IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Zero-Bit Biometric Watermarking Using Machine Learning and Deep Learning

Chandan K N[*1], Lavanya D[*2], Chaithresh S[*3], Likith Gowda H S[*4], Yogesh H C[*5]

[*1]Asst professor, Department of Information Science & Engineering, Maharaja Institute of Technology Mysore, Karnataka, India

[*2,3,4,5]Student, Department of Information Science & Engineering, Maharaja Institute of Technology Mysore, Karnataka, India

ABSTRACT

The Zero-Biometric Watermarking System secures digital files using iris and fingerprint biometrics as cryptographic keys. It integrates Machine Learning and Deep Learning for encryption and user authentication across images, audio, and PDFs. DWT-SVD is used for watermark embedding, AES for encryption, and CNNs for biometric verification. Telegram-based OTPs and secret keys enhance real-time security. The system ensures tamper resistance, format flexibility, and reliable protection for sensitive data.

Keywords:

Biometric Watermarking, Iris Authentication, Fingerprint Recognition, Machine Learning, Deep Learning, DWT-SVD, AES Encryption, CNN Classification, Secure File Transfer, Telegram OTP

I. INTRODUCTION

In today's digital age, securing multimedia files from tampering and unauthorized access is crucial. Our project uses iris and fingerprint biometrics for authentication and encryption, securing images, audio, and PDFs. It combines DWT-SVD watermarking, AES encryption, and CNN-based verification with Telegram OTPs for real-time access control. The system enhances data protection, supports web integration, and minimizes reliance on traditional passwords.

II. METHODOLOGY

The proposed system ensures secure authentication and encryption of multimedia files (images, audio, PDFs) using iris and fingerprint biometrics. Users register their biometric data, which is processed via CNNs and used as secret keys for embedding watermarks using DWT-SVD, followed by AES encryption to protect file contents.

During encryption, a Telegram-based OTP is generated, adding real-time identity verification. Decryption requires re-uploading the same biometric data, entering the OTP, and the secret key. This multi-factor, CNN-verified approach ensures high security, making the system ideal for safeguarding sensitive digital content in sectors like healthcare, law, and finance.

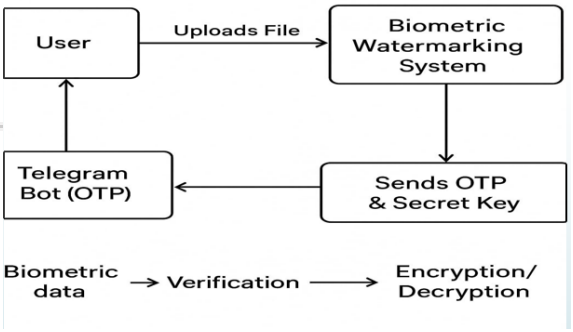

Figure 1:Context Diagram for Biometric Watermarking

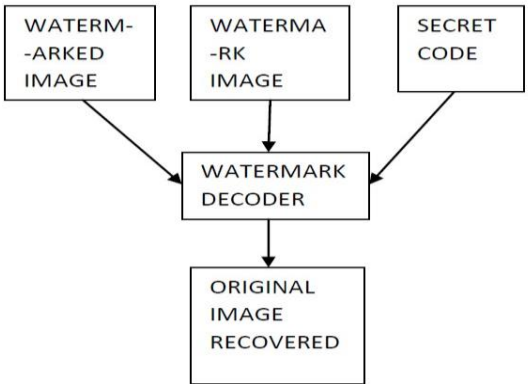

Figure 2: System Architecture for Biometric Watermarking

III. PROBLEM STATEMENT

As digital file exchange becomes more prevalent, authenticating and keeping confidential sensitive information such as images, sound, and text has emerged as an essential problem. Conventional password-based solutions are susceptible to attacks, and watermarking alone is insufficient to provide secure access control.

A strong security mechanism is urgently needed, incorporating biometric authentication with high-end encryption and watermarking methods. The system proposed herein addresses this issue by employing distinctive biometric features (iris and fingerprint), along with DWT-SVD-based watermarking and AES encryption, for secure, tamper-proof data preservation and controlled access via OTP authentication.

IV. EXISTING SYSTEM

Current digital file protection systems primarily depend on password-based encryption and basic watermarking methods like LSB and DCT, which are susceptible to brute-force attacks, phishing, and tampering techniques such as compression and noise. While some systems use single-mode biometric authentication (e.g., fingerprint or facial recognition), these lack adaptability and resilience against spoofing.

