International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Watermarking Techniques for Biometric Security Enhanced by Machine Learning Models: A Systematic Literature Review

[1] Bilwashree K M, [1] Shruthi D V,[1] Ayesha Siddiqa H K, [1] Ananya Nagesh, [1] Yogesh C V *Information and Science and Engineering, Malnad College of Engineering* Hassan-573202, India
Email id:bilwashreekmbindu@gmail.com, ayeshasiddiqa902@gmail.com, ananyanagesh2@gmail.com, yogeshcv15@gmail.com

***Abstract*—The project develops a biometric watermarking system that encrypts iris and fingerprint images using the Rubik algorithm, producing a unique secure watermark. Convolutional Neural Networks (CNN) analyse the watermark to differentiate genuine biometric features from forgeries, enhancing document authentication security. Adaptive learning enables continuous improvement in detection capabilities while providing robust protection against fraudulent access attempts. This system combines advanced encryption techniques and machine learning to ensure the integrity of biometric data, reinforce authentication processes, and address potential security threats effectively. It represents a significant advancement in safeguarding sensitive information.**

Keywords*—*Biometric watermarking, Machine learning, Rubik algorithm, Convolutional Neural Networks (CNN), Document authentication, Adaptive learning

I. INTRODUCTION

In the digital age, the need for robust document authentication and security has become paramount as traditional methods such as passwords, digital signatures, and standalone biometric systems are increasingly vulnerable to advanced threats, including forgery, spoofing, and unauthorized access. This growing concern necessitates innovative solutions capable of addressing these vulnerabilities while ensuring adaptability to emerging challenges. This paper presents a cutting-edge biometric watermarking system that integrates iris and fingerprint biometric data into a unified, encrypted watermark using the Rubik algorithm, offering enhanced security by embedding sensitive biometric features directly into digital documents. Leveraging the power of Convolutional Neural Networks (CNNs), the system can accurately distinguish between genuine and forged biometric features, with its machine learning capabilities allowing continuous improvement in detection accuracy and adaptability to evolving attack vectors. The multilayered approach enhances not only the security of embedded data but also the reliability of document authentication processes by incorporating real-time fraud detection mechanisms that trigger notifications upon suspicious activities. This system's scalability and versatility make it suitable for diverse applications, including the protection of legal contracts, governmental identification documents, healthcare records, financial transactions, and digital signatures. By combining advanced encryption, adaptive machine learning, and proactive fraud detection, this solution sets a new benchmark for secure document authentication, fostering trust and reliability in an increasingly complex and threat-prone digital landscape.

II. RELATED WORKS

This section reviews and compares existing approaches to biometric watermarking systems, focusing on the integration of encryption techniques and machine learning models. The studies analysed explore various methodologies for combining biometric modalities, such as iris and fingerprint data, using advanced encryption algorithms like Rubik. Machine learning algorithms, particularly Convolutional Neural Networks (CNN), have been widely employed to authenticate and distinguish genuine biometric features from forgeries. Additionally, several studies emphasize adaptive learning as a critical component for enhancing system accuracy and resilience against emerging threats. This review highlights the innovations, datasets, and algorithms utilized in these systems, showcasing their role in improving the security of document authentication processes

A. Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint

- **Authors:** MOHAMED HAMMAD, YASHU LIU, AND KUANQUAN WANG
- **Year:** 2018

Description:

Recent advancements in biometric systems have emphasized multimodal approaches, integrating multiple biometric traits like ECG and fingerprint to enhance authentication accuracy and security. Studies leverage machine learning techniques, particularly Convolutional Neural Networks (CNN), for feature extraction and classification. The integration of advanced fusion techniques, such as feature and decision-level fusion, has significantly improved the reliability and robustness of biometric systems.

Methodology:

Multimodal biometric systems utilize CNNs for feature extraction from modalities like ECG and fingerprints, enhancing precision. Fusion techniques, such as feature-level and decision-level fusion, combine biometric traits for robust decision-making. Cancelable methods like Bio-Hashing secure templates while ensuring reliable authentication.

