Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047870

REVIEW

A Comprehensive Survey for Privacy-Preserving Biometrics: Recent Approaches, Challenges, and Future Directions

Shahriar Md Arman[1], Tao Yang[1,*], Shahadat Shahed[2], Alanoud Al Mazroa[3], Afraa Attiah[4] and Linda Mohaisen[4]

[1]School of Computer Science and Technology, Zhejiang Gongshang University, Hangzhou, 310018, China

[2]School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, 310018, China

[3]College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 84428, Saudi Arabia

[4]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia

*Corresponding Author: Tao Yang. Email: yangt@zjgsu.edu.cn

Received: 20 November 2023 Accepted: 26 December 2023 Published: 27 February 2024

ABSTRACT

The rapid growth of smart technologies and services has intensified the challenges surrounding identity authentication techniques. Biometric credentials are increasingly being used for verification due to their advantages over traditional methods, making it crucial to safeguard the privacy of people's biometric data in various scenarios. This paper offers an in-depth exploration for privacy-preserving techniques and potential threats to biometric systems. It proposes a noble and thorough taxonomy survey for privacy-preserving techniques, as well as a systematic framework for categorizing the field's existing literature. We review the state-of-the-art methods and address their advantages and limitations in the context of various biometric modalities, such as face, fingerprint, and eye detection. The survey encompasses various categories of privacy-preserving mechanisms and examines the trade-offs between security, privacy, and recognition performance, as well as the issues and future research directions. It aims to provide researchers, professionals, and decision-makers with a thorough understanding of the existing privacy-preserving solutions in biometric recognition systems and serves as the foundation of the development of more secure and privacy-preserving biometric technologies.

KEYWORDS

Biometric modalities; biometric recognition; biometric security; privacy-preserving; security threats

1 Introduction

The science of identifying people based on their physical, behavioral, and physiological attributes, such as the face, voice, iris, gait, and fingerprints, is known as biometrics [1]. Biometrics offers enhanced assurance by verifying an individual's identity through a unique, tangible trait. They are useful for authentication due to their biometric features, which prevent them from being lost or stolen like tokens and from being forgotten like passwords or pins. However, most users' passwords, PINs, and personal identifying information are susceptible to data breaches, allowing hackers to access billions of accounts [2] and compromise traditional authentication methods [3]. With its speed,

accuracy, and user-friendliness, biometrics is a valuable tool for mitigating cryptography's inherent security vulnerabilities by effectively identifying genuine users. Equipped with sensors like iris or fingerprint scans, biometrics is an efficient and reliable solution in access control systems, offering robust authentication [4]. Using a classical biometric authentication tool, physiological and behavioral biometric parameters are collected, and distinguishing traits are extracted to create a biometric template during enrollment. The system processes a different biometric input during verification or identification and compares it to the stored template to determine acceptance or rejection [5].

Biometric authentication systems offer usability benefits but are vulnerable to threats due to their fuzziness. Traditional encryption cannot protect biometrics due to their complexities. The ramifications of successful attacks in biometric systems can be profound, adversely impacting users' lives and breaching their privacy. Unlike traditional credentials, biometric information cannot be kept secret or concealed; in the event of theft, compromised biometrics are not easily revocable [6]. Biometric templates carry a significant risk of compromise, including capture, cloning, or forgery, which can result in identity theft or individual profiling. This risk is amplified when biometrics are used across multiple databases. Stolen biometrics can potentially expose sensitive information about individuals, such as their ethnic groups and genetic characteristics [7] and medical conditions [8], or even engage in unlawful activity by compromising medical records [9]. Given the risks associated with biometric data, it is crucial to develop procedures that ensure both the efficiency of authentication systems and the privacy of biometric information. An effective biometric protection strategy should be irreversible, making it computationally infeasible to reconstruct the original biometric data from encrypted templates [10].

This paper delves into an extensive exploration of privacy-preserving techniques to protect biometrics data and the potential threats to biometric systems. It introduces a novel and comprehensive taxonomy of privacy-preserving techniques, offering a structured framework for classifying the existing literature in this domain. A thorough review of state-of-the-art methods is presented, accompanied by an analysis of their security, performance, use cases, limitations, and advantages within various biometric modalities, including fingerprint, face, and iris recognition. The survey encompasses a wide range of privacy-preserving mechanisms, scrutinizes the trade-offs between security, privacy, and recognition performance, and addresses pertinent issues while outlining future research directions. This study aims to equip researchers, professionals, and decision-makers with a complete understanding of the existing privacy-preserving solutions in biometric recognition systems, thus laying the foundation for developing more secure and privacy-enhanced biometric technologies.

This paper is organized in a structured manner to provide an extensive exploration of the topic. The following section offers a concise overview of the different biometric modalities employed in authentication systems. Section 3 focuses on classifying major security concerns associated with biometric authentication systems. This section highlights the vulnerabilities and potential threats that must be addressed to ensure robust security in such scenarios. Section 4 is dedicated to the categorization of privacy-preserving techniques. It offers a detailed analysis of various approaches and strategies employed to protect the privacy of individuals in biometric authentication systems. This section provides valuable insights into the different privacy-preserving mechanisms available. Section 5 serves as a significant section, encompassing an overall summary of the findings, a discussion on open research problems, and an exploration of future work in the field. This section consolidates the main points and identifies areas for further investigation, offering a comprehensive view of the current state of research. Section 6 brings the paper to a close, summarizing the key findings and highlighting the significance of the study conducted.

2 Biometric Modalities

A biometric modality is any biometric information that can be used to distinguish individuals. A biometric modality is a specific category within a biometric system, determined by the kind of human characteristic it processes [11]. The majority of biometric data is statistical. More sample information increases the likelihood of a distinct and dependable system. It can measure a person's physical features and behavioral tendencies utilizing a variety of modalities. Some biometric modalities last longer and are more challenging to show and collect. Some are more susceptible to environmental variables that lower sample signal-to-noise ratio and performance. An ideal biometric data set has the following characteristics shown in Table 1.

Table 1: Ideal biometric data characteristics

Characteristics	Description
Uniqueness	Contains unique biometric data for each individual, making it difficult to forge or counterfeit.
Permanency	Maintains relatively unchanged biometric data over time, preventing it from being quickly impacted by aging, injury, or disease.
Collectability	High quality, ensuring reliable data collection, meticulous error review, proper labeling, and organization.
Accuracy	Precisely as possible, requiring reliable data collection and meticulous review for errors.
Universality	Includes biometric data from all individuals, not just specific groups like those with disabilities or geographical locations.
Diversity	Encompassing biometric data from individuals of all ages, genders, races, ethnicities, and locations ensures accurate biometric recognition.
Volume	An extensive database is crucial for training biometric recognition algorithms, ensuring accurate recognition across various conditions.

Ideal biometric features should be universally present, uniquely identifiable, remain constant over time, be secure against spoofing, be affordable, socially acceptable, respect privacy, and be scalable for large-scale deployments. Different features prioritize different aspects, with fingerprints and iris patterns excelling in universality and uniqueness, while facial features and voice offer better cost and social acceptance. These characteristics have varying strengths and weaknesses, and choosing the ideal option depends on the specific application and its priorities [12]. The human characteristics that can serve as biometric modalities encompass a diverse range. As illustrated in Fig. 1, these modalities are commonly referenced in research and commercial applications and can be broadly classified into two groups: (1) Behavioral biometrics and (2) Physical biometrics.

2.1 Behavioral Biometrics

Behavioral biometrics focuses on the patterns of human actions, typically represented as time sequences. This is distinct from physical biometrics, which centers on inherent human features like fingerprints or the iris. Behavioral biometrics evolves with changes in an individual's behavior over time. Common examples include keystroke patterns, walking rhythms, cognitive patterns, and handwriting dynamics. The biometric field also considers other behavioral aspects such as hand grip strength, lip movements, mouse dynamics, multi-touch gestures on mobile devices, facial expressions

like smiling, brain wave patterns (EEG), vocal nuances, online social behaviors, driving habits, and emotional responses. Behavioral biometrics offers a robust defense against fraudulent activities by focusing on a user's digital interactions and cognitive patterns. Instead of relying solely on static data or physical attributes, it evaluates online behaviors to ascertain a user's identity. By leveraging machine learning, behavioral biometrics can discern patterns in human actions, verifying if an online user is genuine or if the activity is potentially a cyber threat.

