REVIEW ARTICLE

A Biometric Authentication Framework Based on Image Watermarking

Mahbuba Begum[1,*], **Fauzia Yasmeen**[2], **Mohammad Shorif Uddin**[3], **Jannatul Ferdush**[4], **Sumaita Binte Shorif**[3], **Taminul Islam**[5], **Anjuman Naher Jui**[6] **and Md. Marufur Rahman**[7]

[1] Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh
[2] Department of Computer Science and Engineering, Fareast International University, Dhaka 1230, Bangladesh
[3] Department of Computer Science and Engineering, Jahangirnagar University, Dhaka 1342, Bangladesh
[4] Department of Computer Science and Engineering, Jashore University of Science and Technology, Jashore 7408, Bangladesh
[5] Department of Computer Science and Engineering, Daffodil International University, Dhaka 1216, Bangladesh
[6] Department of Computer Science and Engineering, University of Science and Technology Chittagong, Chattogram 4202, Bangladesh
[7] Department of Computer Science and Engineering, Dhaka International University, Dhaka 1212, Bangladesh

Abstract

The need for robust information protection techniques has become important in security applications, especially to safeguard secret messages during transmission. The rapid expansion and pervasive use of the Internet have amplified security concerns, particularly regarding the authenticity of digital images, a significant issue in the context of the fourth industrial revolution. Biometric authentication using image watermarking addresses these concerns by embedding biometric information into digital images, thereby ensuring their security and privacy. Numerous recent methods have fused biometric modalities with watermarking techniques to enhance the security and reliability of transmitted messages. Despite these advancements, achieving parallel security and storage efficiency for biometric images remains a complex challenge. To cope with these challenges, this research proposes a standardized robust fusion framework for biometric-based image authentication tailored to various applications.

Keywords: biometric authentication, optimization, robust, security and privacy.

1 Introduction

Biometric authentication has gained popularity due to its ability to address data protection and security issues, especially given the increasing accessibility and misuse of the Internet. This mechanism embeds private data into biometric images, ensuring the

Academic Editor:
Deqiang Han

Submitted: 14 August 2025
Accepted: 23 October 2025
Published: 12 November 2025

Vol. 2, **No.** 4, 2025.
10.62762/CJIF.2025.545927

***Corresponding author:**
✉ Mahbuba Begum
mahbubacse@mbstu.ac.bd

Citation
Begum, M., Yasmeen, F., Uddin, M. S., Ferdush, J., Shorif, S. B., Islam, T., Jui, A. N., & Rahman, M. M. (2025). A Biometric Authentication Framework Based on Image Watermarking. *Chinese Journal of Information Fusion*, 2(4), 340–355.

protection of personal data [1]. Digital image watermarking enhances image authentication by leveraging information duplication from interactive communication [2]. In this process, the watermark image verifies the integrity, authentication, and ownership of the original image.

Biometric authentication using image watermarking protects biometric data without storing human characteristics in a template database [3]. Various biometric features such as fingerprints, retinas, irises, voices, faces, and gait biometrics can be used as watermark images, encrypting homomorphic systems to provide authenticity and confidentiality [4]. Currently, biometric image watermarking can be combined with cryptography and reversible image watermarking to ensure authentication, confidentiality, and integrity in parallel [5].

A fingerprint based image authentication shows how the ridges and valleys pattern is imprinted on the surface of the fingertip which identifies a fingerprint's uniqueness [6, 7], in application of user authentication process. The authenticity of a fingerprint image could be verified using digital watermarking [8] by embedding the watermark data within the original fingerprint image. Before the watermark is placed, we might encrypt the watermark data keeping attackers from accessing the watermark as an extra security measure [9]. The reversible watermarking method effortlessly retrieves fine details from a fingerprint image that has been watermarked. Also, discrete wavelet transform (DWT) and singular value decomposition (SVD) based hybrid approaches provide enhanced robustness against multiple geometric and noise attacks and user identity protection when employing fingerprint and gait biometrics features for image watermarking [10]. Adding biometric features like iris, fingerprint prevent unauthorized access or manipulation of data and also protects copyright that verifies the identity of the claimed person. The iris biometric feature is embedded into the data for ensuring user authentication by providing integriry and confidentiality of the digital system [11]. Strong security and enhanced resistance against traditional threats are guaranteed by this biometric approach. Another dual watermarking technique generates transformed watermark where minor biometric watermark is inserted into the major watermark. Then, this transformed watermark can be used as the watermark image and embedded into the original carrier image [12]. This approach ensures image authenticity by improving security and robustness of the system.

However, it is necessary to present the current status including the state-of-the-art methods of biometric authentication using image watermarking techniques. This paper tries to give such a vivid picture. Our research contributions are as follows:

- We outline the most current advancements in biometric authentication using image watermarking algorithms.
- We list the limitations of existing biometric authentication systems.
- We propose a biometric image authentication framework overcoming the existing research gaps.

The paper is organized as follows: Section 2 describes the fundamental design requirements for embedding biometric features into an image using a watermarking system. The related literature is reviewed in Section 3. The use of image watermarking in recent times is covered in Section 4. Existing limitations are mentioned in Section 5. Section 6 highlights recent advancements in biometric-based image watermarking systems. Our proposed biometric image authentication framework using watermark based on existing research gaps is given in Section 7. Finally, Section 8 provides a summary of the research and recommendations for the future.

2 Generic Biometric Image Watermarking Framework and Design Requirements

We present a general framework for biometric authentication using image watermarking, as illustrated in Figure 1.

Figure 1 illustrates the overall process of biometric watermark embedding and authentication. Initially, biometric features such as fingerprints, irises, or voices are used as watermarks, and the system encrypts the biometric image using lightweight image encryption techniques. The input image is classified by machine learning algorithms, after which the system extracts features from the classified host image. An optimization technique calculates the scaling factor that determines the watermark strength. The encrypted biometric watermark image is then embedded into the classified host image using a hybrid watermarking algorithm with the optimized scaling factor, generating the watermarked image. Subsequently, the system extracts the watermark image from the generated watermarked image in reverse. A matching algorithm compares the extracted biometric

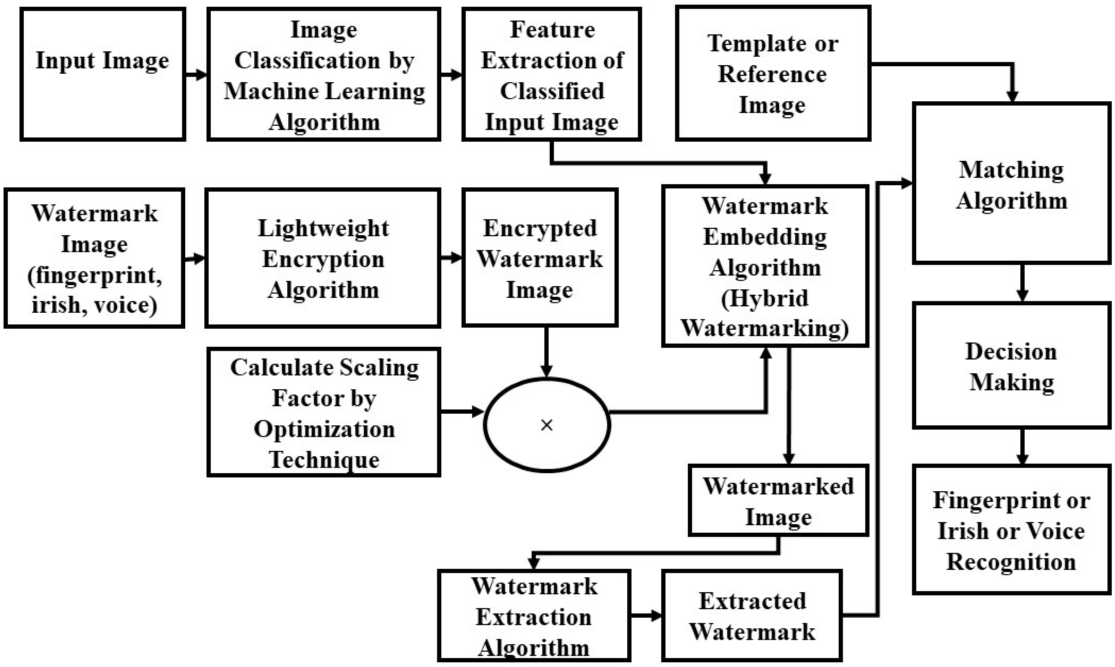
Input Image
Image Classification by Machine Learning Algorithm
Feature Extraction of Classified Input Image
Template or Reference Image
Matching Algorithm
Watermark Image (fingerprint, irish, voice)
Lightweight Encryption Algorithm
Encrypted Watermark Image
Watermark Embedding Algorithm (Hybrid Watermarking)
Decision Making
Calculate Scaling Factor by Optimization Technique
×
Watermarked Image
Fingerprint or Irish or Voice Recognition
Watermark Extraction Algorithm
Extracted Watermark

Figure 1. A general framework of biometric authentication using image watermarking.

