EURASIP Journal on Information Security

RESEARCH

Open Access

Cancelable palmprint: intelligent framework toward secure and privacy-aware recognition system

Hanaa S. Ali[1*], Eman I. Elhefnawy[1] and Mohammed Abo-Zahhad[2,3]

Abstract

Cancelable template protection techniques are indispensable to provide essential security and privacy privileges in biometric systems. This paper introduces an efficient cancelable palmprint recognition technique based on multi-level transformations. Gabor filtering with feature remapping is introduced for extracting highly discriminative features. Histogram remapping is applied to nonlinearly transform the downsampled Gabor features to be normally distributed. This feature-remapping step is proposed to enhance the discriminatory power and alleviate the effect of feature variability and image artifacts. Comb filtering is applied to the mapped features as a first protection layer. To provide security guarantees against linkability attacks, index-based locality-sensitive hashing (LSH) is introduced as a second protection layer to transform the comb-filtered mapped real-valued features into maximum-ranked indices. Recognition is performed in the secured domain to accelerate matching and to preserve the user's privacy. Results show that the proposed scheme provides a large re-issuance ability, protects templates from being inverted, and demonstrates strong unlinkability across different databases. In addition, favorable verification/identification accuracy is obtained and the system satisfies the needs for real-time applications. A global measure $D_{\leftrightarrow}^{sys}$ value of 0.01 is obtained, and thus, correlation attacks are mitigated. The recognition results for the legitimate scenario are 100% identification accuracy and 0% EER. For the worst case (same token scenario), the corresponding results are 99.752% and 0.31%, respectively.

Highlights

- Multi-level transformations are proposed for efficient cancelable palmprints.
- Histogram-remapped downsampled Gabor features are subjected to comb filtering.
- Locality-sensitive hashing follows comb filtering to obtain maximum-ranked indices.
- The algorithm provides significant capability for re-issuance.
- The system protects templates from inversion and ensures unlinkability across databases.

Keywords Cancelable palmprint, Histogram remapping, Comb filtering, Random projection, Locality-sensitive hashing, Linkability attacks

*Correspondence:
Hanaa S. Ali
hanahshaker@zu.edu.eg; hanahshaker@yahoo.com
Full list of author information is available at the end of the article

1 Introduction

Internet of Things (IoT) is essentially the combination of various types of technologies with different communication layers. Different layers necessitate different degrees of security arrangements. Biometric security systems are highly recommended for levels requiring direct human access. These systems have been widely disseminated in numerous applications such as face recognition [1, 2], multimodal biometric systems [3], forensic recovery and identification of marks from an adermatoglyphic individual [4], and palmprint recognition [5, 6]. While the use of biometrics is simple, convenient, and reliable, hidden pitfalls may result in major security weaknesses and privacy invasions. Invaders may intrude into the communication channel for the purpose of replaying or modifying data [7, 8]. The biometric properties are immutable, thus storing templates without protection can provoke serious problems when stolen by opponents. Once compromised, a user's sensitive information will be exposed [9]. Since biometric data is inherently linked to an individual, any breach of a biometric template can result in permanent identity theft [10, 11].

Ratha et al. [12] identified eight potential security holes that are vulnerable to attacks in biometric systems. Among the different issues, providing a stolen template of a genuine user is the current threat to deal with. Similar templates may be stored and shared across different applications, and cross-matching between templates may be performed to trace and track users. If one template is stolen from one database, the identical templates in other databases are rendered unusable. Thus, databases must be protected against information theft to prevent illegitimate access [13, 14].

Palmprints have recently received much attention due to their specific superiorities. Palmprints have the advantages of large areas with rich information, simplicity of image acquisition, and a high level of user acceptability. They contain two types of features: the palmar friction ridges and the palmar flexion creases. To make the palmprint recognition system more user-friendly and sanitary, images should be captured in a contactless manner. Using contact-based sensors, the hand is strictly constrained during image capturing. Persons with arthritis or other health problems may not be able to place their hands on the sensor surface. On the other hand, touchless acquisition uses less constrained mechanisms that do not require direct contact with the sensing device [5, 6, 15, 16].

Cancelable palmprint template protection schemes are indispensable for achieving security and privacy in large-scale system deployment. These schemes require careful attention since there are several concerns to worry about. The design criteria are required to achieve diversity and revocability, which are collectively termed changeability. If a stored template is compromised, it is necessary to revoke the previous template and reissue a new one. Moreover, independent templates need to be created for each user in the different applications, and cross-matching between these templates must not be allowed. Unlinkable templates are generated such that it is computationally infeasible to associate a newly created template instance to any previously stored instances. It is difficult to provide fully unlikable templates due to the intrinsic correlation of biometric templates. The protected samples must also be computationally difficult to reveal by external attacks. Irreversibility is an essential property required to provide the privacy to which persons are entitled. Achieving this property ensures that original biometrics or features cannot be restored from the secured templates.

