IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 December 2022, accepted 13 January 2023, date of publication 23 January 2023, date of current version 27 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3239387

TOPICAL REVIEW

A Review on Protection and Cancelable Techniques in Biometric Systems

JUAN CARLOS BERNAL-ROMERO[1], (Graduate Student Member, IEEE), JUAN MANUEL RAMIREZ-CORTES[1], (Senior Member, IEEE), JOSE DE JESUS RANGEL-MAGDALENO[1], (Senior Member, IEEE), PILAR GOMEZ-GIL[2], (Senior Member, IEEE), HAYDE PEREGRINA-BARRETO[2], (Senior Member, IEEE), AND ISRAEL CRUZ-VEGA[1]

[1]Department of Electronics, National Institute of Astrophysics, Optics and Electronics, Puebla 72840, Mexico
[2]Department of Computer Science, National Institute of Astrophysics, Optics and Electronics, Puebla 72840, Mexico

Corresponding author: Juan Manuel Ramirez-Cortes (jmram@inaoep.mx)

The work of Juan Carlos Bernal-Romero was supported by the National Council of Science and Technology Mexico (CONACYT) under Grant 936140.

ABSTRACT An essential part of cloud computing, IoT, and in general the broad field of digital systems, is constituted by the mechanisms which provide access to a number of services or applications. Biometric techniques aim to manage the access to such systems based on personal data; however, some biometric traits are openly exposed in the daily life, and in consequence, they are not secret, e.g., voice or face in social networks. In many cases, biometric data are non-cancelable and non-renewable when compromised. This document examines the vulnerabilities and proposes hardware and software countermeasures for the protection and confidentiality of biometric information using randomly created supplementary information. Consequently, a taxonomy is proposed according to the operating principle and the type of supplementary information supported by protection techniques, analyzing the security, privacy, revocability, renewability, computational complexity, and distribution of biometric information. The proposed taxonomy has five categories: 1) biometric cryptosystems; 2) cancelable biometrics; 3) protection schemes based on machine learning or deep learning; 4) hybrid protection schemes; and 5) multibiometric protection schemes. Furthermore, this document proposes quantitative evaluation measures to compare the performance of protection techniques. Likewise, this research highlights the advantages of injective and linear mapping for the protection of authentication and identification systems, allowing the non-retraining of these systems when the protected biometric information is canceled and renewed. Finally, this work mentions commercial products for cancelable biometric systems and proposes future directions for adaptive and cancelable biometric systems in low-cost IoT devices.

INDEX TERMS Biometric template protection (BTP), cancelable, irreversibility, privacy, security, unlinkability.

I. INTRODUCTION

Nowadays, a vast majority of digital applications and services use the internet through a cyber-physical ecosystem with human-machine interaction. Therefore, intelligent devices and cloud computing have experienced an exponential increase. In addition, smart devices or the internet of things (IoT) have evolved into wearable devices and must offer good mobility, social acceptance, performance, quality of experience (QoE), security, and privacy to users through limited resources such as computing, storage, and power consumption [1], [2], [3]. Therefore, smart devices or IoT

The associate editor coordinating the review of this manuscript and approving it for publication was Donato Impedovo.

devices are implementing services or applications that need pattern recognition systems to control and manage user access. In fact, IoT devices can be used or not in any area of application of pattern recognition systems.

Currently, the next categories of user recognition are commonly considered: 1) *secret information memorized by the user*, e.g., personal identification number (PIN) or password; 2) *unique symbolic information*, e.g., passport, token or smart card; and 3) physiological (static) or behavioral (dynamic) information constituting *biometric systems*, e.g., fingerprint, electrocardiogram (ECG) [4], or hand veins [5]. However, secret and symbolic information can be forgotten, estimated, stolen, lost, or exchanged; this affects the security and privacy of applications or services. For this reason, biometric systems are an excellent niche opportunity to improve safety in applications or services based on pattern recognition systems, especially pattern recognition systems implemented in IoT devices or wireless and low-cost devices [6], [7], [8].

There are two biometric operation modes: 1) *Authentication*, in which a *one-to-one* matching is performed to verify or authenticate the claimed identity. 2) *Identification*, in which a *one-to-many* matching process is required to distinguish the identity of the subject within a database.

Biometric traits are classified into *hard biometrics* (hard traits) and *soft biometrics* (soft traits). Hard biometrics have a high degree of discrimination (hard) and permanence, e.g., iris, voice, face, etc. On the other hand, soft biometrics is conformed by auxiliary traits with a low degree of discrimination (soft), which provide additional information to profile a user, e.g., hair color, weight, health, emotional status, etc. Therefore, hard traits are used to develop biometric systems. Furthermore, hard traits are divided into physiological traits and behavioral traits. Physiological traits are inherent or static physical characteristics of an individual, e.g., fingerprint, iris, etc. Likewise, behavioral traits are dynamic characteristics of an individual based on the nature of his/her actions, e.g., voice, handwritten signature, etc. In general, physiological traits have less intra-user variability than behavioral traits. However, biometric systems based on behavioral traits have a cancelable approach due to the dynamic characteristics.

Nonetheless, hard and soft biometrics together allow the profiling of people for several purposes, such as the so-called business biometric profiles. IoT devices, biometrics, artificial intelligence (AI), and neuroscience create customer/employee profiles along five levels [9]: 1) identification profiling (who is this person?); 2) physical profiling (what type of person is this?); 3) emotion profiling (what is this person feeling?); 4) behavioral profiling (what is this person doing?); and 5) cognitive profiling (what is the person thinking?). These levels offer great opportunities for companies, such as: 1) deepening consumer perspectives; 2) customizing the marketing mix; 3) automating customer travel; 4) strengthening safety; 5) improving personal health and well-being; and 6) help with employee recruitment, support and management. Therefore, it is evident that the collection, processing, and storage of biometric information requires a high level of attention and care, since it deals with personal and sensitive data. Furthermore, although biometric traits are unique and permanent in a person's life, intra-user variations may appear in the short and long term. In addition, these traits cannot be canceled and renewed as passwords or tokens. Noteworthy, the security and privacy of biometric information is an important research area that has gained much attention in recent years (see Fig. 1).

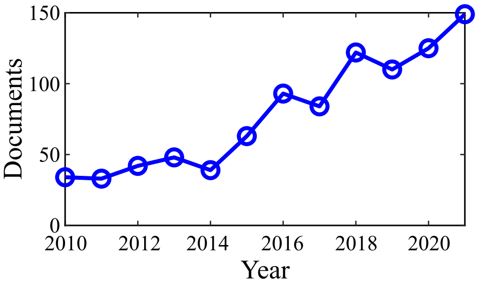


FIGURE 1. Documents published by year in Scopus found with the search formula: (((biometric OR biometrics) AND ((protection OR (security OR privacy)) OR (cancellable OR cancelable))) AND (review OR survey)).

Biometric techniques provide application security, e.g., a fingerprint cannot be exchanged, lost, or forgotten. However, biometrics need security to avoid compromising application interoperability (cross-matching); for instance, if a biometric trait such as the face or iris in a social media photo is compromised (copied or spoofed), all the applications that use that trait are affected in their security level. Additionally, deep learning (DL) techniques artificially synthesize an image, video, or audio by realistically exchanging the biometric traits of one user for another, as shown in Fig. 2. The above process is called *DeepFakes* and threatens applications with biometric systems. DeepFakes enables synthesis, identity swap, attribute manipulation, and expression swap using generative adversarial networks (GAN) [10], [11]. Consequently, applications with biometric systems need to detect DeepFakes, but most of these detection algorithms are computationally expensive. Therefore, the information security field is a promising solution for the confidentiality and privacy of biometrics.

Thus, the landscape of biometric systems presents a significant challenge in information protection. Therefore, the probability of cross-matching attacks decreases using several biometric traits, especially inherent biometric traits of liveliness, e.g., an electroencephalogram (EEG) and voice-based system [13] or a photoplethysmography (PPG) and ECG-based system [14]. Furthermore, biometric systems can also use biometric template protection (BTP) techniques to prevent counterfeiting and increase information security and privacy. BTP techniques allow the cancelation, renewal, and confidentiality of biometric information using random information. Consequently, the focus of this research seeks to answer the following:

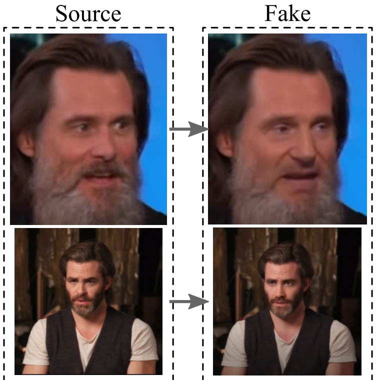


FIGURE 2. Identity swap (DeepFakes), facial images obtained from the Celeb-DF database [12].

- *Qualitative approach*: What BTP techniques currently exist, and how do these operate?
- *Quantitative approach*: How are BTP techniques evaluated?

In addition, this paper contributes to the following objectives through a review of the literature on BTP techniques: 1) examine vulnerabilities and propose countermeasures for biometric systems at the hardware and software levels; 2) expose the formalization and standardization of BTP techniques at the international level; 3) define a novel taxonomy according to the principle of operation and the type of supplementary information supported by BTP techniques; 4) analyze the security, privacy, revocability, renewability, computational complexity, and distribution of biometric information for BTP techniques; and 5) establish evaluation measures to compare BTP techniques.

This document has the following structure: First, section II presents the motivation and justification of BTP techniques through the hardware and software-level vulnerabilities and countermeasures for biometric systems. Consequently, section III covers the formalization and standardization of BTP techniques in the interoperability of different biometric-based applications or services. Concerning the focus of this paper, section IV presents previous works that reviewed the literature and proposed taxonomies of protection techniques. In addition, this section identifies and highlights the contributions and challenges in the field of BTP. Thus, section V describes the protocol of the systematic literature review in BTP techniques implemented in this work. This section also presents the contributions of this research in the area of BTP compared to previous works. As a result of the literature review protocol, section VI proposes a novel taxonomy according to the principle of operation and the type of supplementary information supported by the different protection techniques. Likewise, protection and cancelation techniques for each category of the proposed taxonomy are explained in detail. Therefore, qualities and functioning are analyzed for techniques based on biometric cryptosystems (section VII), cancelable biometrics (section VIII), schemes based on machine learning or deep learning (section IX), hybrid schemes (section X), and multibiometric schemes (section XI). Furthermore, section XII summarizes the techniques studied in the proposed taxonomy, highlighting its strengths and weaknesses. However, the literature review identifies a gap in the mathematical formulation of evaluation metrics for the performance of protection techniques. For this reason, section XIII proposes quantitative evaluation metrics to compare BTP techniques. Additionally, section XIV shows existing commercial products that implement BTP techniques for revocable biometric systems. Finally, section XV presents the conclusions and future directions of this research.

II. VULNERABILITIES AND COUNTERMEASURES FOR BIOMETRIC SYSTEMS

The information of a biometric trait changes slightly in several presentations due to some injury, pathology, variability in the acquisition environment, or variability in the user's body conditions [15]. Therefore, biometric systems can make incorrect decisions due to intra-user variability or failures in the sensing and processing modules; such failures are *intrinsic failures*. On the other hand, *extrinsic failures* are generated by external attacks that modify the environment and the correct operation of the recognition system. Therefore, failures directly affect the performance rate of the system. Then, the most common action to deal with the intrinsic failures is to design a specific technique of pre-processing, feature extraction, and decision-making for the behavior of the biometric trait and its intra-user variability. A particular case facing intra-user variations under practical considerations is presented by [4] for biometric recognition based on ECG signal.

Attacks that generate extrinsic failures can be passive or active. Passive attacks only observe or monitor information, compromising the confidentiality of biometrics. Active attacks manipulate, steal or delete information, compromising the integrity and confidentiality of biometrics [16]. Then, active attacks affect system performance, causing denial-of-service (DoS), unauthorized access to an impostor, or illegal use of biometric information related to user identity.

Biometric information privacy is the power to control and limit its disclosure to third parties, preserving confidentiality, especially unnecessary and unauthorized disclosure; this seeks to prevent spoofing or illegal use of information. In parallel, *biometric information security* ensures that private information is secure, providing the veracity and integrity of the information available only to authorized entities. Therefore, the most common active and passive attacks on biometric systems are the following [17], [18]:

- *Brute force attack*: An attacker sends all possible combinations of the protected information to the decision-making module until successful recognition.
- *Hill-climbing attack*: An attacker iteratively sends fake templates to the decision-making module until successful recognition. The attacker receives feedback to modify the fake template at each attempt.

- *Record Multiplicity attack or attack via Record Multiplicity*: An attacker tries to find the correlation between multiple protected templates of a user to access the original template.
- *Attack via lost supplementary information*: An attacker attempts to estimate the original template when the supplementary information and the protected information have been compromised simultaneously.
- *Dictionary-based attack*: An attacker sends only the protected templates with the highest probability of successful recognition to the decision-making module.
- *Pre-image attack or similarity-based attack*: An attacker tries to find the original template that generates a protected template of reference through the similarity score obtained with the reference template.
- *Known-template attacks*: An attacker attempts to estimate the BTP technique or supplementary information when the original template and the protected template have been compromised simultaneously.

The probability of success in an active or passive attack decreases when the recognition system modules are in the same specialized hardware processing unit [19], e.g., in the same hardware description language (HDL) implementation.

Although a biometric system is implemented in a specialized hardware processing unit, it has several points vulnerable to attacks, as shown in Fig. 3. First, the communication channel between the user and the user interface (point A) can suffer from the physical presentation of false or artificially created synthetic biometrics. Second, the communication channel between the user interface and the processing unit (point B) may receive attacks that generate false or altered digital information, e.g., a DeepFake attack. Third, the communication channel between the processing unit and the database (point C) may be compromised by observation attacks, manipulation, deletion, theft, or replacement of the biometric template generated by feature extraction. Point C attacks imply that the attacker needs prior knowledge about the representation and feature extraction technique implemented in the system [20], [21], [22]. Finally, point C is the communication channel between a client (processing unit) and a server (database).

The production of fake biometrics to attack point A is more costly and time-consuming than producing or modifying false digital information for attacks at points B and C. In other words, attacks on the sensing unit (point A) through a 3D model of a fingerprint, a contact lens with the iris pattern, a voice synthesizer, or a realistic model for facial recognition are more challenging and complex to produce than an active attack on the digitized biometric information. Indeed, spoofing in the sensing unit for a biometric system based on cardiovascular signals is unlikely. Therefore, the vulnerability of point A is overcome using liveness detection techniques or using inherent biometrics of liveliness to ensure that the trait presented is not an artificial reproduction, e.g., an ECG-based biometric system is difficult to falsify and provides psychological, physiological, and clinical information about a user [23]. On the other hand, the threat of point B is solved by using embedded sensor systems (ESS), i.e., user interface and digital processing unit in the same device; otherwise, the communication channel must be secure, not wireless, or not over the internet.

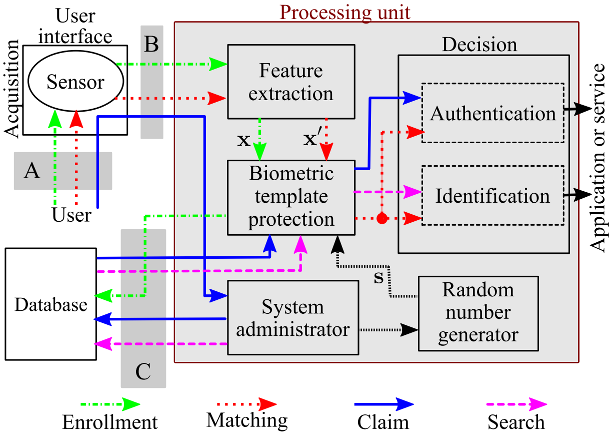


FIGURE 3. Biometric system diagram with vulnerable points and protection scheme.

Techniques that protect the confidentiality and integrity of the information solve the insecurity of point C. These techniques alter the information exchanged and do not degrade the system's performance [18]. Hence, biometric templates protection (BTP) or biometric information protection (BIP) techniques generate protected information that does not reveal important information about user identity or original biometric information. These techniques use randomly created supplementary information to perform protection; protected information is renewed by revoking and renewing random information. Consequently, random number generators (RNG) must have low computational costs and provide security to applications with biometric systems. Therefore, physical unclonable functions (PUF) are an excellent possibility to generate secure random information [24], [25].

In general, there are protection approaches for biometric systems based on hardware and software, whereas BTP techniques are software-based. Then, a biometric system can implement: 1) liveliness certification; 2) a secure channel between the user interface and processing unit; 3) a specialized hardware processing unit; and 4) BTP techniques with secret and unique RNG on each integrated circuit. Additionally, a biometric system can implement physical isolation of the database, in other words, decentralize the database [26], [27]. Hence, the storage of protected information in the enrollment phase has three forms:

1) *Central or online database*: The protected information of all users is on a single storage device, e.g., cloud storage.
2) *Local or offline database*: Each user has a storage device with their protected information (personal

storage). This device can be a physical token, USB, chip, smart card, key chain, magnetic strip, smart phone, smart watch, bracelet, etc.

3) *Hybrid database*: A percentage of the protected information is stored in a central database and the other portion of information in a local database.

A hybrid database improves security because the information is on several devices, and the control of the information is the partial responsibility of the users. However, the management of revocation of protected information is more straightforward with a central database. On the other hand, hybrid storage uses a private key to decrypt data, avoiding vulnerability when the storage device is compromised.

III. FORMALIZATION OF BIOMETRIC TEMPLATES PROTECTION (BTP) TECHNIQUES

Some biometric traits are not secret and can be obtained without a person's consent, e.g., the voice while having a conversation, the face on a social media photo, or the fingerprint when touching a public object. Therefore, the protected template is information that has been altered or processed using some BTP technique to mitigate the security and privacy threats present in biometric systems during the storage and transfer of information. In addition, BTP techniques allow canceling and renewing the versions of the templates protected in the biometric system, modifying the supplementary information that defines the processing parameters or conditions. Consequently, BTP techniques preserve or enhance the privacy of information while preserving the discriminatory power of biometric traits. Moreover, these techniques seek to guarantee non-repudiation and non-coercion in applications with biometric systems.

Each country must regulate the treatment of biometric information from a legal and technical point of view to ensure the interoperability of recognition systems and the non-linking of biometric data between databases or applications. The protection requirements and specifications for biometric information processing have been standardized internationally by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), establishing two important technical subcommittees:

- ISO/IEC JTC 1/SC 37 - Biometrics: It develops generic biometric standards to support interoperability and data exchange between applications and systems.
- ISO/IEC JTC 1/SC 27 - Information security, cybersecurity, and privacy protection: It sets standards for protecting information and communication technologies (ICT).

The subcommittees mentioned above have defined several standards that address aspects related to biometric systems, such as the ISO/IEC 24745:2022 standard - Biometric information protection, which explains the requirements and recommendations that a processing and BTP scheme must meet in terms of security and privacy:

- *Unlinkability:* Different versions of protected information can be obtained from a user's biometric without any link between them or with some version of another user's protected information, avoiding cross-matching and thus guaranteeing *diversity* in protected information between applications or systems.
- *Revocability and renewability:* A version of the protected information can be revoked or canceled and renewed from the database if it is compromised or has expired.
- *Non-reversibility or Non-invertibility:* The original biometric information must be computationally difficult to recover from the protected data.
- *Performance:* BTP techniques should not degrade unprotected system performance.

Furthermore, the protected template $\mathbf{D} = [\mathbf{PI}, \mathbf{HD}]$ is generated from biometric information extracted $\mathbf{x}$ at the enrollment stage. This protected information has two components: 1) pseudonymous identifier ($\mathbf{PI}$), which is the anonymous and renewable information that acquires the discriminatory power for each user; and 2) auxiliary data or helper data ($\mathbf{HD}$), which is the additional user-specific information used to reconstruct a $\mathbf{PI}'$ in the recognition phase using biometric information of query $\mathbf{x}'$ as illustrated in Fig. 4. The stored information $\mathbf{D}$ is also known as a renewable biometric record; such information is protected by supplementary information $\mathbf{s}$. On the other hand, the decision-making process receives stored $\mathbf{PI}$ and compares it with query $\mathbf{PI}'$. Moreover, $\mathbf{PI}$ and $\mathbf{HD}$ do not reveal important information about the user or the original biometric (anonymity). Therefore, protection techniques should maximize the security, trust, and privacy of data and minimize the cost of storage and transmission of protected information [28], [29].

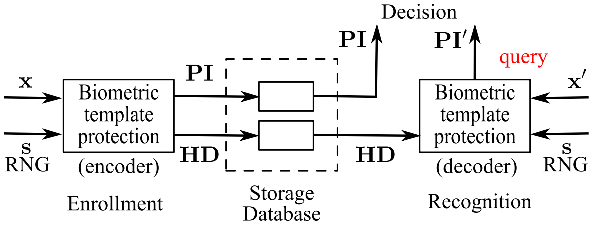


FIGURE 4. Reference architecture for biometric template protection techniques.

Protection techniques use supplementary information in the following way: 1) *user-specific supplementary information*, i.e., each user uses supplementary information unique and independent of other users; and 2) *user-common supplementary information*, i.e., all users use the same system-dependent supplementary information, where the application provider or the biometric system manages random information. Thus, user-specific supplementary information increases the discriminatory power of each user but generates greater complexity and computational cost for generation, storage, and management. Likewise, all supplementary information (common or specific) should be non-public information. Nonetheless, the supplementary information must be different (independent) for each biometric application and service.

A biometric system with BTP techniques needs supplementary information management. Therefore, the biometric system has two databases: 1) protected information; and 2) supplementary information. Consequently, the processing unit stores the user-common supplementary information. In contrast, a central, local, or hybrid database stores user-specific supplementary information [30]. A protection scheme with user-specific management and a local or hybrid database for protected information defines a two- or three-factor recognition model. On the other hand, a protection scheme with user-common management and a central database for protected information establishes a model of a single recognition factor. As a result, a system based on multiple factors increases the difficulty of the success of an attack. Still, it must guarantee the flexibility and comfort of the user in the recognition [28].

The applications, services, or uses of biometric systems with protection schemes must allow non-repudiation, i.e., these link the biometric information and the user's identity as proof of responsibility for the actions performed. Likewise, these applications must guarantee the authenticity of the biometric information through liveness detection [31]. Furthermore, biometric traits are considered personal data. Therefore, biometric systems must comply with the guidelines governing the protection of privacy and the transnational flow of personal data [26]:

1) An application or service should specify the purpose of data collection. In addition, this should limit the data usage to the specified proposition.
2) The regulations, responsibilities, and identity of the personnel responsible for data protection should be open to the public.
3) The collection of personal data should be obtained by lawful means with the knowledge and consent of the user.
4) Personal data should not be available for other purposes except with the user's consent or by the authority of the law.
5) The user can request processes such as deleting, rectifying, completing or modifying the personal data provided.
6) Personal data should be governed by legislation and technical procedures that prevent security and privacy risks, such as unauthorized disclosure or illegal use of data.

IV. BACKGROUND

Traditional user recognition systems are based on non-variable information, e.g., passwords, PINs, tokens, etc. These traditional systems use hash functions to protect the input data, as shown in Fig. 5. Consequently, the first approach to the application of biometrics was inspired by recognition systems based on non-variable information, where biometric traits are used to extract stable features that identify or authenticate users.

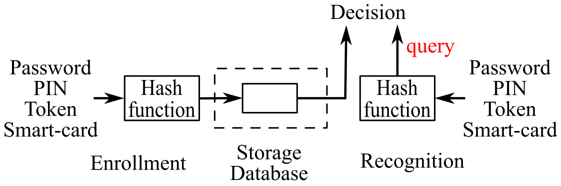


FIGURE 5. Recognition system based on non-variable information.

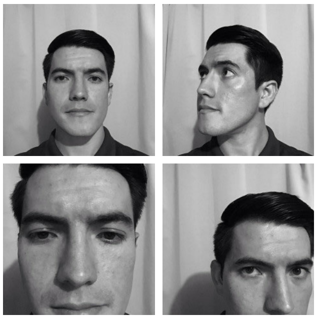


FIGURE 6. Intra-user variability for facial recognition due to the position and angle of the face.

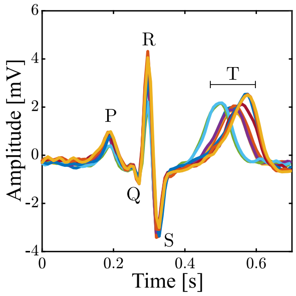


FIGURE 7. Intra-user variability in PQRST complexes due to physical activity or temporary stress [4].