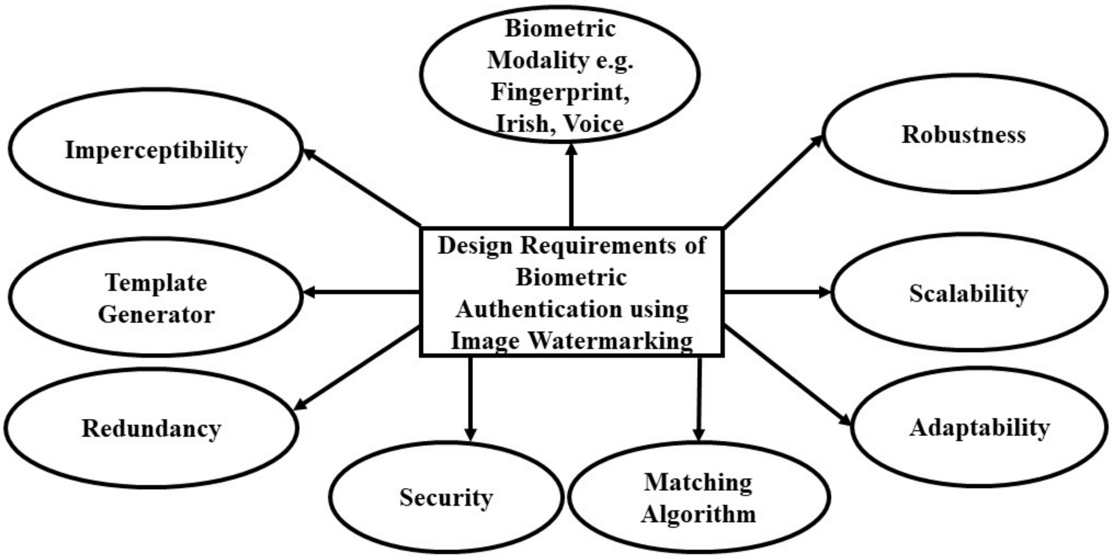
Biometric Modality e.g. Fingerprint, Irish, Voice
Imperceptibility
Robustness
Design Requirements of Biometric Authentication using Image Watermarking
Template Generator
Scalability
Redundancy
Adaptability
Security
Matching Algorithm

Figure 2. Preliminaries of biometric authentication using image watermarking.

watermark with the template biometric storage. The system then makes a decision based on this matching algorithm to verify the authenticity of the biometric image.

In designing a biometric image authentication, we should consider some design requirements, which is depicted in Figure 2.

Figure 2 illustrates biometric authentication design issues including biometric modalities, matching algorithms, scalability, redundancy, security, template storage, and adaptability, etc.

In this section, we have described several requirements for designing a biometric image watermarking-based authentication.

2.1 Extracted Biometric Modalities and Features

Biometric feature extraction is one of the significant design requirements. Figure 3 depicts the workflow of extracting features from biometric modalities.

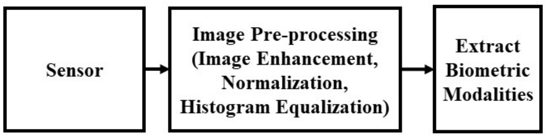
Sensor
Image Pre-processing (Image Enhancement, Normalization, Histogram Equalization)
Extract Biometric Modalities

Figure 3. Workflow of extracting biometric features.

In Figure 3, at first, the system uses a sensor to take the input image. Then, image pre-processing techniques like image enhancement, normalization, histogram equalization, etc. are used to process the image before going to the operation. Then, the system uses techniques to extract efficient features from biometric modalities such as fingerprint, iris, retina, voice, face, etc. For multi-modal biometric fusion, the system extracts minutiae points from fingerprint images and integrates them with other features (e.g., iris codes) via feature-level fusion to generate a robust watermark template [5].

2.2 Template Generator

For designing an efficient biometric image watermarking system, the first step is to embed the biometric data into the host image by developing a template generator. This template helps the system to store multiple biometric features and also enhances the security with an additional layer. This generator guarantees that the watermark image is only extracted for correct biometric features stored in the template. Bhatnagar et al. [13] enhance the authenticity and integrity of the biometric template by blending chaotic sequence, Hessenberg decomposition, and SVD decomposition. Their system is robust against various attacks and ensures improved imperceptibility than existing methods.

2.3 Scalability

The scalability of biometric authentication-based image watermarking embeds biometric data into the host image by maintaining the reliability and efficiency of the system simultaneously. Bergman [14] proposed a Match-on-Card technology for ensuring the security and scalability of biometric authentication networks against cyber-attacks.

2.4 Adaptability

This requirement defines the adjustment or accommodation in changing the biometric imformation accurately for authenticating the system. This adaptability can be achieved through dynamic watermarking, working against a large variety of attacks for testing robustness, adjusting the proper balance between watermark image quality and reliability, and working with a combination of multiple biometric features.

2.5 Redundancy

This requirement adds additional information to the watermark image to increase the robustness and reliability of the watermarking system.

2.6 Imperceptibility

Imperceptibility evaluates the effectiveness of an image watermarking system where the generated watermarked image and the original host image remain the same in quality with respect to the human visual system [2]. A masking-based watermarking system is proposed by Yang et al. [15] that ensures better imperceptibility of the system. This method ensures minimum loss of the watermarked image in quality.

The watermark imperceptibility is assessed using the structural similarity index (SSIM). The procedure of embedding the watermark may result a detoriation of image quality. Nonetheless, in invisible watermarking, the human visual system frequently fails to detect it. Improved imperceptibility is implied by high peak-signal-to-noise ratio (PSNR) values. The best watermarking strategies guarantee greater imperceptibility, or the absence of any discernible difference between the watermarked and host images [16]. Equations (1) and (2) express the representations of SSIM and PSNR, respectively.

$$\mathrm{SSIM} = \frac{(2\mu_w\mu_{w'} + C_1)(2\sigma_w\sigma_{w'} + C_2)}{(\mu_w^2 + \mu_{w'}^2 + C_1)(\sigma_w^2 + \sigma_{w'}^2 + C_2)} \tag{1}$$

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}}\mathrm{dB} \tag{2}$$

where w is the host image and w' is the watermarked image. μ and σ are the image mean and variance, respectively, and C_1 and C_2 are constants. MSE is the mean squared error between the host and the watermarked images, which is shown by the following equation (3).

$$\mathrm{MSE} = \frac{\sum_1^n (w'[n] - w[n])^2}{n} \tag{3}$$

2.7 Robustness

Robustness detects the watermark even after some common manipulation or attacks in the watermarking system such as: analog to digital conversion or vice-versa, image enhancement, resizing, scaling, etc. [17]. Zhou et al. [18] proposed a hybrid transform domain-based watermarking method where the watermark image is embedded into the high-frequency components of the host image. This ensures improved robustness against a large variety of attacks. Generally, the resilience of the image watermarking system is assessed using bit-error-rate (BER), normalized correlation (NC), and signal-to-noise ratio (SNR) metrics whose representations are given in Equations (4) to (6).

$$\mathrm{NC}(x, x') = \frac{\sum_1^n x[n] \sum_1^n x'[n]}{\sqrt{\sum_1^n (x[n])^2 \sum_1^n (x'[n])^2}} \tag{4}$$

$$\mathrm{BER}(x, x') = \frac{\sum_1^n x[n] \oplus x'[n]}{N} \tag{5}$$

$$\mathrm{SNR} = 10 \log_{10} \frac{\sum_1^n x^2[n]}{\sum_1^n (x[n] - x'[n])^2} \,\mathrm{dB} \tag{6}$$

where x is the watermark image and x' is extracted watermark image, and the symbol $\oplus$ indicates the exclusive OR (XOR) operator between x and x'.

2.8 Security

Security is a major issue in designing a biometric-based image watermarking system which is guaranteed by a secret key with various encryption techniques like chaos-based, logistic map, and others [19]. In [20], the watermark image is encrypted using pseudo-random sequences before embedding the watermark image. Security is mostly required in telecommunication, imaging, multimedia content. The degree of watermarking system security is determined by the key of the encryption method. Various encryption strategies such as logistic map-based and chaos-based Discrete Cosine Transform (DCT) have been employed to guarantee the security and privacy of the embedded watermark [19].

