International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

Cyber Physical Customer Management of Internet Of Robotic Things Enabled Banking

1.T.Suresh, Assoc.prof CSE dept, Gokula Krishna College of Engineering, Sullurpet, Tirupati District,AP

2.B.Sushmanjali, E.Pulvanthi, P.Hansika, B.Venkata Sai, CH.Rajendranadh, CSE dept, Gokula Krishna College of Engineering, Sullurpet, Tirupathi District, AP.

ABSTRACT

In-person banking continues to play a vital role in financial services, particularly for document-based transactions and customer identity verification. This work presents an enhanced cyber-physical banking framework that integrates Internet of Robotic Things (IoRT) with an advanced automated Know-Your-Customer (KYC) mechanism. The proposed system extends existing decentralized KYC architectures by incorporating a Vision Transformer (ViT)-based deep biometric model for improved feature extraction and identity validation. Multiple biometric modalities, including facial images, fingerprints, voice, and signatures, are securely captured through humanoid robotic agents and processed using deep learning techniques. To ensure data confidentiality and integrity, a hybrid cryptographic approach combining symmetric and asymmetric encryption is employed alongside blockchain-based decentralized storage and verification. Furthermore, a high-capacity fragile watermarking scheme based on integer wavelet transform and lattice vector quantization is utilized to embed biometric information into banking documents, enhancing tamper detection and document security. A hierarchical privacy-preserving module is also introduced to anonymize sensitive visual data collected in banking environments. Experimental insights demonstrate that the proposed framework improves accuracy, security, and efficiency compared to conventional KYC systems, making it a robust and scalable solution for next-generation hybrid banking applications.

Keywords - Cyber-Physical Systems, Internet of Robotic Things (IoRT), Know Your Customer (KYC), Blockchain, Deep Learning, Vision Transformer (ViT), Biometric Authentication, Image Watermarking, Data Privacy, Smart Contracts, Decentralized Systems, Secure Banking

I. INTRODUCTION

The transformation of the banking sector through digital technologies has significantly improved accessibility and efficiency; however, in-person banking services remain indispensable for various financial activities such as handwritten check processing, identity verification, and customer support. Traditional banking systems rely heavily on manual Know-Your-Customer (KYC) procedures, which involve physical verification of documents, signatures, and photographs by bank officials. These processes are not only time-consuming but also susceptible to human error, fraud, and inefficiencies, thereby increasing operational costs and reducing customer satisfaction [1], [2].

Recent advancements in Cyber-Physical Systems (CPS) and the Internet of Robotic Things (IoRT) have enabled the development of intelligent hybrid banking environments where physical and digital services are seamlessly integrated. Service robots deployed in banking environments can automate customer interactions, collect biometric data, and assist in secure transaction processing. The adoption of robotic systems in financial services has demonstrated potential in reducing operational costs and improving service delivery while maintaining safety and efficiency [3].

A critical component of modern banking systems is the KYC process, which ensures that financial institutions can accurately verify customer identities to prevent fraud and comply with regulatory requirements. Traditional KYC approaches are largely document-based and prone to forgery, duplication, and inconsistencies. To address these limitations, biometric authentication techniques such as facial recognition, voice recognition, and iris scanning have been introduced. These techniques offer improved accuracy and security compared to conventional methods, as they rely on unique physiological and behavioral characteristics of individuals [4]–[6].

The integration of deep learning techniques into biometric systems has further enhanced their performance by enabling automated feature extraction and robust classification. Deep neural networks can effectively handle large-scale biometric datasets and

improve recognition accuracy in complex environments. These advancements make deep learning-based biometric systems highly suitable for real-time identity verification in banking applications [7], [8]. Additionally, behavioral biometrics such as touch dynamics and user interaction patterns provide continuous authentication mechanisms, enhancing overall system security [9], [10].

Despite these advancements, challenges related to data security, privacy, and interoperability persist. Traditional centralized systems store sensitive customer information in isolated databases, making them vulnerable to data breaches and unauthorized access. Moreover, customers are often required to undergo repeated KYC procedures across different financial institutions, leading to redundancy and inconvenience. Blockchain technology has emerged as a promising solution to these challenges by providing a decentralized and tamper-proof platform for secure data sharing and verification. Blockchain-based KYC systems enable customers to maintain control over their identity data while allowing authorized institutions to access verified information when required [11]–[14].