Touchless palmprints show more local variations in scale, rotation, translation, and illumination, compared with contact-based imagery. These variations increase the intra-class differences and potentially reduce the system's accuracy. Moreover, recognition accuracy often degrades with protected templates, due to insufficient intra-class variations handling capability. It is not feasible to just simply add an encryption scheme and expect to obtain the same results that are obtained without protection. It is essential to achieve efficient discriminability of cancelable features such that the accuracy of secured templates is comparable to its original counterpart. The extracted features should show robustness to even small misalignment between two samples in the encrypted domain. Securing palmprint templates meanwhile achieving superior recognition accuracy is one of the big challenges, which is still not satisfactorily solved.

For multimodal biometric systems, the issue of normalizing features and/or matching scores has been frequently investigated. For the unimodal biometric case, normalization at the feature level has not received enough attention. This motivated us to investigate the effect of feature distribution mapping on system recognition accuracy. In addition, palmprint is one of the large-area biometric modalities, which requires a large storage capacity. One of the important issues is to find a compact representation that achieves fast matching and light storage, meanwhile maintaining high system performance.

In light of the above challenges and concerns, the key contributions of the paper are as follows:

1) A new Gabor-based palmprint feature representation technique is introduced. Each downsampled Gabor vector is subjected to Gaussianization by remapping its histogram to a normal distribution with predefined parameters. The normal histogram-remapping step perfectly reflects the discriminative nature

of Gabor features and leads to better performance compared to other non-uniform remapping functions. Reliable stable representation, regardless of the variable test sample characteristics, is achieved, and thus, enhanced identification/verification accuracy is obtained.

2) Comb filtering was introduced as a cancelable technique by Soliman et al. [17] for iris recognition. Efforts were directed to the development of revocable and non-invertible templates. However, unlinkability analysis was not provided. In our work, it is shown that cancelable templates based on comb filtering alone do not satisfy template diversity. Locality-sensitive hashing (LSH) with random projection is proposed for transforming the comb-filtered normalized Gabor features such that similar items are mapped to the same bucket based on collision probability. A ranking-based method is applied to obtain the maximum-ranked index feature vectors. Changing the random projection matrix and/or the filter order leads to cancelable templates that are independent across the different applications. This provides high security against linkability attacks.
3) The random projection step not only exploits the discriminative nature of the comb-filtered Gabor features but also provides a compact representation to handle the high dimensional input and reduce the recognition time. The matching stage is performed in the encrypted domain without decrypting the data. The dual benefit of enhanced security and improved accuracy is a key contribution to our work.

This paper is structured as follows: Section 2 reviews the related work. The proposed system is explained in detail in Section 3. Results and discussions are given in Section 4. Section 5 concludes the paper and suggests some future directions.

2 Related work

PalmHash Code and PalmPhasor Code were proposed in [18] as two cancelable palmprint coding methods. For PalmHash, palmprint images were filtered using a circular Gabor filter to extract their discriminative features. Pseudo-random number (PRN) vectors were generated using tokens and multiplied by the biometric feature vectors. For PalmPhasor, the Gabor features and the PRNs were mixed to form complex number vectors. A normalized hamming distance was used to measure the similarity between cancelable templates. Perpendicular orientation transposition was adopted to solve the problem of performance deterioration along the perpendicular orientation, which is caused by the correlation between adjacent rows. The real and imaginary parts of Gabor features along that direction were transposed, to scatter the correlation and provide robustness against statistical attacks. To further enhance the verification performance, multi-orientation score level fusion was employed. The codes were shifted horizontally and vertically and matched repeatedly. To reduce the computational complexity and relieve the vertical and horizontal dislocation problems, Leng et al. [19] introduced a simplified 2D PalmHash code. The image was filtered using a circular Gabor filter, and a random matrix following the standard normal distribution was generated with a token. The 2D hash projection was performed, and the obtained code was only vertically shifted and matched with another hashing code. The shifting step was employed to remedy the dislocation problem due to the imperfect preprocessing. Discarding the horizontal shift led to reducing the matching complexity, reducing the matching processing time, and enhancing the changeability performance. However, the minimum equal error rate (EER) % values obtained using the PolyU database were 0.246% and 0.948% for the best and worst scenarios, respectively.

Liu et al. [20] proposed a hybrid technique that combined random projection with fuzzy vaults using heterogeneous space. The fuzzy vault was used for enhancing security and binding independent random cryptographic keys to meet security requirements. Long keys were segmented into multiple shorter sequences, which were encoded into small sequences using an error-correcting code (ECC) algorithm. A chaff point generation technique was also proposed for security enhancement. Chaff vectors were added between genuine and imposter-matching distances to prevent the adversary from knowing genuine vectors, even having imposter palmprint features. All points in the heterogeneous space were sorted depending on the first value elements in the real-valued vectors. The system performance was evaluated using the Handmetric Authentication Beijing Jiao Tong University (HA-BJTU) database. Results indicated the trade-off between accuracy and security. Correcting more symbol errors could decrease the false rejection rate (FRR), but it could also decrease security, and vice versa.

