Received: 21 January 2023 | Revised: 14 September 2023 | Accepted: 6 October 2023

CAAI Transactions on Intelligence Technology

DOI: 10.1049/cit2.12283

REVIEW

Feature extraction and learning approaches for cancellable biometrics: A survey

Wencheng Yang[1] | Song Wang[2] | Jiankun Hu[3] | Xiaohui Tao[1] | Yan Li[1]

[1]School of Mathematics, Physics and Computing, University of Southern Queensland, Toowoomba, Queensland, Australia

[2]School of Computing, Engineering and Mathematical Sciences, La Trobe University, Melbourne, Victoria, Australia

[3]School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra, Australian Capital Territory, Australia

Correspondence

Jiankun Hu, School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy (UNSW@ADFA), Canberra, ACT 2600, Australia.
Email: j.hu@adfa.edu.au

Funding information

Australian Research Council, Grant/Award Numbers: DP190103660, DP200103207, LP180100663; UniSQ Capacity Building Grants, Grant/Award Number: 1008313

Abstract

Biometric recognition is a widely used technology for user authentication. In the application of this technology, biometric security and recognition accuracy are two important issues that should be considered. In terms of biometric security, cancellable biometrics is an effective technique for protecting biometric data. Regarding recognition accuracy, feature representation plays a significant role in the performance and reliability of cancellable biometric systems. How to design good feature representations for cancellable biometrics is a challenging topic that has attracted a great deal of attention from the computer vision community, especially from researchers of cancellable biometrics. Feature extraction and learning in cancellable biometrics is to find suitable feature representations with a view to achieving satisfactory recognition performance, while the privacy of biometric data is protected. This survey informs the progress, trend and challenges of feature extraction and learning for cancellable biometrics, thus shedding light on the latest developments and future research of this area.

KEYWORDS

biometrics, feature extraction

1 | INTRODUCTION

Biometric recognition is a well-known technology to authenticate the identity of a person using their biological traits [1] (e.g. face, fingerprint and iris). Biometric recognition systems are widely used in various applications, such as access control [2], healthcare [3], Internet of Things [4]. Because biometric data are unique and permanent for every individual and cannot be forgotten, lost, or passed on to others, these characteristics make biometric recognition more advantageous than traditional authentication systems that are based on knowledge or possession [5]. A typical biometric recognition system usually includes two phases—enrolment and verification/identification [6]. Specifically, in the enrolment phase, biometric systems capture, store and process users' biometric data. This typically involves users presenting a sample of their biometrics (e.g. fingerprint or face) to the biometric system. The system would then process the sample and create a biometric template, namely a digital representation of each user's unique biometric information. The template is stored in a database together with other relevant personal information, such as the user's name and ID number. During the verification or identification phase, the biometric system handles another biometric input (i.e. a query's biometric), compares it with the stored template and determines the outcome of acceptance or rejection.

Despite the benefits associated with the use of biometrics, the storage of raw biometric data raises privacy and security concerns, such as data breach [7], privacy invasion and identity theft [8]. If raw biometric templates are stored without protection, the original biometric data would be at risk of being

compromised. Attackers breaking into biometric databases could acquire the biometric data of registered users and eventually impersonate them to access the corresponding authentication system [5]. What is even worse is that biometric data cannot be changed like passwords. Once compromised, they are lost forever. There are a number of ways to protect biometric data through biometric security techniques, among which cancellable biometrics is a commonly used and effective technique. In the enrolment phase, the original template data are intentionally distorted by an irreversible transformation function. The same irreversible transformation is applied to query data in the verification or identification phase. The transformed template and query data are matched in the transformed domain [9]. In other words, cancellable biometrics use transformed biometric data rather than the original data for authentication purposes [10]. If a set of biometric data is found to be corrupted, they can be revoked and replaced by a new set of biometric data. The ISO/IEC 24745 standard [11] sets some key criteria for cancellable biometrics [12, 13]. They are:

- Unlinkability: Distinct templates produced from a user's biometrics should be specific to an application. No similar transformed templates can be used in more than one application.
- Non-invertibility: To protect the privacy of biometric data, it should not be computationally feasible to restore the original biometric data from transformed templates.
- Revocability (or renewability): As an essential property of cancellable biometrics, revocability refers to revoking a compromised biometric template and replacing it with a new one.
- Performance: Template protection techniques should not worsen the recognition performance of biometric systems. That is, recognition accuracy should be comparable before and after feature transformation for cancellable biometrics.

In this survey paper, we focus on feature extraction and learning approaches to achieving good recognition performance in cancellable biometrics [14], while preserving the privacy of biometric data. The taxonomy of feature representation is studied from a number of viewpoints. A comprehensive review is conducted on the following three aspects: types of cancellable transformation functions, feature extraction and learning approaches and performance comparisons of cancellable biometric systems that use these feature extraction and learning approaches.

1.1 | Motivation and contributions of this work

1.1.1 | Motivation

In order to demonstrate our motivation and in particular, distinguish this survey from other surveys, we first summarise relevant existing review articles. Choudhary et al. [15] analysed various feature extraction methods for iris recognition and compared the performance of different feature extraction methods. Pflug and Busch [16] surveyed the algorithms of ear detection and recognition using both 2D and 3D images. Many feature extraction methods are introduced and discussed. Fei et al. [17] reviewed the feature extraction of different types of palmprint images, and studied the feature representation and recognition of palmprints. The authors also analysed the theoretical side of feature extraction and matching methods for different types of palmprint images. Prabakaran and Shyamala [18] described and evaluated the performance of many voice recognition techniques, especially various feature representations and the extraction of features from digital voice signals.

Zhang et al. [19] gave a thorough review of sparse feature representations, where existing algorithms are empirically classified into four categories. The rationale of the algorithms in each category is analysed and summarised, elucidating the underlying properties of the sparse feature representation theory. In addition, an experimental comparative investigation into these sparse feature representation algorithms is conducted. Sundararajan and Woodard [20] surveyed the impact of deep learning and feature learning on biometrics. About 100 deep learning approaches to the recognition of individuals using a range of biometric modalities are examined in this study. The authors found that the majority of deep learning studies in biometrics are focused on face and speaker recognition. Wang et al. [21] reviewed cognitive biometrics, covering most biosignature patterns and applications. The authors first devised a taxonomy to build the respective knowledge and steer the investigation, and then provided a unified view of methodological advances from signal acquisition and preprocessing to feature learning and pattern recognition.

As shown above, while several existing surveys cover the feature extraction and learning of specific biometric traits (e.g. iris [15], palmprint [17] and voice [18]), as well as deep learning-based feature learning for biometrics [20], none of them have specifically investigated feature extraction and learning for cancellable biometrics. In contrast to the conventional feature extraction and learning approaches, cancellable biometrics-related feature extraction and learning include additional constraints, such as performance retain, and irreversibility, which makes our survey paper distinctive. In this context, our survey on feature extraction and learning regarding cancellable biometrics refers to these special characteristics unless stated otherwise. Hence, this survey will help fill the gap in the literature.

1.1.2 | Contributions

In this paper, we present an inclusive survey of feature representation for cancellable biometrics. The main contributions of this work are summarised below.

- *In-depth review*: This survey provides a comprehensive and thorough review of feature extraction and learning approaches, especially targeting cancellable biometrics, which is not covered by existing survey papers.

- *New taxonomy*: Feature representation requirements for biometrics in general as well as cancellable biometrics are discussed and summarised. A taxonomy of feature extraction and learning approaches specifically for cancellable biometrics is proposed.
- *Challenges and future directions*: Based on the insightful discussions of state-of-the-art feature extraction and learning approaches for cancellable biometrics, challenges and future research directions are presented, shedding light on the future study of cancellable biometrics.
- *Guide for novices*: This survey lays a foundation for novice researchers in computer vision and biometrics to gain a good understanding of feature extraction and learning for cancellable biometrics; in particular, readers who are interested in cancellable biometrics will benefit from this survey paper. While a number of survey papers (e.g. [1, 6]) on cancellable biometrics cover feature transformation techniques, in this survey we focus on feature extraction and learning approaches for cancellable biometrics.

1.2 | Organisation of this work

The rest of this paper is organised into several sections starting with a discussion about requirements of good feature representation and their relationship with cancellable biometric criteria in Section 2. In Section 3, different types of transformation techniques for generating cancellable biometric templates are described. Section 4 covers a host of feature extraction and learning approaches. Performance comparisons of these approaches are presented in Section 5, followed by discussions and suggestions about future research directions in Section 6. The paper is concluded in Section 7.

2 | REQUIREMENTS OF GOOD FEATURE REPRESENTATION AND THEIR RELATIONSHIP WITH CANCELLABLE BIOMETRICS CRITERIA

Biometric feature representation is concerned with encoding and representing biometric data (e.g. facial features and iris patterns) that can be used for biometric recognition. Good feature representations should describe biometric data in a way that is discriminative, invariant, robust, efficient, secure and renders satisfactory recognition performance. Good feature representation should meet the following requirements:

- Discriminativeness: Good feature representation should be discriminative enough for each individual so that different users can be effectively distinguished [22].
- Invariance: Good feature representations should be invariant to changes in the input data, such as rotations and shifts in fingerprint images [22].
- Robustness: Good feature representation should be tolerant and resilient to the noise and other disturbances in the input data [23].
- Efficiency: Good feature representation should be compact, cost-effective and user friendly so that it can be stored and processed efficiently and deployed readily [24].
- Irreversibility: Good feature representation should be secure so that it cannot be easily be reversed or undone [25].
- Compatibility: One important aspect of cancellable biometrics is that transformed biometric data should be compatible with existing template protection algorithms and protocols. This means that data after transformation should not introduce additional vulnerabilities. Also, transformed data should be able to be revoked when they are compromised or no longer needed, so that biometric data attack and misuse can be prevented [26].

Cancellable biometrics consist of two major components: feature representation and feature transformation, both of which are closely related to the four criteria (i.e. unlinkability, non-invertibility, revocability and performance) for cancellable biometrics, set by the ISO/IEC 24745 standard [11]. Numerous existing surveys (e.g. [1, 6]) discuss about feature transformation in cancellable biometrics. In this survey, however, we explore feature representation and its impact on the ISO/IEC criteria. As illustrated in Figure 1, the discriminativeness, invariance and robustness of feature representation are intimately connected to the performance of cancellable biometric systems. Discriminativeness describes the ability of feature representation to accurately differentiate individual entities. A high discriminative power enables the extracted features to effectively distinguish between different individuals, leading to enhanced recognition performance. Invariance and robustness refer to the capability of keeping recognition performance under challenging conditions, such as lighting variations, pose, noise and other environmental factors that might affect the quality of feature representation. Consequently, discriminativeness, invariance and robustness are pivotal to the development of reliable, high-performing biometric systems. More discussions about how feature representation impacts the recognition performance of cancellable biometrics are given in Section 6.2. Although for cancellable biometrics, non-invertibility hinges on the design of non-invertible transform, the irreversibility and compatibility of feature representation can affect the non-invertibility of cancellable biometric templates. For example, feature representation should be compatible with the designed transformation function. The impact of feature representation on the non-invertibility of cancellable biometrics is further elaborated in Section 6.3.

3 | DIFFERENT TYPES OF CANCELLABLE TRANSFORMATION FUNCTIONS

Transformation functions play a vital role in cancellable biometrics. They are designed in ways that it should be computationally infeasible to recover the original biometric data from transformed templates. There is a variety of transformation techniques for generating cancellable biometric templates [1].

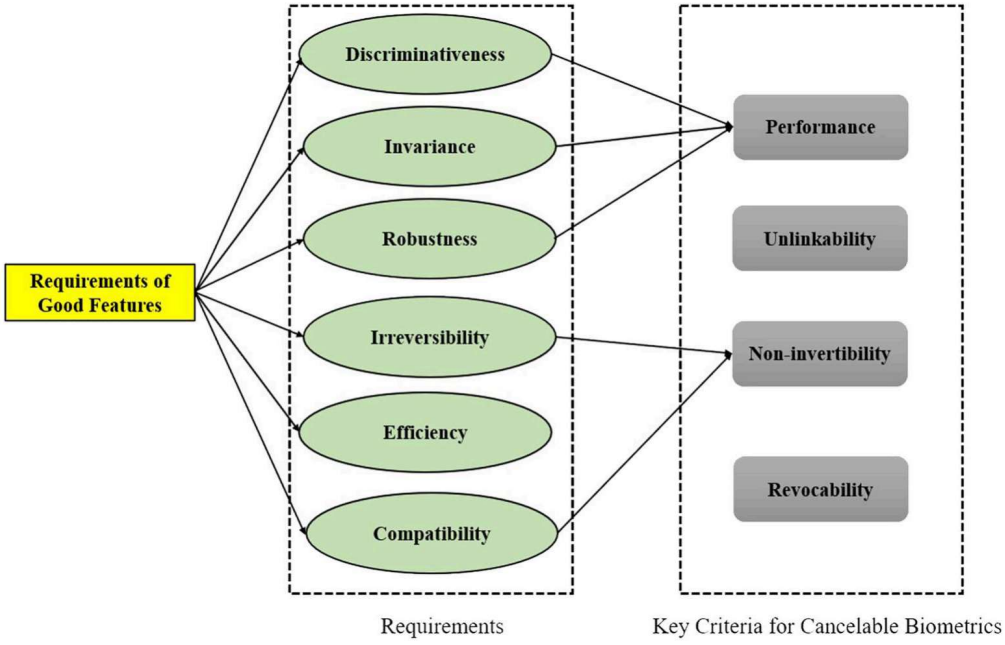

FIGURE 1 Requirements of good feature representation and their correlation with the key criteria for cancellable biometrics.