A *hash function* is a one-way mathematical transformation that receives variable-length information and generates fixed-length protected information. The avalanche effect is the principle of operation of hash functions, where a slight change in the input creates significant changes in the output. Therefore, hash functions are ideal for recognition systems based on exact information (non-variable), but these functions face substantial challenges in biometric systems due to intra-user variations (see Fig. 6 and Fig. 7).

Quantification or encoding techniques are frequently used to generate stable keys. Furthermore, personalized hash functions have been developed based on the biometric information of each user, called *robust hash functions* [32], [33] or *kernelized hash functions* [34], [35]. These functions preserve the privacy and discriminatory power of biometric information while addressing intra-user variability. Still, the revocation and renewal capacity depends on the capacity of the quantization technique and the hash function itself. Then, behavioral biometrics allows extending the protected information's revocation and renewal capacity by changing the activity's pattern or action, such as protection schemes based on: 1) a user's voice while speaking a password [36]; 2) dynamic or on-line handwritten signatures [37], [38]; and 3) brain activity responses (EEG) under mathematical calculations, visual stimuli or optical effects [39], [40].

Biometric cryptosystems are the first proposed category of protection techniques [15], [20]. These use renewable keys, error correction codes (ECC), and cryptographic techniques to address intra-user variability and preserve information privacy. In 2001, the concept of cancelable biometrics (CB) proposed protection, privacy, and revocability of biometric information through one-way transformations [41], where renewable random information sets the transformation parameters. Over time, various BTP techniques have been proposed and categorized differently.

Cancelable biometrics and biometric cryptosystems are the two main categories of BTP techniques [17], [19], [21], [22], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53]. Thus, key binding schemes and key generation schemes often integrate the cryptosystems, and transformations and salting schemes are the frequent subcategories in cancelable biometrics. Another technique introduced in biometric cryptosystems is secure multiparty computation, such as homomorphic encryption [42]. Moreover, the digital representation of the biometric information introduced to the protection technique divides the BTP techniques into schemes that support information with discrete distribution and schemes that support information with continuous distribution [54], i.e., protection techniques that operate with integers or binary numbers and protection techniques that receive rational numbers or numbers with fixed-point representation. Previous works discussed below propose different taxonomies and relevant aspects of BTP techniques.

The research developed by [22] analyzes the principle of operation of some biometric cryptosystem techniques based on key release schemes. In addition, this paper discusses the security-level vulnerabilities of biometric systems. On the other hand, [43] reviewed the advances, limitations, and vulnerabilities of cancelable biometrics. Also, this work analyzes different techniques of cancelable biometrics, such as non-invertible geometric transformations, random projections, correlation filters, BioConvolving, Bloom filters, knowledge signatures, BioHashing, random permutations, salting methods, and hybrid methods.

The work published by [46] performs a systematic literature review of approaches and modalities of BTP techniques between 2005 and 2016. This paper presents a taxonomy with four categories: 1) cancelable biometrics with techniques such as geometric transforms, robust hashing, random projections, biometric filters, random permutations, and BioHashing; 2) biometric cryptosystems with techniques such as biometric encryption, fuzzy commitment, fuzzy vault, quantization schemes, and secure sketch; 3) hybrid methods; and 4) homomorphic encryption. In addition, this paper reports that 49% of the literature reviewed uses cancelable biometrics, 35% cryptosystems, 8% homomorphic encryption, and 8% hybrid methods. Likewise, 44% of the BTP schemes developed use fingerprint, 21% iris, 12% face, 10% signature, 5% multibiometrics, 4% palmprint, 3% voice, and 1% finger vein traits. Finally, this paper highlights that most of the investigations on BTP techniques are developed for small and midsize databases; therefore, analyzing these techniques on more extensive databases is challenging.

The research presented by [17] performs a comprehensive survey of attacks and protection techniques for biometric systems. This paper presents a taxonomy consisting of: 1) cryptography-based methods such as visual cryptography, image hashing, knowledge signature, elliptic curve cryptography, chaos, steganography, fuzzy commitment, fuzzy vault, and Hill cipher; 2) transformation-based methods with techniques such as non-invertible transformation, partial Hadamard transformation, and random projection; 3) filter-based methods; 4) hybrid methods; 5) multimodal-based methods; and 6) other methods such as BioConvolving, random permutations, deep learning, etc. Furthermore, this work proposes to improve the performance rate, time, and computational cost of BTP techniques as a future challenge.

Finally, [19] discussed problems related to biometric systems and provided state of the art for various protection techniques with different biometric traits. In addition, this paper proposes a taxonomy categorized into: 1) biometric cryptosystems; 2) feature transformations; 3) homomorphic encryption; 4) visual cryptography; 5) hybrid methods; and 6) steganography and watermarking-based approaches. Likewise, this article highlights: 1) the dominance of authentication systems compared to identification systems; 2) feature extraction using deep learning techniques to address alignment issues and intra-user variability; and 3) the need to develop biometric protection systems and adaptive biometric systems for low-cost devices as a future challenge.

Table 1 illustrates a comparative analysis of proposed taxonomies, analysis of evaluation metrics, and contributions made by previous surveys and reviews in BTP. This comparative analysis concludes that the principle of operation of the protection techniques has been the primary criterion for classifying the different techniques; some of these taxonomies differ in the classification of some techniques, as shown in the second column of Table 1. Therefore, one of this work's contributions is proposing a novel taxonomy for BTP techniques based not only on the principle of operation but also on the type of supplementary information supported by each technique. In addition, the taxonomy proposed in this paper considers whether the BTP technique allows decision-making or not in the protected/transformed domain. In particular, the latest review of the systematic literature corresponds to the research published by [46] in 2017, where a protocol for searching and selecting relevant information on

BTP techniques was defined. Still, this review did not cover the evaluation metrics of protection techniques.

The third column of Table 1 highlights the investigations that have contributed to the analysis and study of evaluation metrics for BTP techniques. These works qualitatively suggest some metrics but not a clear, practical, and complete mathematical formulation, i.e., a mathematical formulation based on the variance and correlation of random templates and not on the probability estimation function of random templates. For example, the research developed in [42] suggests: 1) privacy leakage (unlinkability) through mutual information; 2) the successful attack rate (SAR) with SAR $\geq$ FAR; and 3) storage requirements. Likewise, the paper published in [44] qualitatively recommends: 1) non-invertibility through normalized Shannon conditional entropy; and 2) unlinkability through mutual information. In addition, the authors in [45] also guide qualitatively: 1) non-invertibility through conditional Shannon entropy; 2) non-linkability through privacy leakage with mutual information; 3) revocability condition; 4) computational complexity through processing speed; and 5) storage requirements. On the other hand, the survey developed in [17] defines quantitatively: 1) linear correlation through the co-relational coefficient and co-relation index; 2) efficiency; and (3) template capacity (revocability). Furthermore, this work also qualitatively suggested diversity or unlinkability through mutual information but did not define how to measure irreversibility. Finally, the study developed in [50] qualitatively recommends: 1) non-invertibility through the probability of an imposter obtaining the original template; 2) unlinkability through mutual information; and 3) performance or usability (efficacy) in a quantitative way.

A. CHALLENGES IDENTIFIED FOR BTP

On the other hand, the Table 1 summarizes our systematic literature review, which identifies three significant challenges in the field of BTP:

1) ALIGNMENT-FREE PROTECTION TECHNIQUES

The first challenge corresponds to the degradation of the recognition rate by BTP techniques due to intra-user variations. To date, the appropriate selection of pre-processing, feature extraction, and decision-making techniques face this challenge; the above process is called the biometric alignment method. However, this way of facing this challenge demands a great computational effort. Moreover, it is not always compatible with achieving a reasonable recognition rate through the protection technique implemented. Therefore, the challenge of facing the intra-user variations, protecting and revoking the information, and not degrading the recognition rate through the same processing technique needs a solution. In particular, the iris, face, and fingerprint are the most advanced biometric traits in this challenge by implementing adaptive Bloom filters [49] because they are biometric traits acquired in two dimensions. Therefore, deep learning techniques and adaptive systems in a dynamic environment are possible general solutions to this challenge.

2) RE-TRAINING

This challenge avoids re-training or re-definition of the parameters of the decision-making strategies when a new cancelation or renewal of the protected information is performed. Previous investigations only analyzed protection systems for a single revocation of protected templates. The re-training of the decision-making parameters demands time and computational effort depending on the length of the protected information and the number of users enrolled in the biometric system. Therefore, the analysis of BTP techniques that do not degrade the recognition rate and do not demand re-training at each revocation is necessary.

3) QUANTITATIVE EVALUATION METRICS

This challenge refers to the mathematical formulation of evaluation metrics based on random templates' variance and correlation coefficients. These metrics should quantify: unlinkability (diversity), non-invertibility, storage cost, and efficiency of BTP techniques under a given number of cancelations (revocations) and users.

V. LITERATURE REVIEW PROTOCOL ON BTP TECHNIQUES

A systematic literature review (SLR) identifies, evaluates, and interprets all relevant research for a set of research questions or topics of interest [55]. Therefore, this systematic literature review aims to: 1) summarize the existing evidence on BTP techniques in a detailed and unbiased manner; and 2) identify some gaps in BTP to provide an overview for future research. Consequently, these purposes inspire the following research questions based on the qualitative approach that this document seeks to answer:

- What are the BTP techniques that currently exist?
- What are the taxonomies of BTP techniques in the background?
- What are the aspects of security, privacy, revocability, renewability, computational complexity, biometric information distribution, and open challenges for existing BTP techniques?
- How could the different BTP techniques be classified according to their principle of operation and the type of supplementary information supported?

A. SEARCH STRATEGY

The protocol for the systematic literature review on BTP techniques established a search strategy based on the following search criteria for investigations written in English in the last decade.

1) DATABASES FOR LITERATURE REVIEW

The following digital databases were used to search for investigations on BTP techniques:

- IEEE Xplore Digital Library.
- ACM Digital Library.

TABLE 1. Comparative analysis of previous surveys and reviews in the area of BTP.

Research	Taxonomy	Evaluation metrics	Contributions
Rathgeb et al. [22] (2011)	**1) Biometric cryptosystems:** • Key binding (biometric encryption, fuzzy commitment, shielding functions, and fuzzy vault) • Key generation (private template and quantization); **2) Cancelable biometrics:** • Non-invertible transforms • Salting (BioHashing and BioPhasor); and **3) Multi-biometric and hybrid schemes**.	No	▶ Presents a comprehensive survey of biometric cryptosystems and cancelable biometrics. ▶ Proposes a taxonomy based on the principle of operation of protection techniques. ▶ Analyzes the potential points of attack in biometric systems. ▶ Presents state of the art for BTP techniques with various biometric features.
Rane et al. [42] (2013)	**1)** Fuzzy commitment; **2)** Secure sketch; **3)** Secure multiparty computation (homomorphic encryption); and **4)** Cancelable biometrics.	Yes	▶ Presents an overview of BTP methods. ▶ Qualitatively analyze performance measures for BTP techniques. ▶ Introduces homomorphic encryption as a new BTP technique.
Patel et at. [43] (2015)	**1) Cancelable biometrics:** • Noninvertible geometric transforms (cartesian, polar, and functional) • Random projection (Gaussian, Bernoulli, and sectored) • Cancelable biometric filters • BioConvolving • Bloom filters • Knowledge signature • BioHashing • Random permutations • Salting methods • Hybrid methods.	No	▶ Develops a general review of various cancelable biometrics schemes, analyzing their strengths and weaknesses. ▶ Proposes a categorization based on the protection techniques' operation principle. ▶ Categorizes the protection techniques according to the matcher used: conventional or special. ▶ Analyzes the vulnerabilities of a standard biometric system.
Natgunanathan et al. [45] (2016)	**1) Biometric encryption:** • Key binding (fuzzy commitment and fuzzy vault) • Key generation (quatization methods and fuzzy extractor); **2) Cancelable biometric:** • BioHashing • Non-invertible transforms; **3) Multi-modal and hybrid schemes**; and **4) Secure computation** (Homomorphic encryption and garbled circuits).	Yes	▶ Presents a general review of privacy-preserving biometric schemes (PPBS). ▶ Proposes a categorization of PPBS according to their principles of operation. ▶ Analyzes performance measures in a qualitative way for PPBS.
Sandhya et al. [46] (2017)	**1) Cancelable biometrics:** • Salting (BioHashing) • Non-invertible transforms (geometric transforms, robust hashing, random projection, biometric filters, and random permutation); **2) Biometric Cryptosystems:** • Key binding (biometric encryption, fuzzy commitment, and fuzzy vault) • Key generation (quantization schemes and secure sketch); **3) Hybrid methods**; and **4) Homomorphic encryption**.	No	▶ Presents a systematic literature review of BTP techniques under a search methodology. ▶ Proposes a novel taxonomy based on the principle of operation of BTP techniques. ▶ Provides a state of the art of protection techniques. ▶ Analyzes the participation (percentage) of each biometric trait in BTP techniques. ▶ Lists the research communities active in the development of BTP techniques. ▶ Provides a general overview of biometric trait databases for developing and evaluating protection techniques.
Choudhury et al. [47] (2018)	**1) Cancelable biometrics:** • Salting scheme • Non-invertible transformation (geometric transforms, random projection, cancelable biometric filters, BioHashing, permutation, BioConvolving, and Bloom filters); **2) Biometric cryptosystems:** • Key binding • Key generation; and **3) Hybrid techinques**.	No	▶ Presents a survey and a state-of-the-art of different cancelable biometric schemes. ▶ Studies standard biometric systems with different biometric traits. ▶ Analyzes the security and privacy vulnerabilities of biometric systems and proposes countermeasures. ▶ Develops a novel method of cancelable iris biometrics based on discrete cosine transformation (DCT) and Huffman encoding. ▶ Proposes taxonomy based on the principle of BTP techniques.
Manisha and Kumar N. [17] (2020)	**1) Cryptography based methods** (visual cryptography, image hashing/BioHashing, knowledge signature, elliptic curve cryptography, chaos, steganography, fuzzy commitment, and Hill cipher); **2) Non invertible Transformacions** (cartesian, polar and functional transforms, Hadamard transform, and random projection / sectored / dynamic / sparse); **3) Filter based methods**; **4) Hybrid schemes**; **5) Multimodal schemes**; and **6) Other methods** (BioConvolving, permutations, salting methods, deep learning, watermarking, etc.)	Yes	▶ Presents a comprehensive survey of cancelable biometrics techniques. ▶ Proposes a novel taxonomy based on the principle of operation of cancelable biometrics techniques. ▶ Reviews various performance measures used in cancelable biometrics. ▶ Analyzes the vulnerabilities of biometric systems. ▶ Presents a review of the available databases for biometric systems. ▶ Introduces deep learning in the creation of secure templates. ▶ Reports some evaluation metrics for BTP techniques but does not analyze irreversibility.
Sarkar et al. [19] (2020)	**1) Biometric cryptosystems:** • Key binding (fuzzy commitment and fuzzy vault) • Key generation (fuzzy extractor and secure sketch); **2) Feature transformations:** • Cancelable biometrics • Salting; **3) Homomorphic encryption**; **4) Visual cryptograhy**; **5) Hybrid methods**; and **6) Other methods** (Steganography and watermarking).	No	▶ Presents a review of BTP schemes in authentication systems, analyzing their advantages and disadvantages. ▶ Analyzes biometric systems' security concerns and privacy threats, proposing countermeasures. ▶ Presents a categorization of BTP techniques according to their principle of operation.
Singh et al. [50] (2020)	**1) Biometric cryptosystems:** • Key binding • Key generation; and **2) Cancelable biometrics:** • Non-invertible transforms (Random projection, BioHashing, geometric transform, Bloom filter, Cuckoo filter, and Morton filter) • Biometric salting (random noise, random permutation, and random convolution).	Yes	▶ Presents a comprehensive survey of cancelable biometrics techniques, analyzing their advantages and limitations. ▶ Proposes a categorization based on the principle of operation of BTP techniques. ▶ Analyzes security metrics for cancelable biometrics techniques. ▶ Introduces the evolution of Bloom filters: Cuckoo and Morton filters. ▶ Develops a protection scheme for finger dorsal using BioHashing.

- Google Scholar.
- ScienceDirect.
- SpringerLink.
- Hindawi Publishing Corporation.

2) SEARCH STRINGS

The keywords used in the search strategy are: 1) biometric or biometrics; 2) protection; 3) security; 4) privacy; 5) cancellable or cancelable; 6) review; and 7) survey.

3) SEARCH TERM COMBINATION

Search terms were combined to define the following search formula anywhere in a document: *(((biometric* OR *biometrics)* AND *((protection* OR *(security* OR *privacy))* OR *(cancellable* OR *cancelable))))* AND *(review* OR *survey))*. Figure 1 shows an example of documents published under this search function between 2010 and 2021 in the Elsevier abstract and citation database (Scopus).

4) INCLUSION CRITERIA

The included investigations developed the idea of a scheme, method, technique, or protection solution for the privacy and security of biometric information regardless of the biometric trait. Sources included are review and research articles in journals, conference papers, magazine documents, and book chapters.

B. LITERATURE REVIEW METHODOLOGY

The review protocol based on the search criteria identifies 377 relevant documents. On the other hand, the selection criteria are based on: 1) documents that satisfy the inclusion criteria; and 2) documents that contain background, the principle of operation, and strengths and weaknesses of some BTP technique or idea. Therefore, the result of the first stage of exclusion corresponds to 229 documents that meet the selection criteria based on the information extracted from the title, summary, and conclusions of the documents. Likewise, the second and last stage of exclusion based on the synthesis of the full texts corresponds to 174 documents that satisfy the selection criteria and help to answer the research questions proposed for this SLR.

C. CONTRIBUTIONS FROM THIS SLR

According to the *CASP systematic review checklist*, the search strategy and literature review methodology guide the correct type of documents that contributed to the purposes of this review. As a result, the following sections show the synthesis of the extracted data. This synthesis contributes to the existing literature in the following:

1) A novel taxonomy is proposed through the principle of operation and type of supplementary information supported by BTP techniques, i.e., techniques that support user-common or user-specific supplementary information and techniques that support only user-specific supplementary information. In addition, the computational complexity, revocation and renewal capacity, security and privacy characteristics, decision-making in the protected domain or not, and some examples are discussed in each technique of this taxonomy. Furthermore, the protection technique called intrinsic artifacts is introduced as a protection technique that supports only user-specific supplementary information corresponding to the subcategory of salting schemes. Finally, subcategories of protection schemes based on modern cryptography are also presented.
2) The category of protection schemes based on machine learning or deep learning is introduced as an alignment-free protection scheme to deal with the degradation of the recognition rate through BTP techniques due to intra-user variations.
3) The importance of protection techniques based on linear and injective mappings is identified and highlighted to avoid the degradation of the recognition rate and the re-training of the decision-making parameters when a new cancelation or renewal of the protected information is performed.
4) A quantitative formulation of evaluation metrics to compare the performance of BTP techniques is proposed. These metrics quantify the efficiency under various cancelations and renewals, the cost of storage for a given number of users, the capacity of revocations and renewals, unlinkability, non-invertibility, and interoperability supported by the protection techniques.

VI. TAXONOMY OF BTP TECHNIQUES

Biometric information protection is based on hardware, software (digital processing), or both. Section II discussed some hardware-level countermeasures. Therefore, this section proposes a novel taxonomy for protection techniques at the digital processing level. Thus, this categorization results from synthesizing and analyzing the information selected in the systematic literature review.

The taxonomy proposed for this research contains five categories, as shown in Fig. 8: 1) biometric cryptosystems; 2) cancelable biometrics; 3) protection schemes based on machine learning or deep learning; 4) hybrid protection schemes; and 5) multibiometric protection schemes. Nonetheless, this taxonomy is based on the principle of operation of the biometric template protection module in Fig. 3 and the type of random supplementary information used for protection (see section III). Moreover, the taxonomy also considers the domain of operation (protected or unprotected) of the decision-making module and the distribution of the input biometric information in the feature domain or the signal domain.

Biometric cryptosystems and cancelable biometrics are the main categories of BTP techniques, as shown in Fig. 8. As a result, the Table 2 highlights the main differences between the proposed categories or families of protection techniques through the analysis of: 1) the principle of operation; 2) the type of supplementary information supported; 3) the distribution of the input information; and 4) the domain of operation

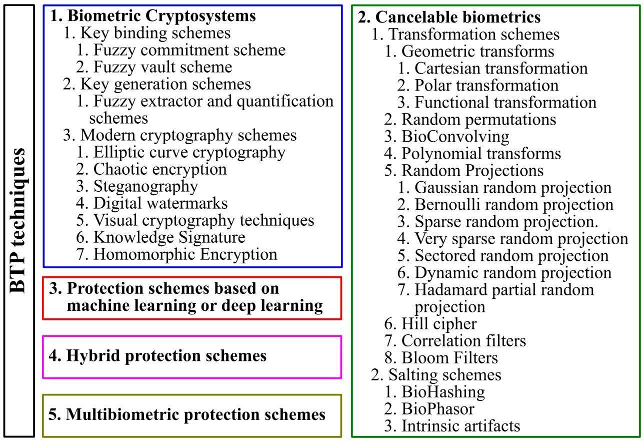

BTP techniques
1. Biometric Cryptosystems
1. Key binding schemes
1. Fuzzy commitment scheme
2. Fuzzy vault scheme
2. Key generation schemes
1. Fuzzy extractor and quantification schemes
3. Modern cryptography schemes
1. Elliptic curve cryptography
2. Chaotic encryption
3. Steganography
4. Digital watermarks
5. Visual cryptography techniques
6. Knowledge Signature
7. Homomorphic Encryption
3. Protection schemes based on machine learning or deep learning
4. Hybrid protection schemes
5. Multibiometric protection schemes
2. Cancelable biometrics
1. Transformation schemes
1. Geometric transforms
1. Cartesian transformation
2. Polar transformation
3. Functional transformation
2. Random permutations
3. BioConvolving
4. Polynomial transforms
5. Random Projections
1. Gaussian random projection
2. Bernoulli random projection
3. Sparse random projection.
4. Very sparse random projection
5. Sectored random projection
6. Dynamic random projection
7. Hadamard partial random projection
6. Hill cipher
7. Correlation filters
8. Bloom Filters
2. Salting schemes
1. BioHashing
2. BioPhasor
3. Intrinsic artifacts

FIGURE 8. Taxonomy of biometric template protection techniques.

of the decision-making module. For example, biometric cryptosystems protect information using cryptographic primitives and error-correcting codes. Therefore, most of their techniques require input information in a finite field or discrete distribution, e.g., integers. In addition, all biometric cryptosystem techniques do not allow decision-making in the protected domain, but all techniques support user-common and user-specific supplementary information.

Nonetheless, the principle of operation of cancelable biometrics is based on injective or non-injective transformations. For this reason, all cancelable biometrics techniques support the rational representation of the input data, i.e., continuous distribution. Likewise, all cancelable biometrics techniques allow decision-making in the protected domain, but all cancelable biometrics techniques do not support user-common supplementary information, e.g., salting schemes.

Anyway, biometric systems can use machine learning and deep learning algorithms in the feature extraction and decision-making modules, where a biometric cryptosystems technique or cancelable biometrics protects the biometric information. For this reason, a new family of protection techniques is defined when the BTP module specifically implements machine or deep learning algorithms. Consequently, protection techniques or schemes based on machine learning or deep learning face the alignment-free protection technique challenge (see section IV). The principle of operation of these techniques is based on machine learning or deep learning algorithms to protect information by renewable supplementary information. Additionally, these techniques aim to extract features in the face of intra-user variability, make the decision in the protected domain and allow the revocation of the protected information. Furthermore, these techniques allow input information with continuous or discrete distribution. Moreover, these techniques support user-common and user-specific supplementary information.

On the other hand, the principle of operation of hybrid protection schemes uses more than one protection technique with one biometric trait or several traits. However, the principle of operation of multibiometric protection schemes uses more than one biometric trait with one protection technique or several techniques for each biometric trait. Therefore, all multibiometric protection schemes are hybrid schemes, but not all hybrid schemes are multibiometric schemes.

Defining the best protection technique is challenging because it depends mainly on the purpose, needs, constraints, and specifications of the biometric service or application to be developed. For this reason, section XII summarizes the most important characteristics of the protection techniques employing the Table 3. In addition, section XIII complements the comparison shown in Table 3. Therefore, the summary of the different protection techniques and the quantitative evaluation measures provide a better overview to select the most suitable protection technique for the desired biometric system.

The following sections present and describe the protection techniques for the proposed categories. For each defined BTP technique, the following is explained: 1) operating principle; 2) security and privacy characteristics; 3) computational complexity; and 4) revocation and renewal capacity. In addition, some relevant examples with different biometrics are mentioned for each technique.