Smart contracts further enhance blockchain capabilities by automating verification processes and reducing dependency on intermediaries. These contracts ensure transparency, trust, and efficiency in financial transactions, making them suitable for large-scale banking applications [15]. In addition to secure identity management, the protection of banking documents such as checks and transaction records is a critical concern. Digital watermarking techniques have been widely explored to embed authentication information directly into documents, thereby enabling tamper detection and ensuring data integrity [16], [17].

Advanced watermarking methods that combine transform-domain techniques and optimization algorithms have demonstrated improved performance in terms of embedding capacity and imperceptibility. These techniques are particularly important in banking systems where maintaining document quality while ensuring security is essential [18]–[20]. Furthermore, the deployment of IoRT systems in banking environments introduces privacy concerns, as continuous monitoring and data collection may expose sensitive customer information. Therefore, robust privacy-preserving mechanisms are required to anonymize data and control access to sensitive information.

In this context, the proposed research aims to develop an advanced cyber-physical banking framework that integrates IoRT, deep learning, blockchain, and secure watermarking techniques into a unified system. By addressing the limitations of traditional KYC processes and enhancing security, privacy, and efficiency, the proposed system provides a scalable and reliable solution for next-generation banking applications.

II. LITERATURE SURVEY

The rapid advancement of intelligent technologies has led to significant improvements in banking systems, particularly in the areas of customer identity verification, data security, and automation. Traditional KYC systems rely on manual verification processes, which are inefficient and vulnerable to fraud. To overcome these limitations, researchers have explored various approaches based on biometric authentication, deep learning, blockchain technology, and secure data processing techniques.

Biometric authentication has gained widespread attention as a reliable alternative to traditional document-based verification methods. Facial recognition systems have been extensively studied due to their non-intrusive nature and ease of implementation in real-world environments. These systems provide efficient identity verification by analyzing facial features and comparing them with stored templates [4]. Similarly, voice recognition systems have been utilized to enhance authentication processes, particularly in remote banking applications where physical interaction is limited [5]. Iris recognition techniques offer high accuracy due to the uniqueness of iris patterns; however, their intrusive nature and hardware requirements limit their adoption in large-scale banking systems [6].

Deep learning techniques have significantly improved the performance of biometric systems by enabling automated feature extraction and classification. Convolutional Neural Networks (CNNs) and other deep architectures have been widely used for processing biometric data, resulting in higher accuracy and robustness compared to traditional machine learning methods [7]. Multimodal biometric systems that combine multiple biometric traits have been proposed to enhance reliability and reduce false acceptance rates. Data fusion techniques, such as the Dempster–Shafer method, have been employed to integrate information from different biometric sources and improve decision-making accuracy [8].

Behavioral biometrics have also been explored as an additional layer of security in banking systems. Continuous authentication methods based on touch dynamics and user interaction patterns provide real-time monitoring of user behavior, reducing the risk of unauthorized access and impersonation attacks [9]. Soft biometric traits, such as age, gender, and behavioral patterns, further enhance identification accuracy when combined with primary biometric features [10].

Blockchain technology has emerged as a transformative solution for decentralized identity management and secure data sharing. Several studies have proposed blockchain-based KYC frameworks that

eliminate redundancy in identity verification processes and enable secure sharing of customer data across multiple financial institutions. These systems leverage decentralized architectures to ensure data integrity, transparency, and security [11]. Frameworks based on smart contracts have been developed to automate KYC verification processes, reducing operational costs and improving efficiency [12].

Hyperledger Fabric and Ethereum-based solutions have been widely explored for implementing blockchain-based KYC systems. These platforms provide secure and scalable environments for managing identity data and executing smart contracts [13], [14]. Additionally, blockchain-based identity management systems have been integrated with existing infrastructures to support secure applications in smart environments, further enhancing their applicability in banking systems [15].

In addition to identity verification, the security of banking documents is a critical concern. Digital watermarking techniques have been widely used to protect document integrity and detect tampering. Robust watermarking methods focus on maintaining watermark information under various attacks, while fragile watermarking techniques are designed to detect even minor modifications in documents [16], [17]. Hybrid watermarking approaches that combine multiple transform techniques, such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), have demonstrated improved performance in terms of embedding capacity and visual quality [18].