2.9 Matching Algorithm

The matching algorithm determines the similarity score between the extracted biometric features and the reference biometric image where high similarity means the system is highly authenticated. In a biometric authentication system, the PSNR, SSIM, BER, and NC are typically used to gauge how well the matching algorithm is working.

3 Watermarking in Biometric Systems: Related Literature Study

Vatsa et al. [21] proposed a multimodal biometric image watermarking system with two levels of authentication for verifying and protecting biometric templates. In this case, the iris template works as watermark which is embedded into the face image for ensuring authentication as well as security of the biometrics data. This method shows 96.8% accuracy by proving robustness against conventional attacks. Also, biometric watermarking embeds an image to the biometric trait of copyright owners to ensure robustness [22]. A biometric feature can be used as a unique identifier that cannot be misplaced or forgotten [23]. SVD based watermarking cannot resist ambiguity attacks which results in biometric key solution where nobody can extract the watermark image without key even after knowing the whole embedding algorithm. This biometric key ensures the high security of watermarking techniques. Hence, for ensuring improved security, Bhatnagar et al. [24] embeds a gray-scale watermark image into the decomposed host image using a biometrically generated key. In this paper, one can not get the exact coefficient for watermark embedding that ensures high security of the system. In 2013, Shaw et al. [25] proposed empirical mode decomposition (EMD) based biometric technology for watermarking where the fingerprint image is embedded into the host image using the hybrid algorithm of lifting-based DWT and SVD. Fingerprint-based biometric image watermarking technology gains popularity in the case of ownership identification and authentication. For ensuring security issues of transmitted data over the communication channel, Vashistha et al. [26] proposed a biometric framework based on integer DCT (IDCT). In this case, the fingerprint is embedded into the host image using IDCT. The method is robust against salt and pepper (SPN) noise, Gaussian noise (GN), and geometric attacks like rotation. However, the filter and hybrid attacks are not observed. Also, the method is robust only for low noise density and doesn't resist rotation more than 1 degree. Also, its imperceptibility is not so good.

In 2019, a new reversible and blind fingerprint image watermarking technique is proposed by Bousnina et al. [27]. First, carry out a zigzag scanning on the coefficients matrix of the original fingerprint image. The vector of the coefficients is decomposed into two sub-vectors, and DCT is applied to these sub-vectors. The sequence bits of the binary watermark are then inserted into the two sub-vectors for embedding, and a secret key is added. The result provides a high visual quality of the watermarked image. The PSNR value was found to be 47dB. Altay et al. [28] suggested two new methods for blending biometric digital watermarks with color images in 2021. The first method is QR decomposition-based redistributed invariant DWT (RIDWT), and the other

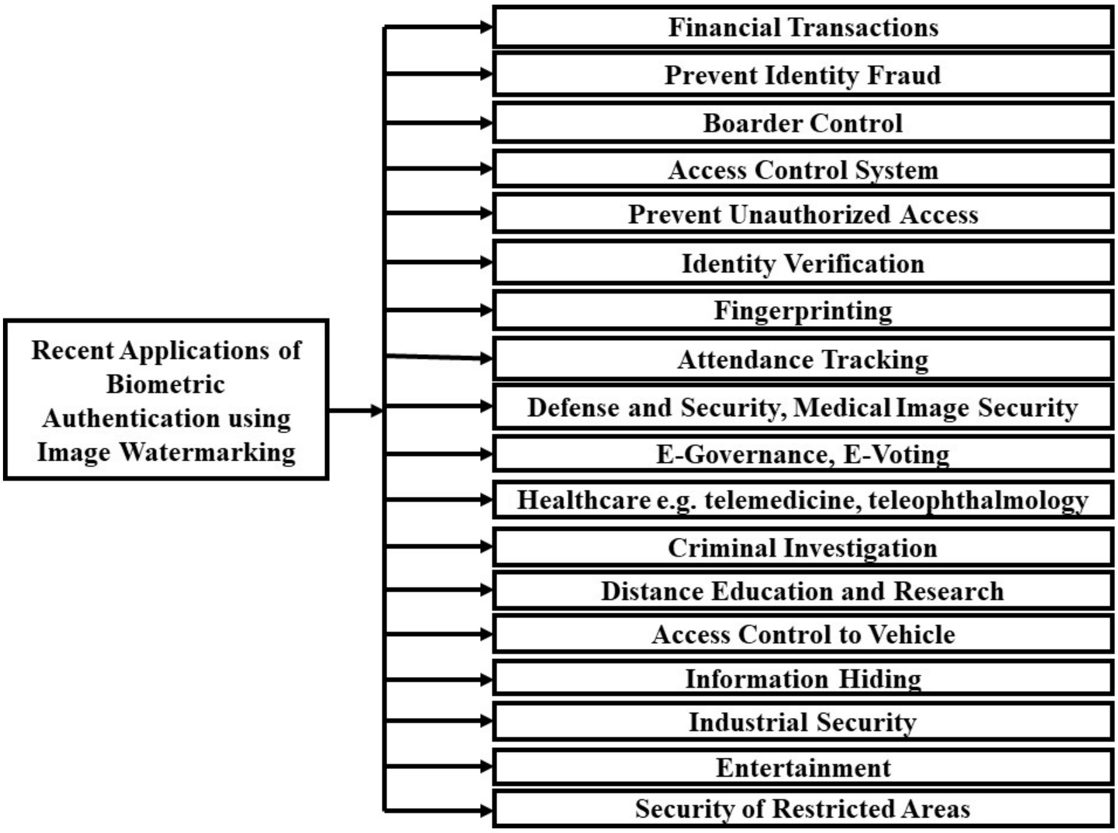
Recent Applications of Biometric Authentication using Image Watermarking
Financial Transactions
Prevent Identity Fraud
Boarder Control
Access Control System
Prevent Unauthorized Access
Identity Verification
Fingerprinting
Attendance Tracking
Defense and Security, Medical Image Security
E-Governance, E-Voting
Healthcare e.g. telemedicine, teleophthalmology
Criminal Investigation
Distance Education and Research
Access Control to Vehicle
Information Hiding
Industrial Security
Entertainment
Security of Restricted Areas

Figure 4. Recent applications of biometric authentication using image watermarking.

is Schur-decomposition-based RIDWT. Both methods convert the RGB image into YCbCr color space, and RIDWT is applied to the Y channel. The LL sub-band is split up into non-overlapping blocks that measure 4×4. QR decomposition is applied on each block for 1st method and schur decomposition for 2nd method, and the watermark is embedded in the R matrix. The PSNR values of RIDWT-QR and RIDWT-Schur are 38.6705dB and 37.3665dB, respectively. In 2023, Gomez-Coronel et al. [29] suggested an invisible, secured, robust hybrid watermarking algorithm based on Hermite Transform and SVD-DCT. This algorithm embeds two watermarks, LOGO as a digital binary image and metadata as a text image. The LOGO watermark is encrypted by Jigsaw Transform (JST) and the Elementary Cellular Automaton (ECA), and metadata is ciphered through XOR operation. However, this method provides the worst results for rotation and cropping attacks.

In 2023, Mohammed et al. [30] used another biometric watermarking system to secure the patient's information. This algorithm used two watermarks. At first, the iris watermark is processed, and segmentation and normalization are done for feature extraction. The iris acts as an authentication key, and the second watermark (patient's data) is encrypted via XOR operation and embedded with the key. The average PSNR value of this method is 57.1920 dB. In 2024, A blind watermarking technique combined Radon transform with DCT improved the visibility and robustness against various attacks in Bao et al. [31]. This method used the host and watermark as color images. The RGB image translated the host image into YUV color space, and the Radon transform is applied to the U component. Furthermore, On the chosen blocks of the radon domain, 2D-DCT is performed. However, the watermark is encrypted through the Arnold transform. But, when the rotation attack on the watermarked image causes inaccurate values of the black pixels. These methods often leverage multi-modal fusion to combine biometric traits, enhancing the overall reliability of watermark extraction against attacks.