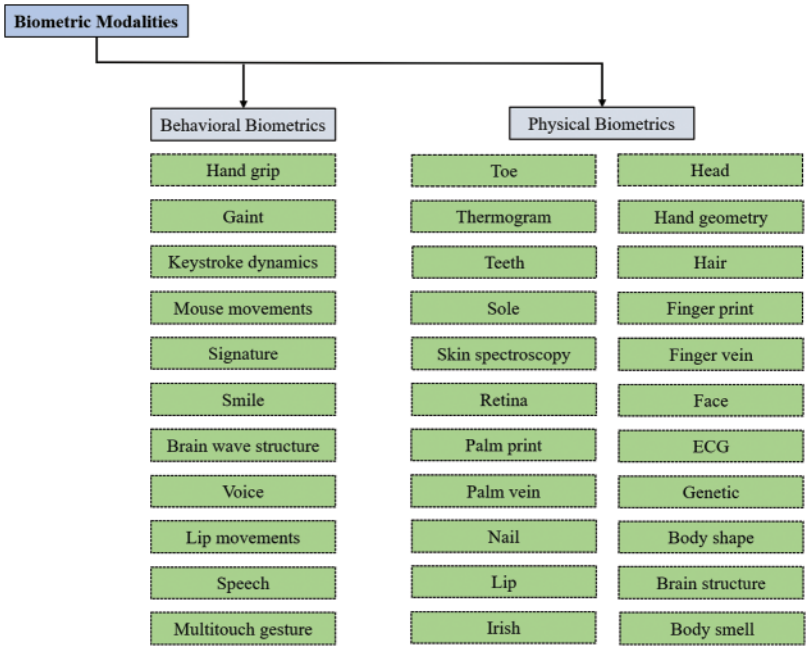

Figure 1: Various biometric modalities used for authentication and research purposes

2.2 Physical Biometrics

Physical biometrics focuses on the inherent physical attributes of an individual. These characteristics, related to the form and structure of the body, typically remain consistent throughout a person's life. However, capturing these traits can be influenced by various external elements, such as the pressure applied to the scanning device, the cleanliness of the scanning surface, and prevailing environmental conditions. Commonly recognized physical biometrics encompass facial features, fingerprints, iris patterns, palm prints, hand geometry, and overall body contour. Research has also delved into other unique identifiers like body scent, brain formations, ear configurations, electrocardiogram (ECG) patterns, genetic markers, hair patterns, head shape, specific imaging of body sections, lip formations, nail characteristics, inner ear sounds, retinal patterns, vascular patterns in hands and fingers, skin properties, footprints, sweat gland patterns, dental structures, thermal images, and toe configurations.

3 Biometrics Security Threats

Biometrics' parameters, potential errors, scenarios, characteristics, system constraints, and modern approaches must be understood to improve or refine existing systems. No biometric system is flawless, and there's a continuous pursuit to boost its precision and efficiency. Despite their uniqueness, biometrics cannot be reset or changed once hacked, making them vulnerable. A biometric data breach

has two effects. First, stolen data might be misused maliciously. Secondly, unlike passwords, biometrics are immutable, making them irreplaceable once compromised. Malicious attacks can compromise biometric security and performance. Issues like spoofing, sensor inaccuracies, variations within classes, and similarities between classes pose challenges. Comprehensive analysis and preventative measures must be implemented into biometric system design for high-risk threats. Table 2 details biometric system risks to present a wide view of biometric security challenges. Privacy-preserving approaches cannot mitigate all of these dangers, although current research protects biometrics from most of them, as mentioned in the next section.

Table 2: Most widely concerned biometric security threats

Threat	Description	Impact	Mitigation strategies
Spoofing/Presentation attacks [13]	Fake biometric sample presentation to the system, such as a fingerprint mold, facial mask, or voice recording.	Unauthorized access to the system.	Multi-factor authentication, implement Anti-spoofing measures, liveness detection, artificial intelligence (AI)-based spoofing detection
Replay attacks [14]	Replaying a previously captured biometric sample to the system.	Illegal access to the system.	Secure communication, session-based tokens, strong encryption
Biometric data theft [15]	Misuse of stored biometric information and unauthorized access to it.	The ability to impersonate the user.	Data encryption, secure storage
Template aging [16]	Changes in biometric traits over time can lead to incorrect matches.	System failure, Interrupt the regular use of the system.	Regular template updating, robust algorithm implementation
Malware attacks [17]	Used to infect the biometric system and steal biometric data or disrupt the system's operation.	Physical/remote access to the system.	Regular system updates, anti-malware software

(Continued)

Table 2 (continued)

Threat	Description	Impact	Mitigation strategies
Privacy invasion [18]	Collecting, using, or disclosing biometric data without the individual's consent.	Physical/remote access to the biometric database.	Strict privacy policies obtain consent from individuals before collecting, using, or disclosing their biometric data
Deepfakes and AI-enhanced spoofing [19]	Exploit the capabilities of deep learning and AI to create realistic fake biometric samples.	Ability to acquire user biometric data or access the biometric system remotely.	AI-based deep fake detection, liveness detection, and anti-spoofing measures
Biometric data breaches [20]	Breaches of the biometric database can lead to the theft of biometric data, which can be used for malicious purposes.	Remote access to the database.	Secure and encrypted data storage, Intrusion detection systems, safe access control
Cross-device variability [21]	Biometric templates collected from different devices may vary, leading to false rejects.	Interrupt the regular use of the system.	Standardization, multi-modal biometrics, robust algorithm for cross-device variability
Physical harm/Coercion [22]	Attackers may use physical harm or coercion to force a user to reveal their biometric data.	Physical access to the user.	Duress detection mechanisms, security guards, and training on resisting attacks.
Function creep [23]	The use of biometric data for purposes other than those for which it was initially collected.	Physical/remote access to the biometric system	Strict data use policies, regulatory oversight
Phishing [24]	Used to trick users into revealing their biometric data or login credentials.	Physical/remote access to the user.	Implement security awareness training for users to help them identify and avoid phishing attacks.

4 Privacy-Preserving Technologies

Privacy-preserving biometric recognition technologies aim to protect an individual's data while allowing for accurate and efficient identity verification. These technologies are essential for ensuring that biometric data is not misused or compromised. This section offers a new viewpoint on classifying privacy-preserving biometric technologies. In this section, we have categorized privacy-preserving techniques into specific groups, as outlined in Fig. 2.

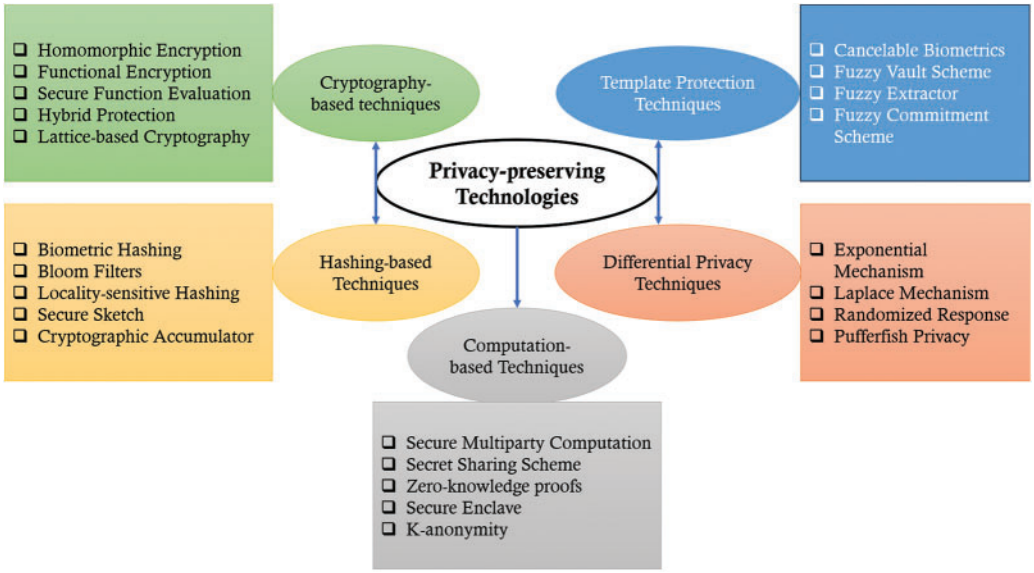

Figure 2: Categorization of privacy-preserving technologies

4.1 Cryptography-Based Techniques

4.1.1 Homomorphic Encryption

Homomorphic Encryption (HE) is a transformative technique that allows data to be encrypted into a form that can still be processed and analyzed as if it remained in its original state. This unique capability ensures that encrypted data can undergo complex mathematical operations without ever being decrypted, making it particularly valuable for preserving privacy in biometric authentication. The idea of homomorphic encryption was first proposed by Rivest et al. [25], and in 2009, Gentry [26] introduced a practical yet computationally intensive HE framework. Fully Homomorphic Encryption (FHE), Partially Homomorphic Encryption, and Somewhat Homomorphic Encryption are three standard HE-based biometric encryption algorithms. Chandrasekhar et al. [27] proposed a methodology using HE for secure facial authentication and data protection in cloud computing by generating facial keys for encryption. They used facial templates for authorization and authentication and compared facial keys with templates of face data for encryption. Chitrapu et al. [28] assessed the feasibility of safeguarding an iris template database using FHE. They also provided an extensive overview of biometric authentication through FHE, detailing HE-compliant algorithms and biometric template extraction methods. Numerous studies have assessed HE methods' robustness to side-channel, fault, and chosen-plaintext assaults. The results reveal that HE-based methods can compute biometric templates accurately and attack resistance. HE encryption promises to improve biometric privacy and security, but additional research is needed to address latency, restrictions, and new applications.

