IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14614

A Survey on Secure Biometric Watermarking Using Rubik Encryption and Convolutional Neural Network

Dr. Sunita Chalgeri[1], Deeksha S[2], Ananya S[3], Abeni B[4] , Harshadithya G V[5]

Associate Professor, Department of Computer Science and Engineering, K.S.Institute of Technology (KSIT), Bengaluru, India[1]

Student, Department of Computer Science and Engineering, K.S. Institute of Technology (KSIT), Bengaluru, India[2-5]

Abstract: In modern digital systems, ensuring data integrity and identity verification has become vital, particularly in areas like government records, legal documents, and banking. This paper presents a survey of a biometric watermarking system that combines iris and fingerprint traits to enhance authentication. The proposed approach uses a Rubik Cube-based encryption algorithm to secure extracted biometric features, which are then verified using Convolutional Neural Networks (CNNs). The objective is to embed the encrypted biometric information into host images, producing a watermark that is resistant to tampering and forgery. This paper reviews the underlying techniques, compares them with existing methods, and highlights the security and privacy advantages of the system. The study is further motivated by recent findings on the privacy risks of facial recognition systems, reinforcing the need for multi-modal, secure biometric authentication.

Keywords: Biometric Watermarking, Iris Recognition, Fingerprint Authentication, Rubik Encryption, CNN, Image Security, Multi-Modal Biometrics.

I. INTRODUCTION

Biometric authentication systems have become essential in modern security infrastructures due to their ability to uniquely identify individuals using physiological or behavioral traits. Traditional systems primarily rely on single-modal biometrics such as facial recognition, fingerprints, or iris scans. While effective, these systems are increasingly vulnerable to forgery, spoofing attacks, and soft-biometric privacy leakage. For example, facial embeddings often unintentionally store personal attributes like age, gender, or ethnicity, raising significant privacy and ethical concerns.

In response to these limitations, the proposed biometric watermarking system integrates two biometric traits—iris and fingerprint—into a multi-modal authentication model. By combining these features, the system strengthens resistance to impersonation and enhances the robustness of verification. The watermarking process encrypts the extracted biometric data using a Rubik Cube-inspired scrambling algorithm, ensuring data confidentiality and complexity. This encrypted data is then embedded into a host image or document using a secure watermarking technique.

To validate user authenticity, the system leverages Convolutional Neural Networks (CNNs), which are trained to distinguish between genuine and fake biometric patterns. CNNs are known for their exceptional ability to extract spatial hierarchies from image data, making them ideal for high-accuracy biometric classification. Furthermore, the system is designed to detect fraud in real-time, issuing alerts when anomalies or tampering attempts are identified.

This paper surveys the technologies used in the project, reviews similar approaches in existing literature, and presents a comparative analysis with traditional methods. The goal is to evaluate the system's ability to offer high security, privacy protection, and real-world applicability in scenarios requiring secure identity verification.

II. RELATED WORK

Biometric authentication has been a widely researched field, with face, fingerprint, and iris recognition systems forming the foundation of many security applications. Over time, researchers have recognized the limitations of relying solely on single-modal biometric systems. These methods, while accurate, often struggle with spoofing vulnerabilities and the unintentional leakage of soft-biometric attributes.

A significant study by Terhörst et al. (2021) investigated how facial embeddings, typically used for recognition, store additional soft-biometric data such as age, gender, or skin tone. This raised ethical and security concerns, particularly when embeddings are exposed to adversarial models capable of predicting sensitive attributes. Such leakage compromises user privacy and calls for systems that avoid embedding unnecessary personal traits.

In parallel, watermarking-based biometric systems have been developed to combat forgery and improve traceability. Zero-watermarking techniques, for instance, focus on embedding biometric features into host media without visibly altering them. These methods are robust but often computationally expensive and not suitable for real-time applications.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14614

Recent approaches combine encryption and machine learning to enhance biometric security. Cryptographic transformations such as chaotic maps, scrambling algorithms, and hybrid models have been explored. However, many of these approaches rely on facial data or limited feature sets, which makes them susceptible to replay and image-based attacks.

The system presented in this paper builds upon these foundations by combining two biometric traits—iris and fingerprint—and securing them with Rubik Cube-based encryption. Unlike face-only models, this multi-modal approach improves both security and privacy. Additionally, the use of CNNs for classification introduces adaptability and learning-based accuracy, which traditional rule-based systems lack.

III. SURVEY ON EXISTING TECHNIQUES

A. Rubik Cube-Based Encryption :

This technique scrambles biometric images using Rubik-like 3D transformations. It adds a visual and structural complexity that makes reverse engineering difficult without the encryption key. As illustrated in Fig. 1, the Rubik Cube algorithm scrambles the biometric data for encryption.

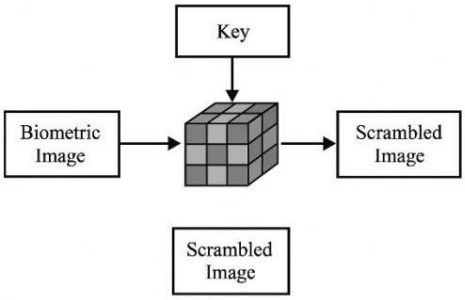

Fig. 1 Rubik Cube-Based Scrambling Process for Biometric Image Encryption

B. CNN-Based Biometric Verification :

Convolutional Neural Networks are widely used to learn and classify complex features in images. When trained on biometric patterns, CNNs can distinguish between authentic and forged traits with high accuracy. Fig. 2 shows the CNN-based classification pipeline used to verify biometric inputs.