4 Recent Applications of Biometric Authentication using Image Watermarking

Biometric authentication based on image watermarking can be used in several applications like financial transactions, preventing identity fraud, controlling border access, access control systems, prevention of unauthorized access, fingerprinting, identity verification, attendance tracking, defense and security, medical image security, E-governance and E-voting, healthcare, criminal investigation, distance education and research, vehicle access control, information hiding, industrial security, entertainment, and security of restricted areas, etc. Aparna et al. [5] used several medical images to improve the biometric security of the system. Their proposed method can be effectively used in recording electronic health data. Motwani et al. [22] used biometric traits as watermark images that are embedded into the 3D graphics in developing digital rights management system. Olaniy et al. [32] proposed a biometric authentication using crypto-watermarking techniques for securing an electronic voting (E-voting) system. Konnurmath et al. [33] used biometric images as watermarks with hybrid transform domain-based watermarking techniques for protecting copyrighted digital images. Lebcir et al. [34] proposed reversible DCT based watermarking techniques for authenticating fingerprint images. Aparna et al. [35] proposed a blind watermarking technique for securing online health records. Thanki et al. [36] proposed fragile biometric image watermarking for detecting tamper in images while accessing shared servers or the cloud. In 2023 [37], Fernandez and Nithyanandam highlighted the associated applications of biometric-based watermarking system including E-helthcare, online voting, and online theft identification, etc. We depicted these applications in the following Figure 4.

Figure 4 illustrates the recent applications of biometric authentication using image watermarking including financial transaction, prevent identity fraud, boarder control, access control system, prevent unauthorized access, identity verification, fingerprinting, attendance tracking, defense and security, medical image security, E-governance, E-voting, healthcare e.g., telemedicine, teleopthalmology, criminal investigation, distance education and research, access control and vehicle, information hiding, industrial security, entertainment along with security of restricted areas.

5 Limitations of Existing Biometric Authentication System using Image Watermarking

In recent years, there has been prominent progress in the development of biometric authentication systems, where image watermarking has surfaced as a prospective method for enhancing security and privacy. It is really a big challenge for researchers to implement a universally effective biometric-based image watermarking technique due to the variation of sensor technologies and image acquisition process. Face problems related to compatibility with various biometric recognition systems. There may be infrastructure and logistical difficulties when implementing biometric authentication systems on a large scale. The authentication procedure could be obtrusive or inconvenient for users. This review critically explores the intrinsic limitations embedded in current biometric authentication systems employing image watermarking. The in-depth analysis encompasses multiple facts such as:

- *Lack of Integration of System Components*: Traditional biometric authentication methods, such as message authentication codes (MAC) or hash functions, are not suitable for authenticating biometric data because small changes can have a significant effect on the input data. Therefore, if system components like sensors, template generators, and feature extractors are not properly integrated via information fusion techniques, leading to failures in multi-modal biometric authentication [38].

- *Accuracy and Reliability*: Impact the accuracy and reliability of biometric systems, affecting their ability to correctly identify individuals. The inclusion of watermarks in biometric images during the embedding process may lead to a decline in image quality. This reduction in quality has the potential to impact the accuracy and reliability of the authentication procedure, potentially resulting in instances of both false positives (erroneously permitting an unauthorized user) and negatives (unable to authenticate an authorized user) [39].

- *Robustness and Imperceptibility*: It's a challenging task to maintain a better trade-off between robustness and imperceptibility, as making watermarks too robust may result in visible distortions that could compromise the integrity of biometric images. The watermarking technique needs to exhibit heightened sensitivity to various image processing and geometric attacks, including spatial filtering, copying, cropping, scaling, translation, compression, and rotation. The correlation between the host image and the watermarked image is crucial, impacting the perceptual quality of the host image during the embedding process. This sensitivity should persist even in case of minor modifications to the image, whether intentionally or unintentionally,

Table 1. Summary of the existing biometric authentication-based image watermarking algorithms.

References, year	Used Methods	Image type and size (host and watermark)	Experimental Results	Advantages	Limitations	Applications
Bhatnagar et al. [24], 2013	Fractional dual-tree complex wavelet transforms (FrDT-CWT) and SVD	Grayscale and 256×256, Grayscale logo image and 64×64	Average PSNR = 44.34 dB	Robust against filtering, noise, geometric, contrast adjustment, and sharpening attacks	A non-blind technique that requires a host image for watermark extraction which increases computational complexity and not robust against arbitrary rotation angle	Security areas
Bousnina et al. [27], 2019	Dual-Tree Complex Wavelet Transform (DTCWT)-DCT	Grayscale image and 512×512, fingerprint grayscale 374×388	Average PSNR =30.88 dB	Blind technique	Reasonable level of robustness and lower level of imperceptibility	Multimodal biometric authentication
Altay et al. [28], 2024	QR decomposition and Schur decomposition in RIDWT Domain	Color image and 512×512, Biometric grayscale 1600 (bits)	Average PSNR =37.3665 dB	Blind technique, Robust against JPEG compression, rotation, flipping, and cropping attacks	lower level of imperceptibility, less robust against resizing and scaling, also, not robust against arbitrary rotation angle	Copyright Protection
Coronel et al. [29], 2023	Hermite Transform and SVD-DCT	Grayscale and 512×512, and Grayscale logo image 100×100	Average PSNR=40.2051dB	Robust against filering, noise, scaling, translation, compression, and histogram equalization attacks	Worst result against rotation and cropping attack	Copyright Protection
Mohammed et al. [30], 2023	Legendre Moment with DCT	Grayscale and 512×512, 1024×1024, 2048×2048, 3072×3072, 4096×4096, Grayscale watermark 1672, 2120, 3048, 3920 and 6000 in bits	Average PSNR=47.2503dB	Maintains imperceptibility with any image size	Not concerned with system's robustness and security of watermark image	E-healthcare System
Bao et al. [31], 2024	Radon and DCT Transform	Color image and 512×512, color image and 32×32	Average PSNR=38.8441 dB	Bind technique, Good imperceptibility, high security and robust against filtering, noise, geometric, sharpening, histogram equalization, and zoom in attacks	Inaccurate calculation of rotation angle due to black pixels in the edge areas of the watermarked image	Copyright Protection
Konnurmath et al. [33], 2017	DWT-DCT-SVD	Grayscale 512×512 and grayscale 256×256	Average PSNR=90 dB	Better imperceptibility	Robustness is not tested	Forensic-proof
Lebcir et al. [34], 2020	DCT	Grayscale and grayscale	Average PSNR=47.53 dB	Blind technique, good imperceptibility of both host and watermark images	Robustness is not tested	Fingerprint recognition system
Yasmeen et al. [50], 2021	DWT-SVD	Grayscale and color image and 512×512, Grayscale 256×256	Average PSNR= 43.8362 dB (grayscale), 34.7266 dB (color)	Robust against noise, stretching, and histogram equalization attacks	low PSNR values for color images, less robust against rotation and cropping, non-blind technique	Security areas
Agilandeeswari et al. [51], 2023	Dual-Tree Complex Wavelet Transform (DTCWT) and pseudo-Zernike moments (PZM)	Color image and 512×512, Color and Grayscale image 32×32	Average PSNR=68.54dB	Analyses false positive and negative issues, detects tamper and recover this issue, robust against common image processing attacks	Not robust against arbitrary rotation angle and won't be suitable for asynchronous transmission, where embedding and extraction happen independently	Content authentication and ownership proofing
Hajiabbasi et al. [52], 2023	DWT with lattice vector quantization	Color image 1093×2372, Grayscale fingerprint image 800×750	Average PSNR= 45.5 dB	Good accuracy, efficient and faster system	Significant variations in customer biometrics and conditions of the bank environment require further training of models, expensive system	Banking service provision during the COVID-19 pandemic
Joyce et al. [53], 2023	Multiband wavelet transforms and singular value decomposition	Grayscale and 512×512, Grayscale and 8×8	Correct Recognition Rate (CRR) = 99.4%	Robust against compression, filtering, and blurring attacks, maintains integrity	Geometric attacks like: cropping, scaling, resizing and others are not observed	Information protection
Harika et al. [54], 2023	DWT-DCT-SVD	Color image 64×64, 128×128, 256×256, Grayscale fingerprint 64×64,	Average PSNR= 37.3336 dB	Robust against salt-and-pepper noise, scaling, and JPEG compression attacks	Not robust against cropping, rotation, Gaussian and speckle noises, filtering, sharpening, motion blur, filtering and histogram equalization attacks	E-Commerce, duplication restriction, and copyright protection