4.1.2 Functional Encryption

Functional encryption (FE) extends the concept of public-key encryption, allowing individuals with a specific secret key to access a particular function of the encrypted content. Amit Sahai and Brent Waters introduced the idea of functional encryption, which was then formalized by Boneh et al. in 2010 [29]. FE can be used to design secure systems that protect sensitive biometric information while enabling selective access based on specific functions or features. Ernst et al. proposed [30] a secure and privacy-preserving biometric-based two-factor authentication protocol in the Universal Composability framework. The protocol uses FE to compute the distance between encrypted biometric templates, achieving high security while protecting user privacy. They also presented an efficient instantiation of the protocol using inner-product functional encryption. Shahzad et al. [31] surveyed the applications of FE in the Internet of Things (IoT). They found that FE can provide fine-grained access control for IoT devices, protecting them from security vulnerabilities. They also identified research trends and open challenges in FE for IoT security. FE for biometrics is a potential encryption method, but it is necessary for rapid and safe biometric authentication procedures, robust and accurate feature extraction and representation, and standardized and interoperable biometric systems.

4.1.3 Secure Function Evaluation

Secure Function Evaluation (SFE) is another field of cryptography that focuses on crafting algorithms that empower parties who might not trust each other to compute functions on their respective inputs without compromising data privacy. SFE was initially introduced by Yao [32] and has been applied in various domains [33], including biometrics, which can be used to compare biometric templates securely or perform biometric identification. Oishi et al. [34] proposed an improved architecture for accelerating SFE using an Field-Programmable Gate Array (**FPGA**)-based GC accelerator. The architecture allows managers to perform multiple rows of pipeline processing simultaneously and optimizes RAM implementation. This results in a 26% performance improvement over the state-of-the-art garbling accelerator while protecting privacy. With the combination of different encryption techniques, various SFE algorithms have been proposed for biometric applications, including Garbled Circuit-based SFE [35] and Oblivious Transfer-based SFE [36]. Each method has unique strengths and challenges concerning efficiency, security, and scalability. Current research endeavors aim to refine SFE's efficiency, ensure its compatibility with prevailing biometric systems, and bolster its defense mechanisms. Addressing these challenges will pave the way for broader SFE adoption, enhancing the confidentiality and security of sensitive information.

4.1.4 Hybrid Protection

The Hybrid Protection technique combines cryptographic techniques that enhance biometric data protection in storage and transmission. The technique combines encryption and obfuscation to protect the biometric data against attacks. Bassit et al. [37] compared Bloom Filter (BF) and Homomorphic Encryption (HE) approaches for biometric template protection. The authors proposed a hybrid approach combining the benefits of both, achieving unlinkability, high accuracy, and seven times faster performance than traditional HE. Shahreza et al. [38] developed a hybrid scheme that merges cancelable biometrics with homomorphic encryption to protect biometric templates while optimizing computational efficiency. Their model, tested on state-of-the-art facial recognition models on MOBIO and LFW datasets, is open-source, inviting further enhancements. The Hybrid Protection technique has consistently demonstrated its superiority in protection and efficiency. Current research efforts aim to perfect this approach, particularly in developing domains like cloud computing.

4.1.5 Lattice-Based Cryptography

The lattice-based cryptography technique, first introduced by Ajtai [39], has shown promise in protecting biometric data. This approach transforms biometric templates into lattice points in cryptographic operations such as encryption, signature schemes, and secure multiparty computation. It offers several advantages for biometric data protection, including resistance to quantum attacks, efficient computation, and strong security guarantees. Fu et al. [40] studied lattice-based attribute-based encryption systems, focusing on expressiveness, complexity assumptions, efficiency, and security and identifying areas for further research in this field. Althobaiti et al. [41] proposed a new face-recognition cryptosystem that combines symmetric and asymmetric cryptography. The proposed system is lightweight and efficient, making it suitable for smart world applications and 6G networks. Lattice-based encryption is being investigated for biometric data security. Some approaches are computationally costly; thus, security and efficiency must be balanced. Lattice-based operations affect biometric matching algorithms, requiring additional design considerations. Key management and safe biometric data exchange may benefit from novel algorithms, constructions, and lattice-based methods.

4.2 Hashing-Based Techniques

4.2.1 Biometric Hashing

Biometrics Hashing (BH) converts biometric data, such as fingerprints or facial recognition, into a unique digital code that can be used for identification or authentication purposes [42]. Yu et al. [43] introduced a Secure BH technique against Relation-Based Attacks that optimizes dependent min-entropy to minimize distance relation leaking on source biometrics and offers improved security with equivalent or superior recognition performance. The technique reduces the Equal Error Rate on the face dataset LFW by 21% and has a low probability of successful white-box attacks. Yu et al. [44] developed anti-similarity-attack hashing for privacy-preserving biometric recognition, enhancing identification performance and security against similarity-based reconstruction attacks based on experiments on publicly available biometric datasets. Raja et al. [45] proposed a unique hashing strategy with semantic labels for biometric template security to avoid biometric data leakage and likability difficulties, which may be extended to individual subjects by employing auxiliary pseudo-user enrollment data. With experimental validation and security analysis, the proposed strategy achieves a high valid match rate and a nearly equal error rate and meets the additional requirements of biometric template safety. BH has the potential to protect biometric data storage and validation, but it faces security vulnerabilities and performance issues. Building solid BH algorithms, studying multi-modal BH, and using blockchain for safe data storage should be future goals.

4.2.2 Bloom Filters

Bloom Filters (BF) are efficient structures for storing and retrieving large data sets that were first introduced by Bloom [46]. They have been studied for enhancing the privacy and security of biometric templates. Bansal et al. [47] introduced a scheme that uses format-preserving encryption and BF to protect biometric templates. It achieves high recognition performance and security for uni-biometric and multi-biometric datasets. Zhou et al. [48] proposed a new BF-based biometric template protection scheme that addresses the linkability issue of the original scheme. The new scheme achieves high recognition accuracy while resisting reverse reconstruction attacks. BF-based biometric methods can improve template security and privacy, but they have drawbacks. Biometric data fluctuation, false positives, and data collisions are potential difficulties. Such systems may require specific equipment and experience to deploy and maintain, and overcoming these problems is essential for practical use.

4.2.3 Locality-Sensitive Hashing

Locality-Sensitive Hashing (LSH) is a method designed to identify approximate nearest neighbors within vast, high-dimensional spaces. It was first proposed by Indyk et al. [49]. This technique benefits biometrics, where data like fingerprints or facial scans must be swiftly compared to a comprehensive database. The essence of LSH is to transform high-dimensional data into more manageable hash codes, ensuring that similar data points likely end up with identical or closely related hash codes. Alshahrani et al. [50] proposed an efficient LSH-based approach for face image retrieval using facial soft biometrics. Their Soft BioHash method outperforms the Hard BioHash approach regarding accuracy and retrieval speed on the LFW database. Mashnoor et al. [51] proposed a novel method for network traffic fingerprinting based on LSH. Their proposed method achieves 12% higher accuracy compared to state-of-the-art ML-based approaches. The biometric applications of LSH are promising, yet obstacles remain. These include balancing security and performance, processing high-dimensional data, and understanding biometric modalities. LSH research might focus on multi-modal biometrics, continuous authentication, and privacy-centric biometric systems. Combining LSH with other new methods can improve biometric system accuracy and security.

4.2.4 Secure Sketch

Secure Sketch (SS) is a cryptographic method designed to compute set operations like intersection, union, or difference between two parties' inputs without compromising privacy. A sketch is a randomized, fixed-length representation of biometric data generated by a one-way function. Encrypting this sketch with a secret key makes it secure enough to save or communicate without revealing the contents. SS in biometric systems increases storage and transmission security, allows data revocation without system disruptions, and protects privacy when sharing or researching biometric data. Jiang et al. [52] presented a face-based authentication system with a computational SS for biometric privacy protection. The computational SS ensures error tolerance on face samplings and guarantees the privacy of face features by preventing public information obtained by an adversary from affecting the pseudo-randomness of the authentication key. SS maintains biometric data, but accuracy and security are issues. Future directions are exploring machine learning, integrating with other biometric systems, and building high-dimensional and multi-modal data structures.

4.2.5 Cryptographic Accumulator

Cryptographic Accumulator (CA) methods, first introduced by Benaloh et al. [53], offer a promising way of safeguarding biometric information. Biometric templates are converted into a single value using a one-way function. The user's biometric input is transformed into this cumulative value and matched with the stored value to verify authentication. The advantage is that the accumulated value is kept, hiding the original biometric data. A comprehensive summary of CA was provided by Ren et al. [54], including descriptions, characteristics, types, and security assumptions. Their research examined the use of CA in many different contexts, including ring signatures, group signatures, encrypted data search, anonymous credentials, and cryptographic promise. CA's biometric data protection method is clever but flawed. Cumulative value vulnerability is a significant risk. The system could be compromised by reverse-engineering or using this value's biometric data. Thus, protecting this value is vital. CA's computational needs, especially with massive biometric information, require more efficient, secure methods. CA can be studied in secure multiparty computation, blockchain, or machine learning to increase efficiency and security. Using CA with other biometrics could improve security.

