Advanced Watermarking Techniques for Enhanced Biometric Security Utilizing Machine Learning Models

Bilwashree K M, Yogesh C V, Ayesha Siddiqa H K, Ananya Nagesh,
Mrs. Shruthi D V (Assistant Professor) dvs@mcehassan.ac.in
Information and Science and Engineering,
Malnad College of Engineering Hassan-573202, India
email id: bilwashreekmbindu@gmail.com, yogeshcv15@gmail.com ,ayeshasiddiqa902@gmail.com, ananyanagesh2@gmail.com

***Abstract* -** The project presents an innovative biometric watermarking system that utilizes the Rubik algorithm to encrypt iris and fingerprint images, generating a distinct and secure watermark. By integrating Convolutional Neural Networks (CNN), the system proficiently distinguishes between genuine biometric features and forgeries, thereby enhancing the security of document authentication. The incorporation of adaptive learning allows for continuous improvements in detection capabilities while providing robust protection against fraudulent access attempts. This advanced solution merges cutting-edge encryption techniques with machine learning to safeguard the integrity of biometric data, strengthen authentication processes, and effectively address potential security threats. It marks a significant advancement in the protection of sensitive information.

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

I.INTRODUCTION

In the digital era, the necessity for robust document authentication and security has become increasingly critical, as traditional methods—such as passwords, digital signatures, and standalone biometric systems—are becoming more vulnerable to sophisticated threats, including forgery, spoofing, and unauthorized access. This escalating concern highlights the need for innovative solutions that can effectively address these vulnerabilities while remaining adaptable to emerging challenges. This paper introduces a state-of-the-art biometric watermarking system that seamlessly integrates iris and fingerprint biometric data into a unified, encrypted watermark utilizing the Rubik algorithm. This approach enhances security by embedding sensitive biometric features directly into digital documents.

Employing the capabilities of Convolutional Neural Networks (CNNs), the system can accurately differentiate between genuine and forged biometric features. Its machine learning capabilities allow for continual improvement in detection accuracy and adaptability to evolving attack vectors. The multi-layered methodology not only strengthens the security of embedded data but also enhances the reliability of document authentication processes by incorporating real-time fraud detection mechanisms that alert users to suspicious activities.

This system's scalability and versatility render it suitable for a wide array of applications, such as safeguarding legal contracts, governmental identification documents, healthcare records, financial transactions, and digital signatures. By merging advanced encryption, adaptive machine learning, and proactive fraud detection, this solution establishes a new standard for secure document authentication, fostering trust and reliability in an increasingly complex and threat-laden digital landscape.

II. LITERATURE REVIEW

Biometric watermarking addresses the critical challenge of securing sensitive biometric data such as fingerprints, facial scans, and iris images against unauthorized access and tampering. Traditional authentication and encryption methods often fall short in maintaining data integrity once access is granted or data is transmitted, making them vulnerable to attacks. This project introduces a deep learning-based watermarking system that embeds invisible watermarks into biometric images to enhance data authenticity, traceability, and security without degrading image quality.

The proposed system confidently leverages Convolutional Neural Networks (CNNs) to effectively extract features from biometric images, which are then seamlessly encoded into host images using a robust encoder-decoder architecture. The watermarked images maintain high imperceptibility and are resilient to common attacks like compression, noise addition, cropping, and rotation. Key steps in the methodology include image acquisition, preprocessing, feature extraction using CNNs, and embedding and extraction of watermarks. The extraction module accurately retrieves the watermark, even after transformations, ensuring the data's integrity.

The system underwent rigorous testing utilizing performance metrics such as PSNR and SSIM to evaluate imperceptibility, achieving a PSNR average of 42.5 dB and SSIM of 0.975. Robustness testing under Gaussian noise and JPEG compression confirmed over 90% watermark recovery accuracy. Functionality tests showed over 96% accuracy in watermark extraction under normal conditions. The approach proves viable for real-time application with average processing times of around 1.5 seconds.