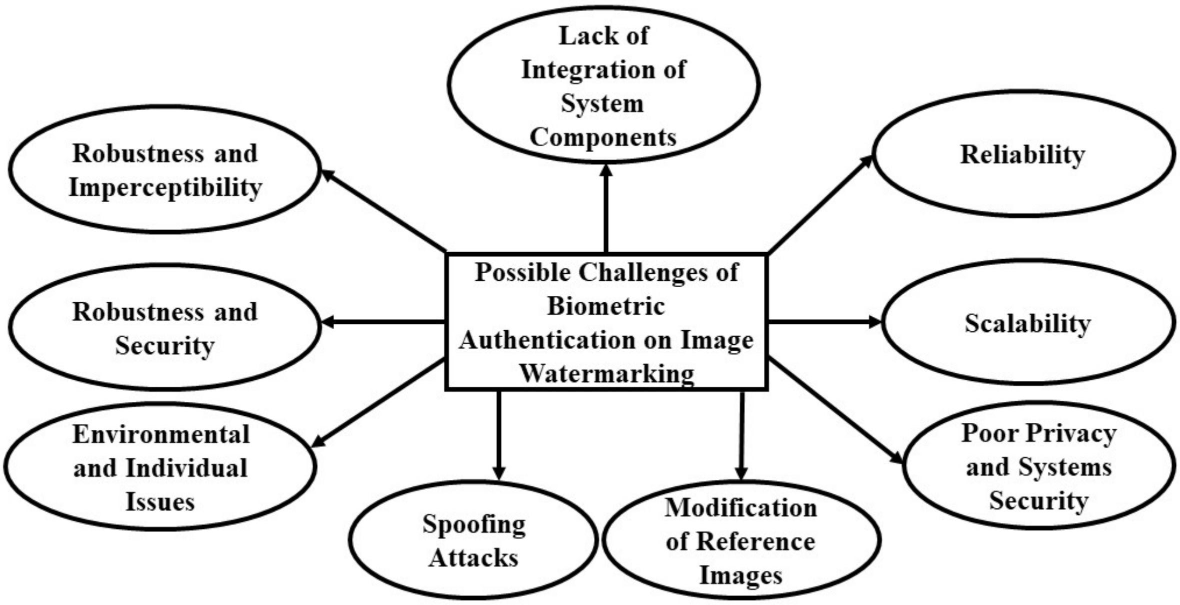
Possible Challenges of Biometric Authentication on Image Watermarking
Lack of Integration of System Components
Robustness and Imperceptibility
Reliability
Robustness and Security
Scalability
Environmental and Individual Issues
Poor Privacy and Systems Security
Spoofing Attacks
Modification of Reference Images

Figure 5. Possible challenges of biometric authentication using image watermarking.

with a high likelihood of detection [40].

- *Robustness and Security*: It is very difficult to maintain a good balance between robustness and security, which makes the system vulnerable to various attacks when transferring biometric data from the watermark embedding stage to the authentication stage.

- *Vulnerability of Attacks*: It is crucial to prevent unwanted access to the stored biometric templates. Although watermarking aims to enhance security measures, it remains susceptible to attacks [41]. Adversaries can utilize diverse methods, including image tampering or the removal of watermarks, potentially compromising the integrity of biometric data.

- *Spoofing Attack*: In a spoofing attack, an attacker tries to gain unauthorized access to the system [42–44], which can affect several biometric traits, such as fingerprints, iris patterns, voice, and facial features.

- *Poor Privacy and systems security*: If the security algorithm for biometric data is weak, the biometric data could be compromised due to poor privacy techniques [45]. Moreover, decrypted biometric data used in the authentication stage poses a security threat to the overall system [46]. When an organization collects or stores biometric data, they face the challenges of ensuring the security and privacy of biometric data as they are very personal and unique to each individual.

- *Modification of Template Database*: Any modification of the template or reference images could lead to false authentication of biometric data [47].

- *Security Concern*: If an attacker successfully removes or manipulates the watermark, it could lead to unauthorized use or tampering of biometric data. This affects the overall security of the biometric system. The security risk arises if a malicious actor manages to eliminate or alter the watermark, potentially resulting in unauthorized access or manipulation of biometric data. Such actions pose significant threats to the overall integrity and security of the entire biometric system, underscoring the importance of robust watermarking techniques to safeguard against such risks [48].

- *Scalability Issues*: Implementing image watermarking at scale, especially on a large scale with various sensor technology biometric systems, can pose challenges. The computational overhead and resource requirements may become prohibitive, impacting the system's efficiency and responsiveness [2].

- *Environmental Issues*: Biometric features can be affected by various environmental and individual conditions, such as humidity, lighting, injuries, aging, etc.

- *Ethical Implications*: Ethical consideration must be taken into account as they may raise concerns about individual privacy and consent. Ensuring the prevention of unauthorized access to stored biometric templates is paramount. However, the authentication process must be carefully balanced to avoid being overly intrusive or inconvenient for users. Moreover, ethical considerations surrounding individual privacy and consent must be thoroughly addressed, as these concerns may arise and necessitate careful deliberation [49]. We have identified possible challenges in Figure 5.

Figure 5 illustrates the challenges and limitations including lack of integration of system components, reliability, scalability, poor privacy and systems security, modification of reference images, spoofing attacks, environmental and individual issues, robustness and security, and robustness with imperceptibility.

6 Recent Developments in Biometric Image Watermarking Techniques

Recently biometric authentication using image watermarking can be done through optimization, machine learning techniques, IoT and cloud platforms, blockchain, and other emerging technologies, etc. Table 1 summarizes the existing biometric authentication algorithms that are widely used in image watermarking. This table includes references with year, used methods, host image type and size, experimental results, advantages, limitations, and applications.

From the existing research gaps, we have listed some limitations:

- Existing methods cannot handle geometric attacks like JPEG compression, rotation, and others efficiently.
- They have increased computational complexity.
- Not scalable to other transform domain techniques.
- Imperceptibility is not satisfactory.
- The quality of extracted watermark image is not so good.
- They have less embedding capacity.
- Not concern with watermark image security.

7 Proposed Biometric Authentication Framework

Figure 1 presents the generalized framework for biometric image authentication using watermarking. We have identified several existing research gaps in biometric authentication–based image watermarking methods, which are summarized in Table 1. Based on these research gaps, we propose a biometric authentication framework, illustrated in Figures 6 and 7. Figure 6 shows the proposed framework for biometric watermark embedding, while Figure 7 depicts the proposed framework for biometric authentication.

In Figure 6, the entropy map is computed after preprocessing the host image. Next, high-entropy blocks are identified for watermark embedding, and the block with the highest entropy is selected. Then, transform domain techniques are applied to the host image, and the corresponding sub-bands or coefficients, or singular values (denoted as SH) are selected. An optimization technique is then used to determine the watermark strength, alpha. Subsequently, the particular pixel value in SH corresponding to the highest entropy block is calculated, resulting in SH(P).

The watermark image (biometric features) is encrypted using a chaotic encryption algorithm after preprocessing, and transform domain techniques are applied to the encrypted watermark image to select the sub-bands or coefficients, or singular values (denoted as SW). The watermark embedding algorithm embeds SW into SH(P) using the watermark strength, alpha. The final watermarked image is obtained after performing the inverse transformation.

The proposed framework integrates entropy-based region selection, transform domain techniques, watermark strength optimization, and chaotic encryption to ensure strong robustness, enhanced imperceptibility, high embedding capacity, and improved security. Specifically, after applying transform domain techniques to the host image (such as DWT or SVD), the framework selects the block with the highest entropy within the chosen sub-band for watermark embedding. The watermark image is then embedded into this high-entropy block using an optimized embedding strength, alpha, which is determined to achieve a balance between imperceptibility and robustness. As a result, the framework is expected to yield high PSNR and NC values, indicating excellent visual quality and strong resilience against attacks.