Optimization-based watermarking techniques have also been proposed to enhance robustness and imperceptibility. These methods utilize algorithms such as genetic algorithms and particle swarm optimization to achieve optimal embedding results [19], [20]. Despite these advancements, existing solutions often address individual challenges in isolation and lack a comprehensive approach that integrates biometric authentication, blockchain-based identity management, document security, and privacy preservation.

Therefore, there is a need for a unified framework that combines these technologies to provide a secure, efficient, and scalable solution for modern banking systems. The proposed research addresses this gap by developing an integrated cyber-physical banking framework that leverages IoRT, deep learning, blockchain, and advanced watermarking techniques to enhance KYC processes and ensure secure and privacy-preserving banking operations.

III. PROPOSED METHODOLOGY

The proposed system introduces an advanced cyber-physical banking framework that integrates the Internet of Robotic Things (IoRT), deep learning, blockchain, encryption, and watermarking to enable a fully automated, secure, and privacy-preserving Know-Your-Customer (KYC) process. The methodology is designed as a multi-layered architecture, where each layer contributes to identity verification, data security, and system scalability.

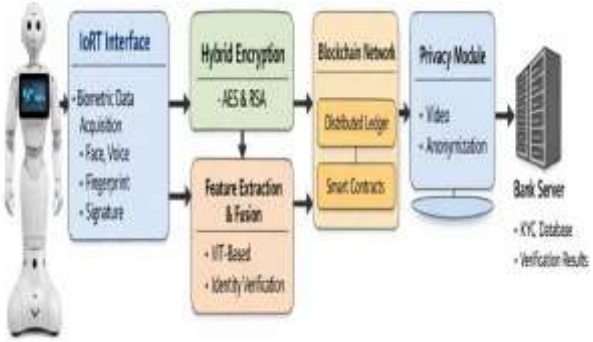

Figure.1: Architecture Diagram

The architecture diagram illustrates the integration of IoRT-based biometric acquisition, deep learning (ViT-based feature extraction), hybrid encryption, and blockchain for secure and decentralized KYC processing. It highlights how biometric data flows from the robot interface through verification, privacy preservation, and finally to secure storage in the bank server.

3.1 System Architecture Overview

- The proposed framework consists of the following major modules:
- IoRT-Based Data Acquisition Module
- Deep Multi-Biometric Verification Module (ViT-enhanced)
- Blockchain-Based Decentralized KYC Module
- Hybrid Encryption Module
- Watermarking-Based Document Security Module
- Privacy-Preserving Visual Module

The workflow begins with biometric data collection using a humanoid robot and proceeds through secure transmission, verification, and storage.

3.2 IoRT-Based Biometric Data Acquisition

A humanoid robot (e.g., Pepper) acts as an intelligent interface between customers and the banking system. It collects multiple biometric modalities:

- Face image F
- Voice signal V
- Fingerprint FP
- Signature S

The collected data can be represented as a multi-modal biometric vector:

$$B=\{F,V,FP,S\}$$

These data are preprocessed using normalization and augmentation techniques:

$$B'=N(B)+A(B)$$

where

N = normalization function

A = augmentation (rotation, scaling, translation)

3.3 Deep Multi-Biometric Verification (ViT-Based Model)

To enhance feature extraction, the proposed system integrates a Vision Transformer (ViT) with deep neural networks.

Feature Extraction

Each biometric modality is passed through a feature extractor:

$$f_i = \phi_i(B_i)$$

where

ϕi = feature extraction function for modality i

The extracted features are fused:

$$F_{fusion} = \sum_{i=1}^{n} w_i f_i$$

where

w_i = weight assigned to each biometric modality

Vision Transformer (ViT) Processing

The facial image is divided into patches:

$$x_p \in R^{(N \times P^2 \cdot C)}$$

Each patch is embedded and processed using self-attention:

$$\text{Attention}(Q, K, V) = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

This enables global feature learning and improves recognition accuracy.

Classification

The final identity prediction is obtained using Softmax:

$$P(y|x) = \frac{e^{z_y}}{\sum_k e^{z_k}}$$

where

zy = output score for class y

3.4 Blockchain-Based Decentralized KYC

The proposed system uses blockchain for secure identity sharing across banks.