Additionally, most existing solutions do not offer a unified framework that combines strong biometric verification with robust, cross-format watermarking. This absence of comprehensive security reduces their practicality for real-world, multi-platform deployments.

V. PROPOSED SYSTEM

The system provides end-to-end protection for multimedia files like images, audio, and PDFs through biometric watermarking and cryptography. CNNs extract distinct iris and fingerprint features, used for hybrid DWT-SVD watermarking and AES encryption to enhance both security and robustness against attacks. OTPs are generated via Telegram Bot API for real-time session authentication, while timestamps ensure auditing and traceability.

At decryption, users must submit the original biometrics, the received OTP, and a secret key; CNN models re-verify features before access is granted. This multi-layer architecture ensures only legitimate users can encrypt or decrypt files. Designed as a web application, it allows easy registration, login, and document management. The system ensures confidentiality, integrity, and accountability, making it suitable for sensitive environments like defense, healthcare, e-governance, and legal storage.

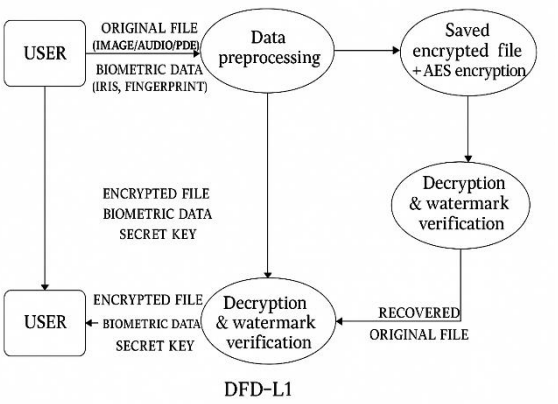

Figure 3: Dataflow Diagram for Biometric Watermarking

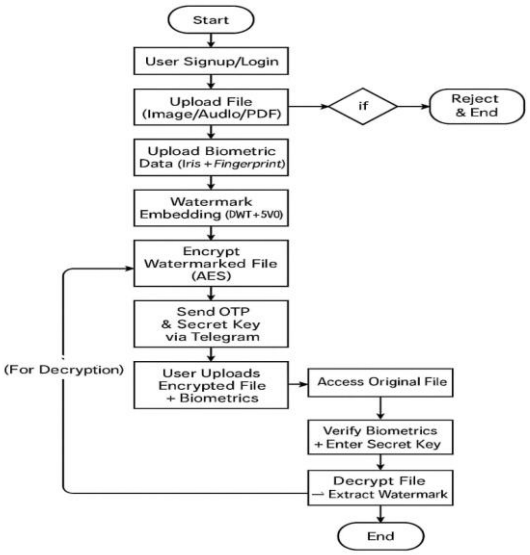

Figure 3: Activity Diagram for Biometric Watermarking

VI. RESULT ANALYSIS

The developed system was evaluated using a diverse set of 60 files—comprising 20 images, 20 audio clips, and 20 PDF documents. Out of these, 56 files were accurately decrypted using the corresponding biometric credentials, yielding a decryption success rate of 93.3%. The few failures were attributed to issues like incorrect iris/fingerprint inputs, invalid OTP entries, or mismatched decryption keys. These results highlight the robustness of the system in maintaining data security across various file formats through user-specific biometric encryption.

The underlying biometric classification model was trained using 419 labeled samples from two distinct classes. During testing, real-time inputs were provided to validate system consistency. The system's ability to securely process multiple file types while maintaining a high success rate demonstrates its practical applicability in scenarios that demand confidentiality, secure access, and identity verification.

VII. CONCLUSION

In this research, a biometric watermarking system was developed to encrypt image, audio, and PDF files. The system had a decryption rate of 93.3% and effective processing rates, with encryption, OTP transmission, and decryption time averaging 2, 2.5, and 3 seconds per file, respectively. These findings validate the feasibility of the

system for real-time practical secure file sharing and biometric identification.

Although the system offers advantages such as multi-format support, high accuracy, and robust security through dynamic AES key generation, certain limitations were identified. That is, the efficiency of the system can be reduced with poor-quality biometric inputs, and CNN-based biometric classification accuracy can be reduced with poorly acquired biometric samples. These aspects point towards scope for improvement in the future to render the system robust and reliable for real-world usage.