Cancellable transformation functions can be broadly divided into four categories as follows.

(1) *Cryptography-based*: This type of transformation function makes use of cryptography-based techniques (e.g. bio-hashing [27]) to construct cancellable biometric templates.
(2) *Transformation-based*: This type of transformation function applies various transformation techniques (e.g. Cartesian transformation [28], polar transformation [29], random projection [30]) to the design of non-invertible transforms such that raw biometric data are transformed irreversibly.
(3) *Filter-based*: This type of transformation function is based on different convolutional filters, such as bloom filters [31], guided filters [32], and inverse filters [33].
(4) *Hybrid-based*: This type of transformation function uses a combination of two or more of the above schemes (e.g. random projection + hashing [34]) to generate cancellable biometric templates.

4 | FEATURE EXTRACTION AND LEARNING APPROACHES

Many feature extraction and learning approaches have been designed and proposed by researchers. In general, they can be classified into three types: hand-engineered feature extraction approaches, machine/deep learning-based feature learning approaches and hybrid feature extraction and learning approaches, all of which are discussed and analysed in detail in this section. The taxonomy of feature extraction and learning approaches for cancellable biometrics is illustrated in Figure 2.

(1) *Hand-engineered feature extraction approaches*: Hand-engineered feature extraction refers to the process of exploring and manually extracting features from biometric data for the purpose of identifying or verifying individuals. For hand-engineered feature extraction, selecting and designing appropriate features entail domain expertise and an understanding of the characteristics of biometric data. The advantage of hand-engineered feature extraction is that it does not require large-scale datasets for training, making it suitable for biometric traits such as fingerprint or palmprint, of which the datasets (e.g. FVC2002) [35] contain only a relatively small number of samples.
(2) *Machine/deep learning-based feature learning approaches*: Machine/deep learning-based feature learning uses machine learning algorithms and/or neural networks to automatically learn and extract features from biometric data. Machine/deep learning-based feature learning approaches can learn and handle complex patterns and features. Also, they often achieve better performance than hand-engineered feature extraction, when dealing with large amounts of data. In addition, deep learning methods [36], a type of machine learning that utilises deep neural networks, are particularly effective in learning complex and complicated patterns and features, yielding optimal performance in many biometric tasks. Machine/deep learning-based feature learning approaches require large-scale datasets, so they suit biometric traits (e.g. face) whose datasets (e.g. VGGFace2) [37] contain millions of samples.
(3) *Hybrid feature extraction and learning approaches*: Hybrid feature extraction and learning for cancellable biometrics involves a combination of multiple feature extraction and learning approaches, such as a combination

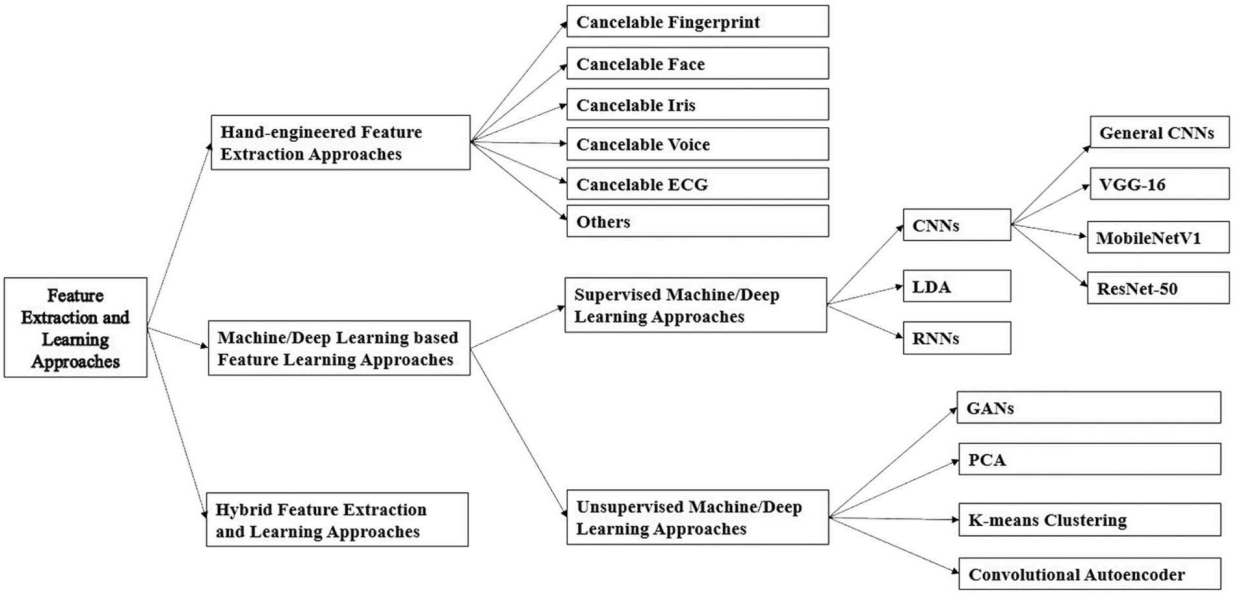

FIGURE 2 The taxonomy of feature extraction and learning approaches. Existing feature extraction and learning approaches are generally classified into three types: hand-engineered feature extraction approaches, machine/deep learning-based feature learning approaches, and hybrid feature extraction and learning approaches.

of hand-engineered and machine/deep learning-based approaches, so that the strength of each type is exploited.

4.1 | Hand-engineered feature extraction approaches

Hand-engineered feature extraction has been widely used in biometric applications. One example of hand-engineered feature extraction is the construction of local structures using minutiae in fingerprint images [38], as minutiae are unique points where the ridges of a fingerprint split or end [39]. Other examples of hand-engineered features include the shape and size of irises, the patterns and shapes of facial features [32], and the unique characteristics of a person's voice [40]. In this section, cancellable biometrics-related hand-engineered feature extraction approaches for various biometric traits (e.g. fingerprint, face, iris and voice) are reviewed.

4.1.1 | Cancellable fingerprint

Fingerprint is one of the oldest known and most common biometric traits owing to its convenience and recognition accuracy [9]. Fingerprint recognition is non-trivial, mainly due to large intra-class variations resulted from displacement, non-linear skin distortion etc. To alleviate intra-class variations, many hand-engineered feature extraction approaches for cancellable fingerprints have been proposed (see Table 1). As shown in Figure 3, some of these feature extraction approaches are detailed below.

Ratha et al. [39] directly took minutiae as features, represented by (x, y) coordinates and ridge directions. After minutiae extraction, a many-to-one mapping-based non-invertible transform is used to protect the original minutiae set and generate the cancellable template. Since wavelets offer a multi-resolution representation of multi-level decomposition for interpretive image information, Jin et al. [27] applied a 2D wavelet transform to fingerprint images. Because the majority of the energy content in signals is centred in low-frequency regions, this study chose the low-frequency components in the vertical and horizontal directions of the original fingerprint image as features. Farooq et al. [41] designed a set of triangles (formed by three minutiae) and represented such triangle features as binary data. Lee et al. [10] constructed features by extracting translation- and rotation-invariant values from orientation data within the neighbourhood of each minutia. Then a user-specific random vector is used to build cancellable fingerprints from the constructed features. To avoid global alignment, Tulyakov et al. [42] formed two vectors as features. The first vector is a triplet of localised minutiae points (e.g. angles between minutiae), while the second vector is produced from the Euclidean distance and orientation difference between a centre minutia and its two nearest neighbours.

Lee and Kim [38] mapped minutiae into a 3D array. If a cell in the 3D array includes more than one minutia, it is assigned binary 1; otherwise, the cell is given the value of binary 0. A binary string is finally obtained as features by ordering 0 and 1s in the cells of the 3D array. Ahmad et al. [29] used pair-polar coordinate vectors containing positional information between two neighbouring minutiae (e.g. radial distance and angle) as features, representing the relative relationship between adjacent minutiae in a polar coordinate system. Wang and Hu [43] developed a densely infinite-to-one mapping (DITOM) model

TABLE 1 Descriptions of hand-engineered feature extraction approaches for cancellable fingerprint.

Approach	Publication year	Trait	Brief description of feature extraction
Ratha et al. [39]	2001	Fingerprint	Minutiae-related feature extraction based on the location of ridge ending and ridge bifurcation
Jin et al. [27]	2004	Fingerprint	Invariant features built from the wavelet and Fourier–Mellin transform
Farooq et al. [41]	2007	Fingerprint	Formation of triangles consisting of three minutiae
Lee et al. [10]	2007	Fingerprint	Features acquired from orientation data within the neighbourhood of each minutia
Tulyakov et al. [42]	2007	Fingerprint	A triplet of localised minutiae points
Lee and Kim [38]	2010	Fingerprint	Features in the form of binary data produced from binarised cell values in a 3D array
Ahmad et al. [29]	2011	Fingerprint	Pair-polar coordinate vectors capturing the positional information between two neighbouring minutiae
Wang and Hu [43]	2012	Fingerprint	Distance and angles of minutiae pairs
Jin et al. [44]	2013	Fingerprint	Sides and angles of triangles in a minutiae vicinity stricture
Zhang et al. [45]	2013	Fingerprint	Spatial and orientation information based on the MCC
Jin et al. [46]	2017	Fingerprint	A fixed-length vector derived from MCC
Bedari et al. [47]	2022	Fingerprint	MCC-based feature representation
Sun et al. [48]	2023	Fingerprint	A framework for converting points to strings produces binary strings of a consistent length
Djebli et al. [49]	2023	Fingerprint	SIFT characteristics from the positions of fingerprint minutiae

Abbreviations: MCC, minutia cylinder-code; SIFT, scale invariant feature transform.

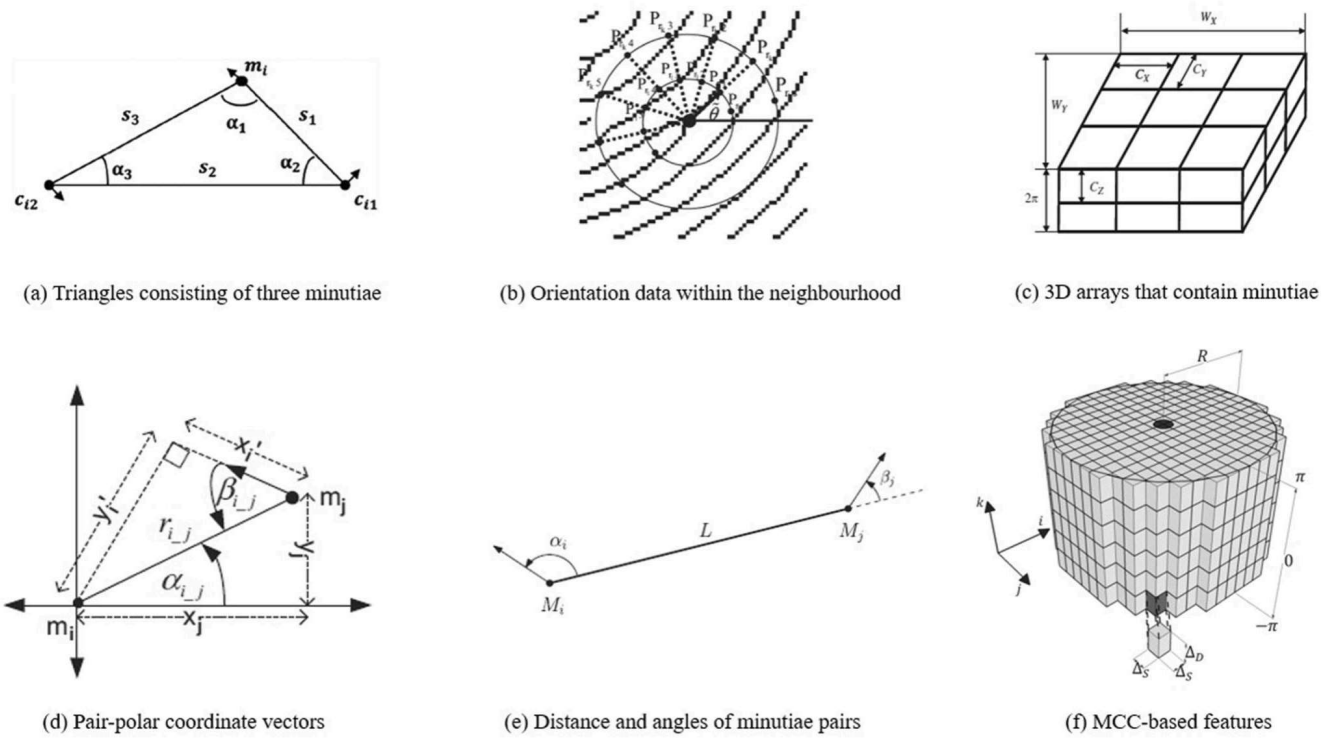

FIGURE 3 Examples of hand-engineered feature extraction approaches for cancellable fingerprints (sourced from: (a) [44], (b) [10], (c) [38], (d) [29], (e) [43], (f) [50]).

to achieve non-invertibility in the design of cancellable fingerprint templates. The DITOM model is applied to minutiae pairs to extract features (i.e. the distance between two minutiae and the angles between the line connecting two minutiae and the orientation of each minutiae). Subsequent works (e.g. [29, 51, 52]) also adopt the same feature extraction approach despite different feature transformation designs. Jin et al. [44] proposed minutiae vicinity decomposition (MVD) features, in which a reference minutia with three nearest minutiae forms a minutiae vicinity that is further used to derive

local features (e.g. sides and angles of triangles). Cancellable fingerprint templates are obtained from MVD-based random projection.

