Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 11
november 2025

Blockchain Enabled Biometric Watermarking with Embedding, Extraction and Robust Authentication under Attacks

Tejaswini S[1]

[1]PG Scholar, Department of ECE, BMS College of Engineering, Bengaluru-560004, India

Abstract

This work improves biometric security by combining iris and fingerprint features to create a unique watermark. Unlike traditional storage, the watermark hash is stored on a blockchain for tamper-proof protection. An audit trail records all registration and authentication attempts, ensuring transparency. The system is tested against attacks like noise, compression, rotation, and blurring, with tolerance-based verification to handle minor errors. Finally, multi-user testing shows that the method is secure, reliable, and resistant to tampering.

Keywords: Biometric security, Watermark, Hash, Blockchain, Audit trail, Authentication, Attacks, Tolerance-based verification, Multi-user testing, Tampering.

1. Introduction

In today's digital world, the demand for secure authentication methods is crucial. It has grown more urgent than ever before. Traditional approaches such as passwords, PINs, and smart cards are increasingly vulnerable to risks like theft, duplication, and brute-force attacks. Once stolen, these methods can be easily misused, creating serious security threats. To address these challenges, biometric authentication has emerged as one of the most reliable alternatives. Biometrics leverages unique and permanent human traits such as fingerprints, iris patterns, facial geometry, and voice for identity verification. Among these, iris and fingerprint biometrics are considered the most accurate and secure due to their uniqueness, stability over time, and difficulty in being forged.

By combining iris and fingerprint features, an authentication system can achieve a higher degree of security compared to single-trait systems. Such multimodal biometric fusion not only strengthens the reliability of identity verification but also reduces the chances of spoofing attacks. As a result, iris-fingerprint fusion has become an attractive choice for designing high-security systems in areas like banking, defence, and healthcare.

Despite this advantage, authentication of biometric is not without challenges. A major issue lies in the permanence of biometric traits. Unlike passwords or PINs, biometrics cannot be changed once compromised. A single breach could expose a user's identity permanently. Therefore, protecting biometric templates against tampering and misuse is a critical concern in biometric system design. To counteract this, researchers have suggested different protection approaches, such as cryptographic techniques, cancellable biometrics, and watermarking. Among these, biometric watermarking has proven to be robust potential because it makes it possible to embed or integrate features into distinctive identifiers that can be safely stored and afterwards compared.

The foundational research for this work utilized watermarking techniques for safeguarding biometric templates. It used in particular Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for extracting significant features from iris and fingerprint images. These features were combined to produce a binary watermark, encrypted for added security. In the authentication process, the watermark was recreated from the query images and matched against the stored watermark. P3erformance was quantified based on metrics like Peak Signal-to-Noise Ratio (PSNR) and Bit Error Rate (BER), so that watermark embedding did not deteriorate image quality and could withstand tiny distortions.

While this base system was effective, it had notable limitations. First, the watermark was stored in a traditional database, which is vulnerable to tampering and insider threats. If an attacker replaced or altered the stored watermark, the entire authentication process could be compromised. Second, the system did not explicitly test robustness against common image-

processing attacks like noise, compression, or rotation. Finally, it lacked an audit trail for recording authentication events, which is essential for transparency, monitoring, and forensic analysis in high-security applications.

To overcome these gaps, the extended work introduces several key enhancements:

Blockchain-based storage: Instead of using a conventional database, biometric watermark hashes are stored on a blockchain. Blockchain ensures immutability, meaning once data is stored, it cannot be modified or deleted. It also provides decentralization, removing single points of failure, and tamper-proof protection, making the system significantly more secure.

Audit trail mechanism: Every registration and authentication attempt is logged into the blockchain ledger. This provides accountability and transparency, allowing system administrators to monitor all activities and ensuring forensic traceability in case of disputes or security breaches.

Robustness testing: The system is evaluated under various attacks, including Gaussian noise, Salt & Pepper noise, JPEG compression, rotation, and blurring. These tests simulate real-world scenarios where images may be distorted during acquisition, transmission, or storage. By evaluating performance under these conditions, the system's resilience and practicality are validated.

Tolerance-based authentication: To reduce false rejections, the system introduces a tolerance mechanism. If the regenerated watermark is slightly different but still within an acceptable Bit Error Rate (BER) threshold (e.g., less than 1%), authentication is considered successful. This ensures usability without compromising security, as minor distortions due to noise or compression are tolerated.