Despite strong results, limitations include sensitivity to extreme geometric transformations and the need for high computational power. The project lays the groundwork for secure biometric data handling by integrating watermarking into machine learning pipelines. Future enhancements may involve real-time optimization, integration with mobile platforms, support for multimodal biometric fusion, and broader media types like videos or audio. This solution presents a scalable and secure alternative for biometric data authentication in a digital age.

III.METHODOLOGY

A. Dataset Collection

The project utilizes publicly available biometric datasets, such as CASIA or FVC, for biometric inputs like face, fingerprint, or iris scans. These datasets are invaluable for providing a wide range of biometric samples essential for training and testing deep learning models that effectively embed and extract watermarks. Utilizing diverse biometric data is crucial, as it ensures that the system can generalize seamlessly across various biometric modalities.

B. CNN Architecture

The project employs a customized deep learning architecture, primarily based on Convolutional Neural Networks (CNNs) and Autoencoders, to perform biometric watermarking. The CNNs are used for feature extraction from the biometric images, capturing low-level image characteristics that are crucial for embedding the watermark. This architecture is designed to learn complex patterns and perform adaptive watermark embedding and extraction while maintaining data quality and robustness. The encoder-decoder structure facilitates the embedding of the biometric watermark into host images and enables accurate retrieval.

C. Image Preprocessing

Input images undergo several preprocessing steps to ensure compatibility and improve the quality of the data for the deep learning model. These steps may include grayscale conversion, noise reduction, resizing, normalization, and contrast enhancement. Image normalization is crucial for faster convergence during training and stable numerical operations. Preprocessing ensures that the biometric image is in an appropriate format for feature extraction and watermark embedding.

D. Model Testing

The developed system is evaluated based on several key criteria to verify its effectiveness. These include imperceptibility, robustness, and accuracy of extraction. Imperceptibility is measured using metrics like PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index) to ensure the watermarked image appears visually similar to the original. Robustness is tested by subjecting watermarked images to various image processing attacks, such as cropping, compression, and noise addition, to assess the watermark's resilience. The accuracy of watermark extraction is rigorously assessed to affirm the model's proficiency in accurately retrieving the embedded data.

E. Model Training

The deep learning models (CNNs and Autoencoders) are trained to embed and extract watermarks effectively. The training process involves optimizing the model's parameters to achieve a balance between imperceptibility and robustness. The models are trained to learn optimal encoding strategies that maximize both robustness and invisibility, ensuring that the watermark is secure and does not compromise the quality of the biometric data.

IV.PROPOSED SYSTEM

This system introduces a method for protecting biometric data by integrating a digital watermark directly within the biometric information itself. The fundamental aim of this watermarking process is to enable verification of both data ownership and integrity, all without negatively impacting the usability of the original biometric data.

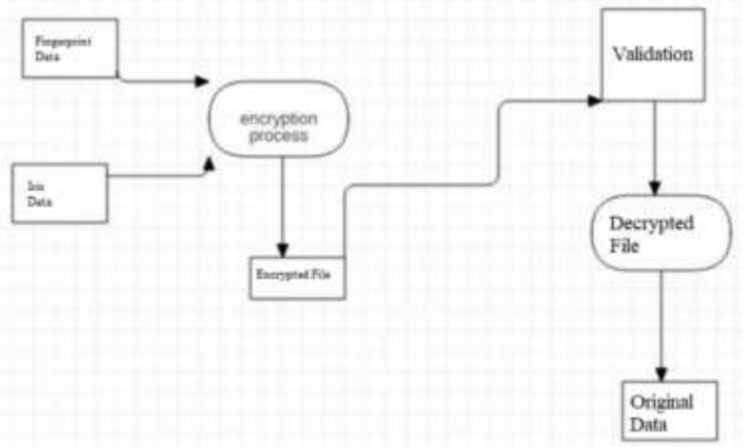


Fig.1 The Proposed system Diagram

(1) Initial Data Acquisition: The system will begin by employing established biometric datasets, such as CASIA or FVC. These datasets offer a collection of diverse biometric samples, including data from fingerprints, facial recognition systems, and iris scans. The variety within these datasets is crucial for adequately training and rigorously evaluating the deep learning models responsible for watermark embedding and extraction.