In [14], a palmprint protection scheme based on random projection and log-Gabor features was proposed to generate cancelable vectors. Log-Gabor magnitude and phase were extracted and salted in a non-invertible manner to obtain transformed binary strings. At the signal level, the image was projected on a Gaussian random matrix, and log-Gabor filtering was applied to the projected image. The extracted features were salted by applying an XOR function with a random grid, followed by median filtering. The obtained binary vectors were concatenated and classified using Kernel discriminant

analysis (KDA). In case of template theft, new templates could be generated by changing the random projection matrix and/or random grid. The EER % values obtained with the PolyU database, for the stolen token (worst case) and the legitimate (best case), were 0.59% and zero %, respectively.

Qiu et al. [5] introduced a template protection method based on random measurement and noise data. A multi-directional anisotropic filter was employed to extract the orientation information of the palmprint. A pseudo-random non-ergodic chaotic matrix was used to generate secured cancelable palmprint templates. To enhance the palmprint privacy further, independent, and identically distributed noise was added to the extracted features. The matching scores of multiple directions were fused at the score level. Verification experiments were conducted on the Tongji University Palmprint (TJU-P) contactless database and PolyU database. Results showed that with 5% and 10% noise levels, genuine, and imposter-matching scores could be distinguished well. When the noise level was increased to 12%, the recognition performance became worse, with an average EER of 0.2483%, since many palmprint features were submerged in the noise data. Thus, increasing the noise level could contribute to security and privacy enhancement, but at the expense of authentication performance. Wang and Li [8] proposed a palmprint cancelable technique using the Orthogonal Index of Maximum (OIOM) hash and Minimum Signature Hash (MSH). The region of interest (ROI) was filtered using an anisotropic filter bank. The feature vector was multiplied with an orthogonal random matrix, and the maximum index was obtained. Then, an XOR operation was performed between a user-specific binary code and the OIOM hash code. The final pseudonymous identifier was obtained using MSH of binary strings. The Jaccard distance was employed in the matching stage. The rank-1 identification accuracy obtained was 99.95% using the PolyU database and 98.07% using the TJU-P more challenging database. In the verification mode, the scheme achieved an EER of 0.32%.

In [11], a palmprint template protection scheme based on randomized cuckoo hashing and MinHash was proposed. Orthogonal features were extracted using anisotropic filtering and were divided into non-overlapping blocks. A randomized cuckoo hashing was applied to the features as the first security layer. To improve template irreversibility, different Gray coding techniques were employed for randomized cuckoo hashing with the same positions. A large number of zeros were noticed after the cuckoo hashing step. The MinHash algorithm was adopted as another layer for privacy enhancement, meanwhile improving low space utilization and increasing system efficiency. The size of the obtained hashing codes increased with a larger block size; thus, better irreversibility could be achieved. However, the resulting average EER increased. Using the PolyU database, with 10×10 and 2×2 block sizes, the system achieved 0.27% and 0% EER, respectively. Shao et al. [16] combined hash coding and knowledge distillation to explore efficient deep palmprint recognition. Palmprints were converted to binary codes to save storage space and speed up matching. A simple XOR operation was used to obtain the distance between codes. A Deep Hashing Network (DHN) based on VGG16 was used, and the soft-max layer was transformed into a coding layer. The adopted database consisted of 30,000 images collected by five different mobile phones. The average EER obtained was 0.607%, and the average recognition accuracy was 97.49%.

Wu et al. [21] suggested fuzzy commitment based on deep hashing codes (DHC-FC) and bit selection discrimination to achieve security in palmprint-based recognition systems. The lowest EER obtained for the Tongji database was 0.3795% with 124 bits. Yang et al. [22] introduced a dual-level cancelable authentication framework, designed to provide protection for palmprint templates in cloud-based systems. The raw template was first encrypted with a first-level token using a competitive hashing network. The protected template was further encrypted using a second-level token for a second-level negative database protection. The framework was specifically designed for one-to-one verification scenarios and was not optimized for identification tasks. The EERs obtained were 0.36232% on IITD, 0.00794% on PolyU, and 0.00007% on NIR datasets. In the cancelable palmprint authentication system introduced by Ashiba et al. [23], the discrete wavelet decomposition was applied to extract palmprint features from different subbands, and the resultant map was encrypted using the homomorphic filtering masking (HFM) technique. Two different random keys were used for feature transformation to ensure diversity and revocability. Without knowing both keys, it was difficult to reverse the encrypted template back to the original one. The minimum EERs obtained were 0.4% and 0.33% for CASIA and IITD databases, respectively.

In [24], an attention module was integrated with ResNet-50 architecture to enhance its feature extraction capability, and chaotic sequences were incorporated to provide dynamically controlled neuron activation, meanwhile achieving diversity for palmprint templates. For security enhancement, random keys were combined with template feature values via matrix multiplication, and a binarization layer was added to reduce computational complexity. The recognition accuracy obtained was 99.17% and 99.36%, with an EER of 0.29% and 0.24%, for Tongji and PolyU datasets, respectively. In [25], convolutional neural networks (CNN), feature transformation,

and the Secure Hash Algorithm (SHA-3) were combined and employed for mapping palmprints to random codes and generating secure templates. The recognition accuracies achieved were 99.05%, 98.99%, and 97.11% for PolyU, CASIA, and IITD databases, respectively. The corresponding EER values were 0.62%, 0.70%, and 1.01%.