Multi-user verification: To demonstrate practical applicability, the system is tested with unknown iris and fingerprint samples. This proves that it can authenticate legitimate users while rejecting imposters, making it scalable and reliable in real-world scenarios.

Through these improvements, the proposed system evolves into a comprehensive biometric authentication framework. It combines iris-fingerprint fusion, encryption, blockchain storage, robustness testing, and audit trails to deliver a solution that is both secure and transparent. Blockchain integration directly addresses the major limitation of insecure database storage, while robustness testing ensures resilience against common attacks. The audit trail enhances accountability, and tolerance-based verification makes the system user-friendly without sacrificing reliability.

This extended work builds on the base watermarking approach to create a more advanced and reliable biometric security system. By integrating DWT-SVD feature fusion, blockchain technology, audit mechanisms, and robustness evaluation, it ensures tamper-proof storage, transparency, and resilience. With its ability to resist attacks and maintain usability, the system is suitable for mission-critical applications such as banking, defence, healthcare, and e-governance, where both security and trust are paramount.

2. BLOCK DIAGRAM OF EMBEDDING PROCESS

The diagram of this block illustrates a biometric watermarking framework where iris and fingerprint images are fused to generate a unique binary watermark. The features are extracted using DWT and SVD, encrypted with XOR, hashed via SHA-256, and finally stored on a blockchain to ensure immutability, transparency, and tamper-proof security. This integration enhances authentication robustness, privacy, and trustworthiness.

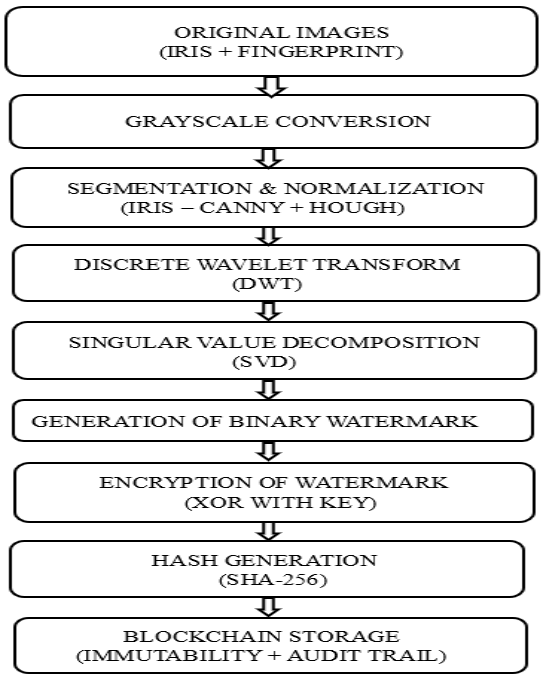


Fig.1. EMBEDDING PROCESS.

Original Images (Iris + Fingerprint):

The procedure starts with9 the biometric input acquisition, i.e., the iris and fingerprint scan of a user. These two modalities are chosen based on their high uniqueness, permanence, and accuracy in identity verification. The iris has rich texture information, and the fingerprint has unique minutiae patterns, hence their combination being very secure against spoofing and reproduction.

Grayscale Conversion:

Since most biometric processing techniques rely on intensity values rather than colour information, both iris and fingerprint images are transformed from RGB (if present) to grayscale. This simplifies computations, reduces storage requirements, and increases the effectual of subsequent feature extraction processes without affecting the quality of biometric details.

Segmentation & Normalization (Iris – Canny + Hough):

During this phase, the iris area is localized and separated from the other areas of the eye image. The detector of the Canny edge is initially used to delineate the iris and pupil boundaries. The Hough Transform is then utilized in order to determine circular boundaries accurately, thus allowing for effective segmentation of the iris. Subsequent to segmentation, normalizing is performed using Daughman's Rubber Sheet Model, which flattens the circular iris pattern onto a rectangle so that differences in pupil dilation, distance, or illumination at the time of image acquisition are accommodated

Discrete Wavelet Transform (DWT):

The normalized iris image undergoes a two-level Discrete Wavelet Transform (DWT), which decomposes the image into four sub-bands (LL, LH, HL, HH). The LL sub-band, containing the approximation and low-frequency details, is chosen for further processing as it retains the most significant biometric information is less sensitive to noise and distortions.

