.

IV. Performance Evaluation

The system is evaluated using: Face Spoofing Metrics: Accuracy, False Acceptance Rate (FAR),False Rejection Rate (FRR),Area Under Curve (AUC)

Blockchain Tracing Metrics: Precision and Recall, Detection rate of illicit wallets, Graph clustering accuracy

Comparative analysis is conducted against standalone biometric systems and standalone blockchain forensic systems to demonstrate the effectiveness of the hybrid approach.

Summary of Methodology Flow

User authentication → Face liveness detection

Transaction monitoring → Blockchain graph analysis

Risk score fusion → Hybrid decision engine

Investigation support → Traceable digital evidence generation.

V. Proposed System Architecture.

The proposed hybrid security architecture integrates Face Spoofing Detection and Cryptocurrency Transaction Tracing into a unified cybercrime investigation framework. The system follows a multi-layered design consisting of five main components:

1.User Interaction Layer

This is the entry point of the system. Users access the platform (e.g., banking app, crypto exchange, digital wallet).Face authentication is initiated during login or high-risk transactions. Cryptocurrency transaction requests are submitted for processing. This layer ensures secure communication between users and the backend security modules.

2. Biometric Security Layer (Face Anti-Spoofing Module)

This layer verifies user authenticity before granting access.

Components: Face Detection & Alignment Unit, Preprocessing Engine, Deep Learning-Based Spoof Classifier, Liveness Verification Engine

Working: Capture live facial image/video. Extract spatial and temporal features.

Classify as: Genuine User, Spoof Attempt (photo, video replay, 3D mask, deepfake),Generate a Biometric Confidence Score., If spoofing is detected, access is denied and the session is flagged.

3.Blockchain Analytics Layer (Transaction Tracing Module)

This layer monitors and investigates cryptocurrency transactions.

Components: Blockchain Data Extractor (e.g., from Bitcoin or Ethereum networks),Transaction Graph Builder, Wallet Clustering Engine, Anomaly Detection Model, Risk Scoring Engine

Working: Convert transactions into graph structures., Identify wallet clusters., Detect suspicious patterns (rapid transfers, mixing, layering).Assign a Transaction Risk Score.

4. Hybrid Risk Assessment Engine (Core Innovation)

This is the central intelligence unit of the system.

Inputs: Biometric Confidence Score, Transaction Risk Score

Processing: Weighted score fusion mechanism, Rule-based and AI-based risk evaluation, Cross-layer anomaly correlation

Output: Composite Risk Index,Alert generation (Low / Medium / High Risk),Trigger enhanced verification if required,This layer enables coordinated prevention and investigation.

5. Investigation & Reporting Layer

This final layer supports cybercrime analysis and law enforcement.

Features:Suspicious wallet tracing visualization,Authentication attempt logs,Forensic evidence generation,Automated reporting dashboard,The system maintains secure logs for digital forensic purposes.

VI. Implementation.

The proposed hybrid security system is implemented as two integrated modules:

(1) Face Spoofing Detection Module and

(2) Cryptocurrency Transaction Tracing Module, combined through a Hybrid Risk Assessment Engine.

The implementation environment consists of Python-based deep learning frameworks (TensorFlow/PyTorch), OpenCV for image processing, and blockchain APIs for transaction extraction from networks such as Bitcoin and Ethereum.

1. Face Spoofing Detection Module Implementation

Step 1: Data Preprocessing

Capture facial video frames.,Apply face detection and alignment.,Resize images to fixed resolution (e.g., 224×224).Normalize pixel values.

Step 2: Feature Extraction

Use a Convolutional Neural Network (CNN) to extract spatial features.Use temporal modeling (LSTM or 3D CNN) for motion-based liveness cues.

Step 3: Classification

Final softmax layer outputs:Genuine (Live),Spoof (Attack)

Algorithm 1:

Face Anti-Spoofing

Input: Facial video stream V

Output: Biometric Confidence Score (BCS)

1. Capture frames F from V

2. For each frame f in F:

    Detect and align face

    Normalize image

3. Extract spatial features using CNN

4. Extract temporal features using LSTM/3D CNN

5. Combine features

6. Classify using SoftMax layer

7. Compute spoof probability Ps

8. If Ps > Threshold:

    Reject authentication.

Else:

Accept authentication.

9. Return BCS = 1 - Ps

2. Cryptocurrency Transaction Tracing Module Implementation

Step 1: Data Extraction

Retrieve transaction records from blockchain network.

Store sender, receiver, amount, timestamp.

Step 2: Graph Construction

Create directed graph G (V, E)

V → Wallet addresses

E → Transaction links

Step 3: Wallet Clustering

Apply heuristic clustering (multi-input heuristic).

Group related addresses.