Zhang et al. [45] utilised the minutia cylinder-code (MCC) [53] as features in the design of cancellable fingerprint templates, because MCC is one of the most advanced local minutia descriptors with a proven record of high recognition accuracy. Jin et al. [46] proposed two-factor cancellable biometrics using ranking-based position-sensitive hashing, called index of maximum (IoM) hashing. In the IoM hashing method, a fixed-length vector as features is acquired from MCC. There are other cancellable fingerprint templates that also use MCC (e.g. [47, 54–56]). Kho et al. [57] defined features with a partial local structure (PLS), which is one of the six equal-area sectors with Π/3 internal angles, divided from a disc centred on a minutia of radius r. A binary cancellable fingerprint template is then built using the PLS. Sun et al. [48] proposed employing a point-to-string conversion framework that generates fixed-length binary strings. This approach is similar to the one proposed by Jin et al. [58]. Additionally, Djebli et al. [49] presented a unique and adaptable fingerprint cancelation method that relies on extracting scale invariant feature transform (SIFT) characteristics from the positions of fingerprint minutiae.

4.1.2 | Cancellable face

Nowadays face-based biometric systems are used extensively. Since sensitive information is contained in a person's facial image (e.g. age and health status), it is vital to preserve the privacy of face data [59]. Designing cancellable face templates is to transform or intentionally distort the original face data in an irreversible manner such that a transformed/distorted version of the original face data can be used for face recognition, whereas the original data cannot be retrieved from the transformed/distorted data, thus enhancing data security. A number of feature extraction approaches for cancellable face are reviewed below and summarised in Table 2.

In the work of Savvides et al. [32], the captured training face images are convolved with a random convolution kernel, produced by a 'seed' (e.g. PIN) of a random number generator. The convolved training images are in turn employed to generate a single biometric filter. Oh et al. [30] directly extracted local random features from partial face image matrices. The random features extracted Intrinsically include compressed horizontal and vertical facial information derived from the structural projection of the original face image. The extracted features are then transformed and averaged at the feature level in each direction to generate a cancellable face template. Faragallah et al. [60] designed numerous encrypted biometric templates that are created and recreated by employing a variety of convolution kernels produced by the chaotic Baker mapping of domains. The encrypted cancellable biometric system mapped from the domain after the discrete wavelet transform (DWT) exhibits the best performance among all implementations.

Xu et al. [59] fully utilised a quaternion feature representation with the structural information consisting of local variance and gradient. The quaternion-based two-dimensional principal component analysis (PCA) is used to extract features, allowing the extreme learning machine to be trained and employed for face recognition. To enable revocability and redistribution capabilities, the authors took a random permutation strategy with the binary matrix. Alhumyani et al. [61] proposed a cancellable face recognition scheme based on quantum image Hilbert permutation. The flexible quantum image representation (FRQI) allows for face image representation on a quantum computer in a natural pattern. FRQI traps and converts face image data into normalised quantum states according to the colour and position to better manage the image information. SP and Thomas [62] partitioned biometric images into Voronoi patches, derived from a rotating and scaling invariant seed point generation solution. The log-Gabor feature vector of every patch is warped by binding it with other patches' feature vectors.

4.1.3 | Cancellable iris

The iris is a biometric trait with high recognition performance both in theory and in practice. The technique of iris recognition utilises pattern identification with high-resolution iris images obtained from a person's eye [15, 63]. Most feature extraction methods use the normalised iris images with techniques such as wavelet encoding, Gabor filters and log-Gabor filters [64]. Some feature extraction approaches for cancellable iris are reviewed below and summarised in Table 3.

Uhl et al. [66] performed a transformation in the image domain before extracting features from iris images. The authors applied a wavelet-based method to obtain bit codes from the texture. The texture is split into N tracks to yield N one-dimensional signals, each averaged over the pixels of M neighbouring rows. Jenisch and Uhl [67] deduced the circular iris shaped as a rectangular iris texture with 512 × 64 pixels. The normalised iris image is factorised to distinct parts with varying resolutions by the use of filterbanks in the wavelet transform. The resultant signal is then converted to an alternating series of 0 and 1s.

Log-Gabor filters are useful for acquiring feature components of normalised iris images. An example of using Log-Gabor filters in the design of cancellable iris templates is given by Zuo et al. [65] with the application of an encoding technique plus a self-developed segmentation algorithm. Rathgeb et al. [68] applied feature extraction to normalised iris textures that are split into bands in order to obtain 10 one-dimensional signals, with each signal averaged from five adjacent rows of pixels. Log-Gabor filters are used in the convolution with texture pixels row by row. The phase of the complex number generated by each pixel is discretised into two bits, leading to a binary code of 10,240 bits. Similar methods of generating iriscode can also be found in refs. [70–73]. Since normalised iris images have a unique texture pattern, Umer et al. [69] made use of statistical methods to extract texture

TABLE 2 Descriptions of hand-engineered feature extraction approaches for cancellable face.

Approach	Publication year	Trait	Brief description of feature extraction
Savvides et al. [32]	2004	Face	The Fourier transform of the training images produces a diagonal matrix comprising the average power spectrum of all training images along the diagonals
Oh et al. [30]	2012	Face	The compressed horizontal and vertical facial information derived from the structural projection of the original face image
Faragallah et al. [60]	2021	Face	A variety of convolution kernels produced by the chaotic Baker mapping of different domains
Xu et al. [59]	2021	Face	A two-dimensional principal component analysis based on quaternions
Alhumyani et al. [61]	2022	Face	Feature representation on a quantum computer in the manner of a natural pattern
S P and Thomas [62]	2022	Face	The log Gabor feature vector of Voronoi patches from the face image

TABLE 3 Descriptions of hand-engineered feature extraction approaches for cancellable iris.

Approach	Publication year	Trait	Brief description of feature extraction
Zuo et al. [65]	2008	Iris	An encoding technique based on a one-dimensional Log-Gabor filter
Uhl et al. [66]	2009	Iris	A wavelet-based method for generating bit codes from texture
Jenisch and Uhl [67]	2011	Iris	10 signal bands are chained together in a specific order and transformed using quadratic spline wavelets. The resultant signal is converted to an alternating series of 0 and 1s
Rathgeb et al. [68]	2013	Iris	Convolution on texture pixels row by row with Log-Gabor filters
Umer et al. [69]	2017	Iris	Use of dense SIFT descriptors to obtain local features of normalised iris images, formed into a global representation of the iris pattern

Abbreviation: SIFY, scale invariant feature transform.

features from the normalised iris pattern. Local features of normalised iris images are acquired through the dense SIFT descriptors and then organised into a global representation of the iris pattern.

4.1.4 | Cancellable voice

Voice recognition relies on the unique characteristics of individuals' voices to identify them [40]. It entails analysis of a person's voice patterns, including the pitch, tone and frequency of their voice, to produce a vocal pattern or template that can be used to verify identity. Cancellable voice recognition is a technique that protects the privacy of individuals by modifying or distorting the original voice pattern in a irreversible manner. A selection of cancellable voice-related feature extraction approaches are reviewed below and summarised in Table 4.

El-wahab et al. [40] proposed a cancellable speech recognition system, in which features are derived from the encrypted speech signal, obtained by the DWT, in the time domain based on Cepstral analysis. The derived features are then used for classification by applying them to an artificial neural network. Elsayed et al. [33] used the DWT to factorise the speech signal into low-frequency and high-frequency components at various resolutions. The extracted features are masked by the linear minimum mean square error technique and an inverse phase filter to keep the original feature data safe. Abdelwahab et al. [74] implemented a watermarking algorithm in the design of cancellable speaker recognition. Watermark strength coefficients are employed to manage the expected level of distortion generated in the speech signal. In this work, a Haar wavelet-based DWT decomposition of the input audio signal is performed to generate feature data.

El-Gazar et al. [75] presented a cancellable speaker recognition system in which the feature data are encrypted through two cascading optical encryption algorithms, namely optical scanning holography and random phase masking. In this system, the feature data are obtained by converting the speech signal into a spectrogram image to which the Fourier transform is applied. El-Wahab et al. [76] proposed cancellable speaker identification suitable for remote access applications. The original feature data are secured by two efficient encryption systems based on chaotic graphs and a single key empirical mode decomposition. In this work, cepstral feature data is extracted from the encrypted speech signal. Specifically, the cepstral analysis is performed on the speech signal, and then the inverse fast Fourier transform is conducted to obtain the cepstral representation of the speech signal.

4.1.5 | Cancellable ECG

Captured by electrodes located on the surface of a person's body, the electrocardiogram (ECG) depicts the electrical activity of the heart during a certain time period [77]. ECG signals are distinctive because they are related to the physiological structure of the heart and dictated by DNA. Moreover, ECG signals are resistant to falsification. Thus, besides medical diagnosis, the unique characteristics of the ECG make it a good candidate for biometric authentication [78]. In this

TABLE 4 Descriptions of hand-engineered feature extraction approaches for cancellable voice.

Approach	Publication year	Trait	Brief description of feature extraction
El-wahab et al. [40]	2018	Voice	Features are derived from the encrypted speech signal in the time domain using Cepstral analysis, in combination with the DWT performed on the encrypted speech signal
Elsayed et al. [33]	2019	Voice	The DWT is carried out to factorise the speech signal into low-frequency and high-frequency components at various resolutions
Abdelwahab et al. [74]	2022	Voice	A Haar wavelet-based DWT decomposition of the input audio signal is performed to generate feature data
El-Gazar et al. [75]	2022	Voice	The feature data is obtained by converting the speech signal to a spectrogram image to which the Fourier transform is applied
El-Wahab et al. [76]	2022	Voice	The cepstral analysis is performed on the speech signal, and then the IFFT is conducted to obtain the cepstral representation of the speech signal

Abbreviations: DWT, discrete wavelet transform; IFFT, inverse fast Fourier transform.

section, several feature extraction approaches for cancellable ECG are introduced below and summarised in Table 5.

To address security and privacy issues in the event of an ECG data breach, Wu et al. [79] took advantage of the concept 'signal subspace collapsing' to build cancellable ECG templates. The authors also used fiducial feature-based algorithms, a popular feature extraction method for ECG biometrics. The construction of the marker features depends on the characteristic points in the heartbeat (i.e. points P, Q, R, S and T). Hammad et al. [80] designed cancellable ECG templates with a modified biohash method and matrix operations. In this work, the Pan-Tompkins algorithm is used to discover and retrieve ECG feature data (e.g. P-P and T-T intervals).

To enable revocability and without sacrificing performance, Kim and Chun [81] proposed a compressive measure of the ECG and permutation-based cancelation. The permutation procedure is purely random, relying on no user-specific information. In this work, the R-peak detection is carried out using methods like the Pan-Tompkins algorithm, thus allowing the extraction of R-peak-aligned ECG pulses to be feature data. Eldesouky et al. [82] transformed ECG signals into spectrograms, whose pixel values constitute the ECG feature data. The authors built a cancellable ECG recognition system using the 3D chaotic logic map. The proposed chaotic encryption process has efficient stochastic properties with confusion and diffusion characteristics.

4.1.6 | Others

In this section, the feature extraction approaches of cancellable biometric systems using other biometric traits (e.g. finger vein, electroencephalography [EEG], palmprint and signature) are reviewed below and summarised in Table 6.

Cancellable finger vein

With block remapping, image warping and the Bloom filter, Kauba et al. [84] proposed cancellable finger vein templates in the binary format with geometric information pertaining to the shape or topology of the observed vein pattern. In this study, feature extraction is carried out through feature extraction algorithms, such as the Gabor filter, isotropic undecided wavelet transform and maximum curvature. Yang et al. [83] developed cancellable finger vein templates using binary decision diagrams and the Multilayer Extreme Learning Machine. For feature extraction, Gabor filters and linear discriminant analysis (LDA) are employed for finger vein texture feature extraction and feature dimensionality reduction.

Cancellable EEG

Wang et al. [85] proposed a cancellable EEG system, named PolyCosGraph, based on polynomial transformation embedded cosine functions with graphical features of EEG signals. PolyCosGraph can protect EEG features and system security from multiple attacks. In this system, beta-band (i.e. 13–30 Hz) signals are extracted from the EEG with band-pass filters, and functional connectivity between channels is estimated according to the Shannon entropy. The authors designed a fully collected network, where each node stands for an EEG channel and each edge represents the degree of phase synchronisation of the signals from two respective channels. A number of graph features (e.g. pagerank centrality, transitivity and modularity) are extracted from the designed network.

Cancellable palmprint

Leng and Zhang [86] developed a two-key binding cancellable palmprint cryptosystem. The two-dimensional palmprint phasor template is perturbed by a scrambling operation based on a chaotic sequence, generated jointly by the user's token/key and a strong key derived from the palmprint. For feature extraction, PalmCode is extracted as palmprint texture features in the form of a texture feature matrix of size 32×64, which is further transformed to produce the cancellable palmprint.

Cancellable signature

Maiorana et al. [87] proposed a cancellable online signature recognition method, called BioConvolving, which ensures the security and updatability of online signatures. As for feature extraction, from each online signature, pressure signals and horizontal and vertical position traces are obtained, from which discrete time series are derived, giving rise to sequence-based features.

