iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71155

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Facial Recognition for Biometric Authentication: A Literature Survey

Prof. Poornima M[1], Noor Saniya[2], Preethi J[3], Ruthu S[4], Yogitha C[5]
Department of Information Science & Engineering, S J B Institute of Technology

Abstract: Within this research paper, the imperative to enhance security in biometric authentication systems is treated by analyzing zero-bit watermarking to extract distinctive identifiers from biometric images. The general goal is to hunt and study existing research on zero-bit watermarking techniques specifically created for application within biometrics and how they can generate strong and secure distinctive IDs without compromising the authenticity of the original biometric data. The value addition of this research paper is that it offers a systematic review of existing state of zero-bit watermarking methods for generating unique IDs for biometric images. It consolidates prominent methodologies, discussions and results within the new research area, reflecting its importance for enhancing biometric data security and privacy.

Keywords: Zero-bit watermarking, Biometric security, Unique ID generation, Biometric data, protection, Watermarking method, Template protection, Iris recognition, Fingerprint recognition, Secure watermarking.

I. INTRODUCTION

The different biometric protection methods were investigated, and zero-bit watermarking has proven to be an efficient process for the protection of biometric images. A secret, usually encrypted, identifier or watermark is added to the biometric information in this new process without causing any perceivable alteration in the quality of the original image. A special ID is assigned to the biometric image with the help of zero-bit watermarking, and an unbreakable data system security and authentication can be achieved. This technique is intended to prevent unauthorized reuse and alteration of sensitive biometric data. Even though use of watermarking for securing biometric data is not new, its particular application and investigation to the application of zero-bit watermarking so that recognizable IDs can be obtained out of biometric images is worth being researched. New watermarking technologies may insert some degree of degradation, which will be harmful for the operation of biometric identification systems. Growing use of biometric identification systems emphasizes the imperative need for guaranteeing privacy and protection of an individuals unique biological and behavioral features. Biometrics, based on intrinsic personal traits like iris scans, fingerprints, and facial features, provide a robust connection of an individual and his/her on-line presence with a promise of higher accuracy and security in comparison to the traditional methods of authentication.

II. OBJECTIVES

1) Furnish an overview of the fundamentals of biometric authentication and the imperative necessity of strong security practices, most especially in regard to the protection of biometric templates
2) Synthesize and analyze existing research efforts that explore the application of zero-bit watermarking for the generation of unique identifiers from various biometric modalities, such as iris and fingerprint images.
3) Examine the methodologies employed for embedding and extracting zero-bit watermarks in biometric images for unique ID generation, including techniques like Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).
4) Discuss the significance of zero-bit watermarking in enhancing biometric data security, ensuring data integrity, and enabling secure authentication through the generation of unique and robust identifiers.
5) Identify potential challenges, limitations, and future research directions in the application of zero-bit watermarking for biometric image unique ID generation to guide further advancements in this critical field.

III. LITERATURE REVIEW

Previous studies have identified some of the following methods, such as inserting biometric information into other media, employing biometric features as watermarks, and combining watermarking with encryption, steganography, and error correction methods These techniques are implemented to offer confidentiality and integrity to biometric templates stored in databases, particularly applications like medical imaging and biometric authentication.

More focus has been given to zero-bit watermarking since it stands out from normal watermarking where it derives a unique identifier from biometric features directly without altering the original image. The process does not require embedding additional data, relying on robust feature extraction and safe ID generation to maintain the integrity of biometric images. Some important biometric watermarking trends involve the use of multimodal biometrics for higher recognition accuracy, the use of cryptographic methods for increased security, and the utilization of transform domain methods like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) for attack resistance. Additionally, AI-based methods, including neural networks and fuzzy logic, are being explored to improve watermarking performance. Even with the progress, there are challenges yet to be addressed, mainly achieving the balance between robustness and imperceptibility, providing security against high-level attacks, and preserving biometric recognition accuracy.