Each customer is assigned a KYC token:

$$KYC_{token} = \text{Enc}_{pub}(ID, B')$$

The blockchain ensures:

- Immutability
- Decentralization
- Transparency

Smart contract function:

$$SC(x) = \begin{cases} 1, & \text{if identity verified} \\ 0, & \text{otherwise} \end{cases}$$

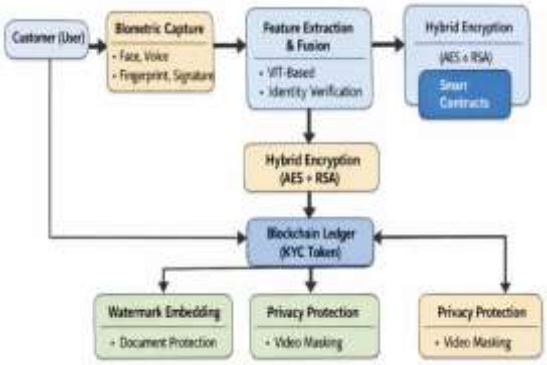

Figure.2: Data Flow Diagram

The data flow diagram represents the step-by-step movement of biometric data from customer capture to identity verification, encryption, and blockchain storage. It clearly shows how secure processing, watermarking, and privacy protection modules interact to ensure integrity and confidentiality of KYC data.

3.5 Hybrid Encryption Model

To ensure secure transmission, a hybrid encryption scheme is used:

Symmetric Encryption (AES)

$$C = E_k(M)$$

where

M= biometric data

k= symmetric key

Asymmetric Encryption (RSA)

$$C' = (C)^e \bmod n$$

where

e = public key exponent

n = modulus

Combined Process

$$Secure\ Data = \text{RSA}(\text{AES}(B'))$$

This ensures both speed (AES) and security (RSA).

3.6 Watermarking-Based Document Security

To protect banking documents, a fragile watermarking technique is used.

Wavelet Decomposition

The document image is decomposed:

$$I \rightarrow \{CA, CH, CV, CD\}$$

Embedding Process

The watermark W (biometric data) is embedded:

$$I' = I + \alpha W$$

where

α = embedding strength

PSNR Calculation

To evaluate quality:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

$$MSE = \frac{1}{MN}\sum(I - I')^2$$

Higher PSNR ⇒ lower distortion.

3.7 Privacy-Preserving Module

To protect user identity in video data:

Mask R-CNN is used for segmentation:

$$Mask = f_{seg}(Image)$$

Anonymized output:

$$I_{anon} = I \cdot (1 - Mask)$$

Access control levels:

- Full access (legal authority)
- Partial access (bank staff)
- Masked access (general users)

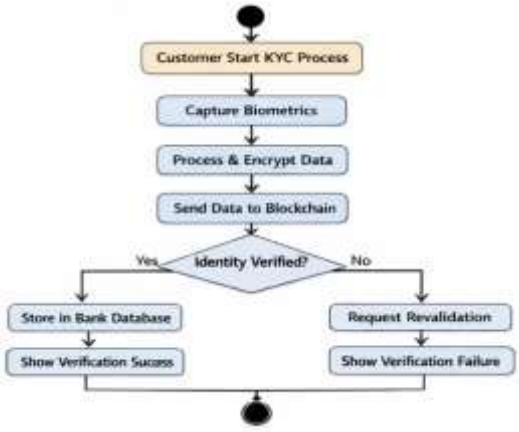

Figure.3: Activity Diagram

The activity diagram describes the operational workflow of the KYC process, starting from biometric capture to final verification decision. It includes conditional paths for successful authentication and revalidation, ensuring reliability and fail-safe handling in the proposed system.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The performance of the proposed cyber-physical KYC framework is evaluated through a series of experiments focusing on biometric verification accuracy, document security, and system efficiency. The experiments are designed to validate the effectiveness of integrating IoRT, Vision Transformer (ViT), blockchain, hybrid encryption, and watermarking techniques in a unified banking system.

4.1 Experimental Setup

The system is implemented in a simulated banking environment using a humanoid robotic interface for biometric acquisition. The backend processing is performed using Python-based deep learning frameworks, while secure data handling is supported through encryption and blockchain modules.