TABLE 5 Descriptions of hand-engineered feature extraction approaches for cancellable ECG.

Approach	Publication year	Trait	Brief description of feature extraction
Wu et al. [79]	2018	ECG	Fiducial feature-based algorithms are used in ECG feature extraction. The construction of the marker features depends on the characteristic points in the heartbeat
Hammad et al. [80]	2019	ECG	The Pan-Tompkins algorithm is used to discover and retrieve ECG feature data
Kim and Chun [81]	2019	ECG	The R-peak detection is carried out using methods like the Pan-Tompkins algorithm, thus allowing the extraction of R-peak-aligned ECG pulses to be feature data
Eldesouky et al. [82]	2022	ECG	The pixel values of the spectrogram are used as the ECG feature data

Abbreviation: ECG, electrocardiogram.

TABLE 6 Descriptions of hand-engineered feature extraction approaches for other biometric traits (e.g. finger vein, EEG, palmprint and signature).

Approach	Publication year	Trait	Brief description of feature extraction
Yang et al. [83]	2019	Finger vein	Gabor filters and LDA are used for finger vein texture feature extraction and feature dimensionality reduction
Kauba et al. [84]	2022	Finger vein	Binary feature vectors are produced via different feature extraction algorithms, such as the Gabor filter, isotropic undecided wavelet transform and maximum curvature
Wang et al. [85]	2022	EEG	A number of graph features (e.g. pagerank centrality, transitivity, and modularity) are extracted from the fully connected network
Leng and Zhang [86]	2011	Palmprint	PalmCode is extracted as palmprint texture features in the form of a texture feature matrix of size 32×64
Maiorana et al. [87]	2010	Signature	Discrete time series are derived from the horizontal and vertical position trajectories to generate sequence-based features

Abbreviations: EEG, electroencephalography; LDA, linear discriminant analysis.

4.2 | Machine/deep learning-based feature learning approaches

Machine/deep learning-based feature learning provides a good direction in terms of improving the performance and reliability of cancellable biometric systems [36]. In the design of cancellable biometrics, there are two types of machine/deep learning approaches available for feature learning—supervised and unsupervised learning, both of which are discussed in this section. The main difference between the two types is that supervised feature learning makes use of labelled data to aid outcome prediction, whereas unsupervised feature learning does not.

4.2.1 | Supervised machine/deep learning approaches

Supervised learning is a machine/deep learning method defined by the use of labelled datasets. These datasets are designed to train or 'supervise' algorithms to classify data or accurately predict outcomes. With labelled inputs and outputs, the supervised machine/deep learning model can measure its accuracy and build learning over time.

A neural network is a kind of artificial intelligence that is inspired by the structure and function of the human brain. It is composed of a large number of interconnected processing units (called 'neurons') that are arranged into layers. Each neuron takes input from other neurons, processes the input using an activation function, and transmits the output to other neurons or output layers. Neural networks are capable of learning and recognising complex patterns and data features and can therefore be used effectively in biometric tasks. Neural networks, such as convolutional neural networks (CNNs) [88], and recurrent neural networks (RNNs) [89], are common supervised machine/deep learning models; see below.

Convolutional neural networks

CNNs are designed to process data with a grid-like topology (e.g. images). CNNs include convolutional layers, which apply a set of filters to input data to extract features, and pooling layers, which reduce the data size and extract the most important features [36]. CNNs comprise general CNN and specific CNN architectures. Below is a brief description of general CNN architectures and some specific CNN architectures (e.g. VGG-16, MobileNetV1 and ResNet-50).

General CNNs. Jang and Cho [88] put forward a deep hash-based (DTH) framework to encode CNN-based features into binary codes using the index of a hash table. The authors did noise embedding and internal normalisation to warp the face data, resulting in increased irreversibility. In addition, a hash table-based binary encoding method uses segmented clustering loss to learn tables and paired Hamming loss to fulfil unlinkability and reusability, while maintaining good matching performance. Abdellatef et al. [31] proposed a cancellable multi-biometric face recognition system that extracts deep features from different facial regions using multiple CNNs. The proposed method uses a region-based technique to detect face,

eye, nose and mouth regions from the original face image. Multiple CNNs are utilised to derive deep features from each region, followed by a fusion network. The final facial descriptors are bio-convolutionally encrypted to provide user privacy and defend against spoofing attacks.

Abdellatef et al. [90] introduced a face and iris cancellable biometric recognition system based on a CNN model. Face and iris images are fed into the CNN model for feature extraction. The bio-convolution is performed on the original feature data to transform them into another version non-invertibly. Sandhya et al. [91] proposed a multi-instance cancellable iris system using a CNN trained with triple loss for feature extraction. Both random projection and random cross-folding are employed to achieve irreversibility. To address the security and privacy issues of biometric templates generated through deep networks, Singh et al. [34] devised a light-weight CNN-based cancellable biometric authentication method. In this method, biometric templates are cast onto a random subspace with an n-bit unique code retrieved by a deep biometric feature extraction network that is robustly trained. The authors also integrated a phase-wise incremental learning paradigm into the proposed cancellable iris authentication system.

VGG-16. VGG-16 [92] is a CNN architecture developed by the Visual Geometry Group from the University of Oxford. VGG-16 is composed of 16 layers, namely 13 convolutional layers and three fully connected (FC) layers. Sakr et al. [93] proposed a cancellable ECG method to protect ECG features used for human authentication. The authors first applied image processing techniques to pre-process the input ECG signal, and then used the VGG-16 pre-training model-based deep learning approach as a feature extraction tool to extract informative and powerful ECG features.

MobileNetV1. Designed to be computationally efficient and consume less resource (e.g. storage and battery) than other deep learning models, MobileNetV1 [94] is a deep CNN architecture developed by Google for effective image classification and object detection on mobile devices. Ma et al. [95] proposed a MobileNetV1-based deep neural network for cancellable face templates. Firstly, after image pre-processing, feature vectors are derived through MobileNetV1. With three FC layers, the extracted feature vectors are converted into a 256-dimensional sequence of real values, and mapped to random binary codes via a mapping network, thus enhancing the security and recognisability of face templates. Secondly, a hash network is utilised to acquire high-entropy templates, improving authentication accuracy and privacy. Finally, a token-based random projection is used to implement revocability of the resultant templates without retraining the deep neural network model.

ResNet-50. ResNet-50 [96] is a deep CNN architecture developed by Microsoft Research for image classification and object detection. It is a variation of the ResNet architecture, which stands for 'Residual Network'. ResNet-50 has 50 layers, including three types of layers, namely convolutional layers, activation layers and batch normalisation layers. Kim et al. [97] investigated an end-to-end multimodal cancellable biometric scheme using a deep learning model called CSMoFN (cancellable SoftmaxOut fusion network). CSMoFN comprises three modules: a feature extraction and fusion module, an enveloping SoftmaxOut transform module, and a multiplicative diagonal compression module. The proposed method uses ResNet-50 as the backbone, consisting of 49 convolutional layers and a linearly activated FC layer with p neurons, producing a p-dimensional feature vector for each face and periocular image. The two feature vectors from the face and periocular regions are fused at the feature level by conjunction. Built on time-varying keys obtained from the One-Time Biometrics via morphing (OTB-morph) random face data, the method proposed by Ghafourian et al. [98] was executed on a pre-trained Resnet-50 for general image recognition tasks. When applied to face images, OTB-morph can produce artificial faces so that users do not have to expose their real faces, thus improving biometric recognition performance and security.

Linear discriminant analysis

LDA is an important dimension reduction technique in machine learning. It is a supervised learning method and labelled data are used for training. Punithavathi and Geetha [99] proposed a method called Random Projection Linear Discriminant Analysis (RPLDA), in which features are extracted from intermediate templates to generate cancellable templates. In the proposed RPLDA, users are identified only when both the cancellable template and the key issued to the user are valid.

Recurrent neural networks

RNNs [89] are a type of single- or multi-layer neural network structure made up of recurrent connections. RNNs are typically used to learn time-series data, such as character strings, video, and speech. RNNs are featured by memorising previous instances of information and applying them to the current input data. While, to the best of our knowledge, no cancellable biometric research using RNNs can be found in the literature, RNNs will potentially be employed for feature learning for cancellable biometrics as they have been used for non-cancellable biometrics. For example, Kim and Pyun [89] designed a bidirectional deep recurrent neural network via late-fusion to exploit a real-time system for ECG-based biometrics. The input ECG signal is divided into a discrete sequence of equidistant data points, where each data point is a vector of individual ECG signals. These samples are passed to an RNN for feature learning and classification after segmentation.

4.2.2 | Unsupervised machine/deep learning approaches

Unsupervised learning uses machine learning algorithms to analyse and cluster unlabelled data sets. These algorithms uncover the hidden patterns in the data with no human interaction. Therefore, they are called unsupervised. A number of unsupervised machine/deep learning approaches are reviewed below.

Generative adversarial networks

GANs [100] are an emerging technique for both semi-supervised and unsupervised learning, used to generate new synthetic data. GANs consist of two neural networks: a generator and a discriminator. Tarek et al. [101] developed a GAN-based multi-instance cancellable biometric system, where a pre-transformation feature-level fusion is performed to connect the binary features of multiple instances. GAN-based keyless biometric salting is applied as feature transformation.

Principal component analysis

PCA [102] is a popular unsupervised learning technique for reducing the dimensionality of data. Kumar et al. [103] proposed two simple yet robust methods for cancellable biometrics: (a) random permutation PCA; and (b) random permutation two-dimensional PCA (RP-2DPCA). In this work, PCA [102] and 2D-PCA [104] are taken to extract features from a given training image. Cancellable templates are generated through random permutations guided by randomly created PIN codes.

K-means clustering

K-means clustering [105] is an unsupervised machine learning algorithm for dividing a set of data points into '*k*' clusters, where '*k*' is a user-specified number. This algorithm operates by first initialising the '*k*' centroids, that is, the points representing the centre of each cluster. The data points are then assigned to clusters whose centroids are closest. Sardar et al. [106] proposed a cancellable palmprint recognition system with good performance and enhanced template protection. In this system, a 200 × 200 palm region is first extracted from the input image in a pre-processing process. Palmprint features are then extracted from small patches of size 25 × 25. Each patch is converted into a normalised feature vector, to which a *K*-means clustering algorithm is applied to obtain local features, which are concatenated to form a global feature representation. The extracted features are analysed using an information encoding scheme to compute user-specific tokens.

Convolutional autoencoders

Convolutional autoencoders (CAEs) [107] are unsupervised dimensionality reduction modules consisting of convolutional layers capable of creating compressed image representations. Bamoriya et al. [108] used a CAE, a rank-based partitioning network and a randnet network to build secure cancellable biometric templates. Specifically, the CAE has two networks (i.e. an encoder and a decoder) trained on a biometric dataset (e.g. a face dataset) to extract features. The rank-based partitioning network partitions the extracted features. These feature partitions are input to the randnet network and the encoder for further processing. Siddhad et al. [109] utilised random noise and random convolution to generate cancellable templates from features extracted from palm vein, wrist vein and palm print images. The CAEs are employed to extract features, which are subsequently salted and convolved with a random kernel of dimension 7 × 7 generated from a uniform distribution.

4.3 | Hybrid feature extraction/learning approaches

Hybrid feature extraction/learning approaches have the potential to improve the performance and reliability of biometric systems, because they combine the flexibility and interpretability of hand-engineered feature extraction approaches and the intelligence of machine/deep learning approaches to learn complex patterns and features. Some hybrid feature extraction and learning approaches for cancellable biometrics are reviewed below.

An example of hybrid feature extraction/learning approaches was given by Abdellatef et al. [110]. In this study, the cancellable fusion-based face recognition methods use CNNs to extract deep features, from which a discriminative facial descriptor is obtained via a fusion network. In region-based methods, deep features are derived from various facial regions. The multi-biometric methods use different biometric traits to train multiple CNNs. Hybrid feature methods combine the advantages of deep learning features and hand-crafted features to obtain a more representative output. Abdellatef et al. [111] proposed an integrative biometric system to jointly identify face, iris, palmprint, fingerprint and ear biometrics. In the proposed system, the CNN-based model is responsible for extracting deep features, which are fused with the hand-crafted features (e.g. the oriented rotation sketch, the histogram of oriented gradients and local binary patterns).

4.4 | Feature extraction/learning in multi-modal cancellable biometrics

While significant progress has been made in single modalities, such as face, fingerprint and speech, many problems in cancellable biometrics involve more than one input modality. Therefore, the study of multi-modal modelling and training is gathering broad interest [112].

With voice and iris data used in a multi-biometric context, Canuto et al. [113] investigated a variety of fusion methods for different biometric modalities. A feature extraction/learning model named Gaussian mixture model-universal background model is employed to generate fixed-size feature vectors. Chin et al. [12] fused multiple biometric modalities (fingerprint and palmprint) at the feature level to obtain an integrated template, which is secured with a mixed template protection method. For feature extraction/learning, the authors utilised a set of Gabor filters with eight different angles to filter the approximate subbands generated by the two-dimensional discrete wavelet transform (2D-DWT). Standard fractional normalisation is then used to transform the filtered images. The normalised subbands are combined to form a fused feature vector. Dwivedi and Dey [114] fused iris and fingerprint data at the score level based on the mean-closure weighting and at the decision level according to the Dempster-Shafer theory. Regarding feature extraction for iris, IrisCode in the form of a binary matrix is extracted from pre-processed iris images using a logarithmic Gabor filter with phase quantisation. For

fingerprint feature extraction, the nearest-neighbour structure around each minutia is constructed and ridge features are derived from thinned fingerprint images and minutiae information.