Singular Value Decomposition (SVD):

Next, the LL band from DWT is processed using Singular Value Decomposition (SVD). This step extracts unique and stable features from the iris by decomposing the image matrix into singular values. Since singular values are not variant to common distortions and transformations, they serve as reliable components for robust biometric feature representation.

Generation of Binary Watermark:

The extracted singular values from the iris are fused with the fingerprint features to generate a binary watermark. This watermark acts as a unique identifier for the user. The fusion ensures that the identifier carries information from both biometric traits, thereby increasing robustness, uniqueness, and security.

Encryption of Watermark (XOR with Key): To prevent unauthorized access or tampering, the generated binary watermark is encrypted using the XOR cipher with a secret key. This step transforms the watermark into an unintelligible form, ensuring that even if intercepted, it cannot be reverse-engineered without the correct encryption key.

Hash Generation (SHA-256):

The encrypted watermark is then passed through the SHA-256 hashing algorithm, producing a fixed-length 256-bit hash value. This hash serves as a compact and unique digital signature of the watermark. Importantly, even a minor change in the watermark will result in a completely different hash, ensuring high sensitivity to alterations.

Blockchain Storage (Immutability + Audit Trail):

Finally, the generated hash is stored on a blockchain ledger. Blockchain provides immutability, meaning once the hash is recorded, it cannot be altered or deleted. Additionally, every registration and authentication attempt is logged in the ledger, creating a transparent audit trail. This ensures accountability, prevents insider attacks, and provides a tamper-proof record of biometric verification events.

3. BLOCK DIAGRAM OF EXTRACTING PROCESS

Input Master Share (Encrypted ID):

The process initiates with the input of a master share, which is essentially the encrypted identity of the user. This encrypted ID is securely stored during the embedding stage and serves as the reference for verification during authentication.

Lossless Decryption (XOR with Key):

To retrieve the original pattern, the encrypted master share undergoes decryption using an XOR operation with a secret key. This step ensures lossless recovery of the stored identity, maintaining the protection of the authentication process.

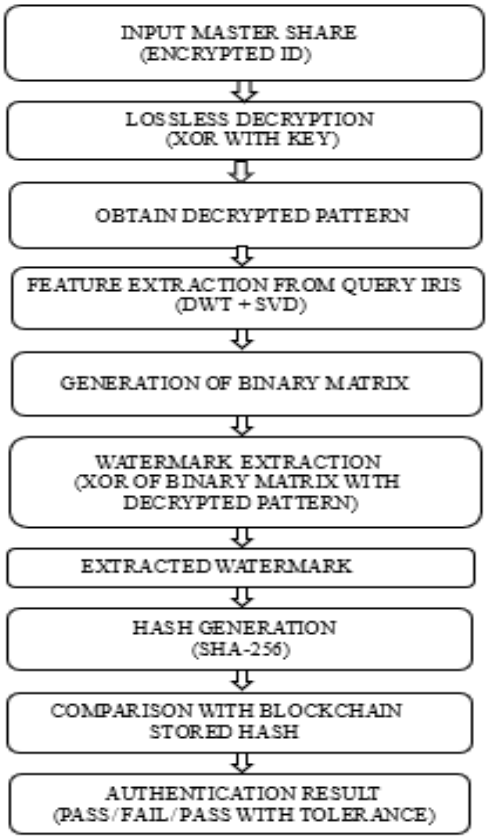


Fig.2. EXTRACTING PROCESS

Obtain Decrypted Pattern:

After decryption, the original decrypted pattern (unique to the user) is obtained. This pattern acts as a reference template and will be compared against the extracted features from the query iris during authentication.

Feature Extraction from Query Iris (DWT + SVD):

The iris image given by the user at the time of authentication undergoes feature extraction. Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are applied to extract stable and robust features from the query iris, ensuring resilience against variations like lighting, scaling, or rotation.

Generation of Binary Matrix:

The extracted features from the query iris are then converted into a binary matrix format. This binary matrix represents the unique biometric watermark derived from the live sample.

Watermark Extraction (XOR of Binary Matrix with Decrypted Pattern):

To retrieve the watermark, the binary matrix of the query iris is XORed with the decrypted pattern obtained earlier. This step effectively extracts the hidden watermark that was embedded during enrolment.