3 Proposed system

3.1 Overview of the proposed technique

Figure 1 shows an overview of the proposed cancelable palmprint recognition system. Gabor filters are employed in the introduced framework to extract features from palmprint images as they provide optimal spatial and frequency localization properties. Following this step, downsampling is applied to reduce feature redundancy and computational load for efficient further analysis. The downsampled patterns are ultimately remapped to a target distribution with selected parameters.

This feature warping is suggested to compensate for the misalignment caused by the image variations and ensure that the extracted features accurately represent the underlying palmprint characteristics. Templates obtained after feature normalization are deformed intentionally using a multi-band infinite impulse response (IIR) comb notch filter. Changing the filter's order leads to variations in the delay experienced by past signal samples, consequently varying the pattern of frequencies that are amplified or suppressed. The proposed concealment method inspired by LSH and quantization revolutionizes template protection by converting the real-valued comb-filtered feature vectors into discrete index hashed codes. It involves a process where finite subsets are embedded in Euclidean space by mapping similar items to the same

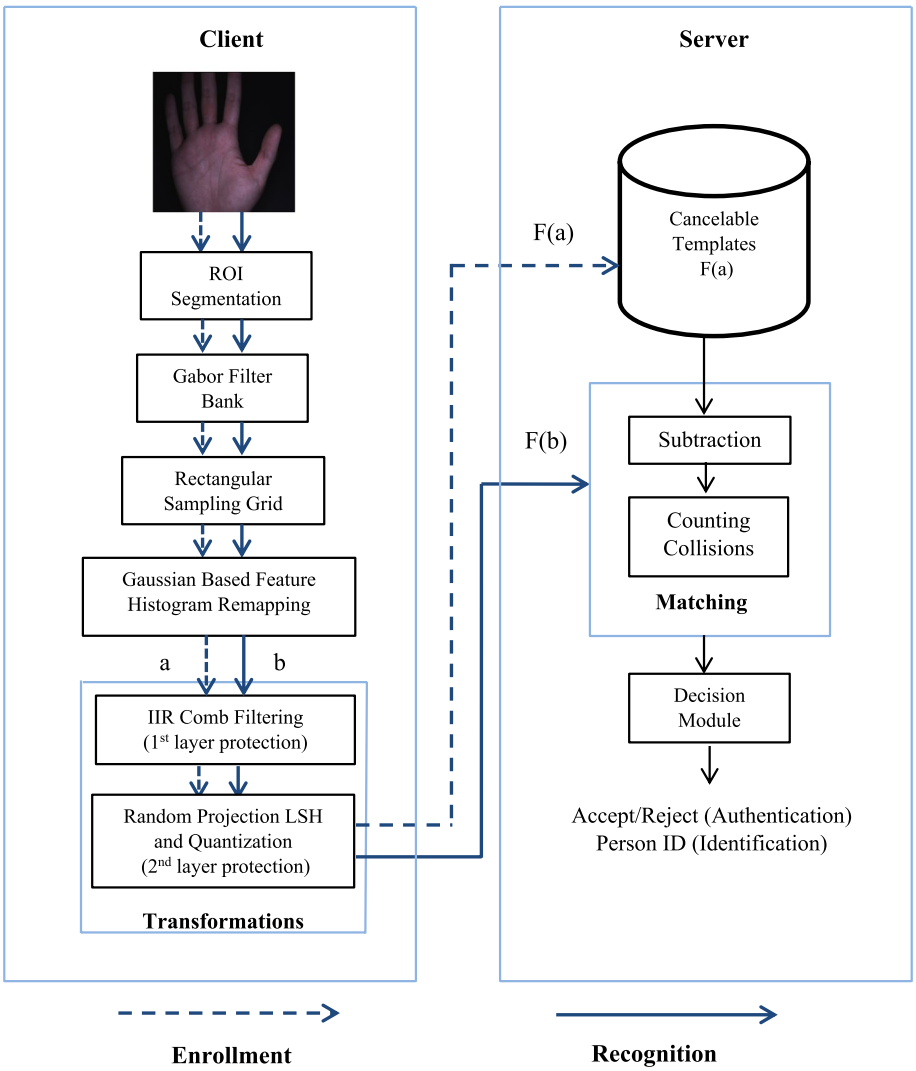

Fig. 1 Proposed system flowchart

bucket to reduce dimensions while preserving local distance information. The matching score is calculated by subtracting enrolled and query elements and counting the number of collisions (represented by zeros). By utilizing externally generated user-specific random multiple Gaussian projections, the suggested method effectively conceals palmprint features while maintaining accuracy performance, revocability, non-linkability, and irreversibility. The details of each stage are given in the following subsections.