In conclusion, the biometric watermarking system is a secure and reliable file encryption and biometric authentication solution, though further refinements are required to counter noted limitations.

VIII. REFERENCES

[1] Maha Charfeddine D1, et al., "Audio Watermarking for Security and Non-Security Applications," IEEE Access, 2022. DOI: 10.1109/ACCESS.2022.3145950

[2] Ruotong Xiang, et al., "A Trusted Medical Image Zero-watermarking Scheme Based On DCNN and Hyperchaotic System," IEEE Journal of Biomedical and Health Informatics, 2025. DOI: 10.1109/JBHI.2025.3550324

[3] T. Balamani et al., "Biometric Authentication for Accident Victims using IoT," Proceedings of the International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI-2025),2025.DOI:10.1109/ICMSCI62561.2025.10894545

[4] B. Mokashi, J. D. Pujari, V. S. Bhat and L. Sagar J, "Dual Watermarking Technique for Image Authentication using Biometrics," 2021 IEEE Mysore Sub Section International Conference (MysuruCon), 2021. DOI: 10.1109/MYSURUCON52639.2021.9641721

[5] Y.-A. Wang, Z. Wang, L. Zou, B. Shen and H. Dong, "Detection of Perfect Stealthy Attacks on Cyber-Physical Systems Subject to Measurement Quantizations: A Watermark-Based Strategy," IEEE/CAA Journal of Automatica Sinica, vol. 12, no. 1, pp. 114-125, Jan. 2025.

[6] C.N. Savithri, S. Lakshman Arun, B.S. Pradyumna Bhat, N. Udhaya Kiran and S. Sriharan, "CRYPTOGUARD – IoT Biometric Home Security," 2024 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), 2024. DOI: 10.1109/ICPECTS62210.2024.10780420

[7] S.M. Kolekar, A.P. Pimpalkar, R.P. More, M.B. Gulame, S.A. Hirve and N.N. Thorat, "Digital Image Tamper-forgery Detection in Security," 2024 2nd International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), 2024. DOI: 10.1109/ICMACC62921.2024.10894413

[8] Deepika R, Shambhavi M, Impana R, Shishira A.P, and Lavanya Krishna, "Zero-Bit Watermarking Technique for Generation of Unique ID Using Biometric Images," 2022 International Conference on Intelligent Technologies(CONIT).DOI: 10.1109/CONITS5038.2022.9848041

[9] A.C.H. Chen, "Evaluation of Advanced Encryption Standard Algorithms for Image Encryption," 2024 International Conference on Smart Systems for Applications in Electrical Sciences (ICSSES), 2024. DOI: 10.1109/ICSSES62373.2024.10561385

[10] K. Yang, P. Miller and J. Martinez-del-Rincon, "Convolutional Neural Network for Software Vulnerability Detection," 2022 Cyber Research Conference Ireland (Cyber-RCI), 2022. DOI: 10.1109/19/Cyber-RC155324.2022.10032684

[11] Kumar and S. Jain, "Deep Learning based Fusion for a Multi-Biometric Identification Using LSTM," 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), 2024. DOI: 10.1109/ACET61898.2024.10730213

[12] Wone, J. Di Manno, C. Charrier and C. Rosenberger, "Fingerprint Spoof Generation Using Style Transfer," IEEE Transactions on Biometrics, Behavior, and Identity Science, 2025. DOI: 10.1109/TBIOM.2025.3545308

[13] Ajmeera Kiran, P. Vijayakarthik, and Suragouni Nikitha, "Implementation of 3-Level Security System Using Image Grid Based Authentication System," 2023 International Conference on Computer Communication and Informatics (ICCCI), Jan. 23-25, 2023, Coimbatore, INDIA. DOI: 10.1109/ICCC156745.2023.10128606

[14] Philipp Terhörst, Daniel Fährmann, Naser Damer, Florian Kirchbuchner, and Arjan Kuijper, "On Soft-Biometric Information Stored in Biometric Face Embeddings," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 4, October 2021. DOI: 10.1109/TBIOM.2021.3093920

[15] Shilin Liu and Yongzhen Li, "Research on Enhanced AES Algorithm Based on Key Operations," 2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT). DOI: 10.1109/ICCASIT58768.2023.10351719