Extracted Watermark:

The result of the XOR operation is the extracted watermark, which uniquely represents the authenticated user's identity. This watermark is crucial for verification and integrity checks.

Hash Generation (SHA-256):

A secure hash value of the extracted watermark is generated using the SHA-256 algorithm. This hash provides a compact digital fingerprint that ensures data integrity and prevents tampering.

Comparison with Blockchain Stored Hash:

The generated hash from the extracted watermark is compared against the corresponding hash securely stored in the blockchain during the embedding phase. Since blockchain guarantees immutability, any mismatch immediately reveals tampering or fraudulent attempts.

Authentication Result (Pass/Fail/Pass with Tolerance):

Finally, based on the comparison result, the system outputs the authentication status. If the generated hash matches the blockchain-stored hash, the result is "Pass." If it does not match, the result is "Fail." In cases of minor acceptable deviations, the system may allow "Pass with tolerance," enhancing flexibility without compromising security.

4. Results

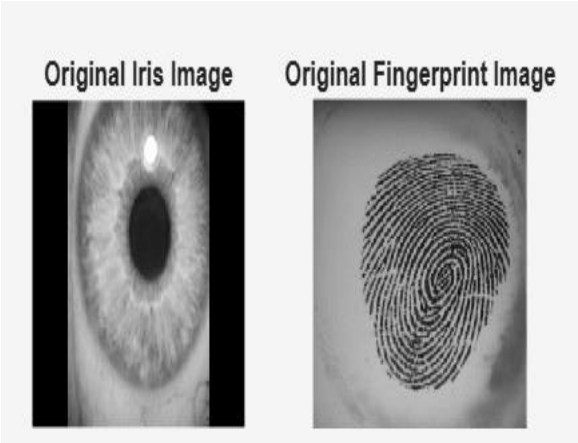


Fig.3. Original iris and fingerprint image

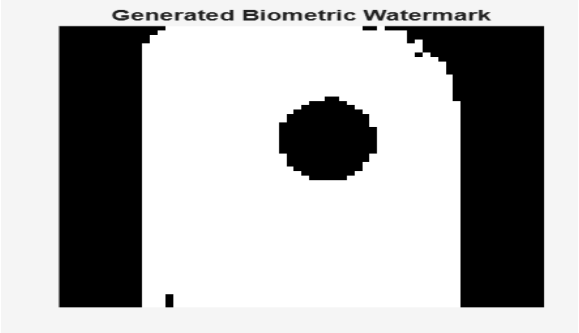


Fig.4. Generated Biometric Watermark

Fig.5. Stored Watermark Hashed

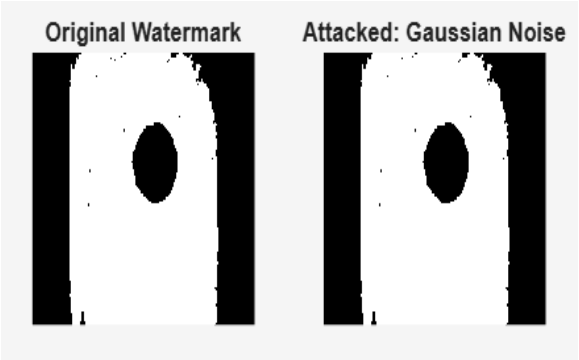


Fig.6. Gaussian Noise attack

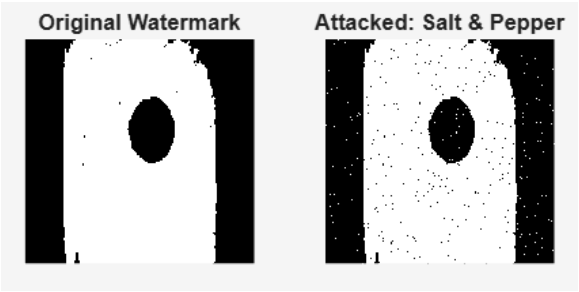


Fig.7. Salt & Pepper attack

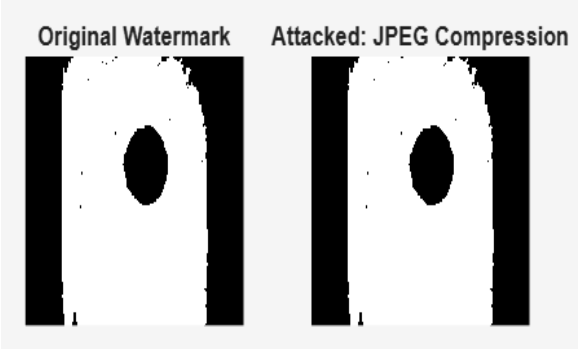


Fig.8. JPEG Compression

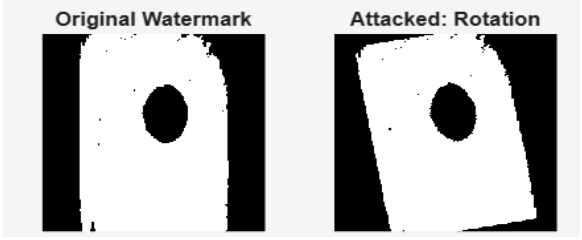


Fig.9. Rotation

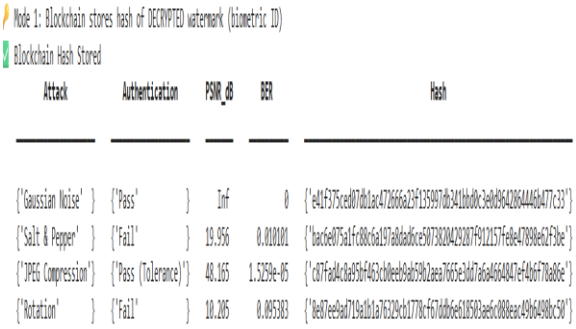
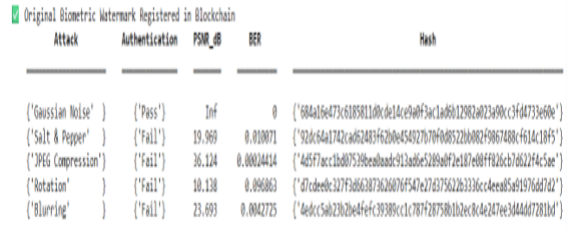


Fig.10. PSNR & BER values of attacks




```
-- Blockchain Ledger Log ---
  Action: 'Register'
    Hash: '684a16e473c6185811d0cde14ce9a0f3ac1ad6b12982a023a90cc3fd4733e60e'