VII. BIOMETRIC CRYPTOSYSTEMS

The word cryptosystem is an abbreviation of the term *cryptographic system*. A cryptographic system guarantees the security of the information exchanged using cryptographic techniques. Hence, biometric cryptosystems offer protection for biometric information through encryption/decryption schemes or biometric-dependent key-release schemes. Therefore, a biometric-dependent key-release scheme aims to recover or rebuild a secret key from **HD** and biometric information of query.

Biometric cryptosystems are composed of two shielding or processing functions; one function in the enrollment phase gives security to information, and another function in the recognition phase reveals and takes advantage of protected information. Then, biometric cryptosystems are divided into three categories: 1) key binding schemes; 2) key generation schemes; and 3) modern cryptography schemes.

In summary, the main advantage of biometric cryptosystems in the security and privacy of original information corresponds to the complexity of encryption schemes, specifically in transmitting and storing data through an insecure communication channel, as shown in Table 2. In other words, the security and privacy of the original information depend on the information revealed from **HD** in the key binding and key generation schemes. Consequently, one difference in information security and privacy is that cancelable biometrics techniques do not generate helper data. Additionally, most biometric cryptosystem techniques based on modern cryptography schemes do not allow decision-making in the protected domain, causing a security and privacy vulnerability of the original information. This vulnerability is the main

TABLE 2. Characteristics and differences between the categories of BTP techniques.

Category	Principle of operation	Supplementary information supported	Distribution of input information	Operational domain of decision-making
Biometric cryptosystems	Cryptographic primitives, error-correcting code, and modern cryptography.	All techniques support user-common and user-specific supplementary information.	Some techniques need input information with discrete distribution.	All techniques do not allow for decision-making in the protected domain.
Cancelable Biometrics	Injective and non-injective transformations.	Some techniques support user-common and user-specific supplementary information (transformation schemes). But other techniques only support user-specific supplementary information (salting schemes).	All techniques support input information with continuous and discrete distribution.	All the techniques allow for decision-making in the protected domain.
Protection schemes based on machine learning or deep learning	Machine learning or deep learning algorithms.	These techniques support user-common and user-specific supplementary information.	These techniques allow input information with continuous or discrete distribution.	These techniques allow for decision-making in the protected domain.
Hybrid protection schemes	It depends on the combined techniques.			
Multibiometric protection schemes	It depends on the technique used or the combined techniques.			

difference with cancelable biometrics techniques. Hence, signature knowledge schemes and homomorphic encryption schemes are presented to solve this vulnerability in biometric cryptosystems.

A. KEY BINDING SCHEMES

A key binding scheme is when **HD** is obtained by binding a secret key to a biometric template, with the key independent of the template. A key binding scheme is associated with an error correction code (ECC), and the tolerance to intra-user variations depends on the ECC's capacity. In addition, the security of these schemes depends on the level of information revealed by **HD**.

1) FUZZY COMMITMENT SCHEME

This scheme combines ECC and cryptography (hash functions) to make the system more tolerant to intra-user variations [56]. The information processed by this scheme has a binary representation of length $n \in \mathbb{N}^{+}$.

The binding process is based on the idea of *commit*: 1) a binary codeword $\mathbf{c}$ generated by an ECC applied to a secret digital key $\mathbf{s}$ of n bits; 2) binary biometric information or witness $\mathbf{x}$ represented in n bits; and 3) a off-set or difference vector $\boldsymbol{\delta}$, such that, $\mathbf{x} = \mathbf{c} \oplus \boldsymbol{\delta}$, under the constraint that the enrollment template $\mathbf{x}$ and query $\mathbf{x}'$ have sufficient similarity through the Hamming distance, i.e., $\text{dist}(\mathbf{x}, \mathbf{x}') \leq \tau$, being τ the similarity threshold. Under these constraints, the scheme should be able to reconstruct in the recognition phase the codeword $\mathbf{c}'$ using $\boldsymbol{\delta}$ and $\mathbf{x}'$, as shown in Fig. 9.

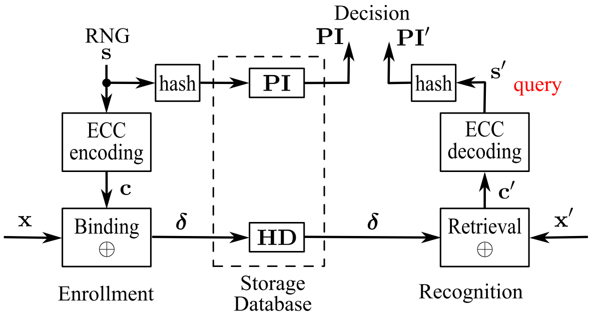


FIGURE 9. Operation mode of fuzzy commitment scheme.

The helper data in the scheme illustrated in Fig. 9 corresponds to the off-set or difference vector, and the pseudonymous identifier is the result of applying a hash function to the linked secret digital key $\mathbf{s}$, i.e., the protected information stored is $\mathbf{D} = [\text{hash}(\mathbf{s}), \boldsymbol{\delta}]$. Revocation and renewal of protected information are done by generating a new key and changing the ECC or hash function parameters. Usually, the cancelation and renewal capacity of the protected templates $\mathbf{D}$ depends on the number of keys that the associated RNG can produce. Therefore, this scheme allows only authentication systems because it is a key-release scheme.

This protection technique receives biometric information with a discrete probability distribution; this is a challenge due to intra-user variations and discretization resolution. Furthermore, this technique has no tolerance for variation in the order of the biometric information. On the other hand, this protection scheme has a medium computational complexity due to the ECC and the hash function. Some examples of biometric systems with fuzzy commitment-based protection are mentioned below.

A fuzzy commitment scheme for iris authentication was developed by [57], using Hadamard and Reed-Solomon's ECC. Furthermore, a system for handwritten signature authentication was developed by [58], using BCH code and SHA-1 as a hash function. In the authentication with fingerprint, a scheme was proposed by [59], using turbo codes and defining a representation known as binarized phase spectrum (BiPS). Likewise, [60] proposed a face authentication scheme using BCH code. Also, [61] developed a voice authentication scheme using the ECC of Hadamard. On the other hand, [62] proposed a palmprint authentication system using the ECC of Reed-Solomon. Similarly, an authentication scheme based on finger veins was developed by [63], using BCH code in mobile healthcare data protection. Finally, [64] proposed an authentication scheme with EEG signals using BCH code.

2) FUZZY VAULT SCHEME

This scheme uses an unordered set $\mathcal{A}$ (order invariance) of elements in a public universe $\mathcal{U}$ and a secret $\mathbf{s}$ to generate a locked vault $\mathbf{V}$. Then, an unordered set $\mathcal{B}$ of equal length and similar to $\mathcal{A}$ allows unlocking the vault and retrieving $\mathbf{s}$ [65]. The secret $\mathbf{s}$ is a row vector with a binary representation of length $n \in \mathbb{N}^+$, and an ECC uses this to construct a codeword $\mathbf{c}$. On the other hand, $\mathcal{A}$ and $\mathcal{B}$ elements have a continuous probability distribution.

This scheme performs a polynomial encoding by constructing the coefficients of a polynomial P from $\mathbf{c}$. Later, the created polynomial projects the elements of $\mathcal{A}$. Then, chaff points are added to confuse the genuine projection. The genuine projection points and the chaff points define the fuzzy vault $\mathbf{V}$, equivalent to the helper data. On the other hand, the pseudonymous identifier results from a hash function applied to the secret $\mathbf{s}$. Therefore, the protected information stored is $\mathbf{D} = [\text{hash}(\mathbf{s}), \mathbf{V}]$. In the recognition phase, the fuzzy vault and $\mathcal{B}$ elements allow the reconstruction of the polynomial P' and the secret $\mathbf{s}'$, as shown in Fig. 10. Polynomial interpolation techniques and ECCs recover the secret.

The security of this scheme depends on the infeasibility of the polynomial reconstruction, the degree of the polynomial, and the number of chaff points. The number of chaff points should be much larger than the number of points projected from the biometric. In addition, this scheme is invariant to the order of the information. Still, it does not guarantee security and privacy against attacks via record multiplicity, surreptitious key-inversion attacks, and blended substitution attacks [66]. Furthermore, the capacity to cancel and renew depends on the power of the RNG to create new keys and chaff points; the polynomial order can also be changed. Likewise, this protection technique has medium computational complexity due to the ECC and hash function. Lastly, this scheme only allows authentication systems because it is a key-release scheme.

Some examples of fuzzy vault schemes for biometric authentication systems using cyclic redundancy check (CRC) code and Lagrange interpolation were developed for fingerprint [67], handwritten signature [68], palmprint [69], or with multiple biometric traits such as fingerprint, palmprint, iris and hand veins [70]. On the other hand, an iris authentication scheme was developed by [71], using the ECC of Reed-Solomon and Lagrange interpolation. In addition, [72] developed a fuzzy vault scheme for authentication with fingerprint and password (two-factor recognition), performing a transformation to the biometric data based on the password; the password is independent of the key or secret used to build the vault.

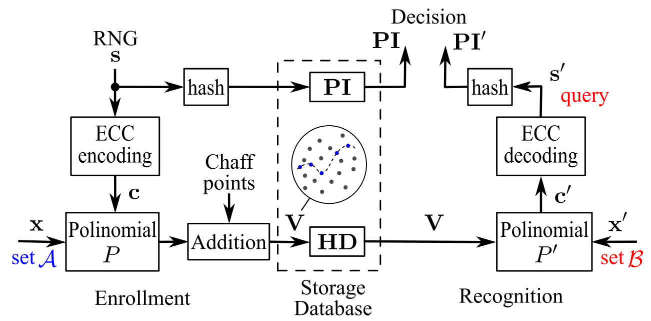


FIGURE 10. Operation mode of fuzzy vault scheme.

B. KEY GENERATION SCHEMES

A key generation scheme is when **HD** is obtained only from the biometric template. These schemes are not very tolerant of intra-user variations. Therefore, stable keys with high entropy are challenging to generate. These schemes use user-specific quantification or coding techniques. Furthermore, security depends on the level of information revealed by **HD**.

1) FUZZY EXTRACTOR AND QUANTIFICATION SCHEMES

A fuzzy extractor is a key generation scheme to combat intra-user variability. Therefore, this scheme generates a uniform random key $\boldsymbol{\lambda}$ of n bits and helper data $\boldsymbol{\Omega}$ from the biometric trait of each user. Then, a secure sketch is a function that produces $\boldsymbol{\Omega}$, revealing little biometric information. In general, few secure sketches use data from an RNG. However, the helper data reconstructs the key from a biometric query $\mathbf{x}'$ very similar to the biometric enrollment $\mathbf{x}$. Besides, the generated secret keys are frequently used in cryptographic systems [73].

Techniques of coding, quantization, discretization, or interval mapping transform biometric data into a representation with a discrete probability distribution. This transformation preserves the class distribution and differentiating power of the original information. Key generation techniques define stable conditions or intervals to perform binary encoding. Therefore, **PI** results from a hash function applied to the key generated $\boldsymbol{\lambda}$ in the enrollment phase. Nevertheless, **HD** corresponds to the information $\boldsymbol{\Omega}$ on each user's specific limits, conditions, or quantification intervals to obtain the stable key in the recognition phase. Fig. 11 illustrates that the query information and helper data obtain the key in the recognition phase. Hence, the protected information stored is $\mathbf{D} = [\text{hash}(\boldsymbol{\lambda}), \boldsymbol{\Omega}]$. To avoid the collision, the generated keys and hash functions must be pairwise independent. Eventually, the quality of the keys depends on the amount of discriminatory information extracted from the biometric information [74].

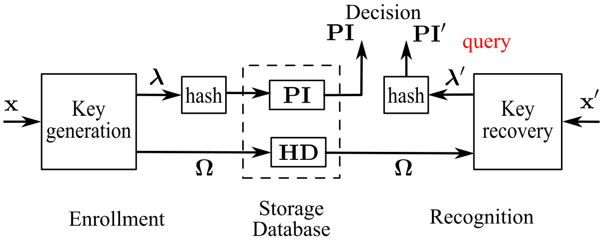


FIGURE 11. Operation mode of fuzzy extractor.

Generally, these schemes suffer from a loss of discrimination power due to the quantization process. Therefore, these schemes degrade the recognition rate. Furthermore, changing the parameters (specifications) of encoding or quantification generates revocation and renewal of the protected information. Nevertheless, this process suffers from the problem of key entropy, i.e., a limited number of keys or forms of quantification. In short, generating keys with high stability and entropy is difficult. Additionally, the storage cost of **HD** is high; for this reason, the storage of user-specific data is based on two- or three-factor recognition schemes. Then, the computational cost of this technique is medium due to the user-specific quantization and the hash function. Finally, the fuzzy extractors protect authentication and identification systems.

The methods and specifications of encoding or quantification depend primarily on the biometric trait. Thus, quantification schemes with equal probability, frequency, and optimized intervals have been proposed, such as the biometric quantification for fingerprint and face presented by [75] called detection rate optimized bit allocation (DROBA). This quantization transforms the actual value of the extracted features into a binary string of fixed length, assigning more bits to the more discriminative features and fewer bits to the less discriminatory features. This transformation maximizes the probability that all features are in genuine intervals, but this task is computationally complex.

A fuzzy extractor for face authentication was developed by [76], using the quantization of specific ranges between the minimum and maximum value of the features extracted from each user. On the other hand, [77] presented a fingerprint authentication system, creating a binary representation through the Gabor filter and a quantification defined by statistical analysis. Furthermore, an iris authentication system based on interval-mapping techniques was proposed by [78]. Moreover, [79] published an authentication system with feature-level fusion for fingerprint and palmprint using a 2^n discretization, which divides the probability density function of features into 2^n intervals with equal probability of occurrence and encodes each interval with n bits.

A key generation method from the pronunciation of a password was proposed by [36], where the features extracted from the voice are quantified, encoded, and used as a look-up table for authentication. Likewise, [80] developed another key generation method, generating keys from facial recognition through binarizing the features within the region $[\mu - \sigma, \mu + \sigma]$ defined by the mean μ and standard deviation σ of the distribution of authentic features and the overall distribution of features. Furthermore, [81] published a fingerprint-based key generation scheme using interval encoding and a two-layer error-correcting technique (Hadamard code with Reed-Solomon code). Other widely used discretization techniques to generate binary keys are local binary pattern (LBP) and local ternary pattern (LTP). Nonetheless, the examples of key generation schemes discussed above have a limited revocation and renewal capacity.

C. MODERN CRYPTOGRAPHY SCHEMES

Modern cryptographic schemes provide secret and secure communication through an insecure channel between a client and a server using encryption and decryption. The encryption stage uses a key $\mathbf{s}_e$ to convert the information $\mathbf{x}$ into incomprehensible and secure information, i.e., $\boldsymbol{\omega} = \text{enc}(\mathbf{x}, \mathbf{s}_e) = \xi(\mathbf{x})$. In contrast, the decryption stage uses a key $\mathbf{s}_d$ to recover the original information sent. Therefore, the most common encryption schemes are:

- *Symmetric cryptography:* It uses a single private key for encryption and decryption, i.e., $\mathbf{s}_e = \mathbf{s}_d$. This cryptography enhances the privacy and confidentiality of information. The most used algorithms are advanced encryption standard (AES) and data encryption standard (DES).
- *Asymmetric cryptography:* It uses one key for encryption and another for decryption, i.e., $\mathbf{s}_e \neq \mathbf{s}_d$, where one key is public and the other is private. This cryptography guarantees the authenticity and non-repudiation of the information. These algorithms are based on: 1) factorization of large prime numbers as the RSA algorithm; 2) discrete logarithm as the ElGamal or Diffie-Hellman key exchange algorithm; and 3) elliptic curves as the elliptic curve cryptography.

The keys of an asymmetric system are longer than the keys of a symmetric design. Furthermore, symmetric cryptography has a higher execution speed and lower computational effort than asymmetric cryptography. However, asymmetric cryptography authenticates information using more efficient digital signatures [82]. A digital signature is a mathematical technique used to validate the authenticity, non-repudiation, and integrity of digital information in public key infrastructure (PKI); this signature depends on some secret information known only to the signer and is associated with an authentication system. Therefore, digital signatures employ asymmetric cryptography and are often used to implement electronic signatures; a standard algorithm is the digital signature algorithm (DSA).

In an encryption and decryption scheme, **PI** is the data encrypted in the enrollment phase, and **HD** is the decryption key used in the recognition phase. Consequently, the protected information stored is $\mathbf{D} = [\xi(\mathbf{x}), \mathbf{s}_d]$. Furthermore, the decryption key can be user-specific or user-common and stored in a central, local, or hybrid database.

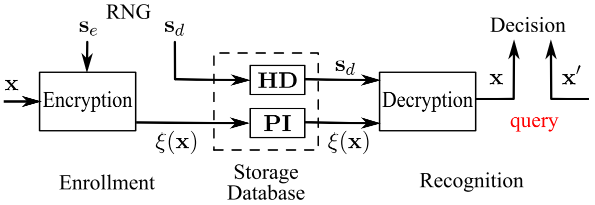


FIGURE 12. Operation mode of a modern cryptograhy scheme.

However, if the key $\mathbf{s}_d$ is disclosed or compromised, then the protected information or encrypted template is not secure. In other words, the problem of biometric template protection evolves into the problem of cryptographic key management and security; this last problem is also a great challenge [31], [44]. In the recognition phase, protected templates are decrypted, as shown in Fig. 12, even when the decryption key is not disclosed or compromised since decision-making is not performed in the encrypted domain. Therefore, the decryption process creates a security and privacy vulnerability by having the original representation of the enrollment biometric $\mathbf{x}$ and query biometric $\mathbf{x}'$ at the recognition phase runtime.

The security of a modern cryptography scheme depends on the complexity (length, entropy, and time of use) of the cryptographic keys and the protection of the biometric information decrypted in the recognition phase. In addition, the cancelation and renewal capacity depends on the power of the RNG and the computational complexity of the cryptographic key creation algorithm. Besides, modern cryptography techniques for BTP enable authentication and identification systems.

The keys of the elliptic curve cryptography are shorter than the keys of the RSA cryptography, offering the same security. Furthermore, elliptic curve cryptography is the best option due to the computational complexity of the discrete logarithm problem. For instance, [83] proposed an e-passport authentication scheme with iris and elliptic curve cryptography, where the iris information generates the cryptographic protocol parameter; these parameters are stored on a chip (passport) to be then used in the verification of the passport holder. Another authentication system with elliptic curve cryptography was developed by [84] using fingerprints on mobile devices.

Chaotic encryption algorithms are efficient, secure, and highly sensitive to the initial conditions, i.e., small changes in the initial conditions generate significant changes in the system's behavior. For example, [85] proposed a fingerprint authentication system using a chaotic encryption algorithm; furthermore, the system was implemented on a 32-bit microcontroller.

Cryptography aims to encrypt secret information by altering its structure in a detectable communication; this information is legible only by authorized entities. On the other hand, steganography seeks to insert and hide secret information in a non-secret media without changing its structure through invisible communication. Steganography uses carrier media such as text, audio, video, and image. In comparison, cryptography is implemented only in alphanumeric text files. For instance, the iris authentication system developed by [86] uses a steganography technique by combining Huffman encoding and discrete cosine transform (DCT).

A digital watermark is information embedded and hidden in noise-tolerant media. The confidential information is not necessarily related to the carrier media but is used to identify copyright ownership of that media. The digital watermarks use steganographic techniques with the difference that there are visible and invisible watermarks. For example, [87] developed an iris authentication system using a chaotic watermark. On the other hand, a face and iris authentication system was proposed by [88], using a watermark based on the discrete Wavelet transform (DWT). Indeed, watermarking techniques prevent counterfeiting and unauthorized distribution of information.

On the other hand, [89] developed a novel protection scheme based on visual cryptography techniques, where an image is partitioned and encrypted into n non-overlapping blocks known as visual secret shares (VSS). The VSS creation process uses random parameters that allow revocability. In addition, these blocks of information are stored and shared. In the recognition phase, all or some shared blocks must be stacked without the need for complex cryptographic algorithms. Another example of visual cryptography-based protection was developed by [90] for fingerprint, iris codes, and face.

Most modern cryptography schemes do not allow processing or decision-making in the encrypted domain. In addition, these schemes generate a significant vulnerability when the information is decrypted in the recognition phase. Consequently, protection techniques that preserve privacy and solve the vulnerability in the recognition phase are presented below.

1) KNOWLEDGE SIGNATURE

This technique is a mathematical construction that allows group members to sign some information, where the signer guarantees to belong to the group through the signature (authenticity). In addition, this signature does not reveal the signer's identity (confidentiality). The knowledge signature is a membership authentication system based on the similarity of the signatures [91].

This technique is developed in a cyclic group G of order $n \in \mathbb{N}^+$ and generator element $g \in G$. The knowledge signature is based on the Schnorr signature scheme of a public verification key $y \in G$ defined by a private signature key $s \in \mathbb{Z}_n^*$ ($\mathbb{Z}_n^*$ denotes the multiplicative group of integers modulo n), such that:

$$y = g^s \bmod n \tag{1}$$

The signature is constructed using an adjustment value $k \in \mathbb{Z}_n$ ($\mathbb{Z}_n$ denotes the ring of integers modulo n) and

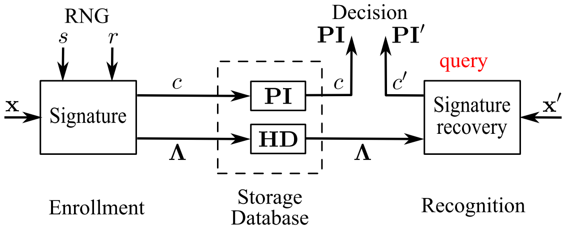


FIGURE 13. Operation mode of knowledge signature scheme.

a hash function applied to the concatenation of biometric information $\mathbf{x}$ and public verification key information [92], i.e.:

$$k = (r - cs) \mod n \tag{2}$$

$$c = \text{hash}\left(\mathbf{x} \| y \| g \| g^r\right) \tag{3}$$

$$g^r = g^k y^c \tag{4}$$

where $r \in \mathbb{Z}_n^*$ is a random element of the allowed set, the signature of the biometric information $\mathbf{x}$ is obtained from a randomly generated s private signature key and a random element r. The signature is the pair of the adjustment value k and the result $c \in \mathbb{Z}_n$. Then, $\mathbf{PI} = [c]$ and $\mathbf{HD} = [\mathbf{\Lambda}]$ with $\mathbf{\Lambda} = [g, y, k, g^r]$, where the private data of the systems are s and r. In the recognition phase, $c' = \text{hash}\left(\mathbf{x}' \| y \| g \| g^r\right)$ is calculated using biometric information of query $\mathbf{x}'$ and the helper data, as shown in Fig. 13. Finally, the match between enrollment c and query c' is validated using a similarity metric, i.e., $\text{dist}(c, c') \leq \tau$, where τ is the similarity threshold.

This technique has a significant security advantage. If c and k are compromised, then the original biometric information cannot be revealed since s and r are secret and not shared by the insecure channel. However, this technique only allows authentication systems. Moreover, the revocation and renewal capacity depends on the RNG's power and the algorithm's complexity to select a signature key s and a random element r from the allowed set. Finally, [93] developed a knowledge signature-based voiceprint authentication system.

2) HOMOMORPHIC ENCRYPTION

The homomorphic encryption allows processing and decision-making with the information in the encrypted domain. The best known homomorphic encryption technique is the Paillier encryption, an asymmetric cryptographic technique that preserves the privacy of information.