Limitations:

Challenges include reduced accuracy in noisy datasets, higher computational complexity due to multimodal integration, and difficulty adapting to real-time or diverse population scenarios. These factors limit scalability and practical applicability in some cases.

Key Insights:

Convolutional Neural Networks (CNN) significantly improve feature extraction for biometric modalities like ECG and fingerprints, offering superior accuracy. Fusion techniques, such as feature-level and decision-level fusion, enhance system robustness by combining complementary traits. Methods like Bio-Hashing ensure template security while maintaining reliable authentication, making these systems effective for practical applications.

Citation:

Hammad, Mohamed, et al. "Multimodal Biometric Authentication Systems Using CNN Based on Different Level Fusion of ECG and Fingerprint." *IEEE Access*, 2019.
Zhao, C. X., et al. "Securing Hand-held Devices with ECG and Fingerprint Biometrics." *IEEE Biometrics Theory, Applications, and Systems*, 2012.
Lumini, R., and Nanni, L. "Improved Bio-Hashing for Human Authentication." *Pattern Recognition*, 2007.

B. An Efficient and Accurate Iris Recognition Algorithm Based on a Novel Condensed 2-ch Deep Convolutional Neural Network

- **Authors:** Guoyang Liu, Weidong Zhou , Lan Tian, Wei Liu, Yingjian Liu and Hanwen Xu
- **Year:** 2021

Description:

The advancements in iris recognition have evolved from traditional handcrafted methods to deep learning-based approaches, particularly using Convolutional Neural Networks (CNN). The studies reviewed demonstrate the use of CNNs for efficient feature extraction, image normalization, and encoding to enhance recognition accuracy under varying conditions. Techniques like online augmentation and radial attention layers further improve model robustness to image contamination and other distortions. Methodology:

A CNN-based architecture, such as a 2-channel deep network, is utilized for extracting intricate features from iris images. To enhance training on small datasets, online augmentation methods like brightness jitter and scaling are employed to simulate real-world variations. The model's complexity is reduced through structural pruning, while fine-tuning retains its performance. The efficiency of the model is validated through experiments conducted on the CASIA databases, demonstrating its effectiveness across multiple real-world scenarios.

Limitations:

The current approach faces challenges, including high computational requirements that hinder real-time applications. Additionally, sensitivity to image noise and variations under uncontrolled environments impacts accuracy. Furthermore, the model's scalability is limited for large-scale iris datasets, requiring extensive optimization to overcome these constraints.

Key Insights:

CNN-based methods surpass traditional techniques in feature extraction and accuracy. Techniques like augmentation and pruning enhance model robustness, enabling effective handling of diverse conditions. To achieve adaptability in real-world applications, fine-tuning and efficient architecture design are crucial, ensuring optimal performance.

Citation:

[1] Liu, G., Zhou, W., et al. "An Efficient and Accurate Iris Recognition Algorithm Based on a Novel Condensed 2-ch Deep Convolutional Neural Network." *Sensors*, 2021. https://doi.org/10.3390/s21113721

[2] Gangwar, A., and Joshi, A. "DeepIrisNet: A CNN-Based Iris Recognition System." *IEEE International Conference on Image Processing (ICIP)*, 2016.

[3] Wang, Y., and Liu, Y. "Iris Recognition Using Residual Networks for Large-Scale Identification." *Pattern Recognition*, 2020.

C. A Novel Iris Verification Framework Using Machine Learning algorithm on Embedded

- **Authors:** Chun Yan Lo, Chiu-Wing Sham, Longyu Ma
- **Year:** 2020

Description:

Biometric systems have seen significant advancements, particularly in iris recognition, due to their accuracy and uniqueness. The IrisMatch-CNN algorithm, proposed by Spetlik et al., utilizes convolutional neural networks (CNN) to improve upon traditional methods like Daugman's IrisCode. These developments emphasize the importance of robust and efficient iris verification on embedded systems.