  Status: 'Stored'

  Action: 'Authentication'
  Attack: 'Gaussian Noise'
    Hash: '684a16e473c6185811d0cde14ce9a0f3ac1ad6b12982a023a90cc3fd4733e60e'
  Status: 'Pass'

  Action: 'Authentication'
  Attack: 'Salt & Pepper'
    Hash: '92dc64a1742cad62483f62b0e454927b70f0d8522bb082f9867488cf614c18f5'
  Status: 'Fail'

  Action: 'Authentication'
  Attack: 'JPEG Compression'
    Hash: '4d5f7acc1bd07539bea0aadc913ad6e5289a0f2e187e08ff826cb7d622f4c5ae'
  Status: 'Fail'

  Action: 'Authentication'
  Attack: 'Rotation'
    Hash: 'd7cdee0c327f3d663873626076f547e27d375622b3336cc4eea85a91976dd7d2'
  Status: 'Fail'

  Action: 'Authentication'
  Attack: 'Blurring'
    Hash: '4edcc5ab23b2be4fefc39389cc1c787f28758b1b2ec8c4e247ee3d44dd7281bd'
  Status: 'Fail'
```

Fig.11. Blockchain Ledger Log

5. Conclusion

This work presented a blockchain-based biometric watermarking system that integrates iris and fingerprint fusion with DWT–SVD feature extraction to generate a unique and robust biometric watermark. By applying encryption and SHA-256 hashing, the system ensures security, immutability, and transparency of stored biometric identities on a blockchain ledger.

The introduction of an audit trail mechanism strengthens accountability, as every registration and authentication attempt is permanently logged with details of the performed action, attack type, hash, and status. Furthermore, robustness testing under common attacks like Gaussian noise, salt & pepper noise, JPEG compression, rotation, and blurring demonstrated that the proposed framework effectively resists tampering while maintaining acceptable performance levels.

Performance evaluation using PSNR (visual quality) and BER (bit error rate) highlights the balance achieved between accuracy and resilience. Even under distortion, authentication tolerance enables reliable verification without compromising system security.