Homomorphic operations are applied in a finite modular domain for an encryption public key $s_e = s_1 s_2$ where s_1 and s_2 are large odd prime numbers with a generator element $g \in \mathbb{Z}_{s_e^2}^*$. Therefore, the N features of the biometric information $\mathbf{x}$ must be mapped to a modular value $x_i \in \mathbb{Z}_{s_e}$ with $i = 1, 2, \ldots, N$. In the above process, calculations cannot overflow, and negative values must be shareable with the operations [94]. Consequently, a constant additive value can be used for all features. Then, the homomorphic encryption of biometric information $\mathbf{x}$ under the Paillier encryption is [95]:

$$\boldsymbol{\omega} = \text{enc}\left(\mathbf{x}, \mathbf{r}, s_e\right) = \xi\left(\mathbf{x}\right) \tag{5}$$

$$\omega_i = \xi\left(x_i\right) = \left(g^{x_i} r_i^{s_e}\right) \mod s_e^2 \tag{6}$$

where $\omega_i \in \mathbb{Z}_{s_e^2}^*$ is the encryption of feature i with $i = 1, 2, \ldots, N$ and $r_i \in \mathbb{Z}_{s_e}^*$ is a random number within the allowed set. However, homomorphic encryption is a technique that performs algebraic operations on the encrypted information, obtaining the result equivalent to algebraic operations on the original information. Therefore, additive homomorphic encryption for two biometric features (x_1 and x_2) with the same encryption public key s_e satisfies [95], [96]:

$$\left(\xi\left(x_1\right)\xi\left(x_2\right)\right) \mod s_e^2 = \xi_{12} \tag{7}$$

$$\xi_{12} = \xi\left(\left(x_1 + x_2\right) \mod s_e\right) \tag{8}$$

$$\xi_{12} = \left(g^{\left(x_1 + x_2\right) \mod s_e}\left(r_1 r_2\right)^{s_e}\right) \mod s_e^2 \tag{9}$$

From the above equations, a consequence of the additive homomorphic property for the power $k \in \mathbb{N}$ of an encrypted result fulfills:

$$\left(\xi\left(x_1\right)\right)^k \mod s_e^2 = \xi_1^k \tag{10}$$

$$\xi_1^k = \xi\left(\left(k x_1\right) \mod s_e\right) \tag{11}$$

$$\xi_1^k = \left(g^{\left(k x_1\right) \mod s_e}\left(r_1\right)^{k s_e}\right) \mod s_e^2 \tag{12}$$

Fig. 14 shows the homomorphic encryption scheme for the BTP. In the enrollment phase, the same public key s_e encrypts all the biometric templates, which are then stored. The decryption key is private to each user. Moreover, a similarity metric is performed on the encrypted domain in the recognition phase. Therefore, this protection technique does not generate helper data, and $\mathbf{PI}$ corresponds to the encrypted information. Then, the protected information stored is $\mathbf{D} = \left[\xi\left(\mathbf{x}\right), 0\right]$. For instance, the squared Euclidean distance in the unencrypted domain for the N features of the biometric information under the additive homomorphic identity is:

$$D = \text{dist}^2\left(\mathbf{x}, \mathbf{x}'\right) = \sum_{i=1}^{N}\left(x_i - x_i'\right)^2 \tag{13}$$

$$D = \sum_{i=1}^{N}\left(x_i^2 + \left(x_i'\right)^2 + \left(-2x_i'\right)x_i\right) \tag{14}$$

$$\xi\left(D\right) = \xi\left(\sum_{i=1}^{N}\left(x_i - x_i'\right)^2\right) \tag{15}$$

Hence, the calculation equivalent to the distance encryption is [42], [97]:

$$\xi\left(D\right) = \prod_{i=1}^{N}\xi\left(x_i^2\right)\cdot\prod_{i=1}^{N}\xi\left(\left(x_i'\right)^2\right)\cdot\prod_{i=1}^{N}\xi\left(x_i\right)^{-2x_i'} \tag{16}$$

Homomorphic encryption preserves the privacy of the biometric information and the distance results in the encrypted

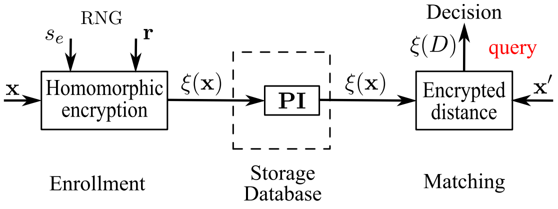


FIGURE 14. Operation mode of an additively homomorphic public key encryption.

domain. Therefore, this encryption protects biometric templates in authentication and identification systems [98]. In addition, the processing in the encrypted environment has allowed obtaining the computation for the Hamming distance, squared Euclidean distance, edit distance, and cosine similarity [99], [100]. However, calculations of other operations have not been obtained, e.g., the Mahalanobis distance. Thus, [101] proposed a BTP scheme based on Paillier encryption, where decision-making is performed in the encrypted domain using the dynamic time warping (DTW) algorithm for variable-length protected templates obtained from the dynamic handwritten signature.

The homomorphic encryption's storage cost and computational complexity are high due to the extended key length and the high overhead of operations on the encrypted domain [42], [45], [97]. In addition, the cancelation and renewal capacity depends on the RNG's power and the algorithm's complexity to generate the encryption keys within the set of allowed elements.

Some authentication systems with protection based on homomorphic encryption that calculates the squared Euclidean distance in the encrypted domain were proposed for biometric traits such as fingerprint [102], iris [103], and face [104], [105]. In addition, [106] proposed an authentication system for speaker recognition that implemented cosine similarity in the encrypted domain. Finally, BTP schemes with binary Hamming distance computation in the encrypted environment were proposed for iris [107] and fingerprint [108].

VIII. CANCELABLE BIOMETRICS

The cancelable biometrics (CB) performs an intentional and repeatable distortion to biometric data through transformations [41]. This distortion is performed in the signal domain or the feature domain, i.e., the biometric information introduced $\mathbf{x}$ to the BTP module in Fig. 3 corresponds to the information acquired and preprocessed by the user interface module or to the information obtained by the feature extraction module, respectively. Furthermore, the transformations perform a mapping of elements from $\mathcal{X}$ to $\mathcal{Y}$ through one-way functions, i.e., $f : \mathcal{X} \to \mathcal{Y}$ for $\mathbf{y} = f(\mathbf{x})$ guaranteeing $\mathbf{x} \neq f(\mathbf{x})$. The purpose of the CB transformations is to maintain the statistical properties, class distribution, and discriminatory power of the biometric information of enrollment $\mathbf{x}$ and query $\mathbf{x}'$. Therefore, the CB performs the matching and decision-making in the transformed or protected domain, fulfilling the *information entropy retention* under a distance of similarity with a decision threshold τ, that is:

$$\text{dist}\left(\mathbf{x}, \mathbf{x}'\right) \leq \tau \tag{17}$$

$$\text{dist}\left(f\left(\mathbf{x}\right), f\left(\mathbf{x}'\right)\right) \leq \tau \tag{18}$$

The parameters of the transformations are given by a vector of random numbers $\mathbf{s}$ created using an RNG. Then, the CB improves the security and privacy of biometric templates. Furthermore, these transforms allow the cancelation and creation of multiple templates for the same user by changing the transform parameters or the one-way functions. The transformation functions are called parameterized distortion functions.

Fig. 15 illustrates the principle of operation of cancelable biometrics. The enrollment phase uses a one-way transform defined by $\mathbf{s}$, and the transformed result is stored. Then, the recognition phase uses the same one-way transform to obtain a protected query $\mathbf{y}'$. Consequently, cancelable biometrics does not generate helper data. Therefore, the protected information stored is $\mathbf{D} = [\mathbf{y}, 0]$. The CB's diversity depends on the RNG's capacity and the function definition.

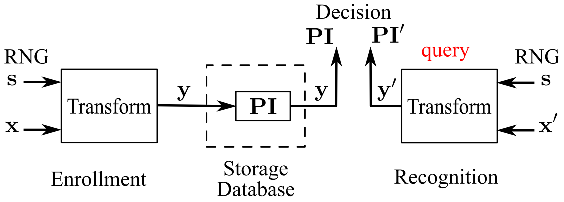


FIGURE 15. Operation mode of a cancelable biometric scheme.

Injective mapping prevents spoofing in identification and authentication systems. On the other hand, non-injective mapping has strength in non-invertibility but is vulnerable to brute-force attacks, attacks via record multiplicity, or solving-equations attacks [109]. In addition, the non-injective mapping facilitates false acceptance due to the *many-to-one* property. For this reason, non-injective mapping is a problem for identification systems, as shown in Fig. 16. Therefore, an injective mapping is a *one-to-one* function, i.e., no element in the domain is mapped to the same element in the codomain, fulfilling:

$$\forall x_1, \quad x_2 \in \mathcal{X}, x_1 \neq x_2 \to f(x_1) \neq f(x_2) \tag{19}$$

$$\forall x_1, \quad x_2 \in \mathcal{X}, x_1 = x_2 \to f(x_1) = f(x_2) \tag{20}$$

Two categories divide the BTP techniques for CB according to the type of implementation of the supplementary information $\mathbf{s}$: 1) transformation schemes, which support user-specific or user-common supplementary information; and 2) salting schemes, which support only user-specific supplementary information. Indeed, the BTP technique and the type of supplementary information are defined by the purpose, constraints, needs, and specifications of the biometric system to be developed.

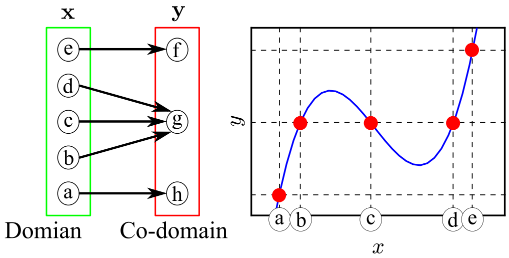


FIGURE 16. Collision or false positive problem of a non-injective mapping. The d user feature may be a non-genuine match for user b or c.

A. TRANSFORMATION SCHEMES

These protection techniques are based on transformations with parameterized one-way functions by secret information **s**. This random information can be user-specific or user-common supplementary information. In addition, the pseudonymous identifier corresponds to the result of the transform. As mentioned above, these techniques based on transformations protect the information in the signal or feature domains.

1) GEOMETRIC TRANSFORMS

Geometric transforms divide and enumerate the two-dimensional biometric information **x** into smaller blocks, cells, or regions of data. The segmentation is performed in geometric regions or sectors oriented with rectangular coordinates (cartesian transformation) or in polar coordinates (polar transformation). Therefore, the transform consists of randomly changing the position of the cells [110]. Nonetheless, the cartesian and polar transform perform non-injective mapping, and the random vector **s** defines the random translation.

Intra-user variability is the main limitation of the cartesian and polar transform. Therefore, a locally smooth transformation solves the above problem. This solution is called *functional transformation*, surface folding transformation, mesh warping transformation, or texture warping transformation. This transform is inspired by an electric potential field parameterized by a random distribution of charges, where renewable information **s** defines the transform's parameters. Fig. 17 illustrates an example of a functional transformation for facial recognition.

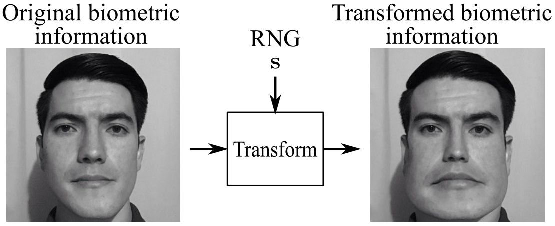

Original biometric information
RNG
s
Transform
Transformed biometric information

FIGURE 17. Example of cancelable biometrics based on functional transformation.

The protected templates' security and privacy depend on the entropy of the translation parameters. Likewise, the cancelation and renewal capacity is directly related to the RNG capacity. Furthermore, geometric transforms have low computational complexity, and protect authentication and identification systems. Below, examples of biometric systems protected with geometric transforms are mentioned.

A cancelable iris authentication system was proposed by [111] using a cartesian transform and texture warping transformation. Furthermore, [112] developed a protected authentication system using a key-dependent geometric transform for fingerprint recognition. Lastly, authentication systems with finger vein patterns was published by [113] and [114] using cartesian transform and functional transform.

2) RANDOM PERMUTATIONS

This BTP technique randomly permutes the biometric information [115]. The first idea of random permutation for non-binary biometric information is called GRAY-COMBO, which divides the original information **x** into smaller segments and randomly exchanges the segments. In addition, addition or multiplication operations can randomly combine the exchanged segments. On the other hand, a similar permutation applied to binary biometric information is called BIN-COMBO, which randomly changes the segmented information, and XOR or XNOR operations can combine the data. The combinations are optional for these two methods, and the data size decreases due to the combinations. Furthermore, the random information **s** defines the segmentation, changes, and combinations.

Random permutations are sensitive to intra-user variations and have low computational complexity. Furthermore, random combinations increase the security and privacy of information but affect the recognition rate. Likewise, the revocation and renewal capacity depends on the power of the RNG. In other matters, the protection of random permutations depends on the metrics or matching techniques in the decision module; in other words, invariant or variable distances to the order of the elements, e.g., Euclidean distance and DTW distance. Finally, the random permutations protect authentication and identification systems.

Fig. 18 illustrates an example of a transform based on random permutation for information from a person's ECG signal, where the information is randomly divided and permuted; even the permuted information can be inverted. In general, random permutations protect one- and two-dimensional biometric information [116].

Cancelable biometric systems based on random permutations are mentioned. For instance, [117] proposed a fingerprint authentication system that performs random permutations and random binary combinations, where the transformation is inspired by the operations of a standard genetic algorithm. On the other hand, a cancelable authentication and identification system for iris recognition was developed by [118]. Finally, [119] developed a random permutation approach for face, iris, and ear recognition, creating a random permutation matrix from an identity matrix, where rows and columns are randomly permuted to obtain a 1 in each row and column. Therefore, the protected information is obtained by multiplying the biometric information with the created matrix.

3) BioConvolving

This technique performs the linear convolution of one-dimensional biometric information sequences $\mathbf{x} \in \mathbb{R}^N$ with N coefficients or features [120]. Consequently, the transform divides the information $\mathbf{x}$ into $h \in \mathbb{N}^+$ non-overlapping segments or sequences. Then, each segment has a length defined through a random vector $\mathbf{s} = [0, s_1, s_2, \ldots, s_{h-1}, 100]$ sorted in ascending order with $s_i \in \mathbb{N}^+ : 1 \leq s_i \leq 99$ for $i = 1, 2, \ldots, (h-1)$. Therefore, the vector $\mathbf{v}$ contains the random lengths of the sequences via an auxiliary vector $\mathbf{b}$ as follows:

$$\mathbf{b} = [0, b_1, b_2, \ldots, b_{h-1}, N] \tag{21}$$

$$b_i = \frac{s_i}{100}N, \quad i = 1, 2, \ldots, (h-1) \tag{22}$$

$$\mathbf{v} = [v_1, v_2, \ldots, v_h] \tag{23}$$

$$v_j = b_j - b_{j-1}, \quad j = 1, 2, \ldots, h \tag{24}$$

$$\mathbf{x} = \left[\mathbf{x}_{v_1}, \mathbf{x}_{v_2}, \ldots, \mathbf{x}_{v_h}\right] \tag{25}$$

The protected information corresponds to the linear convolution ($*$) of the h sequences or segments created, i.e.:

$$\mathbf{y} = f(\mathbf{x}) = \mathbf{x}_{v_1} * \mathbf{x}_{v_2} * \cdots * \mathbf{x}_{v_h} \tag{26}$$

The original information length corresponds to N coefficients, and the sequence protected by BioConvolving has a size of $k = N - h + 1$ coefficients. Furthermore, the protected sequence $\mathbf{y}$ is normalized to have zero mean and unit standard deviation. This protection technique protects authentication and identification systems and is projected as a technique that provides security and privacy to biometric information with low computational complexity. Fig. 19 shows an example of biometric protection based on BioConvolving for speech recognition.

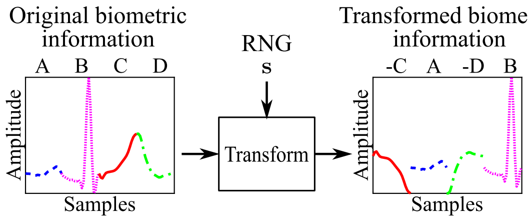

Original biometric information
A
B
C
D
Amplitude
Samples
RNG
s
Transform
Transformed biometric information
-C
A
-D
B
Amplitude
Samples

FIGURE 18. Example of cancelable biometrics based on random permutations.

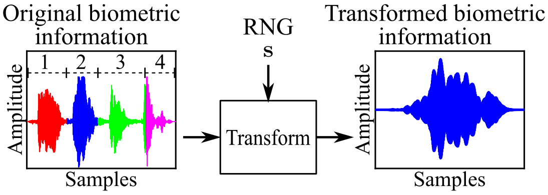

Original biometric information
1
2
3
4
Amplitude
Samples
RNG
s
Transform
Transformed biometric information
Amplitude
Samples

FIGURE 19. Example of cancelable biometrics based on BioConvolving with $h = 4$.

This technique's diversity depends on the RNG's capacity to create several versions of the random vector $\mathbf{s}$. Furthermore, the number of segments h can be changed randomly. Nonetheless, [121] developed an example of this technique for a dynamic handwritten signature-based authentication system, where the decision-making is performed with a hidden Markov model (HMM). On the other hand, an independent recognition scheme for face, iris, palmprint, fingerprint, and ear was proposed by [122], extracting features through a convolutional neural network (CNN) and conventional techniques. In addition, a feature-level fusion is performed, and BioConvolving protects the fused information.

4) POLYNOMIAL TRANSFORMS

This technique maps biometric information using random polynomial functions of order $m \in \mathbb{N}^+$ [41]. For example, independent polynomial functions could map each element of biometric information; otherwise, a polynomial function could map all the information elements, that is:

$$y = f(x) = \sum_{i=0}^{m} s_i x^i \tag{27}$$

where $s_i \in \mathcal{N}(0, 1)$ is the coefficient i of the polynomial for $i = 0, 1, 2, \ldots, m$. Nevertheless, the maximum and minimum values of the features define the range of the roots of the polynomial [116]. Fig. 20 illustrates a third-order polynomial with injective mapping; the coefficients guarantee $s_2^2 - 3s_3s_1 < 0$. Likewise, the point of symmetry $-s_2/(3s_3)$ is approximately in the mean of the enrollment features or within the range $[x_{min}, x_{max}]$ of all the biometric features.

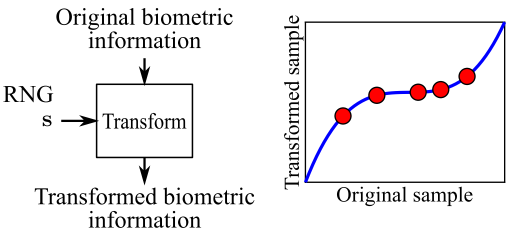

Original biometric information
RNG
s
Transform
Transformed biometric information
Transformed sample
Original sample

FIGURE 20. Example of cancelable biometrics based on third-order polynomial (injective mapping).

This technique's security and privacy depend on the polynomial's order and the entropy of the coefficients defined by the random vector $\mathbf{s}$. In addition, a polynomial transformation for each information element increases the level of protection. On the other hand, the RNG's power defines the cancelation and renewal capacity. Likewise, this technique protects authentication and identification systems using injective mapping, preserving the discriminatory power of the original biometric information. Besides, the computational complexity of this technique is low.

An example of a face authentication system based on a polynomial transform of order one was developed by [123], using the transform $\mathbf{y} = ((\mathbf{x} - \bar{\mathbf{x}}) + \mathbf{d})\,\mathbf{s}$, where $\bar{\mathbf{x}}$ is the mean of the enrollment features, $\mathbf{s} \in \mathcal{N}(1, \sigma^2)$ is a vector of random numbers and $\mathbf{d} \in \mathcal{N}(0, 1)$ is a random translation vector. This system also uses a sorted index number (SIN) to give more security and privacy to protected information. On the other hand, [124] proposed a cancelable authentication system, with protection based on specially defined random polynomials using user-specific tokens and biometric information of face, thermal face, palmprint, palm vein, and finger vein.

5) RANDOM PROJECTIONS

This technique performs a linear transform and is widely used for dimensionality reduction. The Johnson–Lindenstrauss lemma is the crucial idea of random projection, which consists in projecting a set of information $\mathbf{x} \in \mathbb{R}^N$ of N dimensions to a random subspace through a projection random matrix $\mathbf{s} \in \mathbb{R}^{m\times N}$ with $m \leq N$. Hence, the Euclidean distance between pairs of unprojected data is preserved at a value $0 < \epsilon < 1$ to the distance of the projected information, that is:

$$(1 - \epsilon)\,\|x_1 - x_2\|^2 \leq \|f(x_1) - f(x_2)\|^2 \leq (1 + \epsilon)\,\|x_1 - x_2\|^2 \quad (28)$$

When $m < N$, a dimensionality reduction is performed via a non-injective mapping (many-to-one); and when $m = N$, an injective transformation (one-to-one) is performed, called linear operator. Therefore, the random projection is defined by [125]:

$$\mathbf{y} = f(\mathbf{x}) = \frac{1}{\sqrt{m}}\,(\mathbf{s})\,(\mathbf{x}) \quad (29)$$

Being $\mathbf{y} \in \mathbb{R}^m$ the random projection. This technique transforms the original biometric information and preserves the statistical properties useful for recognition. Each element of the matrix $\mathbf{s}$ of $i = 1, 2, \ldots, m$ rows and $j = 1, 2, \ldots, N$ columns is an independent realization of a random variable with a specific probability distribution. Likewise, the rows of $\mathbf{s}$ must be independent to avoid distortion of the statistical properties. In general, the probability distribution of the elements $s_{i,j}$ of the projection matrix defines different random projections.

When the elements of the projection matrix have a standard Gaussian distribution, i.e., $s_{i,j} \in \mathcal{N}(0, 1)$. The projection corresponds to a *Gaussian random projection*, where the matrix rows are orthogonalized using the Gram-Schmidt algorithm, and the norm of each row must be one. The above process is essential to preserve the similarity in the new space and fulfill the isometry property. This projection type has been proposed for cancelable biometric systems based on face [126], [127] and palmprint [128].

Some random projections have been developed to reduce the computational cost and speed up projection processing z times compared to Gaussian random projection. Therefore, each element of the matrix $\mathbf{s}$ can be a realization of a random variable with a probability distribution given by:

$$s_{i,j} = \begin{cases} \sqrt{z} & \text{with probability } 1/(2z) \\ 0 & \text{with probability } 1 - 1/z \\ -\sqrt{z} & \text{with probability } 1/(2z) \end{cases} \quad (30)$$

When $z = 1$, the projection matrix $\mathbf{s}$ must be non-singular and is a realization of the Bernoulli distribution. Thus, this projection is a *Bernoulli random projection*. On the other hand, if $z = 3$, then the projection is called *sparse random projection* [125]. An authentication system with sparse random projection for facial recognition was proposed by [129]. Finally, when $z \gg 3$ for example, $z = \sqrt{N}$, the projection is a *very sparse random projection* [130].

The computational complexity of this protection technique depends on the probability distribution selected for the projection matrix. Furthermore, the cancelation and renewal capacity depends on the power of the RNG to create multiple versions of the matrix $\mathbf{s}$. Thus, the entropy of the random matrix $\mathbf{s}$ establishes the security and privacy of the protected templates. Likewise, random projections protect authentication and identification systems through injective mappings, i.e., $m = N$.

Sectored random projection is another type of random projection that faces intra-user variability. Therefore, the original biometric information is divided into smaller sectors, as shown in Fig. 21. Then, these segments are projected, and the protected information corresponds to the concatenation of the projections [131]. Nonetheless, [132] developed an iris authentication and identification system based on sectored random projection.

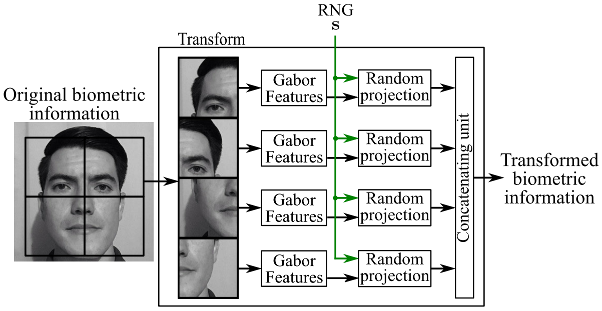


FIGURE 21. Example of cancelable biometrics based on sectored random projection.

A type of non-linear random projection is called *dynamic random projection*, which dynamically assembles or builds a projection matrix by selecting m candidate row vectors. The selection of the vectors depends on the biometric features and is performed using amplitude quantification techniques [133]. For instance, an authentication system with this projection was developed for iris [134] and fingerprint [135].

Another type of projection was proposed for fingerprint authentication by [136]. This projection is based on the

Hadamard transform, formed by the Walsh functions. This transform can be of two types: *Partial Hadamard* and *Full Hadamard*. Therefore, the partial Hadamard transform is performed with a submatrix $\mathbf{H}_p$ formed by the random selection of m rows from the full-order Hadamard matrix $\mathbf{H}$ of $n \times n$ with $m < n$, where n is the order of the full Hadamard matrix. Then, the full-order Hadamard matrix is orthogonal and symmetric, but the submatrix $\mathbf{H}_p$ of $m \times n$ has deficient rank of columns, i.e., non-invertible. Therefore, this projection is called *Hadamard partial random projection* and is defined as:

$$f(\mathbf{x}) = \mathbf{y} = \left(\mathbf{H}_p\right)(\mathbf{x}) \tag{31}$$

where $\mathbf{y} \in \mathbb{R}^n$ is the result of the projection. Furthermore, the biometric information $\mathbf{x}$ is adjusted to the dimension of the full-order Hadamard matrix $\mathbf{H}$. The main advantages of the Hadamard partial random projection are: 1) low computational cost due to the exclusive use of addition and subtraction operations; and 2) low storage cost due to storing the indices of the randomly selected rows. Therefore, the random vector $\mathbf{s}$ sets the indices of the m selected rows of the matrix $\mathbf{H}$.