4.3 Template Protection Techniques

4.3.1 Cancelable Biometrics

Cancelable Biometrics (CB) safeguards biometric data by creating multiple transformed versions of the original template. Biometric data is transformed during authentication, creating a template matched against stored ones, guaranteeing user privacy by making reconstruction difficult even if an attacker acquires the templates. Kauba et al. [55] explored three distinct strategies for creating cancelable templates from finger vein patterns, assessing their efficacy in recognition and renewability. Shahreza et al. [56] benchmarked several CB schemes, including MLP Hashing, BioHashing, Bloom Filters, and two IoM-based strategies, and introduced a user-specific random transformation-based baseline scheme. Their evaluation considers unlikability, irreversibility, and recognition performance on deep learning-based templates extracted from various biometric characteristics, with an open-source implementation provided for reproducibility. Recent CB difficulties include balancing security and performance, template changes, security assaults, usability, and user acceptance. Bernal-Romero et al. [57] examined potential vulnerabilities in biometric authentication and proposed hardware and software solutions to bolster biometric data security. Future research should examine multi-modal systems, adaptive mechanisms, machine learning integrations, standardization, and blockchain synergies to promote CB adoption across industries.

4.3.2 Fuzzy Vault Scheme

The revolutionary Fuzzy Vault Scheme (FVS) uses biometric authentication to secure cryptographic systems. This approach encodes a key as a polynomial whose coefficients form curve points. A "fuzzy" key is created by slightly altering these positions. This changed version underpins cryptographic applications like digital signatures and encryption. One must fix these altered spots using particular error-correcting methods to recover the key. Kaur et al. [58] unveiled a cutting-edge SURF-based Biometric Cryptosystem method. This method integrates the FVS for data protection, and the SURF technique for biometric verification has demonstrated superior performance metrics across various benchmarks. The extended fuzzy vault strategy used to protect face feature vectors created using deep convolutional neural networks for biometric data was examined in a recent paper by Rathgeb et al. [59]. The proposed feature translation technique and template protection strategy protect facial reference data and digital keys, providing excellent security. Abiega-L'Eglisse et al. [60] created a fuzzy vault biometric system without chaff points or polynomial degrees that uses cryptography to prevent brute-force attacks. Firmly without passwords or hybrid systems, the system is secure for the present and future. Song et al. [61] presented a multi-secret sharing FVS to solve identity authentication's computational complexity and communication inefficiency. The strategy improves authentication efficiency by splitting the main secret into multiple sub-secret values and using RS code multi-secret sharing decoding. Future research could address FV's needs for more effective and scalable systems, deep learning integration, multi-modal biometrics, adversarial attacks, and practical deployment in real-world scenarios to improve FV for biometrics.

4.3.3 Fuzzy Extractor

The Fuzzy Extractor (FE) approach utilizes biometric data for enhanced digital security, securely storing and comparing data and generating a secret key for encryption. Zhang et al. [62] proposed a biometric-based authentication and key agreement scheme for WBANs. Their method utilizes a fuzzy extractor for anonymous identity authentication, a privacy-preserving key agreement algorithm, and a blockchain for secure storage of biometric data. Sathish et al. [63] presented a novel method for

secure cloud data access using biometric authentication with Particle Swarm Optimization. Their approach utilizes a three-level security mechanism and Adaptive ElGamal encryption to prevent data loss and unauthorized access. FE faces obstacles and unexplored areas despite substantial research. Standardized practices, privacy, and ethical issues, resilience against threats, efficiency for large-scale biometric endeavors, synergizing with deep learning methodologies, enhancing multi-factor authentication, post-quantum security, and real-world application testing are needed.

4.3.4 Fuzzy Commitment Scheme

The Fuzzy Commitment Mechanism (FCS) introduced by Juels et al. [64] is a biometric cryptosystem that uses cryptography and error correction codes to provide secure biometric recognition. User biometric data is converted into a "fuzzy commitment" and stored on a server. A new biometric sample can be submitted to validate identity. Chang et al. [65] proposed a user-specific random padding scheme to enhance the security of fuzzy commitment biometric template protection techniques by eliminating impersonation attacks. The scheme demonstrated enhanced recognition performance and a 2k attack complexity, where k is the secret message length. Another improved FCS was presented by Chauhan et al. [66] for template protection of biometric data, which uses multiple keys to increase security. Their scheme demonstrated superior security to the traditional FCS. Bajaber et al. [67] created an alternative FCS for touch-gesture templates in a touch authentication system that is deep learning-based. The technique demonstrated its effectiveness in dynamic authentication systems using a binary Bose-Ray-Chaudhuri code with adjustable vital lengths. Wu et al. [68] proposed a palmprint FCS based on a deep hashing network-generated discriminative deep hashing code. The recommended FCS balances accuracy, storage expense, and computational complexity to produce a low EER of 0.0001%. FCS offers secure biometric recognition for access control, financial transactions, and healthcare. Standardization, privacy, and attack resilience require more research and real-world testing.

4.4 Computation-Based Techniques

4.4.1 Secure Multiparty Computation

Secure Multiparty Computation (SMC) is a cryptographic approach that lets many parties compute a function over their inputs without sharing them, first proposed by Yao [32]. It protects data privacy even during computing, making it useful in collaborative situations. SMC's ability to protect biometric data makes it popular in authentication, identification, and access control. Li et al. [69] explored SMC by devising a protocol to compute the least common multiple using Shor's quantum period-finding algorithm. Their work underscored the potential of quantum computation in enhancing the efficiency of secure multiparty computations. An SMC solution was introduced by Pentyala et al. [70] for training DP models that are more accurate than pure DP and provide privacy. The SMC technique faces challenges such as high computational complexity, communication costs, scalability limits, security assumptions dependency, and security vulnerabilities. In this lecture series [71], Choudhury et al. focused on passively secure SMC protocols, which address eavesdropping adversaries during protocol execution. It covers theoretical results, security proofs, and efficiency enhancement techniques. With other privacy-enhancing technologies, SMC can improve privacy with minimal computational overhead. Real-world deployment studies are needed to evaluate usability, efficacy, and efficiency in finance, healthcare, and social media.

4.4.2 Secret Sharing Scheme

Secret Sharing (SS) is a cornerstone in cryptography, primarily designed to protect cryptographic keys. The essence of SS lies in dividing a secret into multiple fragments, known as shares or shadows. These fragments are distributed among users, and only a subset can reconstruct the original secret collaboratively. Francis et al. [72] conducted an in-depth analysis of contemporary SS techniques. Their study also introduced an enhanced threshold scheme to address challenges like cheating detection and cheater identification. Chandramouli et al. [73] surveyed existing perfectly secure Verifiable SS schemes that tolerate computationally unbounded adversaries in three transmission environments: synchronous, asynchronous, and hybrid. Their survey gave scholars interested in advancing the state-of-the-art with a complete grasp of various methods. Li et al. [74] proposed a dynamic quantum SS system that enables sharing of multiple secrets while resisting attacks like collusion and revoked participant attacks. The system uses a one-to-one relationship between shadows and hash values for participant honesty. Due to quantum computing and privacy concerns, standard systems may become unfeasible as participants rise. Designing algorithms for huge numbers without overhead, studying cryptographic approaches to withstand quantum attacks, and adding zero-knowledge proof for privacy are future research priorities.

4.4.3 Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKP), introduced by Goldwasser et al. [75], offer a unique cryptographic method where a prover can validate a statement's truth without revealing any information beyond its veracity. This approach is pivotal for maintaining privacy and security across various digital platforms. Gaba et al. [76] developed an Authenticated Key Agreement protocol based on ZKP for Internet of Healthcare applications to assure confidentiality, anonymity, and security against cyber threats. Their protocol achieves its goals with minimum computing, storage, and transmission costs by utilizing ZKP, physically unclonable functions, biometrics, symmetric cryptography, and message digest. A new method presented by Carney [77] for quantum identity authentication protocols by applying the logic of classical ZKPs to quantum circuits and algorithms. This method wraps a secret in a quantum state. It delivers it to the verifier over a quantum channel, making the protocol resistant to eavesdropping or manipulation and potentially valuable for a future "quantum Internet." Chen et al. [78] provided an overview of privacy-preserving IoT architecture, ZKP authentication methods, and their benefits while highlighting potential challenges and future possibilities. ZKP improves privacy and security but faces complexity, scalability, standards, and adoption. Future ZKP innovations should improve efficiency, applications, standards, education, and awareness.