Computational complexity still remains a challenge, particularly with real-time deployment of advanced watermarking techniques and Zero-Bit Watermarking schemes. There are some gaps in research in this field, including the robustness of Zero- Bit Watermarking against adversarial attacks, real-time adaptation for practical usage, and the impact of watermarking on biometric recognition performance. Standardization of testing measures and datasets is also necessary in order to facilitate comparative studies. Exploring AI-powered Zero-Bit Watermarking methods and constructing secure storage frameworks for unique biometric signatures also present future research opportunities. DWT-based schemes among various watermarking schemes enjoy high robustness against compression and noise with assurance of imperceptibility by embedding data in some frequency sub-bands. DCT methods are JPEG compression resilient but require careful selection of embedding points to strike a balance between robustness and imperceptibility. SVD-based methods utilize the stability of singular values to embed with ensuring image quality but are computationally expensive. Hybrid methods, eg, DWT-DCT and DWT-SVD, integrate the respective strengths of various domains to increase overall robustness and security.

IV. METHODOLOGY

To evaluate robustness, watermarked images are subjected to various attacks such as:

1) Noise addition (e.g., Salt & Pepper, Gaussian).
2) Compression (e.g., JPEG with varying quality factors).
3) Geometric manipulations (e.g., cropping, rotation - though robustness against all geometric attacks can be a limitation).
4) Filtering (e.g., median filtering), Brightness adjustments

.

The following metrics are commonly used to evaluate biometric watermarking schemes:

a) Peak Signal-to-Noise Ratio (PSNR): This is a key metric for assessing the imperceptibility or fidelity of the watermarking. It quantifies the distortion introduced by the embedding process by measuring the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation Higher PSNR values generally indicate better image quality and thus better imperceptibility.
b) Bit Error Rate (BER): In cases where the watermark itself is a binary sequence (which might be the case if your unique ID is encoded as such before embedding using a zero-bit technique), BER measures the number of incorrect bits in the extracted watermark compared to the original embedded watermark. Lower BER values indicate better signal quality and more reliable data transmission.
c) Structural Similarity Index Model (SSIM): SSIM is a perceptual metric that assesses the structural similarity between the original and watermarked images. It considers luminance, contrast, and structure. SSIM values range from -1 to 1, with values closer to 1 indicating higher similarity and better perceptual quality.
d) Normalized Correlation (NC): NC is used to quantify the similarity between the extracted and the originally embedded watermark, particularly after the watermarked image has undergone attacks. It ranges from -1 to 1, with values closer to 1 indicating higher similarity and thus better robustness.
e) Hamming Distance (HD) is specifically mentioned for comparing iris templates, which could be relevant depending on how your zero-bit watermark relates to the underlying iris features. Using the same datasets and evaluation metrics ensures a fair comparison between different models.
f) Comparison with Existing Methods: To demonstrate the efficacy of a proposed watermarking technique, its performance is often compared against other state-of-the-art methods reported in the literature,

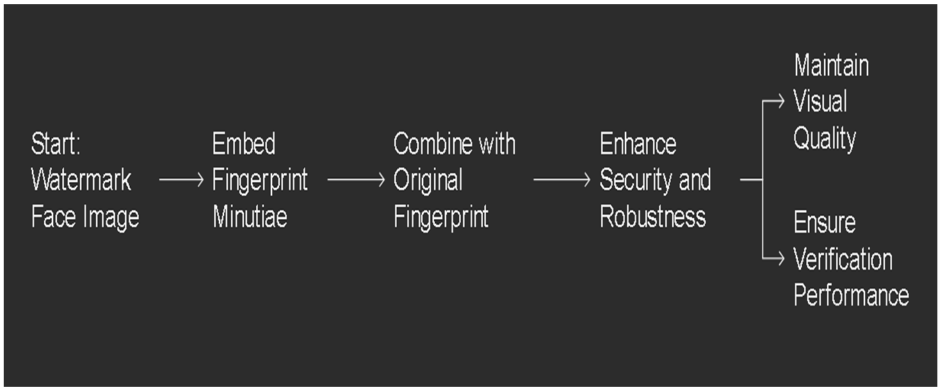
Start: Watermark Face Image
Embed Fingerprint Minutiae
Combine with Original Fingerprint
Enhance Security and Robustness
Maintain Visual Quality
Ensure Verification Performance

Fig 1: Two-level Watermarking Reinforcement Approach

V. RELATED WORK

Relevant Research Studies in Biometric Watermarking:

1) Medical Image Watermarking: Several studies focus on using watermarking for medical image security. Mohammed et al. presented a biometric-based medical watermarking system using the sender's iris code as a key for authentication and chaotic encryption for privacy. Their approach aimed to ensure the authenticity of the source and preserve patient record privacy. Sharma et al. (2015) proposed a system using DWT and DCT to embed a hospital logo and electronic patient records (EPR) into the non-region of interest (NROI) of medical images, employing RSA and MD5 for security. Balamurugan and Senthil (2016) put forth a reversible watermarking system using fingerprint biometrics for authentication and symmetric public key cryptography for confidentiality.
2) The multimodal biometric system Template Protection: Kanta and Chaudhary, proposed a watermarking-based The proposed approach aims to protect templates in multimodal biometrics by embedding secure watermarks, ensuring both privacy and integrity of the biometric data, integrating. The system integrates both iris and face biometrics to enhance the accuracy and security of the authentication process. Their method embeds The iris image is embedded into the face template to enhance biometric security. The iris image is embedded in the face template The iris image is embedded in the face template is embedded in the face template for the safe storage of templates. For authentication, both iris and face patterns are extracted from the watermarked template biometric templates. A key contribution is providing security to both iris and face templates by hiding one within the other.
3) Combined Watermarking for Biometric Data Security: Haddada et al. .proposed a new watermarking reinforcement approach for biometric data protection, validated on fingerprint and face. Their method applies the same watermarking algorithm twice: first embedding fingerprint minutiae into the face, and then embedding the watermarked face into the original fingerprint.
4) Survey of Iris Biometric Watermarking: Taj and Sarkar24 provided a survey of embedding iris biometric watermarking for user authentication. They highlighted that iris biometrics is considered highly reliable due to the uniqueness of iris patterns. The survey discussed various techniques in spatial and transform domains, noting trade-offs between embedding capacity, robustness, and recognition accuracy. It emphasized the potential of iris biometric watermarking for improving user authentication and the need for continued research. Kant et al.. are also mentioned in this survey for utilizing iris and facial features in a watermarking approach for template protection.
5) Soft Computing based Image Watermarking: Singh et al. provided A concise comprehensive survey is provided on image watermarking is implemented using soft computing techniques. techniques, including applications in biometrics. The survey reviewed various soft computing- based watermarking approaches for robustness, imperceptibility, and embedding capacity. It also discussed challenges and potential solutions in this area.
6) Iris Image and Template Protection using Watermarking and Visual Cryptography: Abdullah (2016) proposed a two-stage framework for iris image and template protection using a robust A watermarking algorithm based on Gv is proposed. DCT middle band coefficient exchange for image integrity, and it combines watermarking and visual cryptography for template protection. The watermarking aimed to protect the evidentiary integrity of iris images.

7) Zero-Bit Watermarking for Biometric Image Protection: This method is based on Gv techniques on embedding a watermark or unique identifier without affecting the original image quality Security and attack resilience are emphasized. For instance, Dutta et al.'s research suggested a lossless approach to generating a unique digital code for biometric image identification DWT and SVD are used for image watermarking and extracting differentiating features.

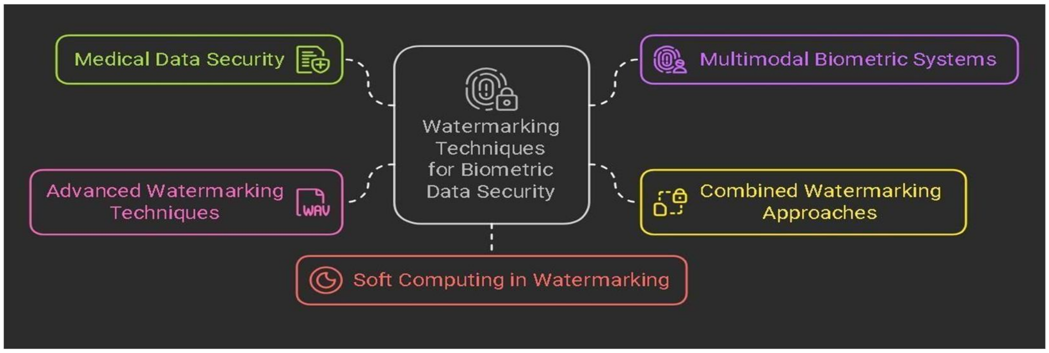
Medical Data Security
Multimodal Biometric Systems
Watermarking Techniques for Biometric Data Security
Advanced Watermarking Techniques
WAV
Combined Watermarking Approaches
Soft Computing in Watermarking