Gupta et al. [115] proposed a cancellable multimodal biometric system that combines multiple features (iris and fingerprint) through a projection-based approach. The cancellable features are generated by projecting feature points onto a random plane controlled by a user-specific key. The projected points are converted to cylindrical coordinates, where combined features are obtained. A minutiae-based method is used for fingerprint feature extraction, while iris feature extraction is conducted on pre-processed iris images by having them quantified using the Local Binary Pattern histogram. Chang et al. [116] introduced a cancellable biometric template protection method which fuses fingerprint and iris features at the feature level. Histogram equalisation and the FFT are used for fingerprint image enhancement and feature extraction. Iris images are smoothed with a Gaussian filter and a Sobel operator is employed to calculate the orientation and intensity of the edges. After pixel values are extracted from fingerprint and iris images, with the PCA and concatenation fusion and through bio-hashing, feature data are converted to a binary bit string, subsequently processed by random index scrambling, the wavelet and discrete Fourier transforms. The cancellable biometric templates are generated by the partial Hadamard transform.

5 | PERFORMANCE COMPARISON

In this section, the performance of cancellable biometric systems, of which different feature extraction and learning approaches are applied, is analysed and compared on available datasets, according to metrics such as the equal error rate (EER) and the recognition rate (RR). Performance comparisons of cancellable biometric systems can help to determine the suitability of biometric traits and feature extraction and learning approaches for specific applications or user cases, thus identifying the strengths and limitations of the feature extraction and learning approaches. The benefit of understanding the relative performance of different biometric traits is twofold. First, it can assist the development of more effective cancellable biometric systems. Second, it can guide researchers towards selecting suitable feature extraction and learning approaches in the cancellable biometrics design. It is worth noting that the performance of cancellable biometric systems depends on feature extraction and learning approaches as well as template protection methods [54], which means that the same feature extraction or learning approach used in two cancellable biometric systems may lead to different performance, because of different feature protection methods (e.g. feature transformation functions).

5.1 | Fingerprint datasets and performance comparison of cancellable fingerprint systems

There are two major fingerprint databases—FVC2002 and FVC2004, introduced below and summarised in Table 7.

- *FVC2002* [35]: FVC stands for fingerprint verification competition, which aimed to establish a common benchmark that would allow companies and academic institutions to unambiguously compete the performance of their fingerprint recognition algorithms and track improvements. Made up of four databases, FVC2002 was the second international competition held in 2002.
- *FVC2004* [117]: FVC2004 was the third international FVC competition held in 2004. FVC2004 contains four databases.

The performance of various cancellable fingerprint systems is listed and compared in Table 8, from which we can see that most systems use hand-engineered feature extraction. This is because minutiae-based features, obtained by hand-engineered feature extraction approaches, tend to be robust and reliable [119]. By using minutiae as the basis for feature representation, fingerprints can be accurately identified and matched even with some uncertainties or variations in fingerprint images. Hand-engineered feature extraction is particularly useful in the case of poor-quality fingerprint images, as minutiae may still be present and detected when other features are not clear, making machine/deep learning-based approaches less effective. It is clear from Table 8 that based on the MCC features, which

TABLE 7 Information about different fingerprint datasets (adapted from Refs [35, 117]).

Dataset	Sensor type	Image size	Resolution	Number of images
FVC2002 DB1	Optical (Identix TouchView II)	388 × 374	500 dpi	100 × 8
FVC2002 DB2	Optical (Biometricka FX2000)	296 × 560	569 dpi	100 × 8
FVC2002 DB3	Capacitive (Precise Biometrics 100SC)	300 × 300	500 dpi	100 × 8
FVC2002 DB4	Synthetic (SFinGe v2.51)	288 × 384	500 dpi	100 × 8
FVC2004 DB1	Optical (CrossMatch V300)	640 × 480	500 dpi	100 × 8
FVC2004 DB2	Optical (Digital Persona U.are.U 4000)	328 × 364	500 dpi	100 × 8
FVC2004 DB3	Thermal (Atmel FingerChip)	300 × 480	512 dpi	100 × 8
FVC2004 DB4	Synthetic (SFinGe v3.0)	288 × 384	500 dpi	100 × 8

TABLE 8 Performance comparison of cancellable fingerprint systems.

Method	Type of feature extraction/learning	Transformation function	Trait	Database	Performance (EER)
Farooq et al. [41]	Hand-engineered	Hybrid-based	Fingerprint	Unknown	1.59%
Tulyakov et al. [42]	Hand-engineered	Cryptography-based	Fingerprint	FVC2002 DB1	3.0%
Lee and Kim [38]	Hand-engineered	Transformation-based	Fingerprint	FVC2004 DB1, DB2 and DB3	10.3%, 9.5%, and 6.8%
Ahmad et al. [29]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1, DB2 and DB3	9%, 6% and 27%
Wang and Hu [43]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1, DB2 and DB3	3.5%, 5% and 7.5%
Jin et al. [44]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1 and DB2	3.07% and 1.02%
Jin et al. [46]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1, DB2, DB3, FVC2004 DB1, DB2, DB3	0.22%, 0.47%, 3.07%, 4.74%, 4.10%, 3.99%
Li et al. [118]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1, DB2, DB3, FVC2004 DB1, DB2, DB3	0.19%, 0.51%, 3.44%, 1.49%, 3.80%, 4.15%
Bedari et al. [47]	Hand-engineered	Transformation-based	Fingerprint	FVC2002 DB1, DB2, DB3, FVC2004 DB1, DB2, DB3	0.04%, 0.50%, 0.99%, 2.77%, 3.28%, 1.75%

Abbreviation: EER, equal error rate.

come from hand-engineered feature extraction, the cancellable fingerprint system proposed by Bedari et al. [47] achieved the best EER on most of the databases, except FVC2002 DB2 and FVC2004 DB1.

5.2 | Face datasets and performance comparison of cancellable face systems

There are many face databases, with information like the number of users, poses and lighting conditions, available for cancellable face research. Some of the most well-known face databases [120] include:

- *The Aberdeen dataset* [121]: This dataset comprises 377 colour facial images of 29 individuals. Each individual has 13 frontal images captured under different lighting conditions and variations in expression.
- *The Georgia Tech dataset* [122]: This dataset contains 750 colour face images from 50 identities, each containing 15 colour images, either frontal views or tilted to various degrees and with different illumination and expressions.
- *The Visible light dataset* [123]: This dataset has 400 colour frontal face images of 100 identities under different lighting conditions. Some of the face images with glasses are obscured.
- *The YMU dataset* [124]: This dataset was collected from makeup courses in YouTube videos. It has 151 users' four frontal view face images with different degrees of makeup and slight expression and posture changes.
- *CMU PIE dataset* [125]: This database contains more than 41,000 face images of 68 people, captured under 13 different poses and lighting conditions.
- *The ORL database* [126]: This database has face images of 40 individuals, each captured in 10 different poses and under different lighting conditions.
- *The FERET database* [127]: This database contains face images of 35 individuals, each captured in 4 different poses and under different lighting conditions.
- *Labeled Faces in the Wild (LFW)* [128]: This database consists of more than 13,000 face images, with each image labelled with the name of the person depicted. The images are collected from the internet and vary in terms of lighting, pose and background.
- *The Yale database* [129]: This database contains face images of 15 individuals, each captured in 11 different poses and under different lighting conditions.
- *YouTube Faces* [130]: This database has an average of 181.3 frames of 3425 videos contributed by 1595 users.
- *VGGFace2* [37]: This dataset contains 3.31 million face images from 9131 subjects, with an average of about 362 images per subject. Images are downloaded from Google Image Search and vary widely in terms of pose, age, lighting, race, and occupation.

Performance of cancellable face systems with either hand-engineered feature extraction or machine/deep learning-based feature learning is compared in Table 9. The performance is measured by the EER or RR. It is shown in Table 9 that ORL [126] is the most commonly used face database, on which a

TABLE 9 Performance comparison of cancellable face systems.

Method	Type of feature extraction/ learning	Transformation function	Trait	Database	Performance (EER or RR)
Savvides et al. [32]	Hand-engineered	Filter-based	Face	CMU PIE	RR = 100%
Oh et al. [30]	Hand-engineered	Transformation-based	Face	ORL, FERET	EER = 1%, 1%
Faragallah et al. [60]	Hand-engineered	Transformation-based	Face	FERET, YALE	EER = 0.014976%, 0%
Xu et al. [59]	Hand-engineered	Transformation-based	Face	Aberdeen, GT, VIS, YMU	RR = 98.85%, 98.67%, 99.00%, 92.72%
Alhumyani et al. [61]	Hand-engineered	Transformation-based	Face	LFW, FERET, ORL	RR = 99.63%, 99.92%, 98.97%
Jang and Cho [88]	CNN	Cryptography-based	Face	YouTube Faces	RR = 99.34%
Abdellatef et al. [31]	CNN	Filter-based	Face	FERET, LFW	RR = 97.14%, 97.94%
Ma et al. [95]	MobileNetV1	Transformation-based	Face	ORL, LFW	EER = 0.2%, 0.2%
Ghafourian et al. [98]	ResNet-50	Cryptography-based	Face	VGGFace2	EER = 2.25%
Punithavathi and Geetha [99]	LDA	Transformation-based	Face	ORL	EER = 4.21%
Kumar et al. [103]	PCA	Transformation-based	Face	ORL	RR = 90%
Bamoriya et al. [108]	CAE	Transformation-based	Face	ORL	EER = 0%

Abbreviations: EER, equal error rate; RR, recognition rate.

number of cancellable face systems are tested and the system of Bamoriya et al. [108] achieves the best performance with EER = 0%. On another database FERET [127], the system designed by Faragallah et al. [60] obtains the best EER of 0.014976%.

5.3 | Iris datasets and performance comparison of cancellable iris systems

The following iris databases have been widely used in the research and development of cancellable iris systems:

- *CASIA-v1 interval iris database* [131]: This database contains a total of 756 eye images with 108 distinctive eyes and 7 images of each distinctive eye.
- *CASIA-v3 interval iris database* [70, 132]: This dataset has 2639 iris images from 396 different classes (eyes).
- *MMU1 database* [133, 134]: This database is made up of 450 iris images from 45 individuals.
- *IIT Delhi (IITD) database* [72, 135]: This database is composed of 1120 iris images in the bitmap format obtained from 224 users (i.e. 176 males and 48 females).
- *UBIRIS* [136]: This database has 1877 iris images of 241 individuals collected in September 2004 in two sessions.

Table 10 shows the performance comparison of cancellable iris systems, measured by the EER. Tested on databases CASIA-v3 and IITD, the system of Umer et al. [69] exhibits the best EER of 0.0001% and 0.0008%, respectively.

5.4 | Performance comparison of cancellable voice systems

Table 11 compares the performance of cancellable voice systems tested on private databases, measured by the EER or RR.

5.5 | ECG datasets and performance comparison of cancellable ECG systems

A ECG dataset is a collection of ECG measurements taken from individuals. Below are some commonly used ECG datasets for cancellable ECG systems. Performance of cancellable ECG systems is compared in Table 12. The metric used for evaluation is the EER.

- *Physikalisch Technische Bundesanstalt Database* [79]: This database contains 549 records from 290 subjects (each subject may have 1–5 records). Each record includes a Frank-lead vectorcardiogram and a standard 12-lead ECG, sampled at 1000 Hz with 16-bit resolution over a range of ±16.384 mV.
- *MIT-BIH arrhythmia dataset* [137]: This database contains 48 ECG records from 47 subjects (i.e. 25 men aged between 32 and 89 and 22 women aged between 23 and 89). The recordings were digitised at 360 samples every second per channel with 11-bit resolution over a 10-mV range.
- *ECG-ID* [138]: This database contains 310 ECG recordings obtained from 90 individuals. These ECG signals record both normal and abnormal rhythms, as well as signals from patients with various cardiac conditions.

TABLE 10 Performance comparison of cancellable iris systems.

Method	Type of feature extraction/learning	Transformation function	Trait	Database	Performance (EER)
Uhl et al. [66]	Hand-engineered	Transformation-based	Iris	CASIA-v3	1.2%
Jenisch and Uhl [67]	Hand-engineered	Transformation-based	Iris	CASIA-v3	1.244%
Rathgeb et al. [68]	Hand-engineered	Filter-based	Iris	CASIA-v3	E1.63%
Umer et al. [69]	Hand-engineered	Cryptography-based	Iris	CASIA-v3, MMU1, IITD	0.0001%, 0%, 0.0008%
Sandhya et al. [91]	CNN	Transformation-based	Iris	IITD, MMU1	0.05%, 0.03%
Singh et al. [34]	CNN	Hybrid-based	Iris	IITD	0.22%
Punithavathi and Geetha [99]	LDA	Transformation-based	Iris	UBIRIS	5.43%

Abbreviation: EER, equal error rate.

TABLE 11 Performance comparison of cancellable voice systems.

Method	Type of feature extraction/learning	Transformation function	Trait	Database	Performance (EER or RR)
Elsayed et al. [33]	Hand-engineered	Filter-based	Voice	Private dataset with 20 speech signals	EER = 0.11%
Abdelwahab et al. [74]	Hand-engineered	Transformation-based	Voice	Private dataset	RR = 98.45%
El-Wahab et al. [76]	Hand-engineered	Hybrid-based	Voice	Private database containing 15 speakers	RR = 100%

Abbreviations: EER, equal error rate; RR, recognition rate.