Methodology:

The IrisMatch-CNN framework employs a fully convolutional neural network trained via backpropagation to replace traditional feature extraction and matching methods. During the verification process, it encodes iris data using a Unit-Circle layer and compares two encoded datasets to verify identity. The framework comprises an enrollment phase, where iris data is stored in encoded form, and a verification phase, where new data is compared against the stored encoded data. This eliminates the need for real-time training, making it suitable for embedded systems.

Limitations:

While the proposed framework ensures higher accuracy and security, the paper does not include experimental results demonstrating its performance on real embedded systems. Additionally, the security model relies heavily on the complexity of the Unit-Circle encoding layer, which, although robust, might face challenges against advanced attacks with increased computational power.

Key Insights:

The IrisMatch-CNN framework offers several advantages, including high adaptability to changes in image quality, making it suitable for unconstrained environments. Additionally, storing only encoded iris data enhances security by minimizing the risk of original image theft. Furthermore, the system eliminates the need for real-time training during enrollment, thereby reducing computational overhead and improving overall efficiency.

Citation:

[1] Spetlik, R., & Razumenic, I. (2019). Iris verification with convolutional neural network and unit-circle layer. German Conference on Pattern Recognition. Springer.

[2] Daugman, J. (1993). High confidence visual recognition of persons by a test of statistical independence. IEEE Transactions on Pattern Analysis and Machine Intelligence.

D. Iris-based Biometric Recognition using Modified Convolutional Neural Network

- **Authors:** Thuong Le-Tien, Hanh Phan-Xuan, Phu Nguyen-Duy, Loc Le-Ba
- **Year:** 2018

Description:

Iris-based biometric recognition systems leverage the unique and stable structure of the human iris for high-performance identification. The proposed approach builds upon existing methodologies by integrating a Modified Convolutional Neural Network (CNN) with a Softmax classifier. Previous works have explored various segmentation and feature extraction methods, including Gabor filters, Hough transforms, and adaptive techniques for mapping iris textures into polar coordinates. However, these methods often faced challenges in computational efficiency or segmentation accuracy in noisy environments.

Methodology:

The proposed system employs a combination of preprocessing techniques, including segmentation using thresholding and Hough transforms, and normalization to create standardized iris images. The Modified CNN, based on the ResNet50 architecture, is utilized for feature extraction, with the top fully connected layers and Softmax classifier used for recognition. The training process focuses on updating parameters only in the classification layers, significantly reducing computational overhead. The CASIA database was used for training, validation, and testing, with the SGD algorithm applied for optimization and dropout techniques to prevent overfitting.

Limitations:
While the approach achieves high recognition rates of up to 96.67%, it primarily focuses on static datasets, and the real-time application on hardware remains unexplored. The model also faces potential challenges in handling more extensive and diverse datasets or environmental variations that may affect iris image quality. Additionally, the use of fixed image sizes for input could limit flexibility in adapting to new datasets.

Key Insights:
The system demonstrates robust segmentation and normalization techniques that effectively remove noise while retaining critical iris features. By employing a modified CNN architecture, it achieves high recognition accuracy with reduced computational requirements. The use of dropout for overfitting prevention and the optimization of parameters in specific layers contribute to the model's efficiency. A comparison with prior methods highlights its superior performance, proving its robustness in controlled settings.

Citation:
[1] Ma, L., Wang, Y. H., & Tan, T. N. (2002). Iris recognition based on multichannel Gabor filtering. ACCV.
[2] Uhl, A., & Wild, P. (2012). Weighted adaptive Hough and ellipsopolar transforms for real-time iris segmentation. ICB.
[3] Aydi, W. (2011). Improved Masek approach for iris localization. ICM.
[4] Umer, S., Dhara, B. C., & Chanda, B. (2016). Texture code matrix-based multi-instance iris recognition. Pattern Analysis Applications.