Overall, the integration of biometric fusion, blockchain storage, attack simulation, and forensic audit trail provides a comprehensive, secure, and future-ready biometric authentication framework. This approach not only enhances robustness against manipulation but also offers decentralized trust and tamper-proof identity verification, making it suitable for real-world security applications.

6. Future Scope

The system proposed above can further be enhanced and extended in various w4ays. For the future, deep learning techniques can be used for feature extraction instead of alone DWT and SVD, which can offer stronger and more precise b9iometric characteristics. The system can be extended to other biometric characteristics such and voice or palmprint, and hence it is a full-fledged multi-modal authentication system. Smart contracts can be added to blockchain to automate the logging and authentication process, and mobile devices and IoT hardware can support lightweight blockchain models for real-time implementation. To maximize privacy, methods like homomorphic encryption or federated learning can be used in conjunction with watermarking such that biometric data is still secure when being processed. The system may also be evaluated against more robust attacks like spoofing, deepfakes, or adversarial manipulation in order to make the system robust. For the large-scale application, scalability of blockchain storage and interoperability across different organizations can be investigated. Lastly, energy-efficient mechanisms and algorithms for updating or revoking biometric data can be incorporated to make the system more practical, secure, and applicable in real-world contexts like banking, healthcare, border control, and e-voting.

References

[1] S. D. Mahmood, F. Drira, H. Falih Mahdi and A. M. Alimi, "Secure Medical Image Sharing: Technologies, Watermarking Insights, and Open Issues," in IEEE Access, vol. 13, 2025.

[2] S. Wu, W. Lu and X. Luo, "Robust Watermarking Based on Multi-Layer Watermark Feature Fusion," in IEEE Transactions on Multimedia, vol. 27, 2025.

[3] R. E. Arevalo-Ancona and M. Cedillo-Hernandez, "Improving the Security of Medical Imaging via DFT-Based Reversible Watermarking and Deep Learning-Based Zero-watermarking," 2024 47th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 2024.

[4] Tong Liu, Si-Nga Lai, Xiaochen Yuan, Yue Liu, Chan-Tong Lam, "A novel blockchain-watermarking mechanism utilizing interplanetary file system and fast walsh hadamard transform," in iScience, Volume 27, Issue 9,2024.

[5] S. K. Padhi, A. Tiwari and S. S. Ali, "Deep Learning-Based Dual Watermarking for Image Copyright Protection and Authentication," in IEEE Transactions on Artificial Intelligence, vol. 5, no. 12, pp. 6134- 6145, Dec. 2024.

[6] S. Tang, J. Ni, W. Su and Y. Zhang, "DWW: Robust Deep Wavelet-Domain Watermarking with Enhanced Frequency Mask," in IEEE Signal Processing Letters, vol. 31, pp. 3074-3078, 2024.

[7] F. Yu, J. Peng, X. Li, C. Li and B. Qu, "A Copyright-Preserving and Fair Image Trading Scheme Based on Blockchain," in Tsinghua Science and Technology, vol. 28, no. 5, pp. 849-861, October 2023.

[8] M. S. Rana, M. M. Hasan and S. K. Sinha Shuva, "Digital Watermarking Image Using Discrete Wavelet Transform and Discrete Cosine Transform with Noise Identification," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022.

[9] B. Wang, S. Jiawei, W. Wang and P. Zhao, "Image Copyright Protection Based on Blockchain and Zero-Watermark," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 4, pp. 2188-2199, 1 July-Aug. 2022.

[10] R. Deepika, M. Shambhavi, R. Impana, A. Shishira and L. Krishna, "Zero-Bit Watermarking Technique for Generation of Unique ID Using Biometric Images," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022.

[11] V. J. Subashini, S. Poornachandra and M. Ramakrishnan, "A fragile watermarking technique for fingerprint protection, "2021 IEEE Recent Advances in Intelligent Computational Systems (RAICS).

[12] B. Samira, R. H. Lamia and E. B. A. Najoua, "Biometric Template Security Using Watermarking Reinforcement Based Cancellable Transformation," 2021 International Conference on Cyberworlds (CW), Caen, France, 2021.

[13] A. Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat and K. Muhammad, "DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5108-5117, July 2021.

[14] W. H. Alshoura, Z. Zainol, J. S. Teh, M. Alawida and A. Alabdulatif, "Hybrid SVD-Based Image Watermarking Schemes: A Review," in IEEE Access, vol. 9, pp. 32931-32968, 2021.