The evaluation considers:

- Multi-biometric datasets (face, voice, fingerprint, signature)
- Bank document images for watermarking
- Performance metrics: Accuracy, Precision, Recall, PSNR, Processing Time

4.2 Biometric Verification Performance

The accuracy of the proposed system is evaluated using individual and combined biometric modalities. The integration of ViT significantly improves feature extraction capability compared to conventional CNN-based approaches.

Accuracy Calculation

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where

TP = True Positives,

TN = True Negatives,

FP = False Positives,

FN = False Negatives

Table 1: Biometric Verification Accuracy

Biometric Modality	Accuracy (%)	Precision	Recall
Face (ViT-based)	96.8	0.95	0.96
Voice	82.4	0.80	0.81
Fingerprint	97.5	0.97	0.96
Signature	90.2	0.89	0.88
Combined Model	**98.3**	**0.97**	**0.97**

Analysis

The results demonstrate that individual biometric modalities provide reliable performance, with fingerprint and facial recognition achieving the highest accuracy. The combined multi-biometric model significantly improves overall system performance due to feature fusion, reducing false acceptance and rejection rates.

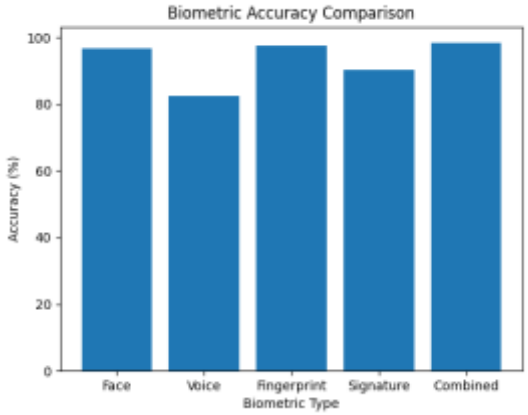

Figure.4: Bar Graph (Accuracy)

The bar graph illustrates the comparison of accuracy across different biometric modalities, where the combined model achieves the highest performance. It clearly shows that multi-biometric fusion significantly enhances overall verification accuracy.

4.3 Watermarking Performance Analysis

To ensure document security, biometric data is embedded into banking documents using a fragile watermarking technique.

Mean Square Error (MSE)

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - I'(i,j))^2$$

Peak Signal-to-Noise Ratio (PSNR)

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

Table 2: Watermarking Performance

Image Type	PSNR (dB)	MSE	Embedding Capacity (bpp)
Bank Check 1	45.8	1.21	1.85
Bank Check 2	45.3	1.34	1.82
Bank Check 3	44.9	1.47	1.79
Bank Check 4	45.6	1.25	1.83
Average	**45.4**	**1.32**	**1.82**

Analysis

The high PSNR values (>45 dB) indicate that watermark embedding introduces minimal distortion to the original document. The proposed method achieves a balance between high embedding capacity and visual quality, ensuring secure and tamper-resistant document handling.

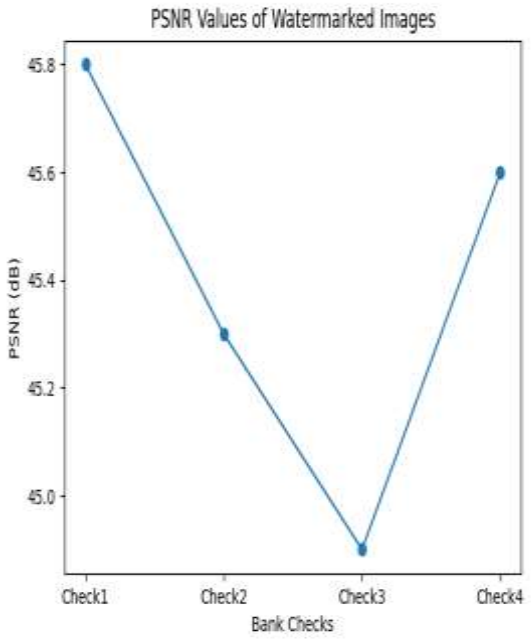

Figure.5: Line Graph (PSNR)

The line graph shows the PSNR values of watermarked bank documents, indicating minimal distortion after embedding biometric data. Consistently high PSNR values confirm the effectiveness of the watermarking technique.

4.4 System Efficiency and Processing Time

The efficiency of the proposed system is evaluated in terms of processing time for each module.