Fig 2: Watermarking Techniques for Biometric Data Security

VI. RESULTS AND DISCUSSION

The performance Analysis of Zero-Bit Watermarking for Biometric Unique ID Generation. This section discusses the expected The performance of the proposed method is evaluated by Zero-Bit A watermarking method for secure data embedding is proposed for biometric image unique ID creation, comparing it on the basis of important parameters like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), attack resistance, and overall security.

1) Image Quality Assessment (PSNR and SSIM): By definition, a Zero-Bit Watermarking technique aims to embed a unique identifier without making any alterations It is compared to the original method biometric image data1... Consequently, in an ideal scenario, the watermarked image is identical to the original. This would result in theoretically infinite PSNR values and an SSIM value of 1, indicating perfect image fidelity. This is a significant advantage over traditional watermarking techniques, which inherently introduce some level of distortion when embedding a watermark, leading to reduced PSNR and SSIM scores.
2) Robustness Against Attacks: The robustness of a Zero-Bit Watermarking technique relies on the stability and uniqueness of the features extracted from the biometric data that are used to generate and verify the unique ID. Instead of embedding data into the image pixels, the unique ID is intrinsically linked to these inherent biometric characteristics. The technique's resilience to attacks such as noise addition, compression, and geometric transformations would depend on how these attacks affect the extracted features. If the chosen features remain relatively invariant under common attacks, the generated unique ID and its verification process would be robust. Experimental results from traditional watermarking studies, like those in Abdullah (2016) showing BER and PSNR after manipulations15, highlight the challenges in maintaining watermark integrity under attacks.
3) Security: Security in your Zero-Bit Watermarking technique is multifaceted. First, generating a distinctive and possibly encrypted ID for every biometric image adds a level of security by linking an identifier that is not immediately distinguishable from the image itself. Using encryption algorithms would add even more to this security of the distinctive ID, rendering it useless to the attackers even if obtained without the corresponding decryption key or database data. Secondly, the integrity of the biometric data is ensured as a result of the lack of direct embedding changes. This avoids possible degradation or tampering that may be caused by conventional watermarking.
4) Comparison with Other Methods: Compared to traditional watermarking techniques that modify image pixels, your Zero-Bit approach offers the significant advantage of preserving the original biometric data without any loss of quality, as indicated by potentially perfect PSNR and SSIM scores. This is particularly critical in biometric systems where the accuracy of recognition is paramount. While traditional methods focus on embedding a tangible watermark payload that can be extracted, your technique focuses on deriving a unique and secure identifier from the inherent properties of the biometric itself.

VII. FUTURE DIRECTIONS

Future research in this area could focus on:

1) Identifying and extracting highly stable and unique features from various biometric modalities that are resilient to a wide range of attacks.
2) Developing robust and secure methods for generating and verifying unique IDs based on these extracted features, potentially incorporating advanced encryption techniques.

3) A comprehensive evaluation of the robustness of Zero-Bit Watermarking techniques against sophisticated attacks, including those specifically targeting feature extraction and matching algorithms.
4) Exploring the integration of machine learning algorithms for improved feature extraction and robust ID generation and verification.
5) Investigating alternative methods for securely storing and managing the generated unique IDs and associated metadata.