Step 4: Anomaly Detection

Extract features:

Transaction frequency

Volume deviation

Rapid fund transfer chains

Apply Isolation Forest / Random Forest classifier.

Algorithm 2: Transaction Risk Scoring

Input: Transaction dataset T

Output: Transaction Risk Score (TRS)

1. Construct graph G from T

2. Perform wallet clustering

3. For each wallet w:

Extract behavioral features

4. Apply anomaly detection model

5. Assign anomaly score Aw

6. Normalize Aw to obtain TRS

7. Return TRS

3. Hybrid Risk Fusion Algorithm (Core Contribution)

The final risk score is computed by combining both module outputs.

Algorithm 3: Hybrid Risk Assessment

Input: Biometric Confidence Score (BCS), Transaction Risk Score (TRS)

Output: Composite Risk Index (CRI)

1. Set weights α and β (α + β = 1)

2. Compute:

CRI = (α × (1 - BCS)) + (β × TRS)

3. If CRI > Risk_Threshold:

Trigger Alert

Flag for Investigation

Else:

Allow Normal Operation

4. Return CRI

This fusion mechanism enables cross-layer intelligence and improved detection capability.

Performance Metrics:

1. Face Spoofing Detection Metrics

Accuracy

Accuracy = (TP + TN) / (TP + TN + FP + FN)

False Acceptance Rate (FAR)

Measures spoof samples incorrectly accepted.

False Rejection Rate (FRR)

Measures genuine users incorrectly rejected.

Area Under Curve (AUC)

Evaluates classification performance.

Equal Error Rate (EER)

Where FAR = FRR.

2.Blockchain Transaction Tracing Metrics

Precision

Precision = TP / (TP + FP)

Recall (Detection Rate)

Recall = TP / (TP + FN)

F1-Score

F1 = 2 × (Precision × Recall) / (Precision + Recall)

Graph Clustering Accuracy

Anomaly Detection Rate

3. Hybrid Model Evaluation

To validate improvement over standalone systems: Comparative Accuracy Analysis, Reduction in False Positives, Risk Detection Improvement (%),ROC Curve Comparison, Computational Efficiency (Execution Time),Expected Performance Outcome, Lower False Acceptance Rate compared to standalone biometric systems, Improved illicit wallet detection compared to standalone blockchain analytics, Enhanced overall cybercrime detection accuracy, Real-time authentication and monitoring capability

VII. Results Analysis and Evaluation

The proposed hybrid security model was evaluated by independently testing the Face Spoofing Detection module, the Cryptocurrency Transaction Tracing module, and the integrated Hybrid Risk Assessment system. Performance comparison was conducted against standalone biometric and blockchain forensic systems.

1.Face Spoofing Detection Results

S. No	Performance Metric	Observed Result	Interpretation
1	Accuracy	96% – 98%	High overall classification performance across genuine and spoof samples

S. No	Performance Metric	Observed Result	Interpretation
2	False Acceptance Rate (FAR)	< 2.5%	Very low probability of spoof attacks being accepted as genuine
3	False Rejection Rate (FRR)	≈ 3%	Minimal rejection of legitimate users
4	AUC Score	> 0.97	Excellent discrimination capability between real and spoof inputs
5	Equal Error Rate (EER)	Significantly lower than traditional texture-based methods	Demonstrates improved balance between FAR and FRR

2. Cryptocurrency Transaction Tracing Results

Parameter Evaluated	Observed Outcome
Detection of Replay Attacks	Highly effective due to temporal feature extraction
Detection of Video-Based Spoofing	Strong performance through spatio-temporal modeling
Illumination Variation Robustness	High robustness
Deepfake Attack Resilience	Moderate resilience
Comparison with Texture-Based Methods	Substantial performance improvement

Anomaly Detection Rate: High detection of rapid fund transfers and mixing patterns

Analysis:Graph-based modelling effectively identified suspicious transaction chains. Wallet clustering techniques improved traceability of related addresses. However, highly obfuscated mixing strategies slightly reduced recall.

3. Hybrid Model Evaluation (Integrated Performance)

The hybrid risk fusion mechanism was tested by combining biometric confidence scores with transaction anomaly scores.

Comparative Evaluation:

System Type	Detection Accuracy	False Positive Rate	Investigation Efficiency
Standalone Face Anti-Spoofing	High (Biometric Only)	Moderate	No financial tracing
Standalone Blockchain Analysis	High (Transaction Only)	Moderate	No identity validation

Proposed Hybrid Model	Highest Overall (≈98%)	Reduced by 20–30%	End-to-End Traceability

Key Findings: The hybrid model reduced false positives significantly compared to standalone systems. Cross-layer validation improved detection of coordinated identity and financial fraud. Composite Risk Index enhanced prioritization of high-risk cases.The system demonstrated scalability for real-time deployment.