3.2 Gabor filtering and distribution remapping

Gabor filters, also called Gabor wavelets or kernels, are complex bandpass filters optimally localized in both spatial and frequency domains. The 2D Gabor filter is defined as follows [26, 27]:

$$\varphi(x,y) = \frac{f^2}{\pi\gamma\eta}\exp\left(-\left(-\frac{f^2}{\gamma^2}x_r^2 + \frac{f^2}{\eta^2}y_r^2\right)\right)\exp(j2\pi f x_r), \quad x_r = x\cos\theta + y\sin\theta, y_r = -x\sin\theta + y cos\theta \tag{1}$$

where f is the frequency of the complex plane wave and θ is the orientation of the elliptical Gaussian major axis. The ratio between the center frequency and the Gaussian envelope size is determined by the parameters γ and η. In our work, the value of both parameters is set to $\sqrt{2}$. The fixed values of these parameters ensure that filters at different scales represent scaled versions of each other. A family of $U \times V$ Gabor filters are defined as follows:

$$f_u = \frac{f_{\max}}{2^{\frac{u}{2}}}, \theta_v = \frac{v}{8}\pi \quad u = 0,1,\ldots.U-1, v = 0,1,\ldots.V-1 \tag{2}$$

A filter bank with five scales ($U=5$) and eight orientations ($V=8$) is constructed to determine the local frequency and orientation. The ROI segmentation algorithm [6] is applied. A Gaussian filter is applied to smooth the input image and convert it to a binary image. The boundaries of two finger gaps are identified and extracted. The tangent line of the gap boundaries is defined and the tangent points X_1 and X_2 are determined. X_1X_2 is set as the X-axis, its midpoint as the origin, and the line perpendicular to it as the Y-axis. A line parallel to the X-axis at a distance $c_1\|X_1X_2\|$ from the origin and intersecting the palm contour at O_1 and O_2 is determined. A square region S symmetric with respect to the Y-axis is extracted, its side length is $c_2\|O_1O_2\|$, and its distance from the X-axis is $c_3\|O_1O_2\|$. The ROI is obtained by normalizing S to the size $N \times N$. The ROI palmprint image is filtered using all 40 filters, and the magnitude responses are returned, resulting in an inflation of the initial size dimension by 40 times. With an image size of 128×128, Gabor filtering results in 655,360 ($128 \times 128 \times 40$) feature space, which is too extensive for processing and storage requirements. To reduce the dimensions of the resulting features, and to make further processing more efficient, downsampling is exploited. A rectangular sampling grid with 16 horizontal and 16 vertical lines is used. This corresponds to a downsampling factor ρ of 64. The size of the feature space after downsampling is 10,240 ($128 \times 128 \times 40/16$). Figure 2 shows examples of Gabor magnitude output before and after downsampling for two different palms.

The histograms of the downsampled patterns are ultimately remapped to a target distribution with selected parameters. The purpose of feature warping is to build a more discriminative representation for the distribution of features. This is achieved by conditioning the extracted palmprint features such that they follow a specific distribution. Histogram remapping starts with transforming the input feature values via the rank transform. For N dimensional feature matrix, each value in the matrix is replaced with the rank R and the value would correspond to if these values were ordered in an ascending manner. After the ranking step, the mapping function $f(x)$ is calculated as follows [28]:

$$\frac{N-R+0.5}{N} = \int_{x=-\infty}^{t} f(x)dx \tag{3}$$

Clearly, the right-hand side is the cumulative distribution function (CDF) of the target histogram, and the aim is to find t. If the CDF is denoted as $F(x)$, and the scalar value on the right as u, then t can be obtained as $t = F^{-1}(u)$. The inverse of the CDF is evaluated as the probability values of u. The result is features processed with anisotropic smoothing.

The normal, lognormal, and exponential distributions are given by Eqs. 4, 5, and 6, respectively:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}}\exp\left(\frac{-(x-\mu)^2}{2\sigma^2}\right) \tag{4}$$

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}}\frac{\exp\left(\frac{-(lnx-\mu)^2}{2\sigma^2}\right)}{x} \tag{5}$$

$$f(x) = \lambda\exp(-\lambda x) \tag{6}$$

where μ is the mean value of the normal distribution and σ is the standard deviation. These two parameters are also used to define the shape of the lognormal histogram. The exponential equation is defined with the rate parameter λ. In our work, μ and σ are set to 0 and 1, respectively, while λ is set to 0.2. The mapping operation can be considered as recognizing the relative positions of Gabor features as more important rather than their absolute