6) HILL CIPHER

This technique is based on modular arithmetic and linear algebra concepts. In addition, this technique performs a random projection between the biometric information $\mathbf{x} \in \mathbb{R}^N$ with N features and a random projection matrix $\mathbf{s} \in \mathbb{R}^{m \times N}$ with $m \leq N$, where the module of q is calculated for each value of the projection, that is:

$$\mathbf{y} = ((\mathbf{s})(\mathbf{x})) \bmod q \tag{32}$$

where $\mathbf{y} \in \mathbb{Z}$ and q can be equal to 26 for the English alphabet or 256 for grayscale values, each element of $\mathbf{s}$ is a rational value with probability distribution $\mathcal{N}(0, 1)$, where $\mathbf{s}$ is an orthogonal matrix by the Gram-Schmidt process. Fig. 22 illustrates an example of this transformation with $q = 256$. On the other hand, matrix elements with negative and non-negative rational values increase the security and privacy of this technique even when the protected information and the projection matrix are simultaneously compromised. Therefore, the information recovered from the compromised data is very noisy and has significant content losses [137], [138]. In addition, the revocation and renewal capacity depends on the power of the RNG. Finally, this technique has medium computational complexity due to modular arithmetic.

This protection technique protects authentication and identification systems. For example, [137], [138] developed a Hill cipher-based authentication system for face and palmprint.

7) CORRELATION FILTERS

This technique transforms images or two-dimensional biometric information using convolution kernels or masks. The random kernel of convolution $\mathbf{s}$ has non-null values created by an RNG. Fig. 23 illustrates the idea of correlation filters for BTP. In the enrollment phase, this technique creates a reference model from the biometric information of enrollment $\mathbf{x}$. In the recognition phase, this technique obtains the cross-correlation in the protected domain between the convolution of a sample query $\mathbf{x}'$ and the created reference.

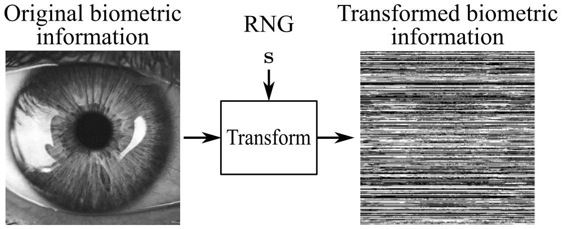

Original biometric information
RNG
s
Transform
Transformed biometric information

FIGURE 22. Example of cancelable biometrics based on Hill cipher.

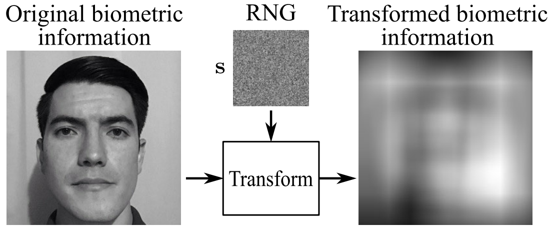

Original biometric information
RNG
s
Transform
Transformed biometric information

FIGURE 23. Example of cancelable biometrics based on correlation filters.

The cross-correlation operation ($\star$) between two protected templates is equivalent to the convolution operation ($*$) between the templates, where one of the templates is in its inverted version, which corresponds to turning 180 degrees or flipping left to right ($\operatorname{fliplr}(\cdot)$), i.e.:

$$\mathbf{y} = \mathbf{x} * \mathbf{s} \tag{33}$$

$$\mathbf{y}' = \mathbf{x}' * \mathbf{s} \tag{34}$$

$$\mathbf{y} \star \mathbf{y}' = \mathbf{y} * \operatorname{fliplr}\left(\mathbf{y}'\right) \tag{35}$$

Furthermore, the cross-correlation satisfies the convolution theorem, obtaining:

$$\mathbf{y} \star \mathbf{y}' = \mathcal{F}^{-1}\left(\mathcal{F}(\mathbf{y})\, \mathcal{F}^{*}\left(\mathbf{y}'\right)\right), \tag{36}$$

where $\mathcal{F}(\cdot)$ is the discrete Fourier transform (DFT), $\mathcal{F}^{-1}(\cdot)$ is its inverse, and $\mathcal{F}^{*}(\cdot)$ the complex conjugate of the DFT. The correlation filters can create reference models using a single sample or a collection of information samples. On the other hand, this protection technique addresses intra-user variations and prevents gradual performance degradation. Furthermore, this technique protects authentication and identification systems for two-dimensional biometric information.

The reference model can be defined by a minimum average correlation energy (MACE) filter, and the result of the cross-correlation is obtained in a peak-to-sidelobe ratio (PSR), which is used for the decision-making of the system [139]. This correlation filter is sensitive to noise but offers good recognition performance. Then, [139] proposed a facial recognition system with a MACE filter for protection. On the other hand, a correlation filter also performs correlation invariant random filtering (CIRF). This filter builds the reference model using a number theoretical transform (NTT); this transform is a kind of discrete Fourier transform over a finite field with matches based on cross-correlation. Finally, an authentication system using a CIRF was developed for finger vein patterns [140] and fingerprint [141].

Protection based on correlation filters does not leak information. Therefore, linkability and reversibility are extremely difficult. On the other hand, the capacity to revoke and renew depends on the RNG's power to create various convolution kernels. Furthermore, the computational complexity is medium for this technique. In particular, a palmprint authentication system was developed by [142], which performs convolution between the biometric information and a Gabor filter defined by random information. Likewise, [143] proposed a cancelable authentication system with protection based on the convolution operation between fingerprint information and a random kernel generated with chaotic maps.

8) BLOOM FILTERS

An adaptive Bloom filter is a probabilistic structure that evaluates membership queries and compares biometric information on the protected domain. Furthermore, [144] introduced the adaptive Bloom filters, which were used for the BTP by [145]. This technique uses two-dimensional biometric information in binary representation.

Fig. 24 illustrates the operating principle of this technique based on two-dimensional biometric information $\mathbf{x}$ of N columns, where each column represents a biometric feature of n bits in length. This information is divided into k blocks of equal size, i.e., $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2, \dots \mathbf{x}_k]$ where each block $\mathbf{x}_i$ with $i = 1, 2, \dots, k$ has $\eta = N/k$ columns of n bits. On the other hand, a Bloom filter $\mathbf{y}$ is a binary matrix of k columns and 2^n rows. Initially, all positions of $\mathbf{y}$ are assigned to zero, and then the positions given by the results of an independent binary operation are set to one. In other words, $c \in \mathbb{N} : 0 \leq c \leq 2^n - 1$ is the result of the binary operation and is used as row index in its decimal value for position $y_{c,z} = 1$ with $z = 1, 2, \dots, k$.

The binary operation performs the XOR operation between a random binary vector $\mathbf{s}$ of n bits and the information vector corresponding to column j of the block i with $j = 1, 2, \dots, \eta$ and $i = 1, 2, \dots, k$, that is:

$$c = \text{bit2int}\left(\mathbf{x}_{i,j} \oplus \mathbf{s}\right) \tag{37}$$

The binary operation is performed with each column vector $\mathbf{x}_{i,j}$ of the η columns of each of the k blocks of binary information. This technique is irreversible under the constraint that $\eta \leq 2^n$ and also by the probability of assigning several column vectors to the same index (non-injective mapping). In other words, a position in $\mathbf{y}$ can be assigned to one multiple times [146]. In the recognition phase, $\mathbf{y}'$ is obtained from $\mathbf{x}'$ in the same way as in the enrollment phase. Therefore, matching or permanence of query information in $\mathbf{y}$ must ensure that all positions in one of $\mathbf{y}'$ are set to one for $\mathbf{y}$; if this is true, the query is successful, and a probability of false positive is assumed. Otherwise, the query information $\mathbf{x}'$ is not a member of $\mathbf{y}$ [145]. An improved evolution of the Bloom filter corresponds to the Cuckoo filter and Morton filter, which provide bounded false positive probability [50].

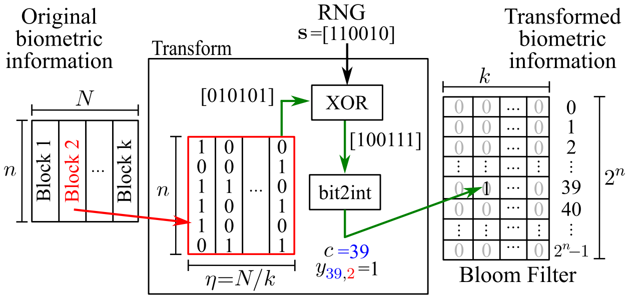


FIGURE 24. Example of cancelable biometrics based on Bloom filters.

The Bloom filters satisfy the irreversibility property but do not efficiently satisfy the unlinkability property due to the non-injective mapping [147]. Additionally, these filters are fast and memory-efficient, specifying when an element is a group member. Likewise, this technique has three significant benefits for biometric recognition: 1) it protects the information; 2) it compresses the information; and 3) it speeds up the processing, reducing the overall response time without degrading the system's performance [148]. On the other hand, this technique has low computational complexity and protects only authentication systems.

The capacity to cancel and revoke protected information depends on the power of the RNG to create multiple vectors $\mathbf{s}$. Furthermore, independent binary operations can be used for each of the k information blocks. Nonetheless, the binary operation can also be changed for another. In fact, some cancelable biometric systems based on Bloom filters have been developed for iris [145], face [149], and fingerprint [150]. Finally, the operating principle of Bloom filters has been transferred to protection techniques based on consistent bit extraction and decimal encoding to perform randomized look-up table mapping. An example of this protection scheme is developed by [151] for an iris-based authentication system.

B. SALTING SCHEMES

The salting schemes are transformations based on the mix or combination of biometric information and user-specific external random patterns, which protect and increase the discriminatory power of biometric information [47], [115], [138]. Therefore, only user-specific supplementary information achieves the above goal. Then, salting schemes use two or more recognition factors. On the other hand, the recognition rate of the protected biometric system is inversely proportional to the dependence, link, or correlation of the user-specific supplementary information. In addition, the security of each user with his supplementary information establishes the probability of reversibility of the protected data. Consequently, the security and privacy of salting schemes are partially user-dependent. For this reason, salting schemes are often called reversible or invertible transformations in literature. However, invertibility is not a specification of salting schemes. Instead, the exclusive use of user-specific random information is a specification of salting schemes.

The additional recognition factors are external, secret, and independent information for each user based on passwords, smart cards, USBs, accessories, tokens, or random noise. Consequently, there are three salting schemes for biometric protection: 1) BioHashing; 2) BioPhasor; and (3) intrinsic artifacts. Therefore, BioHashing and BioPhasor are user-specific discretization or quantization schemes, and the input information corresponds mainly to information in the feature domain. Meanwhile, intrinsic artifact schemes are based on user-specific information added in the acquisition zone, and the input information corresponds primarily to information in the signal domain.

1) BioHashing

BioHashing is based on the binary discretization of random projections between biometric information and user-specific tokenized random numbers [152], [153]. Hence, the one-way transformation based on BioHashing uses two or more recognition factors to obtain the projection matrix and generate compact binary information called *BioCode* or *BioHash*. Furthermore, the random projection matrix is user-specific, i.e., the new projection spaces are different for each user.

This technique is a transform that performs a random multispatial quantification (RMQ) process to generate uncorrelated templates tolerant to intra-user variations. These templates preserve the discriminative power of the original biometric information and amplify inter-user variations [154]. Likewise, the projection matrices were proposed with a Gaussian distribution, but these can have any probability distribution analyzed for random projections.

The protected information or BioCode is a binary vector of n bits obtained in two steps, as shown in Fig. 25. First, the biometric information $\mathbf{x} \in \mathbb{R}^N$ is projected using a user-specific random projection matrix $\mathbf{s} \in \mathbb{R}^{n \times N}$. Second, the result of the projection $\mathbf{b} \in \mathbb{R}^n$ is discretized by a quantification threshold T as follows:

$$\mathbf{b} = [b_1, b_2, \ldots, b_n] = \frac{1}{\sqrt{n}} (\mathbf{s}) (\mathbf{x}) \tag{38}$$

$$\mathbf{y} = [y_1, y_2, \ldots, y_n] \tag{39}$$

$$y_i = \begin{cases} 0 & \text{if } b_i \leq T \\ 1 & \text{if } b_i > T \end{cases} \quad \text{with } i = 1, 2, \ldots, n \tag{40}$$

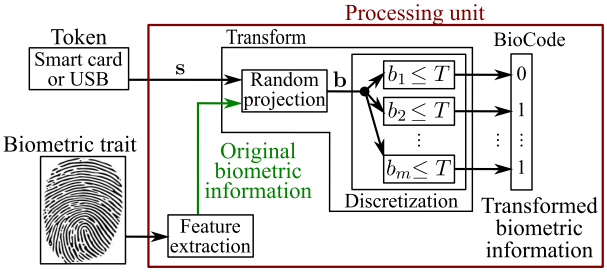


FIGURE 25. Example of cancelable biometrics based on BioHashing.

The threshold T is empirically determined, but in most implementations, it is defined as $T = 0$.

Protected information is the result of the interaction of user-specific supplementary information and original biometric information but is not reproducible in the absence of either. On the other hand, the security and privacy of BioHashing are based on the RMQ process. Still, it is vulnerable to genetic algorithms (GA) when the token and the protected information are compromised simultaneously [155]. Therefore, the security of the token is essential to the security and privacy of the protected biometric system. Furthermore, three additional steps enhance the protection of this technique [156]: 1) normalizing the original biometric information; 2) using various thresholds for the RMQ process; and 3) performing permutations of the information before the projection. Additionally, this technique's revocation and renewal capacity depend on the power of the user-specific supplementary information generation and management processes. Finally, this technique has low computational complexity.

BioHashing protects authentication systems, where the separation between the genuine and impostor population increases, decreasing the false acceptance rate (FAR) without increasing the false rejection rate (FRR), achieving EER = 0% [153]. On the other hand, this technique is not feasible for identification systems due to the lack of prior interaction to present the user-specific supplementary information, as illustrated in Fig. 3. Besides, if tokens are unique, independent, and secret to each user, then biometrics are unnecessary. For example, two scenarios based on fingerprint recognition: 1) identify an employee involved in unauthorized access and distribution of budget in a company; and 2) identify a person with memory or health problems who is disoriented. In both scenarios, only biometric information is present but not supplementary information.

Some examples of BioHashing-based authentication systems have been developed for face [157], iris [158], palmprint [159], handwritten signature [156], fingerprint [160] and finger-knuckle-prints [161].

2) BioPhasor

This technique performs a binary quantization by mixing user-specific tokenized random numbers and biometric information. This cancelable transform is based on the computation of complex arguments to generate a binary

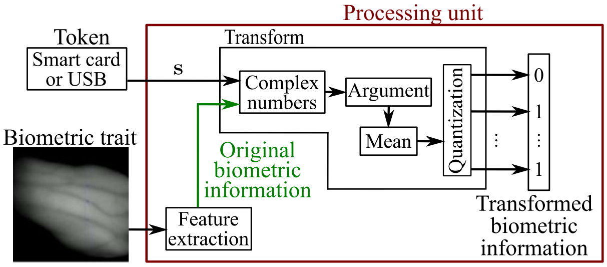


FIGURE 26. Example of cancelable biometrics based on BioPhasor.

vector of n bits [162]. Thus, BioPhasor is a non-linear extension of BioHashing.

A user-specific matrix $\mathbf{s} \in \mathbb{R}^{n \times N}$ with $n \leq N$ is generated from the user-specific supplementary information. Each element of $\mathbf{s}$ has a Gaussian distribution $\mathcal{N}(0, 1)$, and each row of the matrix $\mathbf{s}$ must be orthonormal using the Gram–Schmidt process. Then, the transform of the biometric information $\mathbf{x} \in \mathbb{R}^N$ of N features is obtained in four steps, as shown in Fig. 26. First, the complex numbers $\mathbf{z}_i = \mathbf{x} + j\mathbf{s}_i$ are generated, where $\mathbf{s}_i$ is the row vector i of the matrix $\mathbf{s}$ with $i = 1, 2, \ldots, n$ and $\mathbf{z} \in \mathbb{C}^{n \times N}$. Second, the phase angles or complex arguments of the elements of each row of $\mathbf{z}$ are obtained, i.e., $\boldsymbol{\varphi}_i = \arg(\mathbf{z}_i)$ with $i = 1, 2, \ldots, n$ and $\boldsymbol{\varphi} \in \mathbb{R}^{n \times N}$. Third, average complex arguments are obtained for each row of $\boldsymbol{\varphi}$. Fourth and last, the protected information vector $\mathbf{y}$ of n bits is created through a quantization process as follows:

$$\mathbf{b} = [b_1, b_2, \ldots, b_n] \tag{41}$$

$$b_i = \frac{1}{N}\sum_{j=1}^{N} \varphi_{i,j} \quad \text{with } i = 1, 2, \ldots, n \tag{42}$$

$$\mathbf{y} = [y_1, y_2, \ldots, y_n] \tag{43}$$

$$y_i = \begin{cases} 0 & \text{if } 0 \leq b_i < \pi \\ 1 & \text{if } -\pi < b_i < 0 \end{cases} \tag{44}$$

The protected template does not leak information about the original biometric template. Furthermore, this transform is more secure than BioHashing [162]. Nevertheless, the quantification process degrades the recognition rate; for this reason, the complex plane should be divided into more sectors to perform the quantification. Furthermore, this protection technique has low computational complexity.

BioPhasor protects authentication systems, addressing intra-user variations and increasing inter-user variations to achieve EER = 0%. However, this technique does not protect identification systems. On the other hand, the revocation and renewal capacity depends on the power of the user-specific supplementary information generation and administration processes. Finally, a BioPhasor-based authentication system for face [163], and dynamic handwritten signature [164], where the complex plane is divided into 2^m segments for the quantification in m bits.

3) INTRINSIC ARTIFACTS

This technique is resistant to spoofing due to the combination of biometric information with random artifacts added in the biometric acquisition zone. So, the random artifacts are artificially created patterns that contain user-specific supplementary information. This concept was inspired by the intrinsic patterns from the inherent texture of the magnetic micro-fibers [165]. Therefore, this technique uses the data extracted from the random patterns to create protected templates.

Artifacts can be objects, accessories, garments, elements, or stickers added to the body area of the biometric trait. These intrinsic patterns are unique and permanent for each user. Likewise, these patterns must be repeatable on every query and difficult to clone. An example of this protection technique is illustrated in Fig. 27, where dot stickers are added to the hand. The points' form, position, and direction generate several artifacts that allow cancelable biometrics.

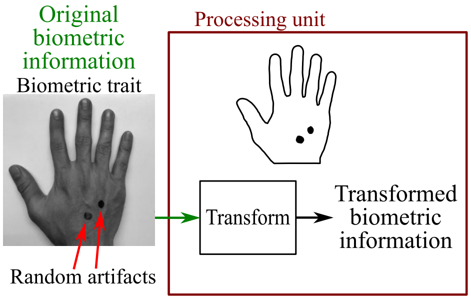

Original biometric information
Biometric trait
Processing unit
Transform
Transformed biometric information
Random artifacts

FIGURE 27. Example of cancelable biometrics based on intrinsic artifacts.

This technique depends on the artifacts designed, the biometric trait used, and intrinsic patterns' role in processing and protection. The transforms allow the repeatability and reproducibility of the pattern, increasing inter-user variability. On the other hand, security and privacy depend on the difficulty of cloning the random artifacts. Furthermore, this protection technique has low computational complexity. Likewise, this technique protects authentication systems when the artifacts are present in the user's body. Finally, the capacity to cancel and renew depends on the ability to generate and manage the unique and intrinsic artifacts.

Some examples of these protection techniques are mentioned below. An authentication system for hotel check-in process was developed by [166] using stickers with a random pattern of points on the thumb's fingernail, the protected template is obtained from the continuous distance between the finger outline and the middle of the two points. Access is allowed to a limited number of users for approximately five days. Another authentication system was proposed by [167], where a hybrid recognition is used between the fingerprint and a circular sticker with a random pattern on the fingernail of the same finger.

IX. PROTECTION SCHEMES BASED ON MACHINE LEARNING OR DEEP LEARNING

Machine learning (ML) and deep learning (DL) algorithms are widely used in pattern recognition. Still, these algorithms have been used in recent years to generate cancelable biometric templates from renewable supplementary information [168], [169], [170]. In other words, these algorithms receive biometric information $\mathbf{x}$ and supplementary information $\mathbf{s}$ to generate protected templates, as shown in Fig. 28. Hence, the focus is on the BTP module, not the feature extraction module or the decision-making module. However, this technique does not create helper data, and the pseudonymous identifier corresponds to the output of the learning algorithm.

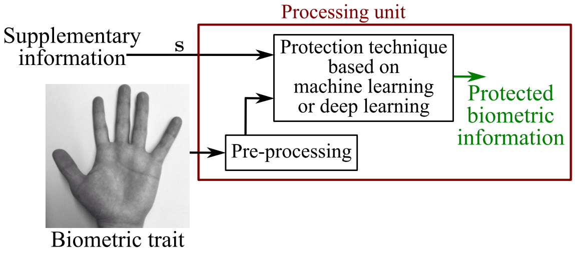

Processing unit
Supplementary information
s
Protection technique based on machine learning or deep learning
Protected biometric information
Pre-processing
Biometric trait

FIGURE 28. Example of a protection scheme based on machine learning or deep learning.

These protection schemes preserve the privacy and confidentiality of biometric information through highly non-linear protection algorithms. Furthermore, these schemes deal with intra-user variations and allow revocation and renewal of the protected template by changing the random data $\mathbf{s}$. Some advantages of these protection schemes are: 1) receiving biometric information with discrete or continuous distribution; and 2) guaranteeing non-invertibility and non-linkability. Consequently, these protection techniques are safe against cross-matching attacks. Likewise, the recognition performance is promising due to the power of ML or DL algorithms for feature extraction and decision-making.

ML and DL-based protection schemes solve the challenge of alignment-free protection techniques, i.e., a processing technique (end-to-end framework) that addresses intra-user variability, protects and revokes information, and does not degrade the recognition rate. In most of these protection schemes, the random information is user-specific supplementary information. Therefore, the cancelation and renewal capacity depends on the power of the RNG. These protection techniques have high computational complexity and protect authentication and identification systems. But DL-based protection techniques need more extensive databases for their enrollment or training phase.

ML or DL-based protection schemes are trained to minimize intra-user variations and maximize inter-user variations. In addition, these techniques are more resistant to active attacks than biometric cryptosystems and cancelable biometrics. Moreover, this family of approaches is being explored; ML and DL algorithms allow the development of multiple individual protection approaches. In general, protection techniques based on deep learning algorithms have longer training time, higher computational complexity, and better address the intra-user variability than protection techniques based on machine learning algorithms. Additionally, the techniques of this family protect biometric information in the feature domain or signal domain, with input information in one or two dimensions. However, investigations of this family of techniques are increasing and are focusing on solving the challenge of re-training when protected information is compromised. This challenge is important because if only one template is compromised, the entire database of protected information must be renewed due to the necessary re-training of all the weights or parameters of the protection algorithm.

Some examples of this family of BTP techniques are mentioned. Such as the protection scheme based on a back-propagation neural network (BPNN) proposed by [169], using user-specific supplementary information for authentication systems based on face, fingerprint, and finger vein. Furthermore, a face and fingerprint authentication system for IoT devices with protection based on an evolutionary genetic algorithm (GA) was published by [171]. Likewise, [172] proposed an iris-based cancelable authentication system using a generative adversarial network (GAN) with renewable supplementary information. Besides, an iris-based cancelable biometric system was proposed by [173]; this scheme utilizes a bidirectional associative memory (BAM) neural network to bind biometric templates to random bit-strings in a secure and efficient manner. Finally, [174] developed a finger vein authentication system with protection based on deep learning (deep belief networks) and random projections.

A representative method of this family of BTP techniques is detailed below.

