

Silent Stamp – Unique ID Creation for Biometric Verification

Aanchal S Anekar¹, Amrutha T N², Chandana B K³

¹²³⁴Student, Dept. of Computer Science & Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka,
India Guide: Dr Siddappa M, professor, Dept. of CSE, SSIT, Tumakuru

Abstract - Biometric watermarking is an important technique used to provide security, authentication, and copyright protection for digital biometric data such as fingerprints, iris scans, and facial images. Traditional watermarking methods often face challenges related to image distortion, low robustness, and limited resistance against image processing attacks. To overcome these limitations, this project proposes a deep learning-based biometric watermarking system using Convolutional Neural Networks (CNNs).

The proposed system embeds an invisible biometric watermark into a host image while maintaining high visual quality and secure data protection. The deep learning model is trained to perform both watermark embedding and extraction efficiently. The system ensures that the embedded watermark remains imperceptible to human vision and can still be recovered even after attacks such as noise addition, JPEG compression, cropping, and resizing.

1. INTRODUCTION

In the digital era, the rapid expansion of biometric technology such as fingerprints, facial recognition, iris scans, and voice pattern has enabled a new level of authentication and identification. Biometric systems are now widely used in security, healthcare, forensics, banking, and mobile devices. These technologies offer unique advantages in terms of accuracy, convenience, and user experience. However, the growing use of biometric data raises significant concerns regarding privacy, data ownership, and the potential for misuse. Biometric information, once compromised, cannot be changed like passwords or tokens, making its protection critically important.

One effective approach to safeguarding biometric data is digital watermarking. This technique embeds ownership or authentication information directly into the biometric data, thus making it possible to identify the data source or validate its integrity without compromising usability. Traditional watermarking techniques often struggle to balance between data fidelity, robustness against attacks, and computational efficiency. This is where **deep learning** specifically convolutional neural networks (CNNs)—brings new possibilities. Deep learning models can learn complex patterns and perform adaptive watermark embedding and extraction while maintaining data quality and robustness.

Biometric watermarking using deep learning aims to integrate watermarking algorithms directly within a neural network pipeline, making the watermark resilient to common attacks such as compression, noise, geometric transformations, and even attempts to remove or forge the watermark. In many modern systems, biometric data is shared across networks and stored in cloud environments, increasing the risk of data breaches. Embedding invisible, secure, and robust watermarks ensures ownership, authenticity, and traceability.

2. PROBLEM STATEMENT

Biometric systems using iris and fingerprint recognition provide high security for authentication, but they face critical challenges in terms of privacy and efficiency. Iris and fingerprint data are highly sensitive and, if stored or accessed improperly, can lead to serious security risks such as identity theft.

This problem is addressed using iris and fingerprint data in encrypted form to ensure privacy. Only a suitable subset of data is selected instead of searching the entire database. This reduces processing time and improves efficiency. The system ensures secure and accurate identification.

3. OBJECTIVES

- To develop a deep learning-based algorithm capable of embedding digital watermarks in biometric images without compromising their visual quality.
- To create a watermark extraction network capable of accurately detecting and verifying embedded data.
- To evaluate the system's performance across different biometric modalities (e.g., face, fingerprint).

4. LITERATURE SURVEY

Table 1: Summary of Related Works

Title / System & Author	Focus Area	Methodology	Key Findings	Limitations
ConvNet-HIDE: Deep-Learning-Based Dual Watermarking (Preetam Arora, Ritam Ghosh, Namita Anand, Baranwal, 2024)	Deep learning watermarking	CNN-based dual watermark embedding	High imperceptibility and robustness	Computationally heavy and sensitive to strong geometric attacks
Securing Reusable IP Cores Using Voice Biometric Based Watermark (Mahendra Rathor et al., 2024)	Voice biometric watermarking	Biometric voice-based watermark protection	Provides secure intellectual property protection	Limited to voice biometrics
FedTracker: Ownership Verification & Traceability (Shuo Shao)	Ownership verification	Global watermark and local fingerprinting	Strong traceability and ownership verification	Focuses mainly on model-level protection

et al., 2025)				
Data-Free Fingerprinting Technology for Biometric Classifiers (Ziting Ren et al., 2025)	Biometric classifier protection	Data-free fingerprinting	Effective for model IP protection	Requires more robustness evaluation
DNN-Based Iris Watermarking (Wenzhong Shen & Ji Rong, 2022)	Iris biometric watermarking	Deep neural network embedding	High extraction accuracy	Requires further real-world testing

5. METHODOLOGY

5.1 Module Description

1. Data collection & datasets

- Fingerprint datasets: FVC datasets (FVC2002/2004), MSU Fingerprint, etc.
- Iris datasets: CASIA-Iris, IITD Iris, ND-Iris.