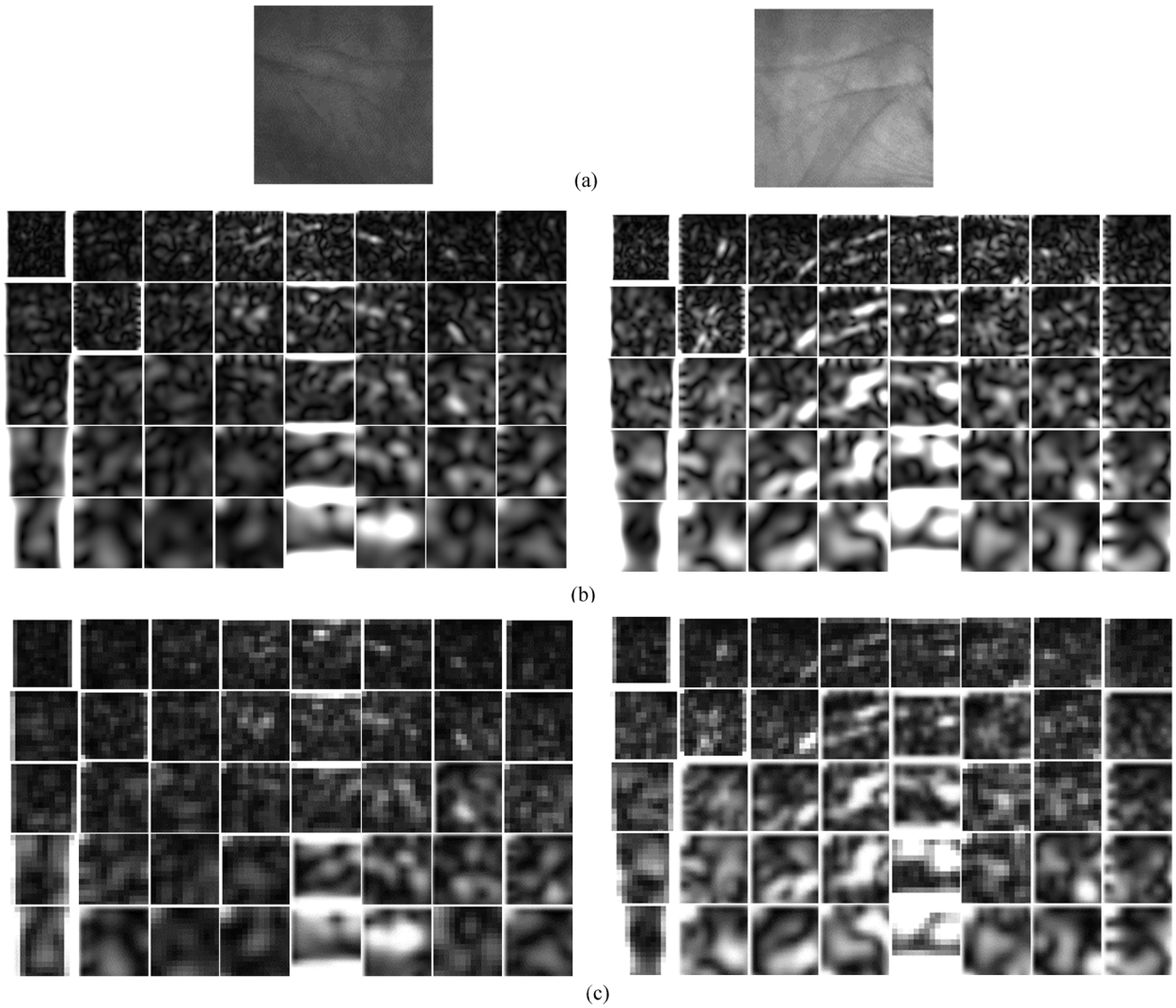

Fig. 2 Examples of Gabor output: **a** Sample images from two different palms; palm no. 41 (left), palm no. 131 (right). **b** The corresponding magnitude output with 40 Gabor filters. **c** The corresponding downsampled magnitude response

values. The mapping methods attempt to conform to the distributive shape and spread of features to yield a better compensation for the mismatch caused by the severe palmprint image variations. The effect of histogram remapping is compared with the well-known zero-mean unit-variance normalization technique, which is used to adjust the dynamic range to a common scale.

3.3 Comb filtering

A comb filter is implemented by deliberately using past input and/or past output samples from a specific moment in the past. This operation causes an instructive and destructive interface and provokes the radical filtering effect. Varying the amount of delay makes the filter sweep through its frequency band, picking up different harmonics as it moves. Each frequency is affected differently, and the filter magnitude response looks like a tooth of a comb. This type of filtering can be considered a combination of notch filters with null frequencies, which occur periodically over the bandwidth [29].

In this work, palmprint templates obtained after Gabor feature remapping are deformed intentionally using a multi-band IIR comb notch filter having the following transfer function:

$$H(z) = b\frac{1 - z^{-m}}{1 - \alpha z^{-m}} \tag{7}$$

where α and b are positive scalars and m is the filter order (number of notches minus 1). Filters of different orders (6, 8, 10, 12) are created, with a bandwidth of 0.02

(normalized frequency) referenced to the −3 dB point. IIR filters generally require less coefficients and memory requirements than finite impulse response (FIR) filters, to meet a similar set of specifications. The phase characteristics of an IIR filter are generally nonlinear.

Certain frequencies at band nulls are removed from the feature map. This leads to pattern content distortion, which is not repetitive from one person to another. Changing the filter order leads to different time delays for the past samples and hence different sets of emphasized and attenuated frequencies. The deformed templates after filtering are used as inputs to the last stage in the proposed system, explained in the following subsection.