4.4.4 Secure Enclave

Secure Enclave (SE) is a technique for securing biometric data and protecting it from unauthorized access. The technique involves using a hardware-based security feature, such as Intel SGX, to create a secure environment within a device or server. Biometric data, such as fingerprints or facial recognition, is stored within the SE, which can only be accessed by authorized applications or users. Gu et al. [79] introduced UniTEE, a ground-breaking programming abstraction that simplifies SE migration between several trusted execution environments technologies, including Intel SGX, AMD SEV, and ARM TrustZone. Their design, rooted in microkernel architecture, offers a consistent programming model and showcases efficient migration with minimal overhead. Privacy-preserving computation SE in biometrics struggles to secure data even on compromised devices or servers. Attackers may evade the SE or steal data, causing data breaches and identity theft. The SE's success depends on biometric data quality and confidentiality. Open-source SE libraries, cloud-based SE

services, and layered security can minimize the cost and time of good encryption. Building effective enclave data encryption and decryption techniques, analyzing SE usage, and developing SE-based biometric data-sharing solutions for several devices and platforms should be the focus of future research.

4.4.5 K-Anonymity

K-anonymity term, proposed by Samarati et al. [80], is a technique designed to protect individual privacy within biometric systems. It operates by modifying biometric data so that each individual's information blends in with at least K-1 others, ensuring that specific data cannot be traced back to a single person. Methods like randomization and perturbation can be employed to achieve k-anonymity. This approach has been applied across various biometric data types, from fingerprints to facial recognition. For instance, large biometric databases, like those maintained by the National Institute of Standards and Technology, have utilized k-anonymity to enhance user privacy. Mobile biometric systems, which gather and transmit data on handheld devices for remote verification, have also benefited from this method. Qian et al. [81] proposed a new k-anonymity technique called "multi-level personalized k-anonymity" that uses a dynamic k-value sequence to achieve personalized anonymization. It allows for greater flexibility and reduces information loss compared to the traditional k-anonymity approach. The authors also presented three practical algorithms to implement the proposed model. K-anonymity must balance privacy with recognition accuracy and securely store and transport biometric data.

4.5 Differential Privacy Techniques

4.5.1 Exponential Mechanism

The Exponential Mechanism (EM) proposed by McSherry et al. [82] is a popular differential privacy method that enables the selection of items from a database while maintaining user privacy. This method randomly selects database items based on their "privacy cost," which measures the information they share. Setting biometric data features less likely to reveal sensitive details protects privacy in biometrics. The EM can be used to choose face traits less likely to expose sensitive information like race or gender, eliminating discrimination and maintaining privacy while allowing facial recognition for identification. Gopi et al. [83] presented a modified EM for non-smooth convex optimization problems, attaining optimal empirical recovery and offering an implementation technique with a nearly matching lower bound on evaluation queries. Ramsay et al. [84] explored concentration inequalities for EM output in the population objective function, focusing on objective functions with modest regularity constraints. They developed finite-sample performance guarantees for depth-based multivariate medians. They numerically demonstrated their results using a Gaussian contamination model. EM is a powerful tool for differential privacy, but it struggles to balance privacy and usability. Future studies should improve process accuracy or utility while maintaining privacy. Given EM's processing expense, high-dimensional data is crucial. Practical algorithms for high-dimensional data and problem-specific processes can boost performance. Customizing mechanisms for different uses is essential.

4.5.2 Laplace Mechanism

The Laplace Mechanism (LM) adds random noise to statistical queries for sensitive data protection. Noise depends on query sensitivity and desired concealment. It is proportional to the query's sensitivity, which evaluates the output difference when a single individual's data is added or deleted.

A new noise addition mechanism was introduced by Muthukrishnan et al. [85] for differential privacy that samples noise from a hybrid density resembling Laplace and Gaussian distributions. Their simulations show that the proposed approach outperforms existing methods in privacy and accuracy. Ünsal et al. [86] explored recognizing adversaries by altering LM output, balancing privacy, sensitivity, and attacker advantage. They also developed a threshold for detecting attacks and applied Kullback-Leibler differential privacy to adversarial classification. LM is a popular data analysis, machine learning, and statistical inference method that calculates average values, scores, or frequency to safeguard individual data. It provides strong privacy protection against attacks, but noise might reduce data analysis accuracy and usability. Researchers must balance privacy, precision, and utility using the LM.

4.5.3 Randomized Response

Randomized Response (RR) is a privacy-enhancing technique introduced by Warner in 1965 [87] for structured survey interviews. It adds random noise to biometric data, making it difficult for attackers to determine the true biometric characteristic. Respondents use a coin flip to hide their responses and protect their anonymity. A random number generator adds a random bit to biometric data with an equal chance of being 0 or 1. An authentication system removes the random bit and matches the biometric data against a template. RR secures biometric data like fingerprints and facial recognition when authenticating. In the early stage of using this technique in the practical field, Blair et al. [88] examined and offered several designs and strategies for employing the RR method as a survey tool to eliminate bias and safeguard respondent privacy when questions regarding sensitive behaviors and beliefs were asked. Later, Chaudhuri et al. [89] gave a complete method for evaluating data relating to sensitive and confidential topics in their book Randomized Response, encompassing both finite and infinite population configurations. However, the RR technique involves authentication inaccuracies that may lower the system's accuracy. Thus, privacy protection must be balanced with application precision.

4.5.4 Pufferfish Privacy

Pufferfish Privacy (PP) is an advanced extension of differential privacy designed to offer enhanced flexibility in defining sensitive data and incorporating domain-specific knowledge into the privacy framework. It was introduced by Kifer et al. [90]. This approach safeguards sensitive datasets, such as health or financial records, while ensuring precise data analysis. PP stands out by integrating explicit prior knowledge into its privacy evaluations, making it adaptable to specific applications. Maughan et al. [91] introduced Tabular dependent differential privacy, a version of PP for high-dimensional statistics with imperfect correlation in survey data, which significantly outperforms the Laplace mechanism of dependent differential privacy. To address privacy issues, Ding et al. [92] discreetly released IoT event data with timestamps. They showed how modifying event timestamps or adding false events may address three privacy concerns. They extensively tested discreetly publishing discrete event timestamps under Pufferfish privacy. Another research by Ding [93] employed the exponential process to obtain pufferfish privacy via generalized Laplace noise. With calibrated noise to Kantorovich's optimum transport plan sensitivity, released data is pufferfish private, and a Gaussian method approximates this privacy. Pufferfish Privacy is a complex data analysis technology that guarantees strong privacy while allowing practical data analysis. Scalability, utility-privacy trade-offs, mathematical model complexity, real-world applications, adversarial attacks, integration with other privacy solutions, and legal and ethical considerations are its obstacles. Future research should improve privacy, scale algorithms, build user-friendly interfaces, and follow data protection laws.

5 Discussion & Analysis

The field of biometric technologies strongly emphasizes protecting the privacy and security of individuals' sensitive biometric data. Various privacy-preserving technologies have emerged to address this imperative, offering methodologies that balance safeguarding personal information and enabling accurate identification and authentication. A comparative overview of the most widely used privacy-preserving techniques for biometric systems is shown in Table 3. This table meticulously outlines the strength, security, performance, ease of use, applications, advantages, and limitations of existing privacy-preserving techniques.

Table 3: Summary of existing privacy-preserving technologies

Method	Security	Performance	Ease of use	Applications	Advantages	Limitations
Cryptography-based techniques						
Homomorphic encryption	High	Low	Medium	Cloud computing, machine learning, data analytics	Secure computations on encrypted data, protects privacy	Computationally intensive, fewer operations than plaintext
Functional encryption	High	Medium	Low	Access control, data sharing,	Granular access control protects computations	Complex scheme with less functionality than HE or SFE.
Secure function evaluation	High	Medium	Medium	Collaborative computation, privacy-preserving data analysis	Protects sensitive inputs and private data, allows joint computations	Computationally intensive, Requires communication and protocol between parties
Hybrid protection	High	Medium	Medium	Data sharing, access control	Provides layered protection, can leverage strengths of different techniques	Complexity and potential overhead require careful integration of different technologies.
Lattice-based cryptography	High	Medium	Medium	Machine learning, data analytics, encryption, key exchange, digital signatures	Resistance to quantum attacks, proven security against specific mathematical problems	Computational overhead, limited practical deployment due to relative newness and complexity

(Continued)

Table 3 (continued)