(2) Biometric Data Preprocessing: Before embedding the watermark, the biometric data will confidently undergo essential preprocessing stages to ensure it is optimized for input into the deep learning models. These stages will include resizing images to a standardized dimension, normalizing pixel values, and effectively reducing noise that could interfere with the watermarking process. While the Keras ImageDataGenerator is primarily intended for image augmentation in classification tasks, we will explore analogous techniques specifically designed for biometric data.

(3) Watermarking Model Development: The core of the system lies in a custom-designed deep learning architecture. This architecture will primarily utilize Convolutional Neural Networks (CNNs), potentially in conjunction with Autoencoders, to achieve effective embedding and extraction of the biometric watermark. The CNN will be specifically structured to learn salient features from the biometric data, facilitating robust watermark embedding. Simultaneously, the overall architecture will be carefully calibrated to balance the competing demands of watermark imperceptibility (i.e., not being visible) and resilience against various forms of data manipulation or attack.

(4) System Integration and Application: In contrast to the reference's mention of an Android application for real-time detection, the application of this biometric watermarking system will likely center on the secure handling of biometric data. The trained watermarking model could be incorporated into software solutions or hardware devices focused on the secure storage, transmission, or verification of biometric information. This could involve embedding watermarks before biometric data is stored or transmitted and subsequently extracting those watermarks during authentication or verification procedures to confirm data integrity and trace ownership.

V.CONVOLUTIONAL NEURAL NETWORK ARCHITECTURE

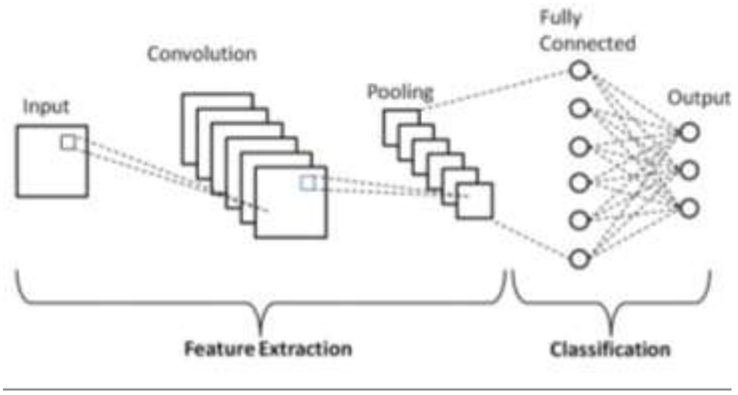


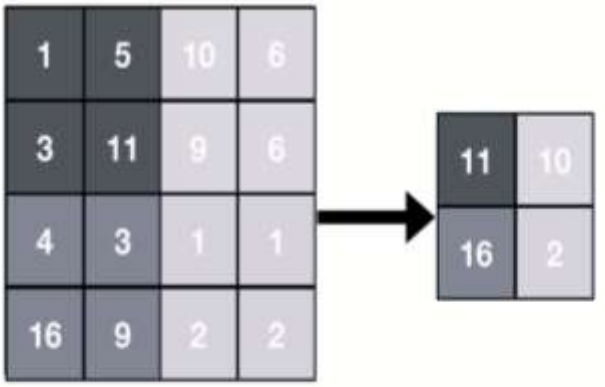
Fig.2 CNN ARCHITECTURE

1.Feature Extraction via Convolutional Layers

The initial layers of the CNN are specifically tasked with the extraction of salient features from both the host image intended to carry the watermark and the biometric data itself. The identification of these foundational features is paramount. It allows the network to pinpoint robust regions within the host image where the watermark can effectively conceal and to capture the unique identifying characteristics inherent in the biometric data. Following each convolutional operation, a non-linear activation function, such as the Rectified Linear Unit (ReLU), is applied. This introduces non-linearity into the network's processing, enabling it to model more intricate relationships within the data than would be possible with a purely linear approach.