3.4 Random projection with locality-sensitive hashing

Despite the downsampling operation, the resulting feature vector is still within a highly dimensional space. The output of the comb filtering stage with a length of 10,240 is projected into random directions that are independent of its input. Random projection is introduced as a LSH and is further condensed by quantization (discretization), for data hiding and security purposes. The proposed algorithm converts the comb-filtered histogram-remapped Gabor features into hashed codes with discrete indices according to maximum ranking. For the projected feature vectors, taking their maximum indices can be regarded as quantizing the output. After hashing, using this quantization step, the nearby points are highly expected to lie in the same bucket. Many elements will be mapped to the same index; thus, it is even harder for the adversary to reconstruct the original data. The aim is strong feature concealment and thus contributing to much solid ground of irreversibility guarantee, meanwhile satisfying the revocability and diversity requirements for the proposed palmprint recognition system. Another target is to have better feature alignment such that the recognition accuracy with encrypted features is approximately the same as with their original counterpart. This is achieved through the magnitude-independence of the hashed codes, thus providing robustness to noise, scale, and different feature variations, as these variations do not affect the implicit ordering.

The dimension and distribution of the random matrices are controlled such that the similarity between comb-filtered features in the lower space is preserved. A common type of random matrices is generated from a Gaussian distribution and exhibits desirable statistical properties [30]. The norm of each column of the matrix is one, and the dot product of all columns taken pairwise is zero, indicating their orthogonality to each other. For each comb-filtered feature vector with dimension 10,240, a number of n random Gaussian projection matrices with q columns are generated, and the resulting n maximum indices, obtained after projection, are taken to represent a hashed output from the LSH point of view. Thus, the dimension of the vector is reduced from 10,240 to n. Different values of n ranging from 300 to 1000 are tested, and the results are recorded. If a template is stolen, the hashed output can be reissued using a new set of n random matrices. For the legitimate real-world scenario, the random projection matrix is user-specific. However, the same-token worst scenario should be taken into consideration, as it is closely related to security attacks. To simulate this scenario, the experiments are performed with the same set of random matrices for all users.

Calculating the matching score is the last phase of the proposed technique. K-nearest neighbor (KNN) classifier is employed with $K=1$, using Euclidean distance, to test the performance after the histogram remapping and the comb filtering stages. The matching procedure permits the most similar enrolled template to be selected. On the other hand, the similarity score between templates after applying the random projection-based LSH is calculated based on subtracting enrolled and query templates and then finding the number of zeros (collisions). This simple and fast operation perfectly reflects the collision probability of two hashed codes.

4 Experiments, results, and discussions

This section commences by presenting the database used in our work, continues by analyzing and assessing the system performance, and finally presents a detained security analysis. Assessment metrics used to evaluate the feasibility of the proposed technique are introduced. A series of experiments and analyses are provided to evaluate the recognition performance and security levels.

4.1 Database

Tongji database available online [6] is the largest in scale and serves as a better benchmark for developing efficient palmprint recognition systems. The database contains a total of 12,000 images from 600 different palms. The left and right palms of the same subject were considered as belonging to different people. Palmprints were collected from 300 persons: 192 males and 108 females, with ages ranging from 20 to 50 years. Images were captured using the proprietary touchless acquisition device described in [6]. Images were collected in two different sessions. In each session, 10 images from each palm were provided. The average time between the two sessions was about 61 days. The image dimension is 600×800. Images obtained in the first session are used as the gallery set, and images from the second session are used as the probe set. Extracting the region of interest is an influential step.

Palmprint images were aligned by constructing a local coordinate system and using it to crop the ROI image. The size of the ROI images is 128×128.

4.2 Performance analysis

The proposed technique is applied in both identification and verification modes. In the identification mode, each sample is compared against all remaining samples, and the identification accuracy is calculated. Two-fold cross-validation, with one partition for training and one partition for testing, is used. The results are averaged over five iterations. In the verification mode, the test sample is matched against a reference template, and the matching score is compared with a threshold to decide the authenticity of the person. Table 1 gives the identification and verification assessment metrics of normalized downsampled Gabor features using different remapping techniques. Histogram remapping after Gabor filtering shows the advantageous capability of extracting significant discriminative features. Remapping to normal distribution gives the most consistent average identification accuracy of 99.946%. For the verification scenario, an EER of 0.15% is achieved. Low EER indicates high verification performance. Since the system requires low risk and high accuracy, it is meaningful to calculate the true positive rate (TPR) at low values of false positive rate (FPR). TPR values of 99.81% and 99.92% are obtained at FPR values of 0.1% and 1%, respectively. With zero-mean unit-variance normalization, the accuracy and EER are 99.552% and 0.54%, respectively.

Compared with this normalization technique, the effectiveness of histogram remapping is proven to have clear evidence of its responsibility for the change in recognition performance. Gaussianization remapping leads to better feature distribution, with increased discriminative ability. It alleviates the extrinsic variability caused by realistic acquisition conditions and hence boosts the performance of conventional methods. The high performance can also be linked to the desirable properties of spatial localization and orientation selectivity of the extracted features. The method derives a compact palmprint representation insensitive to different image degradation. The downsampling operation reduces dimensionality without losing valuable discriminatory information. Table 2 shows the effect of applying comb filtering after featuring normal mapping in both identification and verification modes. It is clear that this filtering stage enhances the recognition performance compared with using templates without protection. The highest average identification accuracy obtained is 99.97% compared with 99.946% without comb filtering. Enhancement in the verification assessment metrics is also noticed. The EER% has decreased from 0.15 to 0.1354 using comb filtering with order 12. The different orders of comb filtering lead to approximately similar performance. Feature transformation using histogram remapping followed by comb filtering noticeably strengthens the useful information and reduces the harmful disturbances often contained in features.