In [55], Kumar and Singh proposed a maximum entropy-based image watermarking method in the DWT domain. First, a single-level (1L) DWT is

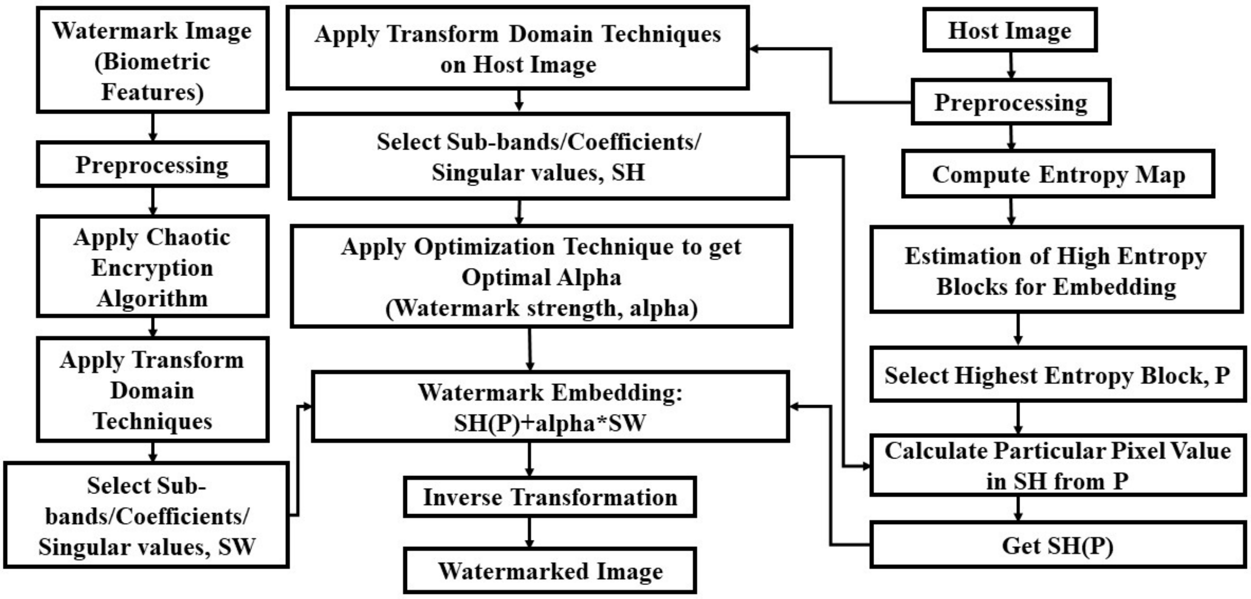
Watermark Image (Biometric Features)
Preprocessing
Apply Chaotic Encryption Algorithm
Apply Transform Domain Techniques
Select Sub-bands/Coefficients/ Singular values, SW
Apply Transform Domain Techniques on Host Image
Select Sub-bands/Coefficients/ Singular values, SH
Apply Optimization Technique to get Optimal Alpha (Watermark strength, alpha)
Watermark Embedding: SH(P)+alpha*SW
Inverse Transformation
Watermarked Image
Host Image
Preprocessing
Compute Entropy Map
Estimation of High Entropy Blocks for Embedding
Select Highest Entropy Block, P
Calculate Particular Pixel Value in SH from P
Get SH(P)

Figure 6. Proposed framework for biometric watermark embedding.

applied to the watermark image, and the high-high (HH) sub-band is extracted. Then, the HH sub-band of the watermark image is embedded into the highest-entropy block of the host image after performing a 1L DWT on it, using the alpha blending technique. The main difference between our proposed framework and the method in [55] is that our framework encrypts the watermark image using a chaotic encryption method before embedding it into the host image. Furthermore, we employ an optimization technique to determine the optimal watermark strength factor (alpha), which is multiplied by the selected watermark sub-band after applying the transform domain techniques and chaotic encryption to the watermark image.

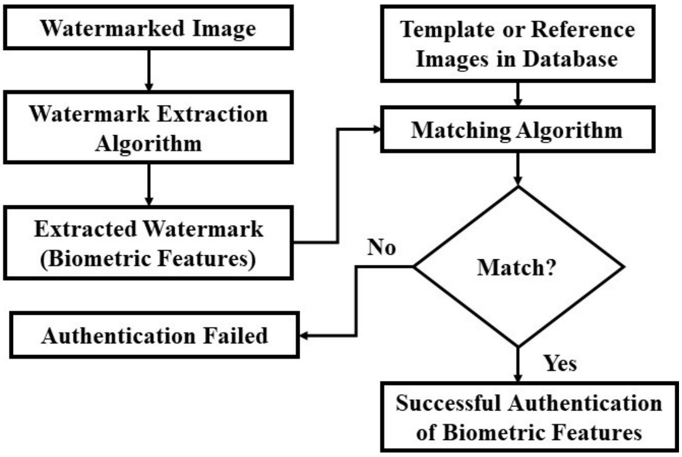
Watermarked Image
Watermark Extraction Algorithm
Extracted Watermark (Biometric Features)
Authentication Failed
Template or Reference Images in Database
Matching Algorithm
No
Match?
Yes
Successful Authentication of Biometric Features

Figure 7. Proposed framework for biometric authentication.

In Figure 7, the watermark extraction algorithm reverses the process to extract the watermark image. The matching algorithm then compares the extracted watermark (biometric features) with the template or reference images stored in the database. If they match, the biometric authentication is successful; otherwise, it fails. This structure ensures that the integrity of biometric data is preserved even after transmission, embedding, and attacks. Thus, it is better to use this framework so that the reliability of the proposed biometric authentication framework is ensured.

This paper proposes solutions to address challenges encountered in existing biometric authentication systems employing image watermarking methods. These suggestions are summarized below:

- *Performance Evaluation Criteria*: When evaluating the effectiveness of any image watermarking algorithm, the following factors should be carefully considered: computational complexity, capacity, security, resilience, and imperceptibility. It is essential to strike a balance how well the watermark is concealed (imperceptibility), how well the watermark survives intentional or unintentional attacks (robustness), protection between against unauthorized access (security), the amount of data that can be embedded (capacity), and the resource needed for embedding and extracting the watermark (computational complexity) when assessing the effectiveness of any image watermarking algorithm. This ensures that the chosen algorithm meets the desired objectives without compromising on key performance metrics [56].

- *Robust Encryption*: Robust encryption techniques should be designed for ensuring security of biometric modalities. These techniques are crucial for protecting biometric data from unauthorized access or tampering throughout its lifecycle. This includes securing both biometric modalities themselves and their stored templates. By employing strong encryption algorithms, the confidentially and integrity of biometric information can be preserved, mitigating the risk of malicious attacks and unauthorized access [57].
- *Privacy-Preserving Image Watermarking*: Privacy-preserving based image watermarking can be obvious solution in respect to ethical consent. This method presents a practical approach to tackling ethical issues surrounding consent and privacy in biometric systems. These techniques allow for the inclusion of biometric data while safeguarding the privacy and anonymity of users. By integrating privacy-enhancing elements into watermarking algorithms, developers can create systems that align with ethical standards and regularity frameworks, fostering user confidence and adoption [58].
- *Cloud-Based Optimization for Scalability*: Cloud-based optimization techniques can be effective solutions for scalability to manage a lot of authentication requests. Utilizing cloud-based optimization methods is an effective approach to managing scalability issues linked with handling a high volume of authentication requests in biometric systems. Cloud infrastructure offers the essential resources and adaptability to scale authentication services according to demand, guaranteeing smooth performance and responsiveness even during times of peak usage [59].
- *User Experience Prioritization*: Designers should prioritize user experience as a top consideration when developing biometric authentication systems. User-friendly interfaces, intuitive interactions, and seamless integration into existing workflows enhance user acceptance and satisfaction. By focusing on usability and accessibility, designers can promote widespread adoption and utilization of biometric technologies [60].
- *Consideration of Adversarial Attacks*: Biometric systems need to withstand adversarial attacks intending to undermine their integrity or circumvent authentication protocols. Designers must preemptively recognize potential vulnerabilities and deploy countermeasures to minimize the threat of attacks, thus ensuring the system's resilience and dependability in practical settings [61].
- *Secure Transmission of Biometric Images*: Transmission of biometric images need more attention to ensure security and privacy. To secure the storage of biometric templates, robust encryption algorithm should be obvious solution. It is crucial to focus on ensuring the secure transmission of biometric images to prevent interception or unauthorized access during data transfer. By implementing encryption protocols and utilizing secure communication channels, sensitive biometric data can be protected from tampering, thereby maintaining confidentiality and integrity throughout the transmission process [62].

8 Conclusion

The incorporation of biometric images through watermarking techniques guarantees robust authentication due to its versatility in various domains like financial transactions, E-government, defense security, IoT securities, and access control among others. This incorporation can be used as a safeguard without disclosing private biometric data as well as authenticate the digital image. This study highlights the innovative integration of biometric images into digital watermarking frameworks to enable secure and reliable authentication. By embedding biometric data using advanced transform domain techniques, entropy-based region selection, optimized embedding strength, and chaotic encryption, the proposed framework achieves a robust balance between imperceptibility, capacity, and security. One of the key innovations lies in selecting high-entropy regions for embedding, which enhances resistance to attacks while maintaining visual quality. Notably, the framework ensures biometric authentication without directly exposing sensitive biometric data, thus offering a dual layer of protection—authenticating digital content while preserving user privacy. Through a comprehensive review of state-of-the-art techniques, the paper also addresses critical challenges such as data privacy, ethical concerns, and secure storage. But, this framework may increase computational complexity and the optimized watermark strength is very much sensitive to parameter selection. Also, embedding in high-entropy regions could lead to loss of watermark integrity under heavy image manipulation. Future researchers also propose forward-looking solutions, including the use of strong encryption algorithms, blockchain integration for secure data management, and adaptive information hiding methods. Furthermore, the study recommends future research directions involving photo response non-uniformity (PRNU), generative adversarial networks (GANs), and user-unaware watermarking schemes to further enhance the robustness and privacy of biometric systems. In summary, the innovations presented in this paper not only contribute to the academic field of biometric watermarking but also offer practical solutions for real-world secure authentication systems.