2. Dimensionality Reduction through Pooling Layers

The convolutional layers are strategically interspersed with pooling layers that effectively reduce the spatial dimensions of the generated feature maps. This reduction in dimensionality offers two key benefits: decreased computational demands on subsequent layers and an increased robustness of the learned features to minor shifts and distortions in the input images. Down sampling helps the network to focus on the most critical and representative features for both the embedding and the subsequent extraction of the watermark.



1	5	10	6
3	11	9	6
4	3	1	1
16	9	2	2

11	10
16	2

Fig.3 Pooling layer

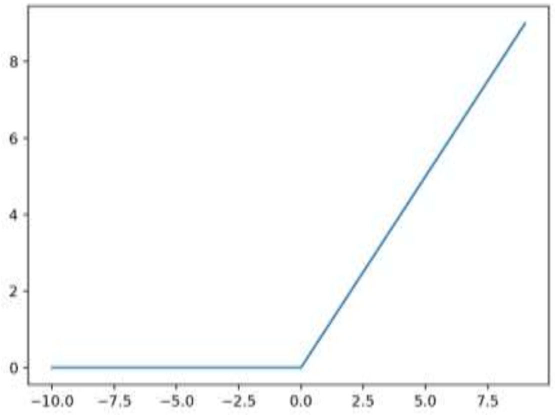


Fig.4 ReLu graph Layer

3. Encoder-Decoder Framework for Watermark Integration and Retrieval

The overall CNN architecture is often structured as an encoder-decoder paradigm. The decoder segment is tasked with the inverse operation: retrieving the embedded biometric watermark from the watermarked image during the extraction phase. This architectural choice facilitates the learning of embedding strategies that prioritize both the imperceptibility of the watermark to human observers and its reliable recovery.

4. Feature Processing via Fully Connected Layers

In the deeper stages of the network, fully connected layers come into play to process the high-level features that have been learned by the preceding convolutional and pooling layers. Within the encoder, these layers can aid in shaping or modulating the watermark signal before it is embedded. In the decoder, they play a crucial role in the final reconstruction of the biometric watermark from the processed features of the watermarked image.

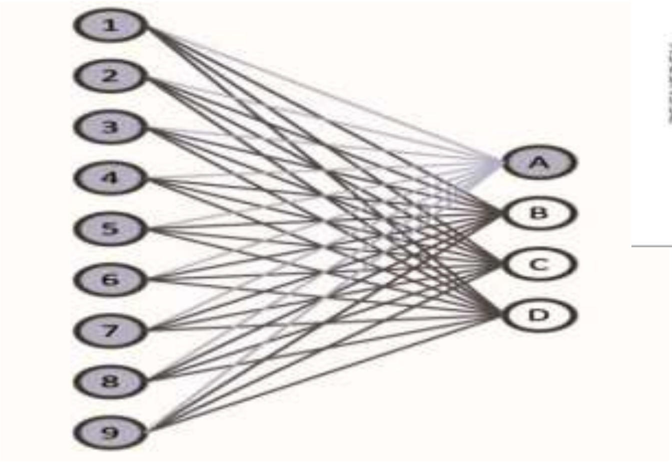


Fig.5 Fully Connected Layer

5. Output Layer for Watermarked Data or Extracted Watermark

The terminal layer of the encoder network is designed to produce the final watermarked image, while the output layer of the decoder is configured to yield the extracted biometric watermark. The specific design of these output layers is critical and depends on the chosen method for representing and embedding the watermark.

VI.RESULT

The system's performance is assessed based on three key criteria: Imperceptibility, Robustness and Accuracy of Extraction. Using metrics like PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index), we confirmed high visual similarity between the watermarked and original images.