Method	Security	Performance	Ease of use	Applications	Advantages	Limitations
			Hashing-based techniques			
Biometric Hashing	Medium	High	Low	Authentication, identification	Protects privacy, enables efficient comparison without revealing sensitive information	Irreversible process, collision possibility, limited to verification scenarios rather than identification
Bloom filters	Medium	High	High	Data filtering, set membership testing	Space-efficient representation of data, enables quick membership testing, and has a low false-negative rate.	Collisions may cause false positives, inability to access initial filter items, and scaling issues as element count increases
Locality-sensitive Hashing	Medium	High	Medium	Data retrieval, data mining	Enables efficient similarity search and nearest neighbor search, allows for approximate matching	Reduces similarity matching precision, and fine-tuning hashing settings to obtain desirable trade-offs is difficult.
Secure sketch	High	Medium	Medium	Data aggregation, data analysis	Offers privacy protection while enabling error correction, efficient data aggregation	Only when error correction is acceptable, noise addition may diminish data utility
Cryptographic accumulator	High	Low	Low	Data integrity, non-repudiation	Enables efficient proof generation and verification and preserves the privacy of individual elements	Some use cases demand accumulation and proof creation, but dynamic data changes are limited
			Template protection techniques			
Cancelable biometrics	Medium	High	Medium	Authentication, identification	Canceled and re-created if compromised	Less accurate than regular biometric authentication

(Continued)

Table 3 (continued)

Method	Security	Performance	Ease of use	Applications	Advantages	Limitations
Fuzzy vault scheme	High	Medium	Medium	Authentication, identification	Identify individuals without revealing their biometric data.	Complex to implement and use
Fuzzy extractor	High	Medium	Medium	Authentication, identification	Extract a unique key from biometric data	Vulnerable to spoofing attacks
Fuzzy commitment scheme	High	Medium	Medium	Authentication, identification	Data commitment validates without releasing it	Vulnerable to replay attacks
Computation-based techniques						
Secure multiparty computation	High	Medium	Medium	Secure collaboration, data sharing	Many parties can compute a function on their inputs without sharing	Computationally expensive
Secret sharing scheme	High	Medium	Medium	Data distribution, secure collaboration	Allows many people to share a secret without reassembling it	Complex to implement and use
Zero-knowledge proofs	High	Medium	Medium	Authentication, data verification	Does not require extra information to verify	Computationally expensive
Secure enclave	High	Medium	Low	Data protection, code execution	Provides a trusted execution environment	Complex to implement and use
K-anonymity	Medium	High	Medium	Data anonymization	Alters data to make it difficult to identify individuals	Vulnerable to re-identification attacks
Differential privacy techniques						
Exponential mechanism	High	Medium	Medium	Data sharing, statistical analysis	Provide robust privacy protection	Computationally expensive
Laplace mechanism	High	Medium	Medium	Data sharing, statistical analysis	Provides strong privacy guarantees	Computationally expensive
Randomized response	Medium	High	Low	Data collection, surveys	Simple to implement and use	Less accurate
Pufferfish privacy	High	Medium	Medium	Data sharing, statistical analysis	Offers robust privacy protection	Computationally expensive

From Table 3, it is shown that the best privacy-preserving technique for a given application depends on specific requirements, such as the desired security level, performance requirements, and ease of use. Cryptography-based methods are secure yet computationally demanding and may not perform well. These are ideal for cloud computing, machine learning, and data analytics. Hashing-based methods provide medium security and excellent performance. They work well for authentication, identification, data filtering, and membership testing. The new lattice-based cryptography technology offers exceptional protection and resistance to quantum attacks. It works well for machine learning, data analytics, encryption, key exchange, and digital signatures. Although computationally intensive, computation-based solutions provide high security. They are ideal for secure collaboration, data sharing, retrieval, communication, matching, and set comparison. Template protection solutions provide medium security and are ideal for authentication and identification. Differential privacy techniques offer good security and protection against re-identification threats. They are ideal for data sharing and statistical analysis.

Many intriguing research gaps exist on this topic. AI-based biometric matching approaches like deep learning emerge as AI deployment develops. AI-related attacks may target these methods increasingly. As mobile biometric authentication becomes increasingly prevalent, privacy-preserving authentication becomes more crucial. IoT and cloud outsourcing are growing. Therefore, cryptographic protocols will use biometric authentication for key management, encryption, and decryption. Biometric data encryption must be continuously researched and developed. Biometrics combined with passwords or tokens can boost security. Multi-factor authentication decreases reliance on a single biometric property and makes system compromise harder. These methods should improve biometric system security while reducing computing overhead and maintaining accuracy. Effectively revoking and replacing compromised biometric templates prevents unauthorized access to compromised data.

Secure key manufacturing, storage, and delivery should be researched to protect encryption keys. Biometric key secrecy can be achieved by key diversity, isolation, and storage. Biometric systems must be checked routinely to identify and fix security vulnerabilities. Continuous monitoring and timely patching strengthen the system against shifting threats. Privacy-preserving biometric technologies must be standardized and compatible to spread. Standardizing protocols and formats enhance system-wide security and efficiency. Biometric system design and deployment require user understanding and agreement. People can make informed decisions about biometric data by explaining biometrics' benefits, risks, and privacy consequences and using transparent permission mechanisms. Biometric technology development should prioritize ethics. Research should address biometric biases, prejudice, and unforeseen consequences. Designing and deploying these technologies must be fair, accountable, and transparent. These strategies and security and efficiency as design principles can improve biometric privacy-preserving technologies to protect individuals' biometric information better while maintaining accuracy and usability in various applications.

6 Conclusion

This study introduces a new way to categorize biometric authentication methods that protect user privacy, taking into account privacy-preserving mechanisms at the protocol level. If researchers in the fields of biometrics and cryptography want to successfully integrate their work, they can use this taxonomy as a neutral roadmap that provides a more holistic view of the area. This article delves into the difficulties of biometric authentication from a privacy perspective, including the pros and cons of the technology, possible dangers to privacy-preserving systems, and attack methods. It highlights the feasibility of privacy-preserving biometric technologies and proposes strategies to lessen

the impact of these dangers. The paper also discusses weaknesses and potential solutions to open research problems that lie at the nexus of biometric security, authentication, and cryptography. New biometric identification technologies are becoming increasingly important, and there is a growing need to preserve privacy; this study also predicts trends based on upcoming research areas, including the Internet of Things, the cloud, and current electronics. Overall, this work offers a thorough taxonomy, tackles open research difficulties, and predicts future developments in privacy-preserving biometric authentication, which is a significant contribution to the area.

Acknowledgement: The authors would like to thank the editor and all anonymous reviewers for their helpful comments and suggestions.

Funding Statement: The research is supported by Nature Science Foundation of Zhejiang Province (LQ20F020008), "Pioneer" and "Leading Goose" R&D Program of Zhejiang (Grant Nos. 2023C03203, 2023C01150).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Shahriar Md Arman, Tao Yang, Shahadat Shahed; data collection: Shahriar Md Arman, Tao Yang, Alanoud Al Mazroa, Afraa Attiah; analysis and interpretation of results: Tao Yang, Shahadat Shahed, Linda Mohaisen; draft manuscript preparation: Shahriar Md Arman, Shahadat Shahed, Alanoud Al Mazroa, Afraa Attiah, Linda Mohaisen. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed and C. Valli, "Biometrics for Internet-of-Things security: A review," *Sens.*, vol. 21, no. 18, pp. 6163, 2021. doi: 10.3390/s21186163.

[2] H. U. Khan, M. Sohail, S. Nazir, T. Hussain, B. Shah and F. Ali, "Role of authentication factors in Fin-tech mobile transaction security," *J. Big Data*, vol. 10, no. 1, pp. 138, 2023. doi: 10.1186/s40537-023-00807-3.

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits. Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004. doi: 10.1109/TCSVT.2003.818349.

[4] T. Duarte, J. P. Pimentão, P. Sousa, and S. Onofre, "Biometric access control systems: A review on technologies to improve their efficiency," in *2016 IEEE Int. Power Electron. Motion Control Conf. (PEMC)*, IEEE, 2016, pp. 795–800.

[5] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimed. Tools Appl.*, vol. 79, pp. 27721–27776, 2020. doi: 10.1007/s11042-020-09197-7.

[6] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *Australas. Conf. Inf. Secur. Privacy*, Springer, 2005, pp. 242–252.

[7] A. Harmanci and M. Gerstein, "Analysis of sensitive information leakage in functional genomics signal profiles through genomic deletions," *Nat. Commun.*, vol. 9, no. 1, pp. 2453, 2018. doi: 10.1038/s41467-018-04875-5.

[8] A. Chiavegatto Filho, A. F. D. M. Batista, and H. G. Dos Santos, "Data leakage in health outcomes prediction with machine learning. Comment on "Prediction of incident hypertension within the next year: Prospective study using statewide electronic health records and machine learning"," *J Med. Internet. Res.*, vol. 23, no. 2, pp. e10969, 2021. doi: 10.2196/10969.