1) PROTECTION SCHEMES BASED ON CONVOLUTIONAL NEURAL NETWORKS

This deep learning protection scheme employs convolutional neural networks (CNN) to create the protected templates using renewable supplementary information [168], [175]. These schemes address the challenge of alignment-free protection techniques, achieving robustness against intra-user variability. Moreover, these protection schemes allow decision-making in the protected domain and do not generate helper data, i.e., the protected information stored corresponds to the output of the CNN. Likewise, the revocability and renewability of the protected information are achieved when the supplementary information (common or specific) is canceled and renewed. In other words, the cancelation and renewal capacity of these schemes depends on the power of the RNG. Nonetheless, supplementary information may intervene: 1) in the first or any other convolution layer (once or several times); 2) in the flattening layer; or 3) in the fully connected layer. Then, the CNN is trained to minimize intra-user variations and maximize inter-user variations [176].

On the other hand, CNN-based protection schemes allow the development of authentication and identification systems. Furthermore, these protection schemes provide good security and privacy for biometric information due to the non-linear operation principle. In other words, the mutual information between inputs and outputs is minimized, obtaining a good unlinkability index. Likewise, these schemes guarantee a good irreversibility index. But, these schemes have high computational complexity due to the structure of the CNN.

A future direction of CNN-based schemes is to address the challenge of re-training. Some examples of these protection schemes are mentioned. Such as the ECG-based cancelable authentication system proposed by [168], which protects information through CNN using easily changeable keys, where the binding of an input and a key happened before the first dense layer. In addition, [175] proposed a randomized CNN to generate protected face biometric templates given the input face image and a user-specific key. Finally, [177] implemented CNN to learn a mapping from facial images to maximum entropy binary (MEB) codes. This work demonstrated that the exceptional performance of CNN can be utilized to minimize the loss of matching accuracy in template protection algorithms.

X. HYBRID PROTECTION SCHEMES

The protection schemes for biometric information can use two or more techniques from biometric cryptosystems and cancelable biometrics. The above defines the hybrid protection schemes. These schemes seek to achieve the following goals: 1) greater robustness against intra-user variations, improving the recognition rate; and 2) better security and privacy of biometric information, performing decision-making in the protected domain. However, the security, privacy, and diversity of these hybrid schemes depend on the properties of each technique used. Furthermore, there are two representative types of hybrid protection schemes: 1) combination of techniques from the same family; and 2) combination of techniques from different families. These types of schemes address the compatibility of the distribution of biometric data, preserving the discriminatory power. Nonetheless, hybrid protection schemes can use several BTP techniques for the same biometric trait or several biometric traits.

A. COMBINATION OF TECHNIQUES FROM THE SAME FAMILY

These hybrid protection schemes use two or more techniques from the same family, i.e., combine various biometric cryptosystem techniques or various cancelable biometric techniques. An example is the fingerprint authentication system developed by [178], where the information generated by a fuzzy vault scheme is protected with a fuzzy commitment scheme. Another example is the face authentication system proposed by [179], which implements BioHashing and random permutations according to a chaotic sequence.

B. COMBINATION OF TECHNIQUES FROM DIFFERENT FAMILIES

Hybrid protection schemes can use two or more BTP techniques from different families, i.e., combine various biometric cryptosystem techniques with cancelable biometric techniques. Various hybrid protection schemes have been developed for different biometric traits. For instance, [180] reported a fingerprint authentication system, performing random permutations and reliable bit selection for a secure sketch. Another example is the face authentication system designed by [181]; this system is based on random projection, discriminability-preserving transform, and a fuzzy commitment scheme. On the other hand, [182] proposed a voiceprint authentication system, which implements a random projection and fuzzy vault scheme. Lastly, [183] published a fingerprint authentication system with protection based on BioHashing, fuzzy extractor, and fuzzy vault scheme.

XI. MULTIBIOMETRIC PROTECTION SCHEMES

The Multi-biometric or multimodal protection schemes incorporate BTP techniques and the fusion of two or more biometric traits for the security and renewal of information. The fusion of two or more biometric traits decreases the intra-user variation and increases the inter-user variation [184]. Multimodal protection schemes offer better security, privacy, confidentiality, and recognition rate (identification or authentication) than unimodal protection schemes, but the computational cost and complexity of the systems are higher. Furthermore, these schemes are more robust against spoofing or identity theft attacks.

There are three levels of fusion for multiple biometric traits: 1) sensor or feature-level fusion; 2) matching or similarity score-level fusion; and 3) decision-level fusion. Furthermore, various fusion methods are possible, such as the weighted sum rule, decision trees, k-nearest neighbors, majority vote, or linear discriminant function. Likewise, the possible fusions of information and protection techniques applied to the fused information define the cancelation and renewal capacity. Additionally, the information on each biometric trait can be protected before the fusion using one or more BTP techniques mentioned above.

Next, some examples of multibiometric protection schemes are mentioned. For example, [185] proposed different multimodal fusions of biometric traits such as the face, thermal face, palmprint, palm vein, and finger vein. The protected information is generated from the distance between the original features and random points derived from the user-specific key. This protection technique is called random distance method. Another protection system for multimodal recognition was developed by [186], with decision-level fusion for iris and voice. In addition, the protection is based on BioHashing, polynomial interpolation, and BioConvolving.

On the other hand, a multimodal protection scheme based on Paillier's homomorphic encryption was developed by [100], with biometric information obtained from dynamic handwritten signature and fingerprint. Three levels of fusion and two matching distances in the encrypted domain are analyzed: cosine similarity and squared Euclidean distance. Likewise, [187] proposed a protection system with feature-level fusion for ear and face, where the biometric information is divided into equal parts, permuted, and protected by random projection. Finally, [188] designed a feature-level fusion protection scheme for fingerprint, iris, and face using a fuzzy vault scheme and fuzzy commitment scheme.

The authors in [189] proposed a feature-level fusion protection scheme for fingerprint and palmprint, using a random tiling and equal-probable 2^n discretization scheme. On the other hand, [190] developed a multimodal protection scheme for the face and iris, where a CNN extracts features, and a joint representation layer is implemented to fuse extracted features. Furthermore, the protected information is a binary vector created using a quantization scheme, an ECC, and a hash function. Finally, a multimodal protection scheme with feature-level fusion for face, iris, fingerprint, and finger veins was published by [146] using Bloom filters.

XII. SUMMARY OF BTP TECHNIQUES

The previous sections discussed the protection families and techniques that constitute the proposed taxonomy. These BTP families and techniques are the result of the synthesis of the systematic literature review. In general, the selection of the best BTP technique is challenging because it depends on the purpose, constraints, needs, and specifications of the biometric systems to be developed. This challenge is also based on the biometric trait, i.e., an image or a data sequence. Therefore, this section presents Table 3, which summarizes the relevant information on the different BTP techniques. Table 3 aims to highlight the strengths and weaknesses of the protection techniques. In addition, this table contains the following information:

- **Column A**: Storage cost categorized as low (L), medium (M), and high (H).
- **Column B**: Probability distribution of input biometric information categorized into discrete (D) and continuous (C). In short, techniques that support continuous distribution also support discrete distribution.
- **Column C**: Computational complexity is categorized into low (L), medium (M), and high (H).
- **Column D**: Revocability and renewability capacity categorized into limited (L) and non-limited (N).
- **Column E**: Does technique allow decision-making in the protected domain?, answering yes (Y) or no (N).
- **Column F**: BTP techniques support input biometric information in one dimension (O) or two dimensions (T). In other words, protection techniques operate with data sequences or images in the signal domain or the feature domain. In short, the techniques that support two-dimensional information also support data sequences.

Table 3 complements and deepens Table 2. In addition, the Table 3 gives a better overview of the appropriate selection of the protection technique. For example, all protection techniques do not support identification systems; several techniques are non-injective transformers; and some techniques do not allow decision-making in the protected domain. Moreover, the storage cost is essential because there are techniques that increase or decrease the size of the biometric information. Another important aspect of selection is the distribution of the input information because additional discretization steps generate a loss of discriminative power. Likewise, computational complexity is critical due to the implementation constraints of the biometric system. Above all, non-limited revocability and renewability are vital for a BTP system.

The challenges defined in section IV are considered in the synthesis of the literature review and Table 3. Therefore, protection techniques that guarantee the isometric property face the challenge of re-training. In addition, the Table 3 highlights techniques that attempt to address intra-user variability and techniques that are sensitive to intra-user variability. Consequently, protection schemes based on machine learning and deep learning are proposed to solve the challenge of alignment-free protection techniques.

This summary of relevant information for each technique is complemented by the evaluation metrics presented in the next section; this guides the designer in selecting the most appropriate protection technique for developing the biometric system.

XIII. EVALUATION MEASURES FOR BTP TECHNIQUES

This section presents quantitative measures to evaluate the performance of BTP techniques for input data with discrete and continuous distribution. Therefore, the degree of security and privacy at the information level evaluates the quality of BTP techniques under the interpretation of the ISO/IEC 24745 standard. In addition, a benchmarking of technical, protection, and operational performance measures the quality of BTP techniques [191]. The technical performance seeks to evaluate: 1) the recognition rate of the system without and with protection; 2) the storage cost of the protected information; 3) the time and computational cost of creation, comparison, cancelation, and renewal of the protected information; and 4) the maximum number of versions of protected templates generated from the same biometric trait. On the other hand, the performance of the protection estimates the irreversibility and unlinkability of the protected information when it is compromised. Finally, the operational performance aims to assess the interoperability quality of the system.

A. EFFICIENCY

Efficiency (ef) evaluates the recognition rate (RR) before and after implementing the BTP technique [161] as a function of the system's number β of revocations and renewals.

TABLE 3. Summary of protection techniques with relevant information.

Category	Protection technique	A	B	C	D	E	F	Strengths	Weaknesses
Biometric cryptosystems	Fuzzy commitment	L	D	M	N	Y	T	▶ It deals with intra-user variability through ECC. ▶ Security and privacy depend on the hash function.	▶ It supports only authentication systems. ▶ It does not tolerate variance in the order of information.
	Fuzzy vault	M	C	M	N	Y	T	▶ Security and privacy depend on the hash function and the number of chaff points. ▶ It deals with intra-user variability through ECC.	▶ It supports only authentication systems. ▶ Several attacks have been successfully explored.
	Fuzzy extractor and quantification schemes	H	C	M	L	Y	T	▶ It addresses intra-user variability through stable quantification intervals.	▶ Key entropy problem.
	Elliptic curve cryptography	M	D	M	N	N	T	▶ Short encryption keys are available. ▶ Security and privacy are high in the insecure communication channel.	▶ Decision-making is not allowed in the protected domain.
	Chaotic encryption	M	D	M	N	N	T	▶ Security and privacy are based on non-linear systems, i.e., chaotic systems.	▶ Decision-making is not allowed in the protected domain.
	Steganography and digital watermarks	L	C	M	N	N	T	▶ Biometric information is protected in a non-secret medium.	▶ Decision-making is not allowed in the protected domain.
	Visual cryptography	M	D	M	N	Y	T	▶ Security and privacy do not depend on complex cryptographic algorithms.	▶ This technique only applies to images.
	Knowledge signature	M	D	M	N	Y	T	▶ Security and privacy are high. ▶ Decision-making is allowed in the protected domain.	▶ It supports only authentication systems.
	Homomorphic encryption	H	D	H	N	Y	T	▶ It does not generate helper data. ▶ Decision-making is allowed in the protected domain.	▶ All distance metrics are not yet supported.
Cancelable biometrics	Geometric transforms	L	C	L	N	Y	T	▶ Protection is high for two-dimensional information.	▶ It does not address intra-user variability efficiently.
	Random permutations	L	C	L	N	Y	T	▶ It can reduce the size of biometric information.	▶ It is sensitive to intra-user variability. ▶ Non-injective mappings are performed.
	BioConvolving	L	C	L	N	Y	O	▶ It can reduce the size of biometric information.	▶ The diversity of protected templates is low.
	Polynomial transforms	L	C	L	N	Y	T	▶ Independent polynomial transforms increase security and privacy.	▶ Their design demands attention due to non-injective mappings.
	Gaussian random projection	L	C	M	N	Y	T	▶ It guarantees the isometric property.	▶ The processing speed is low.
	Bernoulli random projection	L	C	L	N	Y	T	▶ The processing speed is faster than Gaussian random projection. ▶ It guarantees the isometric property.	▶ The diversity of protected information is lower than Gaussian random projection.
	Sparse random projection	L	C	L	N	Y	T	▶ The processing speed is three times faster than Gaussian random projection.	▶ The random supplementary information is more complex to create.
	Very sparse random projection	L	C	L	N	Y	T	▶ It is the fastest random projection.	▶ The random supplementary information is more complex to create.
	Sectored random projection	L	C	M	N	Y	T	▶ It addresses intra-user variability.	▶ It is the slowest random projection.
	Dynamic random projection	L	C	M	N	Y	T	▶ The non-reversibility index is good due to the dynamic selection of supplementary information.	▶ The diversity of protected templates is sensitive to intra-user variability.
	Hadamard partial random projection	L	C	L	N	Y	T	▶ The non-reversibility index is good due to the deficient rank of columns. ▶ It is a fast random projection.	▶ It is sensitive to intra-user variability.
	Hill cipher	L	C	M	N	Y	T	▶ Security and privacy are high due to modular arithmetic.	▶ It is a non-injective transformer.
	Correlation filters	L	C	M	N	Y	T	▶ The way of creating reference models ensures good security and privacy.	▶ It is sensitive to noise in biometric information.
	Bloom filters	L	D	L	N	Y	T	▶ It is fast and memory efficient. ▶ It addresses intra-user variability.	▶ It is a non-injective transformer. ▶ It supports only authentication systems.
	BioHashing	L	C	M	N	Y	T	▶ User-specific linear quantification addresses intra-user variability.	▶ Security and privacy are partially user-dependent. ▶ It supports only authentication systems.
	BioPhasor	L	C	M	N	Y	T	▶ User-specific non-linear quantification addresses intra-user variability. ▶ It is safer than BioHashing.	▶ Security and privacy are partially user-dependent. ▶ It supports only authentication systems.
	Intrinsic artifacts	L	C	L	N	Y	T	▶ It is resistant to spoofing. ▶ It allows the development of identification systems.	▶ Security and privacy are partially user-dependent.
Protection schemes based on ML or DL	Machine learning	M	C	H	N	Y	T	▶ It addresses intra-user variability. ▶ It minimizes intra-user variability and maximizes inter-user variability. ▶ Highly non-linear protection algorithms.	▶ It has high computational complexity.
	Deep learning	M	C	H	N	Y	T	▶ It addresses intra-user variability. ▶ It solves the challenge of alignment-free protection techniques. ▶ It minimizes intra-user variability and maximizes inter-user variability. ▶ Highly non-linear protection algorithms.	▶ It has a longer enrollment time (training) and needs more extensive databases. ▶ It has a higher computational complexity than ML-based protection techniques.

Therefore, this measure is defined as follows:

$$\mathrm{ef} = \frac{\frac{1}{\beta}\sum_{i=1}^{\beta}\mathrm{RR}_{P,i}}{\mathrm{RR}_{O}} \tag{45}$$

where RR can be the identification rate (IR) of an identification system or the verification rate (VR) of an authentication system ($\mathrm{VR} = 1 - (\mathrm{FRR} + \mathrm{FAR})/2$), the subscripts P and O refer to the recognition rate for the protected and unprotected/original system, respectively. Therefore, $\mathrm{RR}_{P,i}$ corresponds to the protected system recognition rate for version i of the β full versions created in the biometric system.

When $\mathrm{ef} = 1$, the protection system is efficient and does not degrade system performance. A value of $\mathrm{ef} < 1$ means that the protection technique degrades recognition performance. Conversely, a value of $\mathrm{ef} > 1$ indicates that the protection technique increases the recognition rate and the discrimination power of the biometric system. In conclusion, the user-specific supplementary information in two or three recognition factors increases the strength of discrimination.

B. STORAGE COST

The storage cost (SC) is the minimum number of bytes needed to store protected information $\mathbf{D} = [\mathbf{PI}, \mathbf{HD}]$ from the total population of the recognition system:

$$\mathrm{SC} = \theta\left(\mathrm{SC}_{\mathbf{PI}} + \mathrm{SC}_{\mathbf{HD}}\right) \tag{46}$$

where θ is the total number of system users, $\mathrm{SC}_{\mathbf{PI}}$ and $\mathrm{SC}_{\mathbf{HD}}$ are the byte storage cost of the pseudonymous identifier and helper data generated by the protection technique.

C. REVOCABILITY AND RENEWABILITY CAPACITY

This measure indicates the number of protected templates generated from a biometric trait using a BTP technique. This capacity can be *limited* or *non-limited*. Thus, when the number of cancelations and renewals of the protected information depends on the capacity of the RNG and not on the BTP technique, it is called non-limited capacity. On the other hand, a limited capacity is when the number of revocations and renewals depends on the BTP technique and not on the capacity of the RNG.

D. UNLINKABILITY

The unlinkability index (UNI) measures the statistical dependency or linear and non-linear relationship between the versions of protected templates generated for the same user in different applications or biometric systems. This measure evaluates the diversity of the protected templates to avoid cross-matching [192]. Therefore, mutual information measures the linear and non-linear dependencies of a set of random variables. Consequently, the definition of entropy is studied below to establish the mutual information of protected biometric templates with discrete and continuous probability distribution.

1) ENTROPY

Entropy measures the uncertainty or self-information of a random variable; in other words, this is the amount of information provided by the dispersion of all possible states of the variable. Therefore, the entropy depends on the probability function of the variable. So, when a discrete random variable T_1 takes B states with probability function $p(T_{1i})$ for $i = 1, 2, \ldots, B$, the entropy is:

$$H(T_1) = -\sum_{i=1}^{B} p(T_{1i}) \log_2 \{p(T_{1i})\} \tag{47}$$

where $H(T_1) \geq 0$, since $0 \leq p(T_{1i}) \leq 1$. Furthermore, the logarithm is in base two; therefore, the entropy is expressed in bits and quantifies the average number of bits needed to represent the random variable. Thus, the degree of difficulty in predicting the current state of the random variable is more significant if the entropy is greater. Nonetheless, the entropy for a continuous random variable T_1 with probability density function $f(T_1)$ is called differential entropy and is defined as follows [193]:

$$h(T_1) = -\int_{G_1} f(T_1) \log_2 \{f(T_1)\}\, \mathrm{d}T_1 \tag{48}$$

where G_1 is the support set of the random variable. Then, the differential entropy of a continuous random variable T_1 for a normal distribution $\mathcal{N}\left(\mu_1, \sigma_1^2\right)$ with mean $\mu_1 \in \mathbb{R}$ and variance $\sigma_1^2 \in \mathbb{R} > 0$ is:

$$h(T_1) = \frac{1}{2}\log_2\left(2\pi e\sigma_1^2\right) \tag{49}$$

On the other hand, when the random variable T_1 is a binary number of n bits, the random variable follows a binomial distribution $\mathcal{B}(n,p)$ with $n \in \mathbb{N}^+$ and $p = 1/2$, where the probability of obtaining α bits in one regardless of order is described by:

$$f(\alpha) = \binom{n}{\alpha}(p)^{\alpha}(1-p)^{n-\alpha} \tag{50}$$

For $\alpha = 0, 1, 2, \ldots, n$. The binomial distribution can be approximated as a normal distribution $\mathcal{N}(np, np(1-p))$ by the DeMoivre-Laplace theorem when $n \rightarrow \infty$ and p is constant [194], i.e.:

$$f(\alpha) \simeq \frac{e^{-(\alpha-np)^2/2\,np(1-p)}}{\sqrt{(2\pi)\,np\,(1-p)}} \tag{51}$$

As a consequence of the above, the differential entropy for a random binary number T_1 of n bits with binomial distribution $\mathcal{B}(n, 1/2)$ is:

$$h(T_1) \simeq \frac{1}{2}\log_2\left(\frac{\pi e n}{2}\right) \tag{52}$$

2) JOINT ENTROPY

Joint entropy measures the uncertainty associated with a set of random variables. In this order of ideas, the joint differential entropy of two continuous random variables T_1 and T_2 for a two-dimensional joint probability density function $f(\Psi)$ with $\Psi = [T_1, T_2]$ is defined as [193]:

$$h(T_1, T_2) = -\iint_{\mathbf{G}_\Psi} f(\Psi) \log_2 \{f(\Psi)\} \, d\Psi \tag{53}$$

where $\mathbf{G}_\Psi$ is the support set of the random variables T_1 and T_2. Hence, the joint probability density function for the two-dimensional random variable Ψ that has a normal distribution $\mathcal{N}_2(\boldsymbol{\mu}, \Sigma)$ with mean vector $\boldsymbol{\mu}$ and covariance matrix Σ is [195]:

$$f(\Psi) = \frac{e^{-(\Psi-\boldsymbol{\mu})\Sigma^{-1}(\Psi-\boldsymbol{\mu})^T/2}}{2\pi|\Sigma|^{1/2}} \tag{54}$$

Being $|\Sigma|$ the determinant of Σ and also:

$$\boldsymbol{\mu} = [\mu_1, \mu_2] \tag{55}$$

$$\rho_{12} = \frac{\sigma_{12}}{\sigma_1\sigma_2} \tag{56}$$

$$\Sigma = \begin{bmatrix} \sigma_1^2 & \sigma_{12} \\ \sigma_{12} & \sigma_2^2 \end{bmatrix} = \begin{bmatrix} \sigma_1^2 & \rho_{12}\sigma_1\sigma_2 \\ \rho_{12}\sigma_1\sigma_2 & \sigma_2^2 \end{bmatrix} \tag{57}$$

$$|\Sigma| = \sigma_1^2\sigma_2^2\left(1-\rho_{12}^2\right) \tag{58}$$

Then, the joint differential entropy of the normal distribution $\mathcal{N}_2(\boldsymbol{\mu}, \Sigma)$ is defined as follows [193]:

$$h(T_1, T_2) = \frac{1}{2}\log_2\left\{(2\pi e)^2 |\Sigma|\right\} \tag{59}$$

Two n-bit binary random variables T_1 and T_2 that have an approximate normal distribution $\mathcal{N}(n/2, n/4)$ define the following joint differential entropy:

$$h(T_1, T_2) \simeq \frac{1}{2}\log_2\left\{\frac{(\pi en)^2}{4}\left(1-\phi_{12}^2\right)\right\} \tag{60}$$

where ϕ_{12} is the Phi coefficient, which measures the association or linear correlation between two dichotomous variables T_1 and T_2, i.e. two binary numbers. In the binary case $\phi_{12} = \rho_{12}$ [196], [197].

3) CONDITIONAL ENTROPY

The conditional entropy quantifies the uncertainty conditional on a random variable T_1 when another random variable T_2 is known or committed; in other words, this entropy is the amount of information needed to describe the value of T_1 when T_2 is known. Therefore, the conditional differential entropy is:

$$h(T_1|T_2) = h(T_1, T_2) - h(T_2) \tag{61}$$

The variable T_1 can be predicted from T_2 when $h(T1|T2) < h(T1)$, this probability increases if $h(T1|T2)$ decreases. Also, $h(T_1|T_2) \neq h(T_2|T_1)$. The conditional differential entropy of two random variables T_1 and T_2 with normal distribution $\mathcal{N}\left(\mu_1, \sigma_1^2\right)$ and $\mathcal{N}\left(\mu_2, \sigma_2^2\right)$ is defined as follows:

$$h(T_1|T_2) = \frac{1}{2}\log_2\left\{2\pi e\sigma_1^2\left(1-\rho_{12}^2\right)\right\} \tag{62}$$

When the two random variables T_1 and T_2 are binary numbers of n bits, the conditional differential entropy is:

$$h(T_1|T_2) \simeq \frac{1}{2}\log_2\left\{\frac{\pi en}{2}\left(1-\phi_{12}^2\right)\right\} \tag{63}$$

4) MUTUAL INFORMATION

The mutual information measures the statistical dependence and the amount of reciprocal information obtained from a random variable T_1 when another random variable T_2 is observed. Thus, the mutual information corresponds to [193]:

$$I(T_1; T_2) = h(T_1) - h(T_1|T_2) \tag{64}$$

Mutual information is measured in bits when the entropies use logarithm in base two. Moreover, $I(T_1; T_2) \geq 0$ and $I(T_1; T_2) = I(T_2; T_1)$, i.e., T_1 says as much about T_2 as T_2 says about T_1. The mutual information of a random variable with itself is the entropy of the random variable. Finally, two random variables are statistically independent when $I(T_1; T_2) = 0$.