Data Availability Statement

Not applicable.

Funding

This work was partially supported by the Research Cell of Mawlana Bhashani Science and Technology University (MBSTU).

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Li, S., Chen, X., Wang, Z., Qian, Z., & Zhang, X. (2018). Data hiding in iris image for privacy protection. *IETE Technical Review, 35*(sup1), 34–41. [CrossRef]

[2] Begum, M., & Uddin, M. S. (2020). Digital image watermarking techniques: A review. *Information, 11*(2), 110. [CrossRef]

[3] Tašić, J., & Adamović, S. (2017). Digital image watermarking techniques and biometrics data security: A review. In *Sinteza 2017 - International Scientific Conference on Information Technology and Data Related Research* (pp. 55–62). Singidunum University. [CrossRef]

[4] Kumar, G. D., Teja, D. P., Reddy, S. S., & Sasikaladevi, N. (2017). An efficient watermarking technique for biometric images. *Procedia computer science, 115*, 423-430. [CrossRef]

[5] Aparna, P., & Kishore, P. V. V. (2019). Biometric-based efficient medical image watermarking in E-healthcare application. *IET Image Processing, 13*(3), 421-428. [CrossRef]

[6] Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE Transactions on Image Processing, 9*(5), 846–859. [CrossRef]

[7] Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023). A blind and robust color image watermarking scheme based on DCT and DWT domains. *Multimedia Tools and Applications, 82*(21), 32855-32881. [CrossRef]

[8] Balamurugan, G. (2016). A fingerprint based reversible watermarking system for the security of medical information. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)* (pp. 1–6). [CrossRef]

[9] Noore, A., Singh, R., Vasta, M., & Houck, M. M. (2007). Enhancing security of fingerprints through contextual biometric watermarking. *Forensic Science International, 169*(2–3), 188–194. [CrossRef]

[10] Garg, P., & Jain, A. (2023). A robust technique for biometric image authentication using invisible watermarking. *Multimedia Tools and Applications, 82*(2), 2237–2253. [CrossRef]

[11] Taj, T., & Sarkar, M. (2023). A survey on embedding iris biometric watermarking for user authentication. *Cloud Computing and Data Science, 4*(2), 203–211. [CrossRef]

[12] Mokashi, B., Bhat, V. S., Pujari, J. D., & J, L. S. (2021). Dual watermarking technique for image authentication using biometrics. In *2021 IEEE Mysore Sub Section International Conference (MysuruCon)* (pp. 427–432). [CrossRef]

[13] Bhatnagar, G., Wu, Q. J., & Raman, B. (2010). Biometric template security based on watermarking. *Procedia Computer Science, 2*, 227-235. [CrossRef]

[14] Bergman, C. (2008). Match-on-card for secure and scalable biometric authentication. In *Advances in Biometrics: Sensors, Algorithms and Systems* (pp. 407-421). London: Springer London. [CrossRef]

[15] Yang, H. M., Liang, Y. Q., Wang, X. D., & Ji, S. J. (2007, November). A DWT-based evaluation method of imperceptibility of watermark in watermarked color image. In *2007 International Conference on Wavelet Analysis and Pattern Recognition* (Vol. 1, pp. 198-203). IEEE. [CrossRef]

[16] Zhang, H., Wang, C., & Zhou, X. (2017). A robust image watermarking scheme based on SVD in the spatial domain. *Future Internet, 9*(3), 45. [CrossRef]

[17] Zhang, Y. (2009). Digital watermarking technology: A review. In *2009 ETP International Conference on Future Computer and Communication* (pp. 250–252). [CrossRef]

[18] Zhou, X., Zhang, H., & Wang, C. (2018). A robust image watermarking technique based on DWT, APDCBT, and SVD. *Symmetry, 10*(3), 77. [CrossRef]

[19] Loani, N. A., Hurrahi, N. N., Parah, S. A., Lee, J. W., Sheikhi, J. A., & MohiuddinBhat, G. (2018). Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access, 6*, 19876–19897. [CrossRef]

[20] Wang, C., Zhang, H., & Zhou, X. (2018). A self-recovery fragile image watermarking with variable watermark capacity. *Applied Sciences, 8*(4), 548. [CrossRef]

[21] Vatsa, M., Singh, R., Mitra, P., & Noore, A. (2004, October). Digital watermarking based secure multimodal biometric system. In *2004 IEEE International Conference on Systems, Man and Cybernetics (IEEE Cat. No. 04CH37583)* (Vol. 3, pp. 2983-2987). IEEE. [CrossRef]

[22] Motwani, R. C., Harris, F. C., & Bekris, K. E. (2010, January). A proposed digital rights management system for 3d graphics using biometric watermarks. In *2010 7th IEEE Consumer Communications and Networking Conference* (pp. 1-6). IEEE. [CrossRef]

[23] Hämmerle-Uhl, J., Raab, K., & Uhl, A. (2011, May). Watermarking as a means to enhance biometric systems: A critical survey. In *International Workshop on Information Hiding* (pp. 238-254). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[24] Bhatnagar, G., & Wu, Q. M. J. (2013). Biometrics inspired watermarking based on a fractional dual tree complex wavelet transform. *Future Generation Computer Systems, 29*(1), 182–195. [CrossRef]

[25] Shaw, A. K., Majumder, S., Sarkar, S., & Sarkar, S. K. (2013). A novel EMD based watermarking of fingerprint biometric using GEP. *Procedia Technology, 10*, 172–183. [CrossRef]

[26] Vashistha, A., & Joshi, A. M. (2016, November). Fingerprint based biometric watermarking architecture using integer DCT. In *2016 IEEE region 10 conference (TENCON)* (pp. 2818-2821). IEEE. [CrossRef]

[27] Bousnina, N., Ghouzali, S., Mikram, M., & Abdul, W. (2019). DTCWT-DCT watermarking method for multimodal biometric authentication. In *Proceedings of the 2nd International Conference on Networking, Information Systems & Security* (pp. 1–7). [CrossRef]

[28] Altay, S. Y., & Ulutas, G. (2024). Biometric watermarking schemes based on QR decomposition and Schur decomposition in the RIDWT domain. *Signal, Image and Video Processing, 18*(3), 2783-2798. [CrossRef]

[29] Gomez-Coronel, S. L., Moya-Albor, E., Brieva, J., & Romero-Arellano, A. (2023). A robust and secure watermarking approach based on hermite transform and SVD-DCT. *Applied Sciences, 13*(14), 8430. [CrossRef]

[30] Mohammed, A. F., Nahi, H. A., Mosa, A. M., & Kadhim, I. (2023). Secure E-healthcare System Based on Biometric Approach. *Data and Metadata, 2*, 1-56. [CrossRef]

[31] Bao, B., & Wang, Y. (2024). A robust blind color watermarking algorithm based on the Radon-DCT transform. *Multimedia Tools and Applications, 83*(24), 64663-64682. [CrossRef]

[32] Olaniyi, O. M., Folorunso, T. A., Ahmed, A., & Joseph, O. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. *International Journal of Information Engineering and Electronic Business, 8*(5), 9–17.

[33] Konnurmath, G., & Yakkundimath, R. (2017). A combined approach of biometrics and watermarking for digital image's copyright protection. In *2017 2nd National Conference on Challenges and Opportunities in Computer Engineering (NCCOCE)*.