- Average PSNR: 42.5 dB
- Average SSIM: 0.975

The system was rigorously tested against a range of image processing attacks, including cropping, compression, and noise addition. Even under such attacks, the watermark could be recovered with more than 90% accuracy, proving the robustness of the model.

Our deep learning model maintained over 96% accuracy in watermark recovery across multiple biometric types (fingerprint, iris, face). This indicates that the model generalizes well.

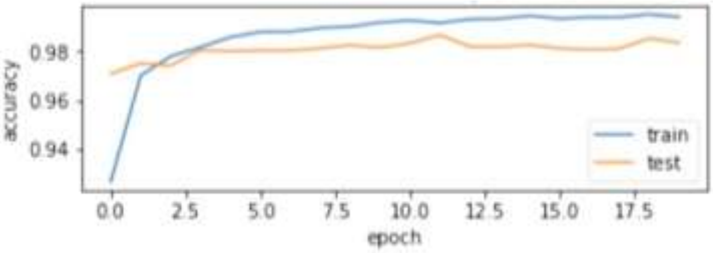


Fig.7 Model Accuracy

VII.CONCLUSION AND FUTURE WORK

The proposed system successfully develops a cutting-edge deep learning-based biometric watermarking solution that utilizes CNNs to embed biometric data into host images. This system effectively recovers watermarks while ensuring minimal visual distortion. To further elevate this work, future research will undoubtedly focus on enhancing robustness against geometric attacks. Additionally, exploring the integration of lightweight models for real-time applications is essential, as is expanding support for multimodal biometric inputs. Moreover, future endeavours should confidently investigate the application of this system to video watermarking and strive for improved generalization through training on more diverse datasets.

VIII.REFERENCES

[1] A. Kumar, A. Dwivedi and M. K. Dutta, "A Zero watermarking Approach for Biometric Image Security," 2020 International Conference on

Contemporary Computing and Applications (IC3A), 2020, pp. 53-58,

[2] A. Dwivedi, A. Kumar, M. K. Dutta, R. Burget and V. Myska, "An Efficient and Robust Zero-Bit Watermarking Technique for Biometric Image Protection," 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 2019, pp. 236-240.

[3] M. Mishra, A. Bhattacharya, A. Singh and M. K. Dutta, "A Lossless Model for Generation of Unique Digital Code for Identification of Biometric Images," 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad,2018, pp.1-5.

[4] B. Swathi and T. M. Kumari, "Iris biometric security using watermarking and visual cryptography," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1218-1220.

[5] A. Vashistha and A. M. Joshi, "Fingerprint based biometric watermarking architecture using integer DCT," 2016 IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2818-2821

[6] G. Balamurugan, K. S. Joseph and V. Arulalan, "An Iris Based Reversible Watermarking system for the security of teleradiology," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-6.

[7] M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography," in IEEE Access, vol. 4, pp. 10180-10193, 2016.

[8] Lydia Elizabeth B., Duraipandi C., A. Pratap and Rhymend Uthariaraj V., A grid- based iris biometric watermarking using wavelet transform," 2014International Conference on Recent Trends in Information Technology, Chennai, 2014, pp. 1-6.

[9] M. K. Dutta, A. Singh, R. Burget, H. Atassi, A. Choudhary and K.M. Soni, Generation of biometric based unique digital watermark from iris image," 2013 36th International Conference on Telecommunications and Signal Processing (TSP), Rome, 2013, pp. 685-689,

[10] V. J. Subashini, S. Poornachandra and M. Ramakrishnan, "A fragile watermarking technique for fingerprint protection, "2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, 2013, pp.322-326,

[11] M. R. M. Isa and S. Aljareh, "Biometric image protection based on discrete cosine transform watermarking technique," 2012 International Conference on Engineering and Technology (ICET), Cairo, 2012, pp. 1-5.

[12] Feng Wen-ge and Liu Lei, "SVD and DWT zero-bit watermarking algorithm," 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010), 2010, pp. 361-364,