[9] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 113, 2008. doi: 10.1155/2008/579416.
[10] M. Faundez-Zanuy, "Biometric security technology," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 21, no. 6, pp. 15–26, 2006. doi: 10.1109/MAES.2006.1662038.
[11] M. El-Abed, C. Charrier, and C. Rosenberger, "Evaluation of biometric systems," *New Trends Develop. Biom.*, pp. 149–169, 2012. doi: 10.5772/52084.
[12] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Inform. Fusion*, vol. 52, pp. 187–205, 2019. doi: 10.1016/j.inffus.2018.12.003.
[13] J. R. van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *2018 Eur. Navig. Conf. (ENC)*, IEEE, 2018, pp. 91–99.
[14] M. Singh and D. Pati, "Countermeasures to replay attacks: A review," *IETE Tech. Rev.*, vol. 37, no. 6, pp. 599–614, 2020. doi: 10.1080/02564602.2019.1684851.
[15] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," in *2013 IEEE Int. Conf. Comput. Intell. and Comput. Res.*, IEEE, 2013, pp. 1–7.
[16] M. Fairhurst, M. Erbilek, and M. da Costa-Abreu, "Selective review and analysis of aging effects in biometric system implementation," *IEEE Trans. Hum. Mach. Syst.*, vol. 45, no. 3, pp. 294–303, 2014. doi: 10.1109/THMS.2014.2376874.
[17] B. Biggio, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Proc. Mag.*, vol. 32, no. 5, pp. 31–41, 2015. doi: 10.1109/MSP.2015.2426728.
[18] A. North-Samardzic, "Biometric technology and ethics: Beyond security applications," *J. Bus. Ethics*, vol. 167, no. 3, pp. 433–450, 2020. doi: 10.1007/s10551-019-04143-6.
[19] T. F. Blauth, O. J. Gstrein, and A. Zwitter, "Artificial intelligence crime: An overview of malicious use and abuse of AI," *IEEE Access*, vol. 10, pp. 77110–77122, 2022. doi: 10.1109/ACCESS.2022.3191790.
[20] Vandana and N. Kaur, "Analytical review of biometric technology employing vivid modalities," *Int. J. Image Graph.*, vol. 22, no. 1, pp. 2250004, 2022. doi: 10.1142/S0219467822500048.
[21] P. Pisani *et al.,* "Adaptive biometric systems: Review and perspectives," *ACM Comput. Surv. (CSUR)*, vol. 52, no. 5, pp. 1–38, 2019. doi: 10.1145/3344255.
[22] K. Thakur and P. Vyas, "Social impact of biometric technology: Myth and implications of biometrics: Issues and challenges," In: G. Sinha (ed.), *Advances in Biometrics: Modern Methods and Implementation Strategies*, Advances in Biometrics. Springer, Cham, 2019, pp. 129–155.
[23] L. Menaria and K. Jain, "A survey on biometric template protection," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 2, pp. 995–999, 2017. doi: 10.32628/CSEIT1722303.
[24] N. Costigan, "The growing pain of phishing: Is biometrics the cure?," *Biometric Technol. Today*, vol. 2016, no. 2, pp. 8–11, 2016. doi: 10.1016/S0969-4765(16)30035-2.
[25] R. L. Rivest and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found Secure Comput.*, vol. 4, pp. 169–180, 1978.
[26] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2009, pp. 169–178.
[27] T. Chandrasekhar and S. Kumar, "A noval method for cloud security and privacy using homomorphic encryption based on facial key templates," *J. Adv. Inf. Technol.*, vol. 13, no. 6, pp. 638–644, 2022. doi: 10.12720/jait.13.6.638-644.
[28] P. Chitrapu and H. K. Kalluri, "A survey on homomorphic encryption for biometrics template security based on machine learning models," in *2023 IEEE Int. Stud' Conf. Electr, Electron. and Comput. Sci. (SCEECS)*, IEEE, 2023, pp. 1–6.
[29] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory Cryptol.: 8th Theory of Cryptol. Conf., TCC 2011,* Providence, RI, USA, Mar. 28–30, Springer, 2011, pp. 253–273.

[30] J. Ernst and A. Mitrokotsa, "A framework for UC secure privacy preserving biometric authentication using efficient functional encryption," in *Int. Conf. Appl. Cryptogr. Netw. Secur.*, Springer, 2023, pp. 167–196.
[31] K. Shahzad, T. Zia, and E. U. H. Qazi, "A review of functional encryption in IoT applications," *Sens.*, vol. 22, no. 19, pp. 7567, 2022.
[32] A. C. Yao, "Protocols for secure computations," in *23rd Annu. Symp. Found. Comput. Sci. (SFCS 1982)*, IEEE, 1982, pp. 160–164.
[33] T. Schneider, "Practical secure function evaluation," in *Informatiktage*, Springer, Berlin, Heidelberg, 2008, pp. 37–40. doi: 10.1007/978-3-540-85230-8_7.
[34] R. Oishi, J. Kadomoto, H. Irie, and S. Sakai, "FPGA-based garbling accelerator with parallel pipeline processing," *IEICE Trans. Inf. Syst.*, vol. 106, no. 12, pp. 1988–1996, 2023.
[35] Y. Wang, "Reducing garbled circuit size while preserving circuit gate privacy," *Cryptol. ePrint Arch.*, vol. 2017, pp. 041, 2017. Accessed: Jun. 25, 2023 https://eprint.iacr.org/2017/041
[36] S. Bettaieb, L. Bidoux, O. Blazy, B. Cottier, and D. Pointcheval, "Post-quantum oblivious transfer from smooth projective hash functions with grey zone," arXiv preprint arXiv:2209.04149, 2022.
[37] A. Bassit, F. Hahn, R. Veldhuis, and A. Peter, "Hybrid biometric template protection: Resolving the agony of choice between bloom filters and homomorphic encryption," *IET Biometrics*, vol. 11, no. 5, pp. 430–444, 2022. doi: 10.1049/bme2.12075.
[38] H. O. Shahreza, C. Rathgeb, D. Osorio-Roig, V. K. Hahn, S. Marcel and C. Busch, "Hybrid protection of biometric templates by combining homomorphic encryption and cancelable biometrics," in *2022 IEEE Int. Joint Conf. Biom. (IJCB)*, IEEE, 2022, pp. 1–10.
[39] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.
[40] X. Fu, Y. Ding, H. Li, J. Ning, T. Wu and F. Li, "A survey of lattice based expressive attribute based encryption," *Comput. Sci. Rev.*, vol. 43, pp. 100438, 2022. doi: 10.1016/j.cosrev.2021.100438.
[41] O. S. Althobaiti, T. Mahmoodi, and M. Dohler, "Intelligent bio-latticed cryptography: A quantum-proof efficient proposal," *Symmetry*, vol. 14, no. 11, pp. 2351, 2022. doi: 10.3390/sym14112351.
[42] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004. doi: 10.1016/j.patcog.2004.04.011.
[43] L. Yu, Q. Wang, Y. Wo, and G. Han, "Secure biometric hashing against relation-based attacks via maximizing min-entropy," *Comput. Secur.*, vol. 118, pp. 102750, 2022. doi: 10.1016/j.cose.2022.102750.
[44] L. Yu and Y. Wo, "A general framework for secure biometric hashing against reconstruction attacks," *Appl. Intell.*, vol. 53, no. 10, pp. 12811–12830, 2023. doi: 10.1007/s10489-022-04153-4.
[45] K. Raja, R. Raghavendra, and C. Busch, "Towards better and unlinkable protected biometric templates using label-assisted discrete hashing," *IET Biom.*, vol. 11, no. 1, pp. 51–62, 2022. doi: 10.1049/bme2.12043.
[46] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, 1970. doi: 10.1145/362686.362692.
[47] V. Bansal and S. Garg, "A cancelable biometric identification scheme based on bloom filter and format-preserving encryption," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5810–5821, 2022. doi: 10.1016/j.jksuci.2022.01.014.
[48] T. Zhou, D. Chen, W. Liu, and X. Yang, "Attacks and improvement of unlinkability of biometric template protection scheme based on bloom filters," *IEEE Trans. Cloud Comput.*, vol. 11, no. 3, pp. 3251–3261, 2023. doi: 10.1109/TCC.2023.3276971.
[49] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in *Proc. 13th Annu. ACM Symp. Theory Comput.*, 1998, pp. 604–613.
[50] A. A. Alshahrani and E. S. Jaha, "Locality-sensitive hashing of soft biometrics for efficient face image database search and retrieval," *Electron.*, vol. 12, no. 6, pp. 1360, 2023. doi: 10.3390/electronics12061360.
[51] N. Mashnoor, J. Thom, A. Rouf, S. Sengupta, and B. Charyyev, "Locality sensitive hashing for network traffic fingerprinting," in *2023 IEEE 29th Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jul. 10–11, 2023, pp. 1–6. doi: 10.1109/LANMAN58293.2023.10189810.