TABLE 12 Performance comparison of cancellable ECG systems.

Method	Type of feature extraction/learning	Transformation function	Trait	Database	Performance (EER)
Wu et al. [79]	Hand-engineered	Transformation-based	ECG	PTB	0.038%
Hammad et al. [80]	Hand-engineered	Cryptography-based	ECG	MIT-BIH, PTB, CYBHi	6%, 14%, 9%
Kim and Chun [81]	Hand-engineered	Hybrid-based	ECG	ECG-ID	4.8%
Sakr et al. [93]	VGG-16	Transformation-based	ECG	PTB, ECG-ID	0.4%, 0.44%

Abbreviations: ECG, electrocardiogram; EER, equal error rate.

5.6 | Other biometric datasets and performance comparison of cancellable biometric systems using other traits

In this section, databases of other biometric traits (e.g. fingervein, palmprint and EEG) are introduced. Performance comparison of cancellable biometric systems using those traits is reported in Table 13. The performance measures include the EER, false accept rate, false rejection rate and RR.

- *University of Twente Finger Vascular Pattern Database (UTFVP)* [139]: This dataset includes a total of 1440 images captured from 60 subjects in two recording sessions, each with six fingers (index, middle and ring fingers) and 4 images for each finger. The resolution of these finger vein images is 672 × 380 pixels.
- *Motor Movement/Imagery Database* [137]: This database has EEG signals of 109 healthy individuals in resting states and motor imagery tasks.
- *CASIA-Palmprint* [140]: This dataset contains 5502 palmprint images from 312 individuals, collected from both left and right palms of each subject. The collected palmprint images are 8-bit grey-level JPEG files.
- *PolyU Palmprint* [86]: This database includes 7752 gray-scale images acquired from 386 palms of individuals with different ages and genders. There are approximately 20 images of size 384 × 284 per palm, acquired in two sessions (10 images per session) with an interval of approximately 2 months.
- *MCYT Online Signature Corpus* [141]: This database contains signatures from 330 subjects, each with 25 real signatures and 25 forged signatures. The genuine signatures are divided into five sets, allowing for some breaks between collection sets.

6 | DISCUSSION

6.1 | Hand-engineered feature extraction versus machine/deep learning-based feature learning

In cancellable biometrics research, hand-engineered feature extraction approaches extract and represent biometric features using manually designed algorithms or techniques. These approaches involve the manual selection and design of features,

TABLE 13 Performance comparison of cancellable biometric systems using other traits (e.g. finger vein, EEG, palmprint and signature).

Method	Type of feature extraction/ learning	Transformation function	Trait	Database	Performance (EER, FAR, FRR or RR)
Kauba et al. [84]	Hand-engineered	Filter-based	Finger vein	UTFVP	EER = 0.36%
Yang et al. [83]	Hand-engineered	Cryptography-based	Finger vein	UTFVP	RR = 98.61%
Wang et al. [85]	Hand-engineered	Transformation-based	EEG	MMIDB	EER = 0.68%
Sardar et al. [106]	*K*-means clustering	Cryptography-based	Palmprint	PolyU Palmprint	FAR = 0.0297% and FRR = 0.6%
Leng and Zhang [86]	Hand-engineered	Transformation-based	Palmprint	CASIA-Palmprint	EER = 0.67%
Maiorana [87]	Hand-engineered	Transformation-based	Signature	MCYT	EER = 7.95%

Abbreviations: EEG, electroencephalography; EER, equal error rate; FAR, false accept rate; FRR, false rejection rate; RR, recognition rate.

based on their specific characteristics and/or analysis outcomes [142]. In contrast, machine/deep learning-based feature learning approaches automatically learn and extract biometric features from biometric data itself using machine/deep learning algorithms [36]. Biometric features are learned through training a machine learning model on a biometric dataset, and then that model is used to extract relevant features to achieve desired results.

There are some key differences between hand-engineered feature extraction and machine/deep learning-based feature learning approaches. These differences include: (a) Expertise required: To select and extract appropriate features, cancellable biometrics researchers need to have domain knowledge and a good understanding of the characteristics of biometric data when using hand-engineered feature extraction. For example, the extraction of minutiae-based fingerprint features requires specific knowledge and information about minutiae and local structures formed by minutiae [143]. Machine/deep learning-based feature learning approaches, on the other hand, can be employed without specific domain knowledge, because machine learning models are able to automatically learn relevant features from biometric data. (b) Scalability: Hand-engineered feature extraction is usually less scalable than machine/deep learning-based feature learning, because manually selecting and designing features can be time-consuming and unsuitable for large and complex datasets. On the other hand, machine/deep learning-based feature learning is applicable to large and complicated datasets with minimum extra effort [143].

6.2 | Impact of feature representation on the recognition performance of cancellable biometrics

Preserving recognition performance is an essential requirement for cancellable biometrics. According to the ISO/IEC 24745 standard [11], any template protection design should not degrade recognition performance. While for cancellable biometrics, the extent of performance decline depends on specific transformation functions, the overall recognition performance of cancellable biometric systems fundamentally relies on the extracted or learned biometric features. Therefore, it is crucial to develop effective feature extraction and learning approaches that can output both discriminative and robust features from raw biometric data (e.g. biometric images), because good feature representation produces strong recognition performance in cancellable biometrics.

The quality of the features selected and designed by hand-engineered feature extraction approaches impacts on recognition performance. If features are not representative of the characteristics of biometric data, recognition performance may suffer [144]. Take cancellable fingerprints as an example. Biometric uncertainty arises from variables such as users' interaction with fingerprint readers (e.g. placement position and applied pressure) and the condition of the finger (e.g. dry or wet) [145]. These factors can have a detrimental effect on the recognition accuracy of cancellable biometric systems. To address this challenge, researchers have developed a range of feature extraction techniques over time, from early approaches like registration-based feature representation [28], stable local structure-based features (e.g. features extracted from Delauney triangles) [146], to the well-known MCC-based feature representation [147]. These diverse techniques are innovative, designed to alleviate the adverse effect of biometric uncertainty, resulting in improved recognition accuracy.

Since machine/deep learning-based feature learning approaches can automatically extract the most relevant features from biometric data, they in turn strengthen recognition performance, particularly for large-scale datasets. Although fingerprint recognition is accessible to relatively small datasets, face recognition benefits significantly from its access to large datasets, such as the CMU PIE dataset [125] and the LFW dataset [128]. Capitalising on these extensive datasets, machine/deep learning models (e.g. CNNs) can capture intricate and subtle patterns inherent in facial images. These intricate patterns, often challenging to discern with hand-engineered feature extraction approaches, are successfully detected by machine/deep learning models, ultimately leading to substantial improvement in recognition performance. It is worth noting that machine/deep learning-based feature learning has its own issues [36], such as potential overfitting. Moreover, it requires large amounts of labelled data for training, so when

labelled data is limited (e.g. small fingerprint datasets), hand-engineered feature extraction is likely more practical.

6.3 | Impact of feature representation on the non-invertibility of cancellable biometrics

Non-invertibility is core for cancellable biometrics. Research shows that both hand-engineered feature representation [148] and machine/deep learning-based feature representation [149] can be inverted to reconstruct raw biometric data (e.g. images). It is common knowledge that the non-invertibility of cancellable biometrics relies on transformation functions designed, which are usually applied to the extracted or learned features to produce transformed templates. If the features themselves exhibit good irreversibility, it makes it harder for attackers to obtain raw biometric data (e.g. images), thereby heightening the overall security of cancellable biometric systems.

The irreversibility of hand-engineered feature representation and machine/deep learning-based feature representation differs. It is not easy to determine which type of feature representation has better irreversibility. Only one study [25] makes a comparison between them on fingerprints. In this work, Wijewardena et al. [25] demonstrated that deep learning-based feature representation is more resistant to reconstruction attacks than hand-engineered feature representation (e.g. minutiae). We cannot find similar research on the irreversibility comparison for biometric traits other than fingerprint, so it would be hard to conclude whether hand-engineered or machine/deep learning-based feature representation possesses better irreversibility. Nevertheless, we believe that cancellable transformation functions should take primary responsibility for the non-invertibility of cancellable biometric systems.

6.4 | Potential research directions of deep learning-based feature learning for cancellable biometrics

Deep learning is a type of machine learning. The objective of deep learning-based feature learning for cancellable biometrics is to explore deep learning algorithms that can learn robust and distinctive features from biometric data. The features learned can then be utilised for authentication but should not be easily inverted. Compared to hand-engineered feature extraction, which has been studied for decades, deep learning-based feature learning is relatively new and still requires more effort and attention from researchers to further develop it. We summarise several research directions in this area as follows.

- Deep learning-based feature representation: One potential direction is to derive deep learning-based feature learning methods which are capable of extracting discriminative features but also ensure that the learned features do not expose raw biometric data. This is a valuable capability for deep learning architectures (e.g. CNNs). Research (e.g. [149]) shows that features learned by deep learning algorithms, if unprotected, can be reversed to retrieve raw biometric data (e.g. face images). Almost all the deep learning-based feature learning approaches discussed in Section 4 follow a two-step process: an initial step involving feature extraction through deep learning algorithms, followed by another step of feature transformation. Hence, it would be most desirable if the features learned are inherently non-invertible so that it is unnecessary to have an additional layer of protection.
- Deep learning-based feature fusion: Another potential direction is to use deep learning techniques to fuse or learn features from multiple biometric modalities [150]. How to design effective and efficient fusion strategies in a multimodal context is worth investigating.
- Deep learning-based privacy protection: An additional potential direction is to make use of deep learning techniques to simultaneously learn and transform the features extracted, thus preserving them and making it difficult for attackers to reverse the transformation or use the transformed data to retrieve the original data. In this way, the privacy of the original biometric data is protected. Regarding the topic of privacy preservation with cancellable biometrics, we suggest researchers exploring modified deep learning architectures (e.g. [151, 152]).

6.5 | Reflections on hybrid feature extraction and learning for cancellable biometrics

Hybrid feature extraction and learning has been introduced in Section 4. There are several ways to implement hybrid feature extraction and learning for cancellable biometrics, including combining resultant features learned in a hybrid feature learning setting, integrating hand-engineered feature extraction and machine/deep learning-based feature learning in a unified framework, and using machine/deep learning techniques to select or refine hand-engineered features [153]. Hybrid feature learning can be especially beneficial when it is applied on complex or noisy data, or when there are only limited training data available. However, the limits and drawbacks of hybrid feature learning need to be considered. For example, hybrid feature learning might be more difficult to carry out and explain than the non-hybrid feature learning. Inappropriately integrating various components of a hybrid feature learning approach could cause low efficiency.

7 | CONCLUSION

This survey paper provided an overview of feature representation and learning approaches used in the field of cancellable biometrics. We discussed the requirements of good feature representation and different data types of biometric feature representation. We also reviewed both hand-engineered feature extraction and machine/deep learning-based feature learning approaches, and compared their performance over various databases. Overall, it is clear that both hand-engineered feature extraction and machine/deep learning-based feature learning

have their own strengths and limitations, and choosing suitable feature extraction and learning approaches depends on the requirements and constraints of specific applications. While hand-engineered feature extraction is mature enough, deep learning-based feature learning has progressed rapidly in the study of cancellable biometrics in recent years. More research is needed to continue improving the performance and reliability of feature extraction and learning approaches for cancellable biometrics. This survey paper has served the purpose of reviewing the latest developments and outlining future research of feature extraction and learning for cancellable biometrics.

ACKNOWLEDGEMENTS

This study was supported by ARC grants: DP190103660, DP200103207 and LP180100663. This research was partially supported by the UniSQ Capacity Building Grants with Grant Number 1008313.

Open access publishing facilitated by University of New South Wales, as part of the Wiley - University of New South Wales agreement via the Council of Australian University Librarians.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analysed in this study.