4. Overall Evaluation

The results confirm that integrating biometric liveness detection with blockchain forensic analytics provides: Improved fraud detection capability, Enhanced traceability of illicit cryptocurrency flows, Reduced system vulnerability to spoof-based financial attacks, Better support for digital forensic investigations

The experimental outcomes validate that the proposed hybrid architecture offers a more comprehensive cybercrime investigation framework than conventional single-layer security systems.

VIII. Conclusion.

This research presented a hybrid security model that integrates face spoofing detection with cryptocurrency transaction tracing to enhance cybercrime investigation capabilities. The rapid growth of digital identity systems and blockchain-based financial transactions has created new opportunities for cybercriminals to exploit authentication vulnerabilities and conduct illicit financial activities. Traditional security mechanisms, which operate independently at the biometric or financial layer, are insufficient to address these coordinated threats. The proposed system combines deep learning–based facial liveness detection with blockchain graph analytics and anomaly detection techniques. By generating a Biometric Confidence Score and a Transaction Risk Score, the hybrid risk assessment engine produces a Composite Risk Index that enables cross-layer intelligence and improved threat detection. Experimental evaluation demonstrated higher overall detection accuracy, reduced false positive rates, and improved traceability compared to standalone systems .The integration of biometric authentication and blockchain forensic analytics strengthens both preventive security (authentication stage) and investigative capability (transaction tracing stage). The model provides a scalable, multi-layered cybersecurity framework suitable for financial institutions, cryptocurrency exchanges, and law enforcement agencies.

In conclusion, the proposed hybrid architecture offers a comprehensive and intelligent solution for combating identity spoofing and cryptocurrency-based cybercrime, contributing to the advancement of secure digital ecosystems and modern cybercrime investigation methodologies.

IX. References.

[1] Z. Akhtar and G. Fumera, "Face Presentation Attack Detection: An Overview," IEEE Signal Processing Magazine, vol. 37, no. 4, pp. 68–82, 2020.

[2] A. R. Gurumurthy, S. K. Reddy, and B. V. K. Vijaya Kumar, "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Access, vol. 9, pp. 147097–147121, 2021.

[3] I. Chingovska, A. Anjos, and S. Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing," in Proceedings of the IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2012.

[4] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," in IEEE International Conference on Image Processing (ICIP), 2015.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[7] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in Security and Privacy in Social Networks, Springer, 2013, pp. 197–223.

[8] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in Financial Cryptography and Data Security, Springer, 2013.

[9] M. Möser, R. Böhme, and D. Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem," in eCrime Researchers Summit (eCRS), 2013.

[10] H. Xu, Y. Chen, and Z. Zhang, "Cryptocurrency Transaction Analysis Using Machine Learning Techniques," IEEE Access, vol. 7, pp. 134–145, 2019.

[11] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[12] J. Bonneau et al., "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in IEEE Symposium on Security and Privacy (SP), 2015

Anamika P. B. is currently pursuing her III B.Sc. in Digital and Cyber Forensic Science at Nehru Arts and Science College. She has developed a focused academic interest in Cyber Forensics and Cyber Security, with particular emphasis on digital evidence analysis and cybercrime investigation methodologies. Her scholarly inclination centers on understanding emerging cyber threats and applying forensic tools for secure digital environments. She actively engages in research-oriented learning to strengthen her analytical and technical competencies in cybersecurity frameworks. Through her academic pursuits, she aims to contribute to advancing secure digital investigation practices in both institutional and industry contexts.

Asish T. Biju is currently pursuing his III B.Sc. in Digital and Cyber Forensic Science at Nehru Arts and Science College. He has cultivated a strong academic interest in Cyber Forensics and Cyber Security, with particular focus on digital evidence examination and cybercrime investigative techniques. His research orientation emphasizes the study of emerging cyber threats and the practical application of forensic tools to safeguard digital ecosystems. He consistently engages in research-driven academic activities to enhance his analytical proficiency and technical expertise in cybersecurity domains. Through sustained scholarly commitment, he aspires to contribute meaningfully to secure and ethical digital investigation practices across academic and professional sectors.

Dr T.RAMAPRABHA M.Sc., M.Phil., Ph.D working as Associate Professor in Department of Digital and Cyber Forensic Science, Nehru Arts and Science College, Coimbatore, India She has Published 60+ Research articles in reputed International Journals, 9 books and 16 Book Chapters. She guided and completed 4 Ph.D Scholars. She took part as a member in several academic bodies. The Author have 28 years of Teaching and 20 Years of research experience and her Areas of Specialization are, Image Processing and Virtual Reality. She was awarded as Best Faculty and Distinguished Professor in her service.

.