[52] M. Jiang, S. Liu, Y. Lyu and Y. Zhou, "Face-based authentication using computational secure sketch," *IEEE Trans. Mob. Comput.*, vol. 22, no. 12, pp. 7172–7187, 2023. doi: 10.1109/TMC.2022.3207830.
[53] J. Benaloh and M. de Mare, "One-way accumulators: A decentralized alternative to digital signatures," in *Workshop Theory Appl. Cryptogr. Tech.*, Springer, 1993, pp. 274–285.
[54] Y. Ren, X. Liu, Q. Wu, L. Wang and W. Zhang, "Cryptographic accumulator and its application: A survey," *Secur. Commun. Netw.*, vol. 2022, pp. 5429195, 2022. doi: 10.1155/2022/5429195.
[55] C. Kauba *et al.*, "Towards practical cancelable biometrics for finger vein recognition," *Inform. Sci.*, vol. 585, pp. 395–417, 2022. doi: 10.1016/j.ins.2021.11.018.
[56] H. Shahreza *et al.*, "Benchmarking of cancelable biometrics for deep templates," arXiv preprint arXiv:2302.13286, 2023.
[57] J. C. Bernal-Romero, J. M. Ramirez-Cortes, J. Rangel-Magdaleno, H. Peregrina-Barreto, and I. Cruz-Vega, "A review on protection and cancelable techniques in biometric systems," *IEEE Access*, vol. 11, pp. 8531–8568, 2023. doi: 10.1109/ACCESS.2023.3239387.
[58] P. Kaur, N. Kumar and M. Singh, "SURFBCS: Speeded up robust features based fuzzy vault scheme in biometric cryptosystem," *J. Supercomput.*, vol. 79, pp. 12292–12316, 2023. doi: 10.1007/s11227-023-05142-1.
[59] C. Rathgeb, J. Merkle, J. Scholz, B. Tams, and V. Nesterowicz, "Deep face fuzzy vault: Implementation and performance," *Comput. Secur.*, vol. 113, pp. 102539, 2022. doi: 10.1016/j.cose.2021.102539.
[60] A. F. D. Abiega-L'Eglisse, M. Rosas Otero, V. Azpeitia Hernández, G. Gallegos-Garcia, and M. Nakano-Miyatake, "A new fuzzy vault based biometric system robust to brute-force attack," *Computación y Sistemas*, vol. 26, no. 3, pp. 1151–1165, 2022. doi: 10.13053/cys-26-3-4184.
[61] Z. Song, D. Chen, J. He, W. Yuan, and P. Chen, "A fuzzy vault scheme with multi-secret sharing," in *3rd Int. Conf. Comput. Commun. Netw. Secur. (CCNS 2022)*, SPIE, vol. 12453, 2022, pp. 326–331.
[62] S. Zhang, Z. Yan, W. Liang, K. C. Li and C. Dobre, "BAKA: Biometric authentication and key agreement scheme based on fuzzy extractor for wireless body area networks," *IEEE Internet Things*, vol. 2023, pp. 1, 2023. doi: 10.1109/JIOT.2023.3302620.
[63] A. Sathish, A. Bajulunisha, R. Sridevi, and S. Vatchala, "Biometric authentication utilizing fuzzy extractor with PSO based security ensuring the data security mechanism as trio in cloud," *J. Intell. Fuzzy Syst.*, vol. 42, no. 6, pp. 4805–4819, 2022. doi: 10.3233/JIFS-200469.
[64] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.
[65] D. Chang, S. Garg, M. Hasan, and S. Mishra, "On security of fuzzy commitment scheme for biometric authentication," in *Austral. Conf. Informat. Secur. Priv.*, Springer, 2022, pp. 399–419.
[66] S. Chauhan and A. Sharma, "Improved fuzzy commitment scheme," *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1321–1331, 2022.
[67] A. Bajaber and L. Elrefaei, "Biometric template protection for dynamic touch gestures based on fuzzy commitment scheme and deep learning," *Math*, vol. 10, no. 3, pp. 362, 2022. doi: 10.3390/math10030362.
[68] T. Wu, L. Leng, and M. K. Khan, "A multi-spectral palmprint fuzzy commitment based on deep hashing code with discriminative bit selection," *Artif. Intell. Rev.*, vol. 56, no. 7, pp. 6169–6186, 2023. doi: 10.1007/s10462-022-10334-x.
[69] Z. Li and W. Liu, "A quantum secure multiparty computation protocol for least common multiple," arXiv preprint arXiv:2210.08165, 2022.
[70] S. Pentyala *et al.,* "Training differentially private models with secure multiparty computation," arXiv preprint arXiv:2202.02625, 2022.
[71] A. Choudhury and A. Patra, *Secure Multi-Party Computation Against Passive Adversaries*. Springer Nature, Switzerland AG, 2022.
[72] N. Francis, and T. Monoth, "An analytical appraisal on recent trends and challenges in secret sharing schemes," in *Proc. Int. Conf. Paradigms Comput. Commun. Data Sci.: PCCDS 2022*, Springer, 2023, pp. 345–357.
[73] A. Chandramouli, A. Choudhury, and A. Patra, "A survey on perfectly secure verifiable secret-sharing," *ACM Comput. Surv. (CSUR)*, vol. 54, no. 11s, pp. 1–36, 2022. doi: 10.1145/3512344.

[74] F. Li, H. Hu, S. Zhu, J. Yan, and J. Ding, "A verifiable (k, n)-threshold dynamic quantum secret sharing scheme," *Quantum Inf. Process*, vol. 21, no. 7, pp. 259, 2022. doi: 10.1007/s11128-022-03617-3.
[75] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, 1989. doi: 10.1137/0218012.
[76] G. S. Gaba *et al.,* "Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare," *Sustain. Cities Soc.*, vol. 80, pp. 103766, 2022. doi: 10.1016/j.scs.2022.103766.
[77] M. Carney, "On zero-knowledge proofs over the quantum Internet," arXiv preprint arXiv:2212.03027, 2022.
[78] Z. Chen, Y. Jiang, X. Song, and L. Chen, "A survey on zero-knowledge authentication for Internet of Things," *Electronics*, vol. 12, no. 5, pp. 1145, 2023. doi: 10.3390/electronics12051145.
[79] J. Y. Gu, H. Li, Y. B. Xia, H. B. Chen, C. G. Qin and Z. Y. He, "Unified enclave abstraction and secure enclave migration on heterogeneous security architectures," *J. Comput. Sci. Tech.*, vol. 37, no. 2, pp. 468–486, 2022. doi: 10.1007/s11390-021-1083-8.
[80] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: K-anonymity and its enforcement through generalization and suppression," 1998. Accessed: Jul. 18, 2023 https://dataprivacylab.org/dataprivacy/projects/kanonymity/index3.html
[81] J. Qian, H. Jiang, Y. Yu, H. Wang, and D. Miao, "Multi-level personalized k-anonymity privacy-preserving model based on sequential three-way decisions," *Expert Syst. Appl.*, vol. 239, pp. 122343, 2024. doi: 10.1016/j.eswa.2023.122343.
[82] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS'07)*, IEEE, 2007, pp. 94–103.
[83] S. Gopi, Y. T. Lee, and D. Liu, "Private convex optimization via exponential mechanism," in *Conf. Learn. Theory*, PMLR, 2022, pp. 1948–1989.
[84] K. Ramsay, A. Jagannath and S. E. Chenouri, "Concentration of the exponential mechanism and differentially private multivariate medians," arXiv preprint arXiv:2210.06459, 2022.
[85] G. Muthukrishnan and S. Kalyani, "Grafting Laplace and Gaussian distributions: A new noise mechanism for differential privacy," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5359–5374, 2023. doi: 10.1109/TIFS.2023.3306159.
[86] A. Ünsal and M. Önen, "A statistical threshold for adversarial classification in Laplace mechanisms," in *2021 IEEE Informat. Theory Workshop (ITW)*, IEEE, 2021, pp. 1–6.
[87] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *J. Am. Stat. Assoc.*, vol. 60, no. 309, pp. 63–69, 1965. doi: 10.1080/01621459.1965.10480775.
[88] G. Blair, K. Imai, and Y. Y. Zhou, "Design and analysis of the randomized response technique," *J. Am. Stat. Assoc.*, vol. 110, no. 511, pp. 1304–1319, 2015. doi: 10.1080/01621459.2015.1050028.
[89] A. Chaudhuri and R. Mukerjee, *Randomized Response: Theory and Techniques*. Indian Statisitical Institute in Calcutta, Routledge, 2020.
[90] D. Kifer and A. Machanavajjhala, "A rigorous and customizable framework for privacy," in *Proc. 31st ACM SIGMOD-SIGACT-SIGAI Symp. Princ. Database Syst.*, Scottsdale, Arizona, USA, 2012, pp. 77–88.
[91] K. Maughan and J. P. Near, "Improving utility for privacy-preserving analysis of correlated columns using pufferfish privacy," arXiv preprint arXiv:2209.10908, 2022.
[92] J. Ding, A. Ghosh, R. Sarkar, and J. Gao, "Publishing asynchronous event times with pufferfish privacy," in *2022 18th Int. Conf. Distrib. Comput. Sens. Syst. (DCOSS)*, IEEE, 2022, pp. 53–60.
[93] N. Ding, "Kantorovich mechanism for pufferfish privacy," in *Int. Conf. Artif. Intell. Stat.*, PMLR, 2022, pp. 5084–5103.