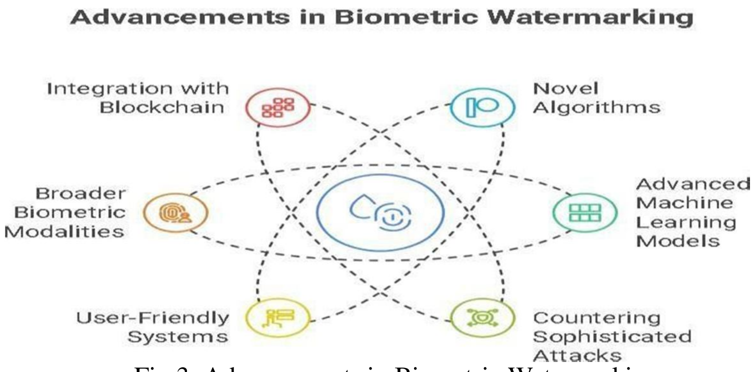
Advancements in Biometric Watermarking
Integration with Blockchain
Novel Algorithms
Broader Biometric Modalities
Advanced Machine Learning Models
User-Friendly Systems
Countering Sophisticated Attacks

Fig 3: Advancements in Biometric Watermarking

VIII. CONCLUSION

Although DWT and DCT fight well against general image manipulations, SVD fights with stability through embedding in intrinsic properties. Hybrid approaches merge the advantages of various techniques for enhanced security. In spite of this, there are still problems with balancing robustness and imperceptibility, as well as computational complexity of sophisticated techniques, ruling out real-time usage. Zero-Bit Watermarking, a recently proposed technique, aims to steer clear of these trade- offs by obtaining a biometric watermark from biometric traits without altering the original data. Despite progress, research gaps remain, such as enhancing adversarial robustness, enhancing real-time applicability, evaluating impact on recognition performance, creating standard metrics, and exploring AI-assisted advancements. Subsequent research should focus on the guarantee of secure identifier storage and boosting security to ward off prospective attacks to tap into the maximum capability of traditional and Zero-Bit watermarking to secure biometric data.

REFERENCES

[1] Nada Fadhil Mohammed, Majid Jabbar Jawad, and Suhad AAli, Biometric-based medical watermarking system for verifying privacy and source authentication, Kuwait Journal of Science, Vol.

[2] Chander Kant and Sheetal Chaudhary, "A watermarking- based approach for protection of templates in multimodal biometrics system," Procedia Computer Science, Vol. 167, pp. 932–941, 2020.3

[3] Sinan Q. Salih, Ravi Sekhar, Jamal Fadhil Tawfeq, Amer Ibrahim, Pritesh Shah, and Ahmed Dheyaa, "Integrated Digital Signature Based Watermarking Technology for Securing Online Electronic Documents," Fusion: Practice and Applications, Vol. 14, No. 01, pp. 120-128, 2024.4

[4] Taskeen Taj and Manash Sarkar, "A Survey on Embedding Iris Biometric Watermarking for User Authentication,"

[5] Cloud Computing and Data Science, Vol. 4, Iss. 2, pp. 203-211, 2023.5

[6] Om Prakash Singh, A. K. Singh, Gautam Srivastava, and Neeraj Kumar, "Image Watermarking using soft computing techniques: A comprehensive review survey," Multimedia Tools and Applications, DOI: 10.1007/s11042-020- 09606-x, August 2021.6

[7] Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers, "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography," IEEE Access, [Information inferred from the text suggests it's an IEEE publication, though specific volume/issue/pages are not directly stated. If this is critical, please provide more precise citation details for this source].7

[8] S. D. Shinde and P. S. Malge, "Efficient reversible watermarking technique for secure data embedding protected templates of biometric authentication system," international journal of innovations in engineering research and technology [IJIERT], Vol. 5, Iss. 5, May-2018.8

[9] Kumar, et al., [Information inferred from the text suggests a conference or journal paper on Rubik's cube scrambling for image encryption, though full details are not provided in this excerpt].9

[10] G. Balamurugan, et al., [Information inferred from the text suggests a paper on iris verification using IrisMatch-CNN, though full details are not provided in this excerpt].10

[11] M. A. M. Abdullah et al., [Information inferred from the text suggests a paper on multimodal iris recognition using deep learning, though full details are not provided in this excerpt].11

[12] Lydia Elizabeth et al., [Information inferred from the text suggests a paper reviewing watermarking system frameworks and the effectiveness of DWT, though full details are not provided in this excerpt].12

[13] M. K. Dutta, et al., [Information inferred from the text suggests a paper on distinguishing forged and original printed documents, though full details are not provided in this excerpt].