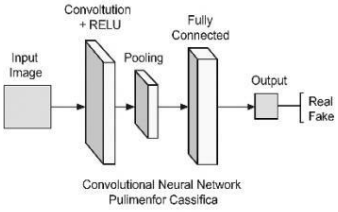

Fig. 2 Convolutional Neural Network Pipeline for Biometric Classification

C. Biometric Watermarking :

Watermarking involves embedding biometric data into host content (e.g., a legal document) in such a way that it is imperceptible but verifiable. It ensures ownership, authenticity, and tamper evidence. The normalized iris and extracted fingerprint minutiae used for watermarking are shown in Fig. 3.

(a) (b)

Fig. 3 (a) Normalized Iris Image (b) Extracted Fingerprint Minutiae for Biometric Watermarking

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025

DOI: 10.17148/IJARCCE.2025.14614

D. Real-Time Intrusion Detection :

Advanced systems are designed to trigger alerts if unauthorized access or forgery is detected during verification, adding a dynamic security layer. The overall watermarking process using fingerprint and iris features is shown in Fig.4.

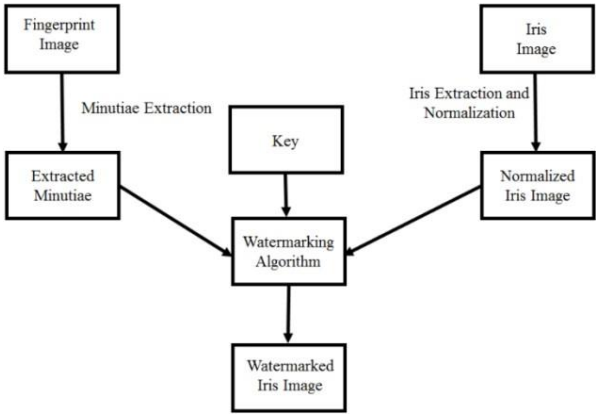

Fig. 4 Watermarking of Normalized Iris Image Using Fingerprint Minutiae and Encryption Key

IV. COMPARISON OF TECHNIQUES

TABLE I COMPARISON OF BIOMETRIC AUTHENTICATION TECHNIQUES

Technique	Security	Accuracy	Complexity	Privacy
Traditional Face Embeddings	Medium	High	Low	No
Rubik + CNN (Iris + Fingerprint)	High	High	Medium	Yes
Digital Signature Based Authentication	Medium	Medium	Low	No
Zero-Watermarking	High	Medium	High	Yes

- **Traditional Face Embeddings** offer high accuracy in identification but fall short in terms of privacy and security. They often store soft-biometric traits (like age or gender) unintentionally, which leads to privacy leakage. They're also more vulnerable to spoofing using photos or videos.

- **Rubik + CNN (Iris + Fingerprint)** provides strong security and privacy. Encryption with the Rubik algorithm makes reverse engineering difficult, and using CNNs for biometric verification adds robustness. It strikes a balance between accuracy and implementation complexity.

- **Digital Signature-Based Authentication** is easy to implement but lacks biometric uniqueness. It's moderately secure but doesn't verify the person's identity—only the document's origin.
- **Zero-Watermarking Techniques** are highly secure and preserve privacy since no actual biometric data is embedded. However, they are complex to design and require more computational resources for verification

V. DISCUSSION

The proposed biometric watermarking system combines the advantages of multi-modal biometrics, encryption, and deep learning to enhance document and identity security. Unlike single-modal systems, using both iris and fingerprint traits increases resistance to spoofing and ensures stronger user verification. The Rubik Cube-based encryption method effectively secures biometric data through a complex yet lightweight transformation, suitable for real-time systems. Additionally, the use of CNNs allows the model to learn from real-world data, improving detection of manipulated or synthetic inputs.

Compared to existing methods, the proposed approach strikes a practical balance between computational efficiency and security. While zero-watermarking techniques offer high security, they are often too complex for real-time use. On the other hand, digital signatures, although simple, lack biometric binding. This system fills that gap by embedding encrypted biometric data in a way that links users uniquely and securely to the content or transaction.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2025
DOI: 10.17148/IJARCCE.2025.14614

VI. CONCLUSION

This survey has explored a biometric watermarking system that enhances authentication using fingerprint and iris modalities. The core contribution lies in the integration of Rubik Cube-based encryption and CNN-based biometric classification, providing a secure and tamper-resistant method for identity verification. The system not only strengthens security but also addresses privacy concerns by avoiding face-based recognition and its associated soft-biometric leakage risks.

Through literature comparison and technical evaluation, the proposed model demonstrates superior privacy, forgery resistance, and real-time fraud detection capabilities. It presents a viable solution for applications in e-governance, healthcare, banking, and legal domains, where document authenticity and user identity must be strongly protected.

ACKNOWLEDGMENT

We express our sincere gratitude to **Dr. Sunita Chalageri**, Associate Professor, Department of Computer Science and Engineering, K.S. Institute of Technology, Bengaluru, for her consistent support, expert guidance, and encouragement throughout the development of this project and the preparation of this paper.

REFERENCES

[1]. P. Terhörst, D. Fährmann, N. Damer, F. Kirchbuchner, and A. Kuijper, "On soft-biometric information stored in biometric face embeddings," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 519– 534, 2021.

[2]. Kumar, A. Dwivedi, and M. K. Dutta, "A zero watermarking approach for biometric image security," in *Proceedings of the International Conference on Computing, Communication, and Automation (IC3A)*, 2020, pp. 53–58.

[3]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019.

[4]. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, "CosFace: Large margin cosine loss for deep face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018.