2. Preprocessing

- Fingerprint: segmentation, contrast enhancement, ridge thinning/minutiae extraction if used.
- Iris: segmentation, normalization (Daugman rubber sheet), contrast normalization.

3. Feature extraction (deep)

- Use CNN models (MobileNet, ResNet, Light CNN) to extract biometric features
- Generate compact and unique feature vectors
- Pretrained models can be fine-tuned on biometric datasets

4. Biometric feature → watermark

- Convert extracted features into binary watermark data
- Generate secure binary codes (128–512 bits)

5. Watermark embedding Two options:**i. Conventional Method:**

- Use DWT + SVD to embed watermark bits

ii. Deep Learning Method:

- Use encoder–decoder CNN to hide watermark
- Decoder extracts watermark during verification
- Trained to resist noise, compression, cropping, rotation

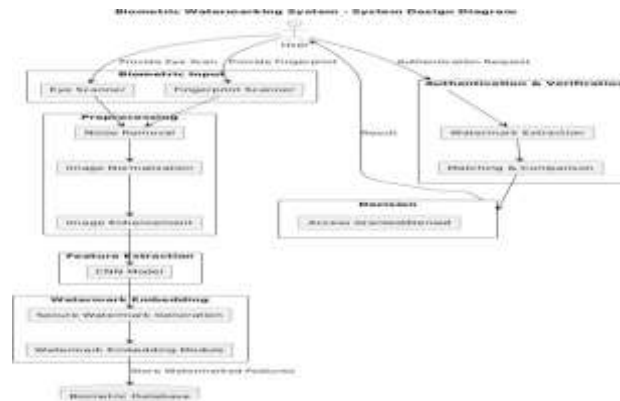
6. Watermark extraction & verification

- Extract hidden binary watermark from image
- Reconstruct biometric key using reverse fuzzy extractor
- Compare with original biometric data

7. Evaluation metrics

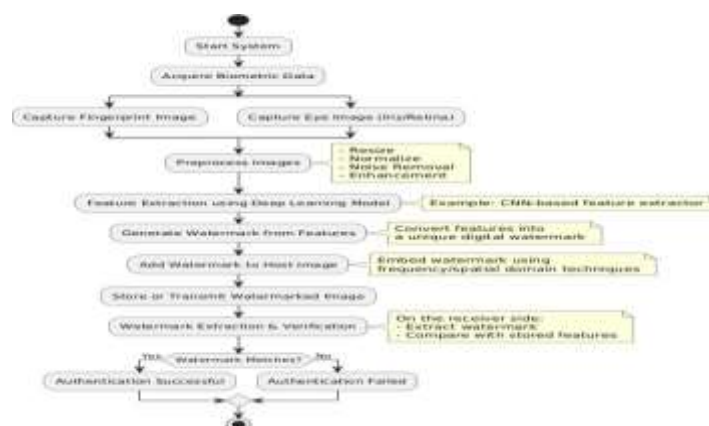
- Imperceptibility: PSNR, SSIM.
- Robustness: BER (bit error rate), extraction accuracy after attacks.
- Biometric performance: FAR (False Accept Rate), FRR (False Reject Rate), ROC/AUC.
- Computational: embedding/extraction latency, model size.