Then, the mutual information of two continuous random variables T_1 and T_2 is obtained as follows:

$$I(T_1; T_2) = -\frac{1}{2}\log_2\left(1-\rho_{12}^2\right) \tag{65}$$

On the other hand, when the two random variables T_1 and T_2 are binary numbers of n bits, the mutual information is approximated as follows:

$$I(T_1; T_2) \simeq -\frac{1}{2}\log_2\left(1-\phi_{12}^2\right) \tag{66}$$

Fig. 29 illustrates the behavior of (65) and (66). If $\rho_{12} = \phi_{12} = \pm 1$ then two variables are perfectly correlated and the mutual information or statistical dependence is infinite.

5) UNLINKABILITY INDEX

This measure quantifies the linear and non-linear relationship between the β versions of protected templates from the same biometric source. Then, the calculation of the mutual information of template pairs produces the unlinkability index (UNI) in a system of θ users under the same BTP technique:

$$\text{UNI} = \varphi \sum_{i=1}^{\theta} \sum_{j=1}^{\beta-1} \sum_{k=j+1}^{\beta} I\left(T_{i,j}; T_{i,k}\right) \tag{67}$$

$$\varphi = \frac{2}{\theta\beta(\beta-1)} \tag{68}$$

where $T_{i,j}$ is the version j of the protected template for user i and $T_{i,k}$ is the version k of the protected template for user i. Assuming that $T_{i,k}$ is committed. Therefore, UNI at zero or close to zero indicates good diversity.

E. IRREVERSIBILITY

An original biometric template must be computationally difficult to obtain when a protected version is compromised. Therefore, the degree of irreversibility is an essential measure in evaluating BTP techniques.

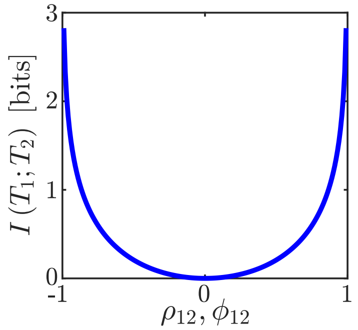


FIGURE 29. Mutual information as a function of the correlation coefficient ρ_{12}.

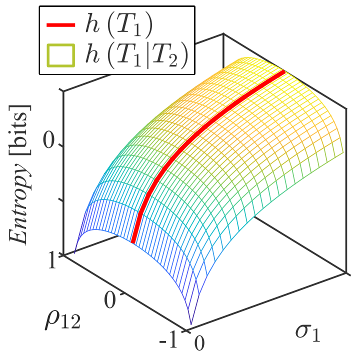


FIGURE 30. Conditional differential entropy with $-1 \leq \rho_{12} \leq 1$ and $\sigma_1 > 0$.

1) IRREVERSIBILITY INDEX

The irreversibility index (IRI) uses conditional entropy to quantify the difficulty of reverting a protected template. Fig. 30 illustrates the uncertainty or difficulty of obtaining T_1 when T_2 is known. The most significant degree of difficulty occurs for two statistically independent variables, i.e., $h(T_1|T_2) = h(T_1)$. Therefore, a normalized uncertainty corresponds to $h(T_1|T_2)/h(T_1)$; if this relation is equal to one, then the degree of irreversibility is null and the BTP technique preserves the privacy of the biometric information [198].

The irreversibility index is evaluated for the β versions of protected templates of the θ users that use the protection technique, that is:

$$\mathrm{IRI} = \frac{1}{\theta\beta}\sum_{i=1}^{\theta}\sum_{j=1}^{\beta}\frac{h\left(T_{i,O}|T_{i,j}\right)}{h\left(T_{i,O}\right)} \tag{69}$$

where $T_{i,O}$ is the original biometric template of the subject i and $T_{i,j}$ is the version j of the protected template for the user i. Thus, IRI at one or close to one indicates good security and privacy of biometric information, consequently, a reliable BTP technique.

F. INTEROPERABILITY

BTP techniques must be efficient, flexible, safe, fast, and computationally inexpensive. In addition, the techniques must attend to the standardizations in biometric signal processing and personal information management. Therefore, interoperability is the overall evaluation of the performance, cost, security, privacy, flexibility, and scalability of an implemented BTP technique.

XIV. COMMERCIAL PRODUCTS WITH BTP TECHNIQUES

Technology companies are increasingly implementing biometric services or systems in their devices. Therefore, the security and privacy of biometric data are essential. Currently, companies such as Apple, Samsung, Microsoft, Google, Amazon, etc., are developing authentication systems that protect biometric information but do not directly provide the property cancelation and renewal of templates. For example, Apple developed *Touch ID* and *Face ID* authentication technologies, which safeguard biometric data's privacy and security using AES algorithms. However, these authentication technologies do not allow decision-making in the protected domain. Therefore, this section presents commercial (non-academics) products based on revocable biometric systems using BTP techniques.

- **GenKey Group** [199]: This company develops biometric software and provides various biometric recognition products and services used globally by governments, public institutions, and businesses. GenKey was developed out of a merger with Priv-ID. This company offers a BTP implementation using *BioHASH*®, a patented software that provides privacy and security to biometric templates through a stable code generation and hash function. This product complies with ISO/IEC 24745 for biometric traits such as fingerprint, vein, iris, voice, and face. In addition, this product has limited biometric entropy.
- **Precise Biometrics** [200]: This company offers biometric identification software worldwide. This company provides a facial recognition product called *Precise YOUNiQ*™, which maximizes the security and privacy of biometric information using AES 256-bit algorithms with unique keys for each image.
- **Hitachi Group** [201]: This company developed a finger vein authentication technology called *VeinID*. This technology offers physical and logical access control for multiple applications or services, e.g., cardless payment systems. Moreover, this company provides authentication modules with finger veins and fingerprints for embedding in devices. Furthermore, this company offers cancelable authentication technology, where biometric data can be revoked by changing the encryption key [202]. Likewise, this company develops cancelable authentication systems based on correlation filters, specifically correlation-invariant random filtering [141].
- **Private Identity LLC** [203]: This company developed and patented a solution for fully homomorphic encryption. This company developed a technology called *Private ID*®, which provides revocable biometric systems based on face, voice, and fingerprint. This

technology preserves the user's privacy and security by efficiently implementing homomorphic encryption.

The development of commercial products with revocable biometric systems is limited. However, several companies are implementing biometric systems in their devices but still need to develop cancelable systems. Therefore, the implementation of protection techniques in real-life biometric applications or services is an open challenge in the field of BTP.

XV. CONCLUSION AND FUTURE DIRECTIONS

Biometric data consists of non-cancelable and non-renewable personal information. Therefore, the security and privacy of biometrics are critical challenges in the rise of IoT devices implementing biometric systems. This research examined vulnerabilities and proposed countermeasures for biometric systems at the hardware and software level (BTP techniques under ISO standardization). In addition, this work defined a taxonomy according to the operating principle and the type of supplementary information supported by the BTP techniques, analyzing the security, privacy, revocability, renewability, computational complexity, and distribution of biometric information for these protection techniques. Moreover, this document established quantitative evaluation measures based on information theory to compare BTP techniques. Currently, there is no obsolete protection technique. However, this manuscript gives a better overview of the advantages and disadvantages of each BTP technique.

The selection of the most suitable protection technique for a biometric system is challenging, but this research provided a detailed review of existing BTP techniques. Moreover, the proposed metrics have real-life application scenarios when different techniques need to be compared to analyze their security (irreversibility), privacy (unlikability), lifetime (revocability and renewability capacity), and performance (efficiency). This comparison helps to select the most suitable technique, e.g., in biometric applications or services with limited resources. Another application scenario is the selection of the most appropriate technique to avoid tracking, linking, cross-matching, and other personal data mining attacks in the interoperability of biometric applications or services.

On the other hand, protection techniques based on injective mappings safeguard authentication and identification systems. Furthermore, linear and injective mappings do not need to re-train the biometric system when the information is canceled and renewed. Likewise, cancelable biometrics techniques allow decision-making in the protected domain, reducing computational costs and increasing processing speed. Additionally, protection schemes based on user-specific supplementary information improve the recognition rate only in authentication systems. Finally, protection schemes based on machine learning or deep learning address the challenge of alignment-free protection systems.

Investigations in the area of BTP have solved several challenges, e.g., the three challenges addressed in this document: alignment-free protection techniques, re-training, and quantitative evaluation metrics. However, some challenges need to be addressed. Therefore, the following list of future directions is presented:

- BTP techniques must be implemented and compared under evaluation metrics using authentication and identification systems with extensive databases. A secure option is to use databases based on biometric signals of liveliness, e.g., ECG, PPG, and others.
- BTP techniques are based on randomly created supplementary information. Therefore, secure and stable RNGs should be studied in detail because each BTP technique demands supplementary information with a unique distribution and range of values. In addition, RNGs should contribute to the security and privacy of supplementary information. For this reason, physical unclonable functions (PUF) are an excellent opportunity to generate secure supplementary information.
- Intra-user variability in the short and long term is a current challenge for biometric systems, but the security and privacy of biometric information are necessary. Therefore, new BTP techniques can help to address this challenge and protect biometric data. Even adaptive and cancelable biometric systems are the future direction in the field of biometrics.
- Cancelable biometrics will minimize intra-user variability and maximize inter-user variability while protecting and revoking biometric information. Consequently, the future perspective of cancelable biometrics corresponds to binding hardware and software countermeasures that reduce the computational cost and execution time, increasing the security and privacy of biometric information.
- Biometric cryptosystems need to develop new techniques and improve the techniques that enable decision-making in the protected domain, e.g., knowledge signature and homomorphic encryption. Furthermore, this family of techniques has the challenge of dealing with intra-user variability through error correction codes with low computational costs.
- ML or DL-based protection techniques need to address the re-training challenge, i.e., if a single protected template is compromised, then all parameters of the decision-making module should not be re-enrolled.
- BTP techniques must be tested and analyzed for active and passive attacks. This study would help to identify the vulnerabilities of the protection techniques. As a result, BTP techniques can be improved to prevent successful attacks, disclosure, or undesired learning of sensitive and non-private biometric information.
- More commercial biometric products with BTP techniques need to be developed. Most biometric systems with BTP techniques are in academia, and existing commercial products are mostly authentication systems. However, the implementation of BTP techniques in

the real world considers the computational cost and execution time.

- The protection of biometric information safeguards privacy and prevents the disclosure of permanent information in the user's life. Therefore, the protection of biometric information should have greater social acceptance.

REFERENCES

[1] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "EHealth cloud security challenges: A survey," *J. Healthcare Eng.*, vol. 2019, pp. 1–15, Sep. 2019.

[2] A. Khanna and S. Kaur, "Internet of Things (IoT), applications and challenges: A comprehensive review," *Wireless Pers. Commun.*, vol. 114, no. 2, pp. 1687–1762, Sep. 2020.

[3] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. Mcguire, "Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security," *ACM Comput. Surveys*, vol. 53, no. 4, pp. 1–29, Jul. 2020.

[4] J. C. Bernal-Romero, J. M. Ruíz-Echeverri, J. M. Ramírez-Cortés, P. Gomez-Gil, J. Rangel-Magdaleno, and I. Cruz-Vega, "On signal variability of ECG-based biometric system under practical considerations," in *Proc. IEEE Mex. Humanitarian Technol. Conf. (MHTC)*, Puebla, Mexico, Apr. 2021, pp. 19–24.

[5] J. M. Ruiz-Echeverri, J. C. Bernal-Romero, J. M. Ramirez-Cortes, P. Gomez-Gil, J. Rangel-Magdaleno, and H. Peregrina-Barreto, "Dorsal hand veins biometrics using NIR images with fusion of classifiers at score level," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (IMTC)*, Glasgow, U.K., May 2021, pp. 1–6.

[6] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things security: A review," *Sensors*, vol. 21, no. 18, p. 6163, Sep. 2021.

[7] M. S. Obaidat, S. P. Rana, T. Maitra, D. Giri, and S. Dutta, "Biometric security and Internet of Things (IoT)," in *Biometric-Based Physical and Cybersecurity Systems*, M. S. Obaidat, I. Traore, and I. Woungang, Eds. Berlin, Germany: Springer, 2019, ch. 19, pp. 477–509.

[8] A. Sundararajan, A. I. Sarwat, and A. Pons, "A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems," *ACM Comput. Surveys*, vol. 52, no. 2, pp. 1–36, May 2019.

[9] A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, "Opportunities and challenges of using biometrics for business: Developing a research agenda," *J. Bus. Res.*, vol. 136, pp. 52–62, Nov. 2021.

[10] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognit. Lett.*, vol. 138, pp. 346–354, Oct. 2020.

[11] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection," *Inf. Fusion*, vol. 64, pp. 131–148, Dec. 2020.

[12] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-DF: A large-scale challenging dataset for DeepFake forensics," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Seattle, WA, USA, Jun. 2020, pp. 3204–3213.

[13] J. C. Moreno-Rodriguez, J. M. Ramirez-Cortes, J. C. Atenco-Vazquez, and R. Arechiga-Martinez, "EEG and voice bimodal biometric authentication scheme with fusion at signal level," in *Proc. IEEE Mex. Humanitarian Technol. Conf. (MHTC)*, Puebla, Mexico, Apr. 2021, pp. 52–58.

[14] D. E. Mancilla-Palestina, J. A. Jimenez-Duarte, J. M. Ramirez-Cortes, A. Hernandez, P. Gomez-Gil, and J. Rangel-Magdaleno, "Embedded system for bimodal biometrics with fiducial feature extraction on ECG and PPG signals," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (IMTC)*, Dubrovnik, Croatia, May 2020, pp. 1–6.

[15] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[16] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, pp. 1–44, Jul. 2021.

[17] Manisha and N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, no. 5, pp. 3403–3446, Jun. 2020.

[18] M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101700.

[19] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 27721–27776, Oct. 2020.

[20] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.

[21] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 113, pp. 1–17, Jan. 2008.

[22] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, Dec. 2011.

[23] J. C. B. Romero, "Sistema biométrico basado en ECG e implementación en un sistema embebido con VHDL," M.S. thesis, Maestría en Electrónica, INAOE, Puebla, Mexico, 2020. [Online]. Available: http://inaoe.repositorioinstitucional.mx/jspui/handle/1009/1990

[24] R. Arjona and I. Baturone, "A dual-factor access control system based on device and user intrinsic identifiers," in *Proc. 42nd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Florence, Italy, Oct. 2016, pp. 4731–4736.

[25] R. Arjona, M. A. Prada-Delgado, I. Baturone, and A. Ross, "Securing minutia cylinder codes for fingerprints through physically unclonable functions: An exploratory study," in *Proc. Int. Conf. Biometrics (ICB)*, Gold Coast, QLD, Australia, Feb. 2018, pp. 54–60.

[26] P. Campisi, "Security and privacy in biometrics: Towards a holistic approach," in *Security and Privacy in Biometrics*. London, U.K.: Springer, 2013, ch. 1, pp. 1–23.

[27] B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 31–41, Sep. 2015.

[28] J. Breebaart, C. Busch, J. Grave, and E. Kindt, "A reference architecture for biometric template protection based on pseudo identities," in *Proc. BIOSIG Biometrics Electron. Signatures*, 2008, pp. 25–37.

[29] S. Rane, "Standardization of biometric template protection," *IEEE MultimediaMag.*, vol. 21, no. 4, pp. 94–99, Oct. 2014.

[30] K. Takahashi and S. Hirata, "Parameter management schemes for cancelable biometrics," in *Proc. IEEE Workshop Comput. Intell. Biometrics Identity Manage. (CIBIM)*, Paris, France, Apr. 2011, pp. 145–151.

[31] C. Vielhauer, J. Dittmann, and S. Katzenbeisser, "Design aspects of secure biometric systems and biometrics in the encrypted domain," in *Security and Privacy in Biometrics*, P. Campisi, Ed. London, U.K.: Springer, 2013, ch. 2, pp. 25–43.

[32] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proc. 7th workshop Multimedia Secur.*, New York, NY, USA, Aug. 2005, pp. 111–116.

[33] S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric hash functions for fingerprint minutiae," in *Pattern Recognition and Image Analysis*, S. Singh, M. Singh, C. Apte, and P. Perner, Eds. Berlin, Germany: Springer, Aug. 2005, pp. 30–38.

[34] K. B. Raja, R. Raghavendra, and C. Busch, "Towards protected and cancelable multi-spectral face templates using feature fusion and kernalized hashing," in *Proc. 21st Int. Conf. Inf. Fusion (FUSION)*, Cambridge, U.K., Jul. 2018, pp. 2098–2106.

[35] K. B. Raja, R. Raghavendra, and C. Busch, "Manifold-structure preserving biometric templates—A preliminary study on fully cancelable smartphone biometric templates," in *Proc. IEEE Int. Conf. Multimedia Expo. Workshops (ICMEW)*, San Diego, CA, USA, Jul. 2018, pp. 1–7.

[36] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Proc. IEEE Symp. Secur. Privacy. (SP)*, Oakland, CA, USA, May 2001, pp. 202–213.

[37] H. Feng and C. Choong Wah, "Private key generation from on-line handwritten signatures," *Inf. Manage. Comput. Secur.*, vol. 10, no. 4, pp. 159–164, Oct. 2002.

[38] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," in *Proc. Int. Conf. Pattern Recognit.*, Quebec City, QC, Canada, vol. 1, Aug. 2002, pp. 123–126.

[39] C. M. Issac and E. Grace Mary Kanaga, "Probing on classification algorithms and features of brain signals suitable for cancelable biometric authentication," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Coimbatore, India, Dec. 2017, pp. 1–4.

[40] F. Lin, K. W. Cho, C. Song, W. Xu, and Z. Jin, "Brain password: A secure and truly cancelable brain biometrics for smart headwear," in *Proc. MobiSys*, New York, NY, USA, Jun. 2018, pp. 296–309.

[41] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.

[42] S. Rane, Y. Wang, S. Drape, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[43] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[44] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[45] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, 2016.

[46] M. Sandhya and M. V. N. K. Prasad, "Biometric template protection: A systematic literature review of approaches and modalities," in *Biometric Security and Privacy: Opportunities & Challenges in The Big Data Era*, R. Jiang, S. Al-maadeed, A. Bouridane, P. D. Crookes, and A. Beghdadi, Eds. Cham, Switzerland: Springer, 2017, ch. 14, pp. 323–370.

[47] B. Choudhury, P. Then, B. Issac, V. Raman, and M. K. Haldar, "A survey on biometrics and cancelable biometrics systems," *Int. J. Image Graph.*, vol. 18, no. 1, Jan. 2018, Art. no. 1850006.

[48] P. Sharma, G. S. Walia, and R. Rohilla, "Recent advancement in cancelable biometric for user recognition: A brief survey," in *Proc. 9th Int. Conf. Syst. Model. Advancement Res. Trends (SMART)*, Moradabad, India, Dec. 2020, pp. 137–146.

[49] P. Sharma, G. S. Walia, and R. Rohilla, "Alignment-free cancelable biometric: A contemporary survey, opportunities & challenges," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Thoothukudi, India, Dec. 2020, pp. 881–889.

[50] A. Singh, A. Arora, G. Jaswal, and A. Nigam, "Comprehensive survey on cancelable biometrics with novel case study on finger dorsal template protection," *J. Banking Financial Technol.*, vol. 4, no. 1, pp. 37–52, Apr. 2020.

[51] P. Jayapriya, R. R. Manimegalai, R. L. Kumar, S. Kadry, and S. Seo, "A survey on different techniques for biometric template protection," *J. Internet Technol.*, vol. 21, no. 5, pp. 1347–1362, Sep. 2020.

[52] A. Thawre, A. Hariyale, and B. R. Chandavarkar, "Survey on security of biometric data using cryptography," in *Proc. 2nd Int. Conf. Secure Cyber Comput. Commun. (ICSCCC)*, Jalandhar, India, May 2021, pp. 90–95.

[53] Q. N. Tran, B. P. Turnbull, and J. Hu, "Biometrics and privacy-preservation: How do they evolve?" *IEEE Open J. Comput. Soc.*, vol. 2, pp. 179–191, 2021.

[54] M. Lim, A.-B. Teoh, and J. Kim, "Biometric feature-type transformation: Making templates compatible for secret protection," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 77–87, Sep. 2015.

[55] B. Kitchenham, "Procedures for performing systematic reviews," Keele Univ., Keele, U.K., Tech. Rep. TR/SE-0401, 2004.

[56] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 1999, pp. 28–36.

[57] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[58] E. Maiorana, P. Campisi, and A. Neri, "User adaptive fuzzy commitment for signature template protection and renewability," *J. Electron. Imag.*, vol. 17, no. 1, 2008, Art. no. 011011.

[59] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *Proc. IEEE Workshop Inf. Forensics Secur.*, Seattle, WA, USA, Dec. 2010, pp. 1–6.

[60] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. J. Veldhuis, and C. Busch, "Multi-algorithm fusion with template protection," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory Appl. Syst.*, Washington, DC, USA, Sep. 2009, pp. 1–8.

[61] S. Billeb, C. Rathgeb, H. Reininger, K. Kasper, and C. Busch, "Biometric template protection for speaker recognition based on universal background models," *IET Biometrics*, vol. 4, no. 2, pp. 116–126, Jun. 2015.

[62] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature," in *Proc. ICPR*, Tampa, FL, USA, Dec. 2008, pp. 1–4.

[63] W. Yang, S. Wang, J. Hu, G. Zheng, J. Chaudhry, E. Adi, and C. Valli, "Securing mobile healthcare data: A smart card based cancelable finger-vein bio-cryptosystem," *IEEE Access*, vol. 6, pp. 36939–36947, 2018.

[64] R. Damaševičius, R. Maskeliūnas, E. Kazanavičius, and M. Woźniak, "Combining cryptography with EEG biometrics," *Comput. Intell. Neurosci.*, vol. 2018, pp. 1–11, May 2018.

[65] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Lausanne, Switzerland, Feb. 2002, pp. 237–257.

[66] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in *Proc. IEEE Biometrics Symp.*, Baltimore, MD, USA, Sep. 2007, pp. 1–6.

[67] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[68] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Cryptographic key generation using handwritten signature," *Proc. SPIE*, vol. 6202, pp. 225–231, Apr. 2006.

[69] H. Liu, D. Sun, K. Xiong, and Z. Qiu, "Palmprint based multidimensional fuzzy vault scheme," *Sci. World J.*, vol. 2014, pp. 1–8, Apr. 2014.

[70] A. Kumar, M. Hanmandlu, and H. M. Gupta, "A new scheme for the polynomial based biometric cryptosystems," *ISRN Mach. Vis.*, vol. 2014, pp. 1–13, Apr. 2014.

[71] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim, "Biometric key binding: Fuzzy vault based on iris images," in *Advanced Biometrics*, S.-W. Lee and S. Z. Li, Eds. Berlin, Germany: Springer, Aug. 2007, pp. 800–808.

[72] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in *Advanced Biometrics*, S.-W. Lee and S. Z. Li, Eds. Berlin, Germany: Springer, Aug. 2007, pp. 927–937.

[73] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology—EUROCRYPT 2004*, C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer, 2004, pp. 523–540.

[74] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *Proc. 2nd ACM Symp. Inf. Comput. Commun. Secur.*, New York, NY, USA, Mar. 2007, pp. 353–355.

[75] C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaar, and A. H. M. Akkermans, "Biometric quantization through detection rate optimized bit allocation," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, May 2009, Art. no. 784834.

[76] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[77] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *Audio- and Video-Based Biometric Person Authentication*, T. Kanade, A. Jain, and N. K. Ratha, Eds. Berlin, Germany: Springer, 2005, pp. 436–446.

[78] C. Rathgeb and A. Uhl, "An iris-based interval-mapping scheme for biometric key generation," in *Proc. 6th Int. Symp. Image Signal Process. Anal.*, Salzburg, Austria, Sep. 2009, pp. 511–516.

[79] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and M. K. O. Goh, "Multimodal biometrics based bit extraction method for template security," in *Proc. 6th IEEE Conf. Ind. Electron. Appl.*, Beijing, China, Jun. 2011, pp. 1971–1976.

[80] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proc. IEEE Int. Conf. Multimedia Expo. (ICME)*, Taipei, Taiwan, vol. 3, Jun. 2004, pp. 2203–2206.

[81] P. Wang, L. You, G. Hu, L. Hu, Z. Jian, and C. Xing, "Biometric key generation based on generated intervals and two-layer error correcting technique," *Pattern Recognit.*, vol. 111, Mar. 2021, Art. no. 107733.

[82] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, "Digital signatures," in *Handbook of Applied Cryptography*, 5th ed. Boca Raton, FL, USA: CRC Press, 2001, ch. 11.

[83] M. Abid, S. Kanade, D. Petrovska-Delacretaz, B. Dorizzi, and H. Afifi, "Iris based authentication mechanism for e-passports," in *Proc. 2nd Int. Workshop Secur. Commun. Netw. (IWSCN)*, Karlstad, Sweden, May 2010, pp. 1–5.