ORCID

Wencheng Yang https://orcid.org/0000-0001-7800-2215
Jiankun Hu https://orcid.org/0000-0003-0230-1432
Xiaohui Tao https://orcid.org/0000-0002-0020-077X

REFERENCES

1. Kumar, N.: Cancelable biometrics: a comprehensive survey. Artif. Intell. Rev. 53(5), 3403–3446 (2020)
2. Yang, W., et al.: Biometrics for internet-of-things security: a review. Sensors 21(18), 6163 (2021). https://www.mdpi.com/1424-8220/21/18/6163
3. Zheng, G., et al.: From WannaCry to WannaDie: security trade-offs and design for implantable medical devices. In: Communications and Information Technologies (ISCIT), 2017 17th International Symposium on IEEE, pp. 1–5 (2017)
4. Yang, W., et al.: Security and forensics in the internet of things: research advances and challenges. In: Workshop on Emerging Technologies for Security in IoT (ETSecIoT), pp. 12–17. IEEE (2020)
5. Lee, M.J., et al.: Alignment-robust cancelable biometric scheme for iris verification. IEEE Trans. Inf. Forensics Secur. 17, 3449–3464 (2022). https://doi.org/10.1109/tifs.2022.3208812
6. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. 2011(1), 1–25 (2011). https://doi.org/10.1186/1687-417x-2011-3
7. Yang, W., et al.: Multimedia security and privacy protection in the internet of things: research developments and challenges. Int. J. Multimed. Intell. Secur. 2022(January), 27 (2022)
8. Yang, W., et al.: A review on security issues and solutions of the internet of drones. IEEE Open J. Comput. Soc. 3, 96–110 (2022). https://doi.org/10.1109/ojcs.2022.3183003
9. Yang, W., et al.: Security and accuracy of fingerprint-based biometrics: a review. Symmetry 11(2), 141 (2019). https://doi.org/10.3390/sym11020141
10. Lee, C., et al.: Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Trans. Syst. Man Cybern. B Cybern. 37(4), 980–992 (2007)
11. Standard IOfSI, ISO/IEC 24745:2022(E) (2022)
12. Chin, Y., et al.: Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf. Fusion 18, 161–174 (2014). https://doi.org/10.1016/j.inffus.2013.09.001
13. Jain, A.K., Ross, A., Uludag, U.: Biometric template security: challenges and solutions. In: 2005 13th European Signal Processing Conference, pp. 1–4 (2005)
14. Rida, I., et al.: A comprehensive overview of feature representation for biometric recognition. Multimed. Tool. Appl. 79(7), 4867–4890 (2020). https://doi.org/10.1007/s11042-018-6808-5
15. Choudhary, D., Tiwari, S., Singh, A.K.: A survey: feature extraction methods for iris recognition. Int. J. Electron. Commun. Comput. Technol. 2(6), 275–279 (2012)
16. Pflug, A., Busch, C.: Ear biometrics: a survey of detection, feature extraction and recognition methods. IET Biom. 1(2), 114–129 (2012). https://doi.org/10.1049/iet-bmt.2011.0003
17. Fei, L., et al.: Feature extraction methods for palmprint recognition: a survey and evaluation. IEEE Trans. Syst. Man Cybern. Syst. 49(2), 346–363 (2018). https://doi.org/10.1109/tsmc.2018.2795609
18. Prabakaran, D., Shyamala, R.: A review on performance of voice feature extraction techniques. In: 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), pp. 221–231. IEEE (2019)
19. Zhang, Z., et al.: A survey of sparse representation: algorithms and applications. IEEE Access 3, 490–530 (2015). https://doi.org/10.1109/access.2015.2430359
20. Sundararajan, K., Woodard, D.L.: Deep learning for biometrics: a survey. ACM Comput. Surv. 51(3), 1–34 (2018). https://doi.org/10.1145/3190618
21. Wang, M., et al.: Representation learning and pattern recognition in cognitive biometrics: a survey. Sensors 22(14), 5111 (2022). https://doi.org/10.3390/s22145111
22. Jain, A.K., Kumar, A.: Biometrics of next generation: an overview. Sec. Generat. Biometrics 12(1), 2–3 (2010)
23. Gafurov, D., Snekkenes, E., Buvarp, T.E.: Robustness of biometric gait authentication against impersonation attack. In: OTM Confederated International Conferences" on the Move to Meaningful Internet Systems", pp. 479–488. Springer (2006)
24. Jain, A.K., Kumar, A.: Biometric Recognition: An Overview. Second Generation Biometrics: The Ethical, Legal and Social Context, pp. 49–79 (2012)
25. Wijewardena, K.P., et al.: Fingerprint template invertibility: minutiae vs. deep templates. IEEE Trans. Inf. Forensics Secur. 18, 744–757 (2022). https://doi.org/10.1109/tifs.2022.3229587
26. Lim, M., Teoh, A.B.J., Kim, J.: Biometric feature-type transformation: making templates compatible for secret protection. IEEE Signal Process. Mag. 32(5), 77–87 (2015). https://doi.org/10.1109/msp.2015.2423693
27. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. 37(11), 2245–2255 (2004). https://doi.org/10.1016/j.patcog.2004.04.011
28. Ratha, N.K., et al.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 561–572 (2007). https://doi.org/10.1109/tpami.2007.1004
29. Ahmad, T., Hu, J., Wang, S.: Pair-polar coordinate-based cancelable fingerprint templates. Pattern Recogn. 44(10), 2555–2564 (2011). https://doi.org/10.1016/j.patcog.2011.03.015
30. Oh, B.S., et al.: Extraction and fusion of partial face features for cancelable identity verification. Pattern Recogn. 45(9), 3288–3303 (2012). https://doi.org/10.1016/j.patcog.2012.02.027

31. Abdellatef, E., et al.: Cancelable multi-biometric recognition system based on deep learning. Vis. Comput. 36(6), 1097–1109 (2020). https://doi.org/10.1007/s00371-019-01715-5
32. Savvides, M., Kumar, B.V., Khosla, P.K.: Cancelable biometric filters for face recognition. In: Proceedings of the 17th International Conference on Pattern Recognition, 2004, vol. 3, pp. 922–925. IEEE (2004)
33. Elsayed, M., et al.: Cancelable speaker identification based on inverse filter. Menoufia J. Electron. Eng. Res. 28(ICEEM2019-Special Issue), 133–137 (2019). https://doi.org/10.21608/mjeer.2019.76969
34. Singh, A., et al.: A generic framework for deep incremental cancelable template generation. Neurocomputing 467, 83–98 (2022). https://doi.org/10.1016/j.neucom.2021.09.055
35. Maio, D., et al.: FVC2002: second fingerprint verification competition. In: 2002 International Conference on Pattern Recognition, vol. 3, pp. 811–814. IEEE (2002)
36. Goodfellow, I., Bengio, Y., Courville, A.: Deep Learning, vol. 1. MIT press (2016)
37. Cao, Q., et al.: Vggface2: a dataset for recognising faces across pose and age. In: 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), pp. 67–74. IEEE (2018)
38. Lee, C., Kim, J.: Cancelable fingerprint templates using minutiae-based bit-strings. J. Netw. Comput. Appl. 33(3), 236–246 (2010). https://doi.org/10.1016/j.jnca.2009.12.011
39. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 40(3), 614–634 (2001). https://doi.org/10.1147/sj.403.0614
40. El-wahab, A., et al.: Discrete wavelet transform based cancelable biometric system for speaker recognition. J. Eng. Res. 2(December), 102–110 (2018). https://doi.org/10.21608/erjeng.2018.126039
41. Farooq, F., et al.: Anonymous and revocable fingerprint recognition. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–7. IEEE (2007)
42. Tulyakov, S., et al.: Symmetric hash functions for secure fingerprint biometric systems. Pattern Recogn. Lett. 28(16), 2427–2436 (2007)
43. Wang, S., Hu, J.: Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. Pattern Recogn. 45, 4129–4137 (2012)
44. Jin, Z., et al.: A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template. Secur. Commun. Network. 7(11), 1691–1701 (2013)
45. Ning, Z., et al.: Generating registration-free cancelable fingerprint templates based on minutia cylinder-code representation. In: Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pp. 1–6 (2013)
46. Jin, Z., et al.: Ranking based locality sensitive hashing enabled cancelable biometrics: index-of-max hashing. IEEE Trans. Inf. Forensics Secur. 13(2), 393–407 (2017)
47. Bedari, A., Wang, S., Yang, W.: A secure online fingerprint authentication system for industrial IoT devices over 5G networks. Sensors 22(19), 7609 (2022)
48. Sun, Y., Li, H., Li, N.: A novel cancelable fingerprint scheme based on random security sampling mechanism and relocation bloom filter. Comput. Secur. 125, 103021 (2023)
49. Djebli, H., Ait-Aoudia, S., Michelucci, D.: Quantized random projections of SIFT features for cancelable fingerprints. Multimed. Tool. Appl. 82(5), 7917–7937 (2023)
50. Cappelli, R., et al.: MCC: a baseline algorithm for fingerprint verification in FVC-onGoing. In: Control Automation Robotics & Vision (ICARCV), 2010 11th International Conference on IEEE, pp. 19–23 (2010)
51. Wang, S., Hu, J.: A blind system identification approach to cancelable fingerprint templates. Pattern Recogn. 54, 14–22 (2016)
52. Wang, S., Deng, G., Hu, J.: A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn. 61, 447–458 (2017)
53. Cappelli, R., Ferrara, M., Maltoni, D.: Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern Anal. Mach. Intell. 32(12), 2128–2141 (2010)
54. Shahzad, M., et al.: Alignment-free cancelable fingerprint templates with dual protection. Pattern Recogn. 111, 107735 (2020)
55. Bedari, A., Wang, S., Yang, W.: Design of cancelable MCC-based fingerprint templates using Dyno-key model. Pattern Recogn. 119, 108074 (2021)
56. Bedari, A., Wang, S., Yang, W.: Design of cancelable MCC-based fingerprint templates using Dyno-key model. Pattern Recogn. 119, 108074 (2021)
57. Kho, J.B., et al.: Cancelable fingerprint template design with randomized non-negative least squares. Pattern Recogn. 91, 245–260 (2019)
58. Jin, Z., et al.: Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication. IEEE Trans. Syst. Man Cybern. Syst. 46(10), 1415–1428 (2016)
59. Xu, Z., et al.: Fusing structure and color features for cancelable face recognition. Multimed. Tool. Appl. 80(9), 14477–14494 (2021). https://doi.org/10.1007/s11042-020-10234-8
60. Faragallah, O.S., et al.: Efficient chaotic-Baker-map-based cancelable face recognition. J. Ambient Intell. Hum. Comput. 14(3), 1837–1875 (2021). https://doi.org/10.1007/s12652-021-03398-0
61. Alhumyani, H., et al.: Efficient generation of cancelable face templates based on quantum image Hilbert permutation. Electronics 11(7), 1040 (2022). https://doi.org/10.3390/electronics11071040
62. SP, R., Thomas, T.: Cancelable biometric scheme based on dynamic salting of random patches. Multimed. Tool. Appl. 8(20), 14337–14366 (2022). https://doi.org/10.1007/s11042-022-13764-5
63. Yang, W., et al.: A cancelable iris- and steganography-based user authentication system for the internet of things. Sensors 19(13), 2985 (2019). https://doi.org/10.3390/s19132985
64. Ajish, S., AnilKumar, K.: Iris template protection using double bloom filter based feature transformation. Comput. Secur. 97, 101985 (2020). https://doi.org/10.1016/j.cose.2020.101985
65. Zuo, J., Ratha, N.K., Connell, J.H.: Cancelable iris biometric. In: 2008 19th International Conference on Pattern Recognition, pp. 4. IEEE (2008)
66. Hämmerle-Uhl, J., Pschernig, E., Uhl, A.: Cancelable iris biometrics using block re-mapping and image warping. In: International Conference on Information Security, pp. 135–142. Springer (2009)
67. Jenisch, S., Uhl, A.: Security analysis of a cancelable iris recognition system based on block remapping. In: 2011 18th IEEE International Conference on Image Processing (ICIP), pp. 3213–3216. IEEE (2011)
68. Rathgeb, C., Breitinger, F., Busch, C.: Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In: 2013 International Conference on Biometrics (ICB), pp. 8. IEEE (2013)
69. Umer, S., Dhara, B.C., Chanda, B.: A novel cancelable iris recognition system based on feature learning techniques. Inf. Sci. 406, 102–118 (2017)
70. Lai, Y.L., et al.: Cancellable iris template generation based on indexing-first-one hashing. Pattern Recogn. 64, 105–117 (2017)
71. Asaker, A.A., et al.: A novel cancellable Iris template generation based on salting approach. Multimed. Tool. Appl. 80(3), 3703–3721 (2020)
72. Sadhya, D., Raman, B.: Generation of cancelable iris templates via randomized bit sampling. IEEE Trans. Inf. Forensics Secur. 14(11), 2972–2986 (2019)
73. Kausar, F.: Iris based cancelable biometric cryptosystem for secure healthcare smart card. Egypt. Inf. J. 22(4), 447–453 (2021)
74. Abdelwahab, K.M., et al.: Efficient cancelable speaker identification system based on a hybrid structure of DWT and SVD. Int. J. Speech Technol. 25(1), 279–288 (2022). https://doi.org/10.1007/s10772-020-09778-9
75. El-Gazar, S., et al.: Cancelable speaker identification system based on optical-like encryption algorithms. Comput. Syst. Sci. Eng. 43(1), 87–102 (2022). https://doi.org/10.32604/csse.2022.022722
76. El-Wahab, A., et al.: A cancelable biometric approach for efficient identification of speakers from encrypted speech. Wireless Pers. Commun. 124(3), 1899–1921 (2022). https://doi.org/10.1007/s11277-021-08384-5