[34] Lebcir, M., Awang, S., & Benziane, A. (2020, February). Reversible Watermarking Technique for Fingerprint authentication based on DCT. In *IOP Conference Series: Materials Science and Engineering* (Vol. 769, No. 1, p. 012070). IOP Publishing. [CrossRef]

[35] Aparna, P., & V. V. Kishore, P. (2020). A blind medical image watermarking for secure E-healthcare application using crypto-watermarking system. *Journal of Intelligent Systems, 29*(1), 1558–1575. [CrossRef]

[36] Thanki, R., Borra, S., & Kothari, A. (2021). Fragile watermarking framework for tamper detection of color biometric images. *International Journal of Digital Crime and Forensics (IJDCF), 13*(2), 35-56. [CrossRef]

[37] Fernandez, J. J., & Nithyanandam, P. (2023). Biometric watermarking: an application-based review. *International Journal of Information Privacy, Security and Integrity, 5*(3), 211-226. [CrossRef]

[38] Ma, B., Wang, Y., Li, C., Zhang, Z., & Huang, D. (2014). Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking. *Multimedia Tools and Applications, 72*(1), 637–666. [CrossRef]

[39] Anand, A., & Singh, A. K. (2021). Watermarking techniques for medical data authentication: A survey. *Multimedia Tools and Applications, 80*(20), 30165–30197. [CrossRef]

[40] Kadian, P., Arora, S. M., & Arora, N. (2021). Robust digital watermarking techniques for copyright protection of digital data: A survey. *Wireless Personal Communications, 118*(4), 3225–3249. [CrossRef]

[41] Sharma, S., Zou, J. J., Fang, G., Shukla, P., & Cai, W. (2024). A review of image watermarking for identity protection and verification. *Multimedia Tools and Applications, 83*(11), 31829-31891. [CrossRef]

[42] Ergünay, S. K., Khoury, E., Lazaridis, A., & Marcel, S. (2015). On the vulnerability of speaker verification

to realistic voice spoofing. In *2015 IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS)* (pp. 1–6). [CrossRef]

[43] Evans, N. W., Kinnunen, T., & Yamagishi, J. (2013, August). Spoofing and countermeasures for automatic speaker verification. In *INTERSPEECH 2013, 14th Annual Conference of the International Speech Communication Association*.

[44] Evans, N. (Ed.). (2019). *Handbook of biometric anti-spoofing: Presentation attack detection* (2nd ed.). Springer.

[45] Vaidya, S. P. (2023). Fingerprint-based robust medical image watermarking in hybrid transform. *The Visual Computer, 39*(6), 2245-2260. [CrossRef]

[46] Moad, M. S., Kafi, M. R., & Khaldi, A. (2022). Medical image watermarking for secure e-healthcare applications. *Multimedia Tools and Applications, 81*(30), 44087-44107. [CrossRef]

[47] Thanki, R., & Borisagar, K. (2013). A novel robust digital watermarking technique using compressive sensing for biometric data protection. *International Journal of Electronics, Communication and Computer Engineering, 4*(4), 1133–1139.

[48] Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: A systematic review. *Multimedia Tools and Applications, 81*(18), 25101–25145. [CrossRef]

[49] North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. *Journal of Business Ethics, 167*(3), 433-450. [CrossRef]

[50] Yasmeen, F., & Uddin, M. S. (2021). An efficient watermarking approach based on LL and HH edges of DWT–SVD. *SN Computer Science, 2*(2), 82. [CrossRef]

[51] Agilandeeswari, L., Prabukumar, M., & Alenizi, F. A. (2023). A robust semi-fragile watermarking system using pseudo-Zernike moments and dual tree complex wavelet transform for social media content authentication. *Multimedia Tools and Applications, 82*(28), 43367–43419. [CrossRef]

[52] Hajiabbasi, M., Akhtarkavan, E., & Majidi, B. (2023). Cyber-physical customer management for Internet of Robotic Things-enabled banking. *IEEE Access, 11*, 34062–34079. [CrossRef]

[53] Joyce, S., & Veni, S. (2023). Iris biometric watermarking for authentication using multiband discrete wavelet transform and singular-value decomposition. *International Journal of Electrical and Computer Engineering Systems, 14*(3), 259–266. [CrossRef]

[54] Harika, D., & Noorullah, S. (2023). Implementation of image authentication using digital watermarking with biometric. *International Journal of Engineering Technology and Management Sciences, 7*(1), 154–167.

[55] Kumar, S., & Singh, B. K. (2021). DWT based color image watermarking using maximum entropy. *Multimedia Tools and Applications, 80*(10), 15487–15510. [CrossRef]

[56] Mohammed, N. F., Jawad, M. J., & Ali, S. A. (2020). Biometric-based medical watermarking system for verifying privacy and source authentication. *Kuwait Journal of Science, 47*(3), 1–12.

[57] Sanivarapu, P. V., Rajesh, K. N. V. P. S., Hosny, K. M., & Fouda, M. M. (2022). Digital watermarking system for copyright protection and authentication of images using cryptographic techniques. *Applied Sciences, 12*(17), 8724. [CrossRef]

[58] Qin, Y., & Zhang, B. (2023). Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal. *Applied Sciences, 13*(14), 8117. [CrossRef]

[59] Li, H., Yu, C., & Wang, X. (2021). A novel 1D chaotic system for image encryption, authentication and compression in cloud. *Multimedia Tools and Applications, 80*(6), 8721–8758. [CrossRef]

[60] Chen, Y. P., Fan, T. Y., & Chao, H. C. (2021). WMNet: A lossless watermarking technique using deep learning for medical image authentication. *Electronics, 10*(8), 932. [CrossRef]

[61] Vakhshiteh, F., Nickabadi, A., & Ramachandra, R. (2021). Adversarial attacks against face recognition: A comprehensive study. *IEEE Access, 9*, 92735–92756. [CrossRef]

[62] Priya, S., & Santhi, B. (2021). A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. *Mobile Networks and Applications, 26*(6), 2501–2508. [CrossRef]

Mahbuba Begum completed her Doctor of Philosophy, Master of Science (M.S.) and Bachelor of Science (B.Sc.) Honors in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh. Cuurently, she is working at Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh as the position of "Associate Professor". She earned her Ph.D. degree on Image watermarking entitled "Image Authentication through Watermarking Techniques" at the Department of Computer Science and Engineering, Jahangirnagar University in 2023. Her research is based on Image security. She has published a total no. of ten (10) research papers on image security. Most of her published Journals are indexed in Scopus and ESCI or SCIE (Web of Science). (Email: mahbubacse@mbstu.ac.bd)

Fauzia Yasmeen completed her Doctor of Philosophy (Ph.D.) from Bangladesh University of Professionals (BUP) and her Master of Science (M.S.) and Bachelor of Science (B.Sc.) (Honors) degrees in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh. She is currently working as an Associate Professor in the Department of Computer Science and Engineering at Fareast International University, Dhaka, Bangladesh. She has published numerous research papers on image security, many of which are indexed in Scopus and ESCI/SCIE (Web of Science). (Email: fauzia328@yahoo.com)

Mohammad Shorif Uddin received his PhD in Engineering from the Kyoto Institute of Technology, Japan, in 2002; an MEd in Technology Education from Shiga University, Japan, in 1999; a BSc in Electrical and Electronic Engineering from BUET, Bangladesh, in 1991; and an MBA in Marketing from Jahangirnagar University in 2013. He began his academic career at the Bangladesh Institute of Technology, Chittagong (now CUET), in 1991 and joined the Department of Computer Science and Engineering at Jahangirnagar University in 1992, where he is currently a Professor. His research interests include Computer Vision, Agro-Biomedical Imaging, Image Security, Artificial Intelligence, Machine Learning, and the Internet of Things (IoT). He has published over 250 research papers, holds two patents, and serves as an Associate Editor of IEEE Access. His invention of the "Electronic Eye" for the visually impaired received international recognition from CNN, BBC, and other global media outlets. Prof. Uddin is a Fellow of IEB and BCS, a Senior Member of IEEE, and currently serves as the Vice Chancellor of Green University of Bangladesh. (Email: shorifuddin@juniv.edu)

Jannatul Ferdush is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Jashore University of Science and Technology, Jashore, Bangladesh. Her research interests include natural language processing and image security. (Email: jannatulferdush@just.edu.bd)

Sumaita Binte Shorif received her BSc (Hons.) degree in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh. She has a strong enthusiasm for research, competitive programming, graphic design, digital art, and social media, complemented by excellent communication and leadership skills. She is currently pursuing her PhD in Software Engineering Analytics at Wayne State University, USA. (Email: sumaita.bs@gmail.com)

Taminul Islam completed his B.Sc. (Engg.) degree in Computer Science and Engineering from Daffodil International University, Dhaka, Bangladesh. His research interests include natural language processing and image security. (Email: islamtaminul@gmail.com)

Anjuman Naher Jui is currently working in the Department of Computer Science and Engineering at the University of Science and Technology Chittagong, Chattogram-4202, Bangladesh. Her research interests include natural language processing and image security. (Email: anjumannaher109@gmail.com)

Md. Marufur Rahman completed his B.Sc. (Hons.) degree in Mathematics from the University of Dhaka, Dhaka, Bangladesh. He is currently working as a Lecturer in the Department of Computer Science and Engineering at Dhaka International University, Dhaka, Bangladesh. His research interests include natural language processing and image security. (Email: marufrahman147@gmail.com)