[84] K. Xi, T. Ahmad, F. Han, and J. Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 487–499, Dec. 2011.

[85] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Exp. Syst. Appl.*, vol. 42, no. 21, pp. 8198–8211, Nov. 2015.

[86] B. Choudhury, P. Then, V. Raman, B. Issac, and M. K. Haldar, "Cancelable iris biometrics based on data hiding schemes," in *Proc. IEEE Student Conf. Res. Develop.*, Kuala Lumpur, Malaysia, Dec. 2016, pp. 1–6.

[87] M. K. Khan, J. Zhang, and L. Tian, "Protecting biometric data for personal identification," in *Advances in Biometric Person Authentication*, S. Z. Li, J. Lai, T. Tan, G. Feng, and Y. Wang, Eds. Berlin, Germany: Springer, 2005, pp. 629–638.

[88] C. Kant and S. Chaudhary, "A watermarking based approach for protection of templates in multimodal biometric system," *Proc. Comput. Sci.*, vol. 167, pp. 932–941, Jan. 2020.

[89] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools Appl.*, vol. 75, no. 23, pp. 16333–16361, Dec. 2016.

[90] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 70–81, Mar. 2011.

[91] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *Advances in Cryptology—CRYPTO'97*, B. S. Kaliski, Ed. Berlin, Germany: Springer, May 1997, pp. 410–424.

[92] J. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, Dept. Comput. Sci., Econ., Finance, ETH Zürich, Switzerland, 1998. [Online]. Available: https://elibrary.ru/item.asp?id=6884537

[93] W. Xu, Q. He, Y. Li, and T. Li, "Cancelable voiceprint templates based on knowledge signatures," in *Proc. Int. Symp. Electron. Commerce Secur.*, Guangzhou, China, Aug. 2008, pp. 412–415.

[94] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP J. Inf. Secur.*, vol. 2007, pp. 1–20, Jan. 2007.

[95] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT'99*, J. Stern, Ed. Berlin, Germany: Springer, Apr. 1999, pp. 223–238.

[96] J. Katz and Y. Lindell, "Additional public-key encryption schemes," in *Introduction to Modern Cryptography: Principles and Protocols*, 1st ed. London, U.K.: Chapman & Hall CRC, 2007, ch. 11.

[97] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, Jan. 2013.

[98] C. Karabat, M. S. Kiraz, H. Erdogan, and E. Savas, "THRIVE: Threshold homomorphic encryption based secure and privacy preserving biometric verification system," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, pp. 1–18, Aug. 2015.

[99] S. Rane and P. T. Boufounos, "Privacy-preserving nearest neighbor methods: Comparing signals without revealing them," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 18–28, Mar. 2013.

[100] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017.

[101] M. Gomez-Barrero, J. Fierrez, and J. Galbally, "Variable-length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. 4th Int. Conf. Biometrics Forensics (IWBF)*, Limassol, Cyprus, Mar. 2016, pp. 1–6.

[102] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "Privacy-preserving fingercode authentication," in *Proc. 12th ACM workshop Multimedia Secur.*, New York, NY, USA, Sep. 2010, pp. 231–240.

[103] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in *Computer Security—ESORICS 2011*, V. Atluri and C. Diaz, Eds. Berlin, Germany: Springer, 2011, pp. 190–209.

[104] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in *Privacy Enhancing Technologies*, I. Goldberg and M. J. Atallah, Eds. Berlin, Germany: Springer, 2009, pp. 235–253.

[105] X. Yang, H. Zhu, S. Zhang, R. Lu, and X. Gao, "An efficient and privacy-preserving biometric identification scheme based on the FITing-tree," *Secur. Commun. Netw.*, vol. 2021, pp. 1–15, Oct. 2021.

[106] A. Nautsch, S. Isadskiy, J. Kolberg, M. Gomez-Barrero, and C. Busch, "Homomorphic encryption for speaker recognition: Protection of biometric templates and vendor model parameters," 2018, *arXiv:1803.03559*.

[107] J. Kolberg, P. Bauspieß, M. Gomez-Barrero, C. Rathgeb, M. Dürmuth, and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Delft, The Netherlands, Dec. 2019, pp. 1–6.

[108] W. Yang, S. Wang, K. Yu, J. J. Kang, and M. N. Johnstone, "Secure fingerprint authentication with homomorphic encryption," in *Proc. Digit. Image Comput. Techn. Appl. (DICTA)*, Melbourne, VIC, Australia, Nov. 2020, pp. 1–6.

[109] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of Ratha," in *Proc. Int. Symp. Comput. Sci. Comput. Technol.*, Shanghai, China, vol. 2, Dec. 2008, pp. 572–575.

[110] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[111] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Information Security*, Samarati and Ardagna, Eds. Berlin, Germany: Springer, 2009, pp. 135–142.

[112] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *Information Security and Privacy*, C. Boyd and J. González, Eds. Berlin, Germany: Springer, 2005, pp. 242–252.

[113] E. Piciucco, E. Maiorana, C. Kauba, A. Uhl, and P. Campisi, "Cancelable biometrics for finger vein recognition," in *Proc. 1st Int. Workshop Sens., Process. Learn. Intell. Mach. (SPLINE)*, Aalborg, Denmark, Jul. 2016, pp. 1–5.

[114] C. Kauba, E. Piciucco, E. Maiorana, M. Gomez-Barrero, B. Prommegger, P. Campisi, and A. Uhl, "Towards practical cancelable biometrics for finger vein recognition," *Inf. Sci.*, vol. 585, pp. 395–417, Mar. 2022.

[115] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proc. 19th Int. Conf. Pattern Recognit.*, Tampa, FL, USA, Dec. 2008, pp. 1–4.

[116] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, Dec. 2002.

[117] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Proc. CVPR Worshop*, Minneapolis, MN, USA, Jun. 2007, pp. 1–7.

[118] C. Rathgeb and C. Busch, "Comparison score fusion towards an optimal alignment for enhancing cancelable iris biometrics," in *Proc. 4th Int. Conf. Emerg. Secur. Technol.*, Cambridge, U.K., Sep. 2013, pp. 51–54.

[119] N. Kumar, S. Singh, and A. Kumar, "Random permutation principal component analysis for cancelable biometric recognition," *Appl. Intell.*, vol. 48, no. 9, pp. 2824–2836, Sep. 2018.

[120] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 3, pp. 525–538, May 2010.

[121] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, and A. Neri, "Template protection for HMM-based on-line signature authentication," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Anchorage, AK, USA, Jun. 2008, pp. 1–6.

[122] E. Abdellatef, E. M. Omran, R. F. Soliman, N. A. Ismail, S. E. S. E. Abd Elrahman, K. N. Ismail, M. Rihan, F. E. Abd El-Samie, and A. A. Eisa, "Fusion of deep-learned and hand-crafted features for cancelable recognition systems," *Soft Comput.*, vol. 24, no. 20, pp. 15189–15208, Oct. 2020.

[123] Y. Wang and D. Hatzinakos, "Cancelable face recognition using random multiplicative transform," in *Proc. 20th Int. Conf. Pattern Recognit.*, Istanbul, Turkey, Aug. 2010, pp. 1261–1264.

[124] H. Kaur and P. Khanna, "PolyCodes: Generating cancelable biometric features using polynomial transformation," *Multimedia Tools Appl.*, vol. 79, pp. 20729–20752, Aug. 2020.

[125] D. Achlioptas, "Database-friendly random projections," in *Proc. 20th ACM SIGMOD-SIGACT-SIGART Symp. Princ. Database Syst.*, New York, NY, USA, May 2001, pp. 274–281.

[126] Y. Wang and D. Hatzinakos, "Sorted index numbers for privacy preserving face recognition," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, pp. 1–16, Oct. 2009.

[127] Z. Lingli and L. Jianghuang, "Security algorithm of face recognition based on local binary pattern and random projection," in *Proc. 9th IEEE Int. Conf. Cognit. Informat. (ICCI)*, Beijing, China, Jul. 2010, pp. 733–738.

[128] M. Deshmukh and M. K. Balwant, "Generating cancelable palmprint templates using local binary pattern and random projection," in *Proc. 13th Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS)*, Jaipur, India, Dec. 2017, pp. 203–209.

[129] Y. Kim and K.-A. Toh, "Sparse random projection for efficient cancelable face feature extraction," in *Proc. 3rd IEEE Conf. Ind. Electron. Appl.*, Singapore, Jun. 2008, pp. 2139–2144.

[130] P. Li, T. J. Hastie, and K. W. Church, "Very sparse random projections," in *Proc. 12th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, New York, NY, USA, Aug. 2006, pp. 287–296.

[131] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Dallas, TX, USA, Mar. 2010, pp. 1838–1841.

[132] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 9, pp. 1877–1893, Sep. 2011.

[133] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Washington, DC, USA, Sep. 2010, pp. 1–7.

[134] P. Punithavathi and S. Geetha, "Dynamic sectored random projection for cancelable iris template," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Jaipur, India, Sep. 2016, pp. 711–715.

[135] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102704.

[136] S. Wang and J. Hu, "A Hadamard transform-based method for the design of cancellable fingerprint templates," in *Proc. 6th Int. Congr. Image Signal Process. (CISP)*, vol. 3, Hangzhou, China, Dec. 2013, pp. 1682–1687.

[137] H. Kaur and P. Khanna, "Gaussian random projection based non-invertible cancelable biometric templates," *Proc. Comput. Sci.*, vol. 54, pp. 661–670, Jan. 2015.

[138] H. Kaur and P. Khanna, "Non-invertible biometric encryption to generate cancelable biometric templates," in *Proc. World Congr. Eng. Comput. Sci.*, vol. 1, 2017, pp. 432–435.

[139] M. Savvides, B. V. K. Vijaya Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR)*, vol. 3, Cambridge, U.K., Aug. 2004, pp. 922–925.

[140] S. Hirata and K. Takahashi, "Cancelable biometrics with perfect secrecy for correlation-based matching," in *Advanced Biometrics*, M. Tistarelli and M. S. Nixon, Eds. Berlin, Germany: Springer, 2009, pp. 868–878.

[141] K. Takahashi and S. H. Hitachi, "Generating provably secure cancelable fingerprint templates based on correlation-invariant random filtering," in *Proc. IEEE 3rd Int. Conf. Biometrics, Theory, Appl., Syst.*, Washington, DC, USA, Sep. 2009, pp. 1–6.

[142] L. Leng, J. S. Zhang, M. K. Khan, X. Bi, and M. Ji, "Cancelable PalmCode generated from randomized Gabor filters for palmprint protection," in *Proc. Int. Conf. Image Vis. Comput.*, Queenstown, New Zealand, Nov. 2010, pp. 1–6.

[143] H. A. A. El-Hameed, N. Ramadan, W. El-Shafai, A. A. M. Khalaf, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, "Cancelable biometric security system based on advanced chaotic maps," *Vis. Comput.*, vol. 38, no. 6, pp. 2171–2187, Jun. 2022.

[144] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, no. 7, pp. 422–426, Jul. 1970.

[145] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive Bloom filters," in *Proc. Int. Conf. Biometrics (ICB)*, Madrid, Spain, Jun. 2013, pp. 1–8.

[146] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on Bloom filters," *Inf. Fusion*, vol. 42, pp. 37–50, Jul. 2018.

[147] J. Hermans, B. Mennink, and R. Peeters, "When a Bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system," in *Proc. Int. Conf. Biometrics Special Interest Group*, Darmstadt, Germany, Sep. 2014, pp. 1–6.

[148] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of Bloom filters to iris biometrics," *IET Biometrics*, vol. 3, no. 4, pp. 207–218, Dec. 2014.

[149] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch, "Protected facial biometric templates based on local Gabor patterns and adaptive Bloom filters," in *Proc. 22nd Int. Conf. Pattern Recognit.*, Stockholm, Sweden, Dec. 2014, pp. 4483–4488.

[150] G. Li, B. Yang, C. Busch, and C. Rathgeb, "Towards generating protected fingerprint templates based on Bloom filters," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Gjovik, Norway, Mar. 2015, pp. 1–6.

[151] J. Y. Jeong and I. R. Jeong, "Efficient cancelable iris template generation for wearable sensors," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Jul. 2019.

[152] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," in *Communications and Multimedia Security. Advanced Techniques for Network and Data Protection*, A. Lioy and D. Mazzocchi, Eds. Berlin, Germany: Springer, 2003, pp. 1–13.

[153] 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, Apr. 2004.

[154] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[155] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on biohashing," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Reykjavik, Iceland, Jul. 2013, pp. 1–8.

[156] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

[157] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," *Pattern Recognit.*, vol. 39, no. 7, pp. 1359–1368, Jul. 2006.

[158] C. S. Chin, A. T. B. Jin, and D. N. C. Ling, "High security iris verification system based on random secret integration," *Comput. Vis. Image Understand.*, vol. 102, no. 2, pp. 169–177, May 2006.

[159] Y.-H. Pang, A. T. B. Jin, and D. N. C. Ling, "Palmprint based cancelable biometric authentication system," *Int. J. Comput. Inf. Eng.*, vol. 1, no. 9, pp. 2915–2921, 2007.

[160] R. Belguechi, C. Rosenberger, and S. Ait-Aoudia, "Biohashing for securing minutiae template," in *Proc. 20th Int. Conf. Pattern Recognit. (ICPR)*, Istanbul, Turkey, Aug. 2010, pp. 1168–1171.

[161] R. Belguechi, E. Cherrier, M. El Abed, and C. Rosenberger, "Evaluation of cancelable biometric systems: Application to finger-knuckle-prints," in *Proc. Int. Conf. Hand-Based Biometrics*, Hong Kong, Nov. 2011, pp. 1–6.

[162] A. B. J. Teoh and D. C. L. Ngo, "BioPhasor: Token supplemented cancellable biometrics," in *Proc. 9th Int. Conf. Control Automat. Robot. Vis.*, Dec. 2006, pp. 1–5.

[163] A. B. J. Teoh, K.-A. Toh, and W. K. Yip, "2^N discretisation of BioPhasor in cancellable biometrics," in *Advances in Biometrics*, S.-W. Lee and S. Z. Li, Eds. Berlin, Germany: Springer, 2007, pp. 435–444.

[164] Y. Wai Kuan, A. B. J. Teoh, and D. C. L. Ngo, "Secure hashing of dynamic hand signatures using wavelet-fourier compression with BioPhasor mixing and 2^N discretization," *EURASIP J. Adv. Signal Process.*, vol. 2007, pp. 1–8, Dec. 2006.

[165] M. Hiroyuki, T. Itsuo, H. Hidekazu, S. Tsugutaka, and M. Tsutomu, "An artifact-metric system which utilizes inherent texture," *IPSJ J.*, vol. 42, no. 8, pp. 1992–2005, Aug. 2001.

[166] N. Nishiuchi and H. Soya, "Cancelable biometric identification by combining biological data with artifacts," in *Proc. Int. Conf. Biometrics Kansei Eng.*, Takamatsu, Japan, Sep. 2011, pp. 61–64.

[167] M. Yamagishi, N. Nishiuchi, and K. Yamanaka, "Hybrid fingerprint authentication using artifact-metrics," *Int. J. Biometrics*, vol. 1, no. 2, pp. 160–172, Sep. 2008.

[168] J. R. Pinto, J. S. Cardoso, and M. V. Correia, "Secure triplet loss for end-to-end deep biometrics," in *Proc. 8th Int. Workshop Biometrics Forensics (IWBF)*, Porto, Portugal, Apr. 2020, pp. 1–6.

[169] J. Peng, B. Yang, B. B. Gupta, and A. A. Abd El-Latif, "A biometric cryptosystem scheme based on random projection and neural network," *Soft Comput.*, vol. 25, no. 11, pp. 7657–7670, Jun. 2021.

[170] V. Krivokuca Hahn and S. Marcel, "Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 639–666, 2023.

[171] W. El-Shafai, F. A. H. E. Mohamed, H. M. A. Elkamchouchi, M. Abd-Elnaby, and A. Elshafee, "Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm," *IEEE Access*, vol. 9, pp. 77675–77692, 2021.

[172] M. Tarek, E. Hamouda, and A. S. Abohamama, "Multi-instance cancellable biometrics schemes based on generative adversarial network," *Appl. Intell.*, vol. 52, no. 1, pp. 501–513, Jan. 2022.

[173] M. Tarek, O. Ouda, and T. Hamza, "Robust cancellable biometrics scheme based on neural networks," *IET Biometrics*, vol. 5, no. 3, pp. 220–228, Sep. 2016.

[174] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Comput.*, vol. 22, no. 7, pp. 2257–2265, Apr. 2018.

[175] G. Mai, K. Cao, X. Lan, and P. C. Yuen, "SecureFace: Face template protection," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 262–277, 2021.

[176] A. K. Jindal, S. Chalamala, and S. K. Jami, "Face template protection using deep convolutional neural network," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Salt Lake City, UT, USA, Jun. 2018, pp. 575–583.

[177] R. K. Pandey, Y. Zhou, B. U. Kota, and V. Govindaraju, "Deep secure encoding for face template protection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Las Vegas, NV, USA, Jun. 2016, pp. 77–83.

[178] A. Nagar, K. Nandakumar, and A. K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 733–741, Jun. 2010.

[179] S. Nazari, M.-S. Moin, and H. R. Kanan, "Cancelable face using chaos permutation," in *Proc. 7th Int. Symp. Telecommun. (IST)*, Tehran, Iran, Sep. 2014, pp. 925–928.

[180] J. Bringer, H. Chabanne, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Sci. Comput. Program.*, vol. 74, nos. 1–2, pp. 43–51, Dec. 2008.

[181] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 103–117, Mar. 2010.

[182] H.-H. Zhu, Q.-H. He, and Y.-X. Li, "A two-step hybrid approach for voiceprint-biometric template protection," in *Proc. Int. Conf. Mach. Learn. Cybern.*, Xi'an, China, vol. 2, Jul. 2012, pp. 560–565.

[183] K. Govindharaju and M. Ezhilarasan, "Securing biometric template using a hybrid scheme," in *Proc. Int. Conf. Informat. Analytics*, New York, NY, USA, Aug. 2016, pp. 1–5.

[184] C. Rathgeb and C. Busch, "Multi-biometric template protection: Issues and challenges," in *New Trends and Developments in Biometrics*, J. Yang and S. J. Xie, Eds. London, U.K.: IntechOpen, 2012, ch. 8, pp. 173–190.

[185] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancelable biometric features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 709–719, Mar. 2019.

[186] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, "Investigating fusion approaches in multi-biometric cancellable recognition," *Exp. Syst. Appl.*, vol. 40, no. 6, pp. 1971–1980, May 2013.

[187] P. P. Paul and M. Gavrilova, "Multimodal cancelable biometrics," in *Proc. IEEE 11th Int. Conf. Cognit. Inform. Cognit. Comput.*, Kyoto, Japan, Aug. 2012, pp. 43–49.

[188] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 255–268, Feb. 2012.

[189] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Inf. Fusion*, vol. 18, pp. 161–174, Jul. 2014.

[190] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Montreal, QC, Canada, Nov. 2017, pp. 298–302.

[191] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, New Delhi, India, Mar. 2012, pp. 498–505.

[192] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.

[193] T. M. Cover and J. A. Thomas, "Differential entropy," in *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley-InterScience, 2006, ch. 8.

[194] A. Papoulis and S. U. Pillai, "The concept of a random variable," in *Probability, Random Variables and Stochastic Processes*, 4th ed. Europe: McGraw-Hill, 2002, ch. 4.

[195] Y. L. Tong, "The bivariate normal distribution," in *The Multivariate Normal Distribution*, 1st ed. New York, NY, USA: Springer-Verlag, 1990, ch. 2.

[196] A. H. Cheetham and J. E. Hazel, "Binary (presence-absence) similarity coefficients," *J. Paleontol.*, vol. 43, no. 5, pp. 1130–1136, Sep. 1969.

[197] P. C. Austin, "Using the standardized difference to compare the prevalence of a binary variable between two groups in observational research," *Commun. Statist. Simul. Comput.*, vol. 38, no. 6, pp. 1228–1234, Apr. 2009.

[198] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in biometric security systems," in *Proc. 46th Annu. Allerton Conf. Commun., Control Comput.*, Monticello, IL, USA, Sep. 2008, pp. 268–273.

[199] GenKey. *The Next Generation of Identity Security*. Accessed: Nov. 1, 2022. [Online]. Available: https://www.genkey.com/privacy-by-design/

[200] Precise Biometrics. *YOUNiQ—Access With Facial Recognition*. Accessed: Nov. 1, 2022. [Online]. Available: https://precisebiometrics.com/digital-identity/

[201] Hitachi Group. *Vein ID: Hitachi in Oceania*. Accessed: Nov. 1, 2022. [Online]. Available: https://www.hitachi.com.au/products/product-categories/it/veinid.html

[202] Y. Matsui, A. Sawada, S. Kaneko, Y. Nakamaru, R. Ahluwalia, and D. Kumar, "Global deployment of finger vein authentication," *Hitachi Rev.*, vol. 61, no. 1, pp. 35–39, 2012.

[203] Private Identity LLC. *Decentralized Biometrics Using Fully Homomorphic Encryption*. Accessed: Nov. 1, 2022. [Online]. Available: https://private.id

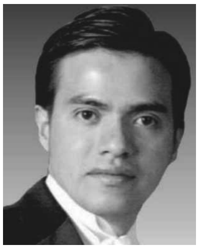
JUAN CARLOS BERNAL-ROMERO (Graduate Student Member, IEEE) received the B.S. degree in electronics engineering from the Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, in 2018, and the M.Sc. degree in electronics from the National Institute of Astrophysics, Optics, and Electronics, Puebla, Mexico, in 2020, where he is currently pursuing the Ph.D. degree in electronics. His research interests include biometrics, machine learning, signal processing, and digital and embedded systems.

JUAN MANUEL RAMIREZ-CORTES (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the National Polytechnic Institute, Mexico, the M.Sc. degree in electrical engineering from the National Institute of Astrophysics, Optics, and Electronics (INAOE), Mexico, and the Ph.D. degree in electrical engineering from Texas Tech University. He is currently a Researcher with INAOE. His research interests include signal and image processing, biometrics, neural networks, fuzzy logic, and digital systems. He is a member of the Mexican National Research System (SNI), Level 2.

JOSE DE JESUS RANGEL-MAGDALENO (Senior Member, IEEE) received the B.E. degree in electronics engineering and the M.E. degree in electrical engineering on hardware signal processing from the Universidad de Guanajuato, Guanajuato, Mexico, in 2006 and 2008, respectively, and the Ph.D. degree from the Universidad Autonoma de Queretaro, Mexico, in 2011. He is currently a Full Researcher with the Department of Electronics, National Institute for Astrophysics, Optics and Electronics, Puebla, Mexico. His current research interests include FPGAs, signal and image processing, instrumentation, and mechatronics. He is a member of the Mexican National Research System, Level 2.

PILAR GOMEZ-GIL (Senior Member, IEEE) received the B.Sc. degree in computer science from the Universidad de las Americas, Mexico, and the M.Sc. and Ph.D. degrees in computer science from Texas Tech University, Lubbock, TX, USA. She is currently a Titular Researcher with the Computer Science Department, National Institute of Astrophysics, Optics, and Electronics (INAOE), Mexico. Her research interests include artificial neural networks, time series prediction, image processing, and pattern recognition. She is a member of the Mexican National Research System (SNI), Level 1.

HAYDE PEREGRINA-BARRETO (Senior Member, IEEE) received the bachelor's degree in computer science from the Instituto Tecnológico de Cuautla, Mexico, in 2006, the master's degree in engineering from the Universidad de Guanajuato, Mexico, in 2008, and the Ph.D. degree in engineering from the Universidad Autónoma de Querétaro, Mexico, in 2011. In 2014, she was a Postdoctoral Researcher of medical imaging with the National Institute for Astrophysics, Optics and Electronics, Puebla, Mexico, where she is currently a Titular Researcher. Her current research interests include image processing and medical imaging. She is a member of the Mexican National Research System, Level 1.



ISRAEL CRUZ-VEGA received the degree in control and automation engineering from the Instituto Politécnico Nacional, in 2001, and the M.Sc. and D.Sc. degrees in automatic control from the Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, in 2004 and 2011, respectively. He is currently a CONACYT Research Fellow with the Department of Electronics, Instituto Nacional de Astrofísica, Óptica y Électronica. His research interests include automatic control, machine learning, intelligent systems, and evolutionary algorithms. He is a member of the Mexican National Research System, Level 1.