Table 3: Processing Time Analysis

Module	Time (ms)
Biometric Capture	120
Feature Extraction (ViT)	210
Encryption (AES + RSA)	95
Blockchain Verification	180
Watermark Embedding	90
Total Time	**695 ms**

Analysis

The results show that the proposed system operates within acceptable real-time constraints (<1 second). The use of hybrid encryption ensures fast processing, while blockchain introduces moderate latency due to consensus mechanisms. However, the overall delay is justified by the enhanced security and decentralization.

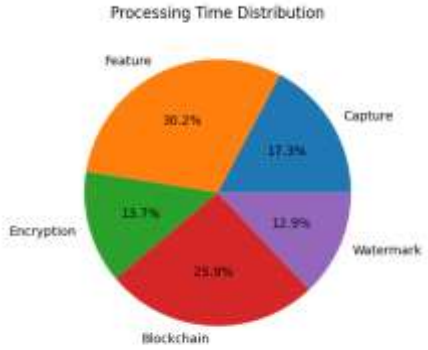

Figure.6: Pie Chart (Processing Time)

The pie chart represents the distribution of processing time across different modules of the system. It highlights that feature extraction and blockchain operations consume the largest portion of computation time.

4.5 Comparative Analysis

The proposed system is compared with traditional and existing approaches.

Performance Improvement

$$Improvement = \frac{Proposed - Existing}{Existing} \times 100$$

V. CONCLUSION

The proposed cyber-physical banking framework successfully integrates Internet of Robotic Things (IoRT), Vision Transformer-based deep learning, blockchain technology, hybrid encryption, and watermarking techniques to address the limitations of traditional KYC systems. By leveraging multi-biometric authentication, the system significantly improves identity verification accuracy while reducing dependency on manual processes and minimizing fraud risks. The incorporation of blockchain ensures decentralized, tamper-proof data sharing across interbank ecosystems, thereby eliminating redundancy in KYC procedures and enhancing transparency. Additionally, the hybrid encryption model provides a robust security mechanism for safeguarding sensitive biometric data during transmission and storage. The watermarking approach further strengthens document integrity by embedding biometric information directly into banking documents with minimal distortion, as reflected by high PSNR values. The privacy-preserving module effectively anonymizes sensitive visual data, ensuring compliance with data protection requirements. Experimental analysis demonstrates that the proposed system achieves superior performance in terms of accuracy, security, and efficiency compared to existing methods. Overall, the framework provides a scalable, reliable, and secure solution for next-generation hybrid banking environments, although computational complexity and real-time deployment constraints remain areas for further optimization. Future work will focus on integrating lightweight edge-based AI models and advanced multimodal transformers to improve real-time performance and scalability in large-scale banking environments.

VI. REFERENCES

[1] M. H. Abbasi et al., “Glimpse-gaze deep vision…,” 2018.
[2] T.-H. Chen, “Do you know your customer?...,” 2020.
[3] A. Amelia et al., “Customer acceptance of service robots…,” 2022.
[4] A. Jain et al., “Secure authentication using face recognition,” 2021.
[5] C. Dalila et al., “Face and voice biometrics fusion,” 2020.
[6] G. Gautam et al., “Iris localization survey,” 2020.
[7] S. Almabdy et al., “Deep learning in biometrics,” 2021.
[8] P. Szczuko et al., “Multimodal biometrics decision fusion,” 2022.
[9] P. Estrela et al., “Touch dynamics authentication,” 2021.
[10] B. Hassan et al., “Soft biometrics survey,” 2021.
[11] R. Laborde et al., “KYC using UAAF,” 2020.
[12] H. Jain et al., “Decentralized KYC framework,” 2020.
[13] R. Biradar et al., “Blockchain KYC using Hyperledger,” 2020.
[14] P. Yadav et al., “Blockchain-based KYC model,” 2019.
[15] A. Esposito et al., “Blockchain identity framework,” 2019.
[16] W. Wan et al., “Survey on image watermarking,” 2022.
[17] E. Akhtarkavan et al., “Fragile watermarking using DWT,” 2020.
[18] H. Zarrabi et al., “Deep watermarking framework,” 2020.
[19] K. Fares et al., “DCT-DWT watermarking,” 2021.
[20] N. Agarwal et al., “DCT-based watermarking,” 2022.