77. Zheng, G., et al.: A critical analysis of ECG-based key distribution for securing wearable and implantable medical devices. IEEE Sensor. J. 19(3), 1–13 (2018). https://doi.org/10.1109/jsen.2018.2879929
78. Yang, W., Wang, S.: A privacy-preserving ECG-based authentication system for securing wireless body sensor networks. IEEE Internet Things J. 9(8), 6148–6158 (2021). https://doi.org/10.1109/jiot.2021.3109609
79. Wu, S.C., et al.: Cancelable biometric recognition with ECGs: subspace-based approaches. IEEE Trans. Inf. Forensics Secur. 14(5), 1323–1336 (2018). https://doi.org/10.1109/tifs.2018.2876838
80. Hammad, M., Luo, G., Wang, K.: Cancelable biometric authentication system based on ECG. Multimed. Tool. Appl. 78(2), 1857–1887 (2019). https://doi.org/10.1007/s11042-018-6300-2
81. Kim, H., Chun, S.Y.: Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test. IEEE Access 7, 9232–9242 (2019). https://doi.org/10.1109/access.2019.2891817
82. Eldesouky, S., et al.: Cancelable electrocardiogram biometric system based on chaotic encryption using three-dimensional logistic map for biometric-based cloud services. Secur. Priv. 5(2), e198 (2022). https://doi.org/10.1002/spy2.198
83. Yang, W., et al.: Securing deep learning based edge finger-vein biometrics with binary decision diagram. IEEE Trans. Ind. Inf. 15(7), 11 (2019)
84. Kauba, C., et al.: Towards practical cancelable biometrics for finger vein recognition. Inf. Sci. 585, 395–417 (2022)
85. Wang, M., Wang, S., Hu, J.: PolyCosGraph: a privacy-preserving cancelable EEG biometric system. IEEE Trans. Dependable Secure Comput. 20(5), 4258–4272 (2022). https://doi.org/10.1109/tdsc.2022.3218782
86. Leng, L., Zhang, J.: Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. J. Netw. Comput. Appl. 34(6), 1979–1989 (2011). https://doi.org/10.1016/j.jnca.2011.07.003
87. Maiorana, E., et al.: Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Trans. Syst. Man Cybern. Syst. Hum. 40(3), 525–538 (2010). https://doi.org/10.1109/tsmca.2010.2041653
88. Jang, Y.K., Cho, N.I.: Deep face image retrieval for cancelable biometric authentication. In: 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1–8. IEEE (2019)
89. Kim, B.H., Pyun, J.Y.: ECG identification for personal authentication using LSTM-based deep recurrent neural networks. Sensors 20(11), 3069 (2020). https://doi.org/10.3390/s20113069
90. Abdellatef, E., et al.: Cancelable face and iris recognition system based on deep learning. Opt. Quant. Electron. 54(11), 1–21 (2022). https://doi.org/10.1007/s11082-022-03770-0
91. Sandhya, M., et al.: Multi-instance cancelable iris authentication system using triplet loss for deep learning models. Vis. Comput. 39(4), 1571–1581 (2022). https://doi.org/10.1007/s00371-022-02429-x
92. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:14091556, 16 (2014)
93. Sakr, A.S., et al.: Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication. Inf. Sci. 585, 127–143 (2022). https://doi.org/10.1016/j.ins.2021.11.066
94. Howard, A.G., et al.: Mobilenets: efficient convolutional neural networks for mobile vision applications. arXiv preprint arXiv:170404861, 9 (2017)
95. Ma, Q., et al.: Cancelable face template protection based on deep neural network. In: 2022 7th International Conference on Signal and Image Processing (ICSIP), pp. 659–664. IEEE (2022)
96. He, K., et al.: Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778 (2016)
97. Kim, J., Jung, Y.G., Teoh, A.B.J.: Multimodal biometric template protection based on a cancelable SoftmaxOut fusion network. Appl. Sci. 12(4), 2023 (2022). https://doi.org/10.3390/app12042023
98. Ghafourian, M., et al.: OTB-morph: one-time biometrics via morphing applied to face templates. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pp. 321–329 (2022)
99. Punithavathi, P., Geetha, S.: Random permutation-based linear discriminant analysis for cancelable biometric recognition. In: Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, pp. 593–603. Springer (2021)
100. Creswell, A., et al.: Generative adversarial networks: an overview. IEEE Signal Process. Mag. 35(1), 53–65 (2018). https://doi.org/10.1109/msp.2017.2765202
101. Tarek, M., Hamouda, E., Abohamama, A.S.: Multi-instance cancellable biometrics schemes based on generative adversarial network. Appl. Intell. 52(1), 501–513 (2022). https://doi.org/10.1007/s10489-021-02401-7
102. Turk, M., Pentland, A.: Eigenfaces for recognition. J. Cognit. Neurosci. 3(1), 71–86 (1991). https://doi.org/10.1162/jocn.1991.3.1.71
103. Kumar, N., Singh, S., Kumar, A.: Random permutation principal component analysis for cancelable biometric recognition. Appl. Intell. 48(9), 2824–2836 (2018). https://doi.org/10.1007/s10489-017-1117-7
104. Yang, J., et al.: Two-dimensional PCA: a new approach to appearance-based face representation and recognition. IEEE Trans. Pattern Anal. Mach. Intell. 26(1), 131–137 (2004). https://doi.org/10.1109/tpami.2004.1261097
105. Hartigan, J.A., Wong, M.A.: Algorithm AS 136: a k-means clustering algorithm. J. Roy. Stat. Soc. Ser. C Appl. Stat. 28(1), 100–108 (1979). https://doi.org/10.2307/2346830
106. Sardar, A., et al.: A secure and efficient biometric template protection scheme for palmprint recognition system. IEEE Trans. Artif. Intell. 4(5), 1–13 (2022)
107. Pintelas, E., et al.: An autoencoder convolutional neural network framework for sarcopenia detection based on multi-frame ultrasound image slices. In: IFIP International Conference on Artificial Intelligence Applications and Innovations, pp. 209–219. Springer (2021)
108. Bamoriya, P., et al.: Cancelable template generation using convolutional autoencoder and RandNet. In: International Conference on Computer Vision and Image Processing, pp. 363–374. Springer (2022)
109. Siddhad, G., Khanna, P., Ojha, A.: Cancelable biometric template generation using convolutional autoencoder. In: International Conference on Computer Vision and Image Processing, pp. 303–314. Springer (2021)
110. Abdellatef, E., et al.: Cancelable fusion-based face recognition. Multimed. Tool. Appl. 78(22), 31557–31580 (2019). https://doi.org/10.1007/s11042-019-07848-y
111. Abdellatef, E., et al.: Fusion of deep-learned and hand-crafted features for cancelable recognition systems. Soft Comput. 24(20), 15189–15208 (2020). https://doi.org/10.1007/s00500-020-04856-1
112. Zhang, C., et al.: Multimodal intelligence: representation learning, information fusion, and applications. IEEE J. Sel. Top. Signal Process. 14(3), 478–493 (2020). https://doi.org/10.1109/jstsp.2020.2987728
113. Canuto, A.M., Pintro, F., Xavier-Junior, J.C.: Investigating fusion approaches in multi-biometric cancellable recognition. Expert Syst. Appl. 40(6), 1971–1980 (2012). https://doi.org/10.1016/j.eswa.2012.10.002
114. Dwivedi, R., Dey, S.: A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. arXiv preprint arXiv:180510433, 28 (2018)
115. Gupta, K., Walia, G.S., Sharma, K.: Novel approach for multimodal feature fusion to generate cancelable biometric. Vis. Comput. 37(6), 1401–1413 (2021). https://doi.org/10.1007/s00371-020-01873-x
116. Chang, Z., Zhang, X., Zhang, J.: PCA based cancelable biometric protection using feature-level fusion of iris and fingerprint. In: 2022 4th International Conference on Natural Language Processing (ICNLP), pp. 74–80. IEEE (2022)
117. Maio, D., et al.: FVC2004: third fingerprint verification competition. In: International Conference on Biometric Authentication, pp. 1–7. Springer (2004)
118. Li, Y., et al.: Compact and cancelable fingerprint binary codes generation via one permutation hashing. IEEE Signal Process. Lett. 28, 738–742 (2021)

119. Yang, W., et al.: A cancelable biometric authentication system based on feature-adaptive random projection. J. Inf. Secur. Appl. 58, 102704 (2021)
120. Gross, R.: Face Databases, pp. 301–327. Springer (2005)
121. Aberdeen face dataset. http://pics.stir.ac.uk/2D_face_sets.htm. Accessed 1 Sept 2023
122. Georgia Tech face dataset. http://www.anefian.com/research/face_reco.htm. Accessed 1 Sept 2023
123. Near Infrared-Visible light face dataset. http://biometrics.idealtest.org/. Accessed 1 Sept 2023
124. Dantcheva, A., Chen, C., Ross, A.: Can facial cosmetics affect the matching accuracy of face recognition systems? In: 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 391–398. IEEE (2012). YMU face dataset
125. Sim, T., Baker, S., Bsat, M.: The CMU pose, illumination, and expression (PIE) database. In: Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition IEEE, pp. 53–58 (2002)
126. AT&T Laboratories Cambridge, Olivetti Research Laboratory (ORL) database. http://www.cl.cam.ac.uk/Research/DTG/attarchive/pub/data/att_faces.zip. Accessed 1 Sept 2023
127. Phillips, P.J., et al.: The FERET evaluation methodology for face-recognition algorithms. IEEE Trans. Pattern Anal. Mach. Intell. 22(10), 1090–1104 (2000). https://doi.org/10.1109/34.879790
128. Huang, G.B., Learned-Miller, E.: Labeled faces in the wild: updates and new reporting procedures. Dept Comput Sci, Univ Massachusetts Amherst, Amherst, MA, USA, Tech Rep 14(003) (2014)
129. Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J.: Eigenfaces vs. fisherfaces: recognition using class specific linear projection. IEEE Trans. Pattern Anal. Mach. Intell. 19(7), 711–720 (1997). Yale Face database. https://doi.org/10.1109/34.598228
130. Wolf, L., Hassner, T., Maoz, I.: Face recognition in unconstrained videos with matched background similarity. In: CVPR 2011, pp. 529–534. IEEE (2021)
131. Chinese Academy of Sciences Institute of Automation: Database of 756 greyscale eye images. http://www.sinobiometrics.com (2022). Accessed 1 Sept 2023
132. CASIA V3 interval iris database. http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp (2022). Accessed 1 Sept 2023
133. Malaysia Multimedia University: MMU1 database. http://pesona.mmu.edu.my/Ëœccteo. Accessed 1 Sept 2023
134. Rafik, H.D., Boubaker, M.: A multi biometric system based on the right iris and the left Iris using the combination of convolutional neural networks. In: 2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS), pp. 1–10. IEEE (2020)
135. Kumar, A., Passi, A.: Comparison and combination of iris matchers for reliable personal authentication. Pattern Recogn. 43(3), 1016–1026 (2010). https://doi.org/10.1016/j.patcog.2009.08.016
136. Proença, H., Alexandre, L.A.: UBIRIS: a noisy iris image database. In: International Conference on Image Analysis and Processing, pp. 970–977. Springer (2005)
137. Goldberger, A.L., et al.: PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. Circulation 101(23), e215–e220 (2000). https://doi.org/10.1161/01.cir.101.23.e215
138. Bassiouni, M.M., et al.: Intelligent hybrid approaches for human ECG signals identification. Signal Image Video Process. 12(5), 941–949 (2018). https://doi.org/10.1007/s11760-018-1237-5
139. Ton, B.T., Veldhuis, R.N.: A high quality finger vascular pattern dataset collected using a custom designed capturing device. In: Biometrics (ICB), 2013 International Conference on IEEE, pp. 1–5 (2013). Description of finger-vein database UTFVP
140. Chinese Academy of Sciences' Institute of Automation: CASIA palmprint database. http://biometrics.idealtest.org/. Accessed 1 Sept 2023
141. Ortega-Garcia, J., et al.: MCYT baseline corpus: a bimodal biometric database. IEE Proc. Vis. Image Signal Process. 150(6), 395–401 (2003). https://doi.org/10.1049/ip-vis:20031078
142. Nasrabadi, N.M.: Pattern recognition and machine learning. J. Electron. Imag. 16(4), 049901 (2007)
143. Moorfield, J., et al.: A Möbius transformation based model for fingerprint minutiae variations. Pattern Recogn. 98, 107054 (2019). https://doi.org/10.1016/j.patcog.2019.107054
144. Yang, W., Hu, J., Wang, S.: A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement. IEEE Trans. Inf. Forensics Secur. 9(7), 1179–1192 (2014). https://doi.org/10.1109/tifs.2014.2328095
145. Engelsma, J.J., Cao, K., Jain, A.K.: Learning a fixed-length fingerprint representation. IEEE Trans. Pattern Anal. Mach. Intell. 43(6), 1981–1997 (2019). https://doi.org/10.1109/tpami.2019.2961349
146. Yang, W., Hu, J., Wang, S.: A Delaunay triangle group based fuzzy vault with cancellability. In: 2013 6th International Congress on Image and Signal Processing (CISP), vol. 03, pp. 1676–1681 (2013)
147. Ferrara, M., Maltoni, D., Cappelli, R.: A two-factor protection scheme for MCC fingerprint templates. In: 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8 (2014)
148. Cao, K., Jain, A.K.: Learning fingerprint reconstruction: from minutiae to image. IEEE Trans. Inf. Forensics Secur. 10(1), 104–117 (2015). https://doi.org/10.1109/tifs.2014.2363951
149. Mai, G., et al.: On the reconstruction of face images from deep face templates. IEEE Trans. Pattern Anal. Mach. Intell. 41(5), 1188–1202 (2018). https://doi.org/10.1109/tpami.2018.2827389
150. Alay, N., Al-Baity, H.H.: Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. Sensors 20(19), 5523 (2020). https://doi.org/10.3390/s20195523
151. Liu, Y., et al.: Finger vein secure biometric template generation based on deep learning. Soft Comput. 22(7), 1–9 (2017). https://doi.org/10.1007/s00500-017-2487-9
152. Pandey, R.K., et al.: Deep secure encoding for face template protection. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 77–83. IEEE (2016)
153. Qin, Z., et al.: A survey of identity recognition via data fusion and feature learning. Inf. Fusion 91, 694–712 (2023). https://doi.org/10.1016/j.inffus.2022.10.032

How to cite this article: Yang, W., et al.: Feature extraction and learning approaches for cancellable biometrics: a survey. CAAI Trans. Intell. Technol. 9(1), 4–25 (2024). https://doi.org/10.1049/cit2.12283