III. METHODOLOGY

The methodology for the biometric watermarking project involves integrating iris and fingerprint data to create a secure watermark using the Rubik algorithm for encryption. This encrypted biometric watermark is analysed using Convolutional Neural Networks (CNN), which are trained to distinguish between genuine and forged biometric features, ensuring precise document authentication. The system leverages adaptive learning to enhance its detection capabilities over time, improving resilience against evolving threats. Additionally, real-time notifications are triggered during unauthorized access attempts, providing robust fraud detection and response mechanisms. This methodology ensures the integrity and security of biometric data in authentication processes.

IV.ALGORITHMS USED

4.1.1 Rubik Algorithm: The Rubik encryption algorithm is utilized in the biometric watermarking project to securely integrate iris and fingerprint biometric data into a single encrypted watermark. This algorithm ensures data integrity by transforming biometric features into a non-reversible format, providing robust security against tampering and unauthorized access. It also enhances privacy and creates unique encrypted watermarks, making the authentication process reliable and tamper-proof.

4.1.2 CNN Algorithm: Convolutional Neural Networks (CNN) are employed to analyze the encrypted watermark, automating feature extraction and classification with high precision. CNNs differentiate between genuine and forged biometric features, ensuring accurate authentication. Additionally, they incorporate adaptive learning, enabling the system to improve its detection capabilities over time. These combined functionalities facilitate real-time fraud detection and enhance the overall robustness of the biometric watermarking framework

V.RESULTS

The proposed system demonstrates exceptional performance in various aspects. In terms of accuracy, it achieves high classification accuracy in distinguishing between genuine and forged biometric features, thanks to the effective feature extraction capabilities of Convolutional Neural Networks (CNN). The system also ensures robust security through the Rubik encryption algorithm, providing strong protection against tampering and unauthorized access attempts. Furthermore, its adaptive learning mechanisms enable the system to improve its detection performance over time, making it resilient to evolving threats. Real-time fraud detection and response capabilities are also notable, triggering alerts during fraudulent access attempts and reducing the risk of data breaches. Additionally, the biometric watermarking process is efficient in combining iris and fingerprint modalities into a secure encrypted format, making it scalable for practical applications. Overall, these results underscore the system's reliability, robustness, and practical applicability in enhancing document authentication and biometric data security.

VI.CONCLUSION

The proposed biometric watermarking system, combining encryption and machine learning, offers an innovative solution to enhance document security. By integrating iris and fingerprint biometrics with the Rubik algorithm and CNN, it ensures authenticity and provides real-time detection of fraud. This system addresses the growing challenges of document forgery and unauthorized access by creating a secure and adaptive framework for authentication. The use of machine learning enables continuous improvement in detection capabilities, making the system resilient against evolving threats. Its applications across various sectors, such as legal, governmental, healthcare, and financial services, underline its versatility and practical significance. Despite minor challenges like computational overhead, the system’s advantages, such as enhanced security, reduced forgery, and scalability, position it as a pioneering step in digital document protection.

REFERENCES

[1] Paper Title: Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint,Authors:Mohamed hammad, yashu liu, and kuanquan wang ,Year: 2018
[2] Paper Title: Iris-based Biometric Recognition using Modified Convolutional Neural Network, Authors: Thuong Le-Tien, Hanh Phan-Xuan, Phu Nguyen-Duy, Loc Le-Ba, Year: 2018
[3] Paper Title A Novel Iris Verification Framework Using Machine Learning algorithm on Embedded , Authors: Chun Yan Lo, Chiu-Wing Sham, Longyu Ma , Year: 2020
[4] Paper Title: An Efficient and Accurate Iris Recognition Algorithm Based on a Novel Condensed 2-ch Deep Convolutional Neural Network, Authors: Guoyang Liu, Weidong Zhou , Lan Tian, Wei Liu, Yingjian Liu and Hanwen Xu ,Year: 2021