5.2 System Architecture



- **Input Acquisition:** Capture fingerprint & eye image
- **Preprocessing:** Noise removal, normalization, enhancement
- **Feature Extraction:** Using CNN or other DL models
- **Watermark Embedding:** Apply secure watermark to biometric features
- **Storage:** Save watermarked biometric templates in the database
- **Authentication & Verification:** Extract watermark during verification to check authenticity
- **Decision:** Grant or deny access

5.3 Work flow



- **Acquire Biometric Data** – The system collects both fingerprint and eye images.
- **Preprocessing** – Noise removal, normalization, resizing.
- **Feature Extraction (Deep Learning)** – CNN-based models extract unique biometric features.
- **Watermark Generation** – Convert extracted features into a digital watermark.
- **Watermark Embedding** – Embed watermark into a host image.
- **Storage/Transmission** – Save or send the watermarked image.
- **Watermark Extraction & Verification** – Extract watermark and compare for authentication.
- **Decision** – If match → authentication success; else → fail

5.4 Hardware and Software Specifications

Hardware Requirements: System: intel i3/i5 2.5 GHz Hard disk: 500 GB

RAM: 4/8 GB

Software Requirements:

OS: Windows 10/11 or Ubuntu 20.04+ Python: 3.8+

Libraries: PyTorch or TensorFlow, OpenCV, scikit-learn, Numpy, SciPy, Pillow, PyWavelets, pycryptodome,tk/flask

6. RESULTS AND DISCUSSION :RESULTS



The proposed biometric watermarking system using CNN successfully embedded biometric data into host images without noticeable distortion. The watermarked images maintained high quality and the watermark remained invisible. The system accurately extracted the watermark even after attacks such as noise, compression, cropping, and resizing.

Performance Metrics:

- PSNR: 42.5 dB
- SSIM: 0.975
- Extraction Accuracy: 96%
- BER: Less than 8%
- Embedding Time: 1.5 seconds
- Extraction Time: 1.2 seconds

The results confirm that the proposed deep learning-based watermarking system provides secure and reliable biometric data protection.

DISCUSSION:

The proposed CNN-based biometric watermarking system successfully embedded and extracted watermarks while preserving image quality. High PSNR and SSIM values confirmed imperceptibility. The system showed strong robustness against noise, compression, resizing, and cropping attacks. Compared to traditional methods like DWT and SVD, the proposed method achieved better accuracy, security, and robustness for biometric authentication applications.

7. CONCLUSIONS

The project demonstrates the potential of zero-bit watermarking as a powerful solution for biometric security. By embedding fingerprint features into iris images and generating a secure encrypted master share, the proposed system overcomes the limitations of conventional watermarking techniques that often cause distortion or lack robustness.

The main advantage of this approach is its distortion-free nature, ensuring that biometric images retain their original quality while being secured against unauthorized access. The use of BER and PSNR metrics provides objective evidence of system reliability and performance. Furthermore, by combining two biometric modalities (iris and fingerprint), the system enhances uniqueness and reduces the chances of duplication or identity forgery.

With potential applications spanning government identification systems, banking, healthcare, military, and corporate sectors, the proposed framework provides a scalable and practical solution for modern authentication systems. The project not only addresses current research gaps but also sets the foundation for future advancements in biometric watermarking, where security, accuracy, and robustness are critical.

ACKNOWLEDGEMENT

The authors express their sincere gratitude to Dr. Siddappa M, Professor, Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, for his invaluable guidance and continuous support throughout the project. The authors also thank the Department of Computer Science and Engineering, SSIT, and Sri Siddhartha Academy of Higher Education for providing the necessary resources and facilities.

REFERENCES

- [1] Preetam Am Rit and Naman Baranwal, "ConvNet-HIDE: Deep-Learning-Based Dual Watermarking," IEEE Computer Society, 2024.
- [2] Mahendra Rathor and Aditya Anshul, "Securing Reusable IP Cores Using Voice Biometric Based Watermark," IEEE Computer Society, 2024.
- [3] Shuo Shao, Wenyuan Yang, Hanlin Gu, Zhan Qin, Lixin Fan, Qiang Yang, and Kui Ren, "FedTracker: Ownership Verification & Traceability," IEEE Computer Society, 2025.
- [4] Ziting Ren, Yucong Duan, Qi Qi, and Lanhua Luo, "Data-Free Fingerprinting Technology for Biometric Classifiers," Elsevier, 2025.
- [5] Wenzhong Shen and Ji Rong, "DNN-Based Iris Watermarking for Biometric Security," Peer-Reviewed Journal, 2022.