The results of the proposed ranking-based hashing algorithm applied after comb filtering are given in

Table 1 Verification assessment metrics and average identification accuracy % of normalized downsampled Gabor features and KNN classifier using different normalization techniques

Normalization Technique	EER %	Verification rate %	TPR % (FPR = 0.1%)	TPR % (FPR = 1%)	Average identification accuracy %
Zero mean unit variance	0.54	99.46	98.33	99.61	99.552
Exponential mapping	0.26	99.74	99.48	99.89	99.906
Log normal mapping	0.17	99.83	99.75	99.90	99.916
Normal mapping	0.15	99.85	99.81	99.92	99.946

Table 2 Verification assessment metrics and average identification accuracy % of comb-filtered normalized downsampled Gabor features at different filter orders

Comb filter order	EER %	Verification rate %	TPR % (FPR = 0.1%)	TPR % (FPR = 1%)	Average identification accuracy %
$m = 6$	0.1428	99.8572	99.8214	99.9167	99.944
$m = 8$	0.1433	99.8567	99.8095	99.9048	99.962
$m = 10$	0.1399	99.8601	99.8095	99.9167	99.970
$m = 12$	0.1354	99.8646	99.8096	99.9167	99.958

Table 3 Average identification accuracy % of the proposed cancelable technique using different numbers of random projection matrices for both legitimate and worst scenarios

Comb filter order	Number of random projection matrices					
	n=300		n=500		n=1000	
	Legitimate scenario	Worst scenario	Legitimate scenario	Worst scenario	Legitimate scenario	Worst scenario
m=6	100	98.63	100	99.348	100	99.714
m=8	100	98.626	100	99.454	100	99.752
m=10	100	98.540	100	99.282	100	99.720
m=12	100	98.356	100	99.458	100	99.750

Table 4 Verification assessment metrics of the proposed cancelable technique using different numbers of random projection matrices for the worst scenario

Comb filter order	Number of random projection matrices								
	n=300			n=500			n=1000		
	EER%	TPR% (FPR = 0.1%)	TPR% (FPR = 1%)	EER%	TPR% (FPR = 0.1%)	TPR% (FPR = 1%)	EER%	TPR% (FPR = 0.1%)	TPR% (FPR = 1%)
m= 6	0.89	97.41	99.18	0.58	98.69	99.64	0.37	99.32	99.83
m= 8	0.77	98.02	99.55	0.57	98.52	99.64	0.31	99.48	99.90
m= 10	0.93	97.92	99.15	0.50	98.92	99.72	0.36	99.35	99.84
m= 12	0.88	97.85	99.21	0.54	98.94	99.65	0.34	99.39	99.79

Tables 3 and 4, for the identification and verification modes, respectively. The ROC curves for the worst-case scenario are shown in Fig. 3. Small number of random projection vectors ($q = 50$) is used to ensure minimum computation cost and thus meet the expectations for real-time implementation. In the real-world (legitimate) scenario, random projection matrices are user-specific. However, the worst case of using the same set of random matrices is analyzed to simulate the stolen-token scenario. The effect of the number of Gaussian random matrices is carefully investigated. For the legitimate scenario, the system exhibits desirable properties and achieves superior performance with 100% identification accuracy and zero EER, even with small values of n. The form of real-valued vectors can be changed, meanwhile perfectly preserving the discriminability of features. With $n = 300$, the size of the feature vector is reduced from 10,240 to 300; thus, storage requirements are effectively minimized. To save space, the verification results of the legitimate case are not presented in Table 4, since optimum values are obtained with all filter orders (EER = 0%, TPR = 100% @FPR = 0.1%, TPR = 100% @FPR = 1%). For the worst scenario, it is clear that increasing n leads to performance enhancement. This confirms the principles of LSH. With $n = 1000$, the highest identification accuracy is 99.752%, and the minimum value of EER is 0.31%. The introduced algorithm ensures that two similar palmprint templates render a high probability of collision, while templates far apart from each other yield a low probability of collision. To assess the time efficiency, the average template generation and recognition times are recorded for different values of n. Results are shown in Table 5. Matlab prototyping environment is employed, and a computer with the following specifications is used: Intel(R) Core (TM) i7-4900MQ CPU (2.80 GHz) and 24 GB RAM. It is clear that the proposed hashing algorithm reduces the recognition time due to the simple matcher used and thus meets the expectations for real-time implementation.

4.3 Security analysis

In this section, unlinkability, revocability, and irreversibility are rigorously analyzed. Unlinkability is a property of one or more biometric references that cannot be linked to each other or to the person from which they were obtained [7]. If each person has multiple templates stored across different applications, attackers may benefit from the correlation between these templates to allow successful break-ins. Specifically, unlinkability is guaranteed when attackers cannot retrieve any information by matching hashed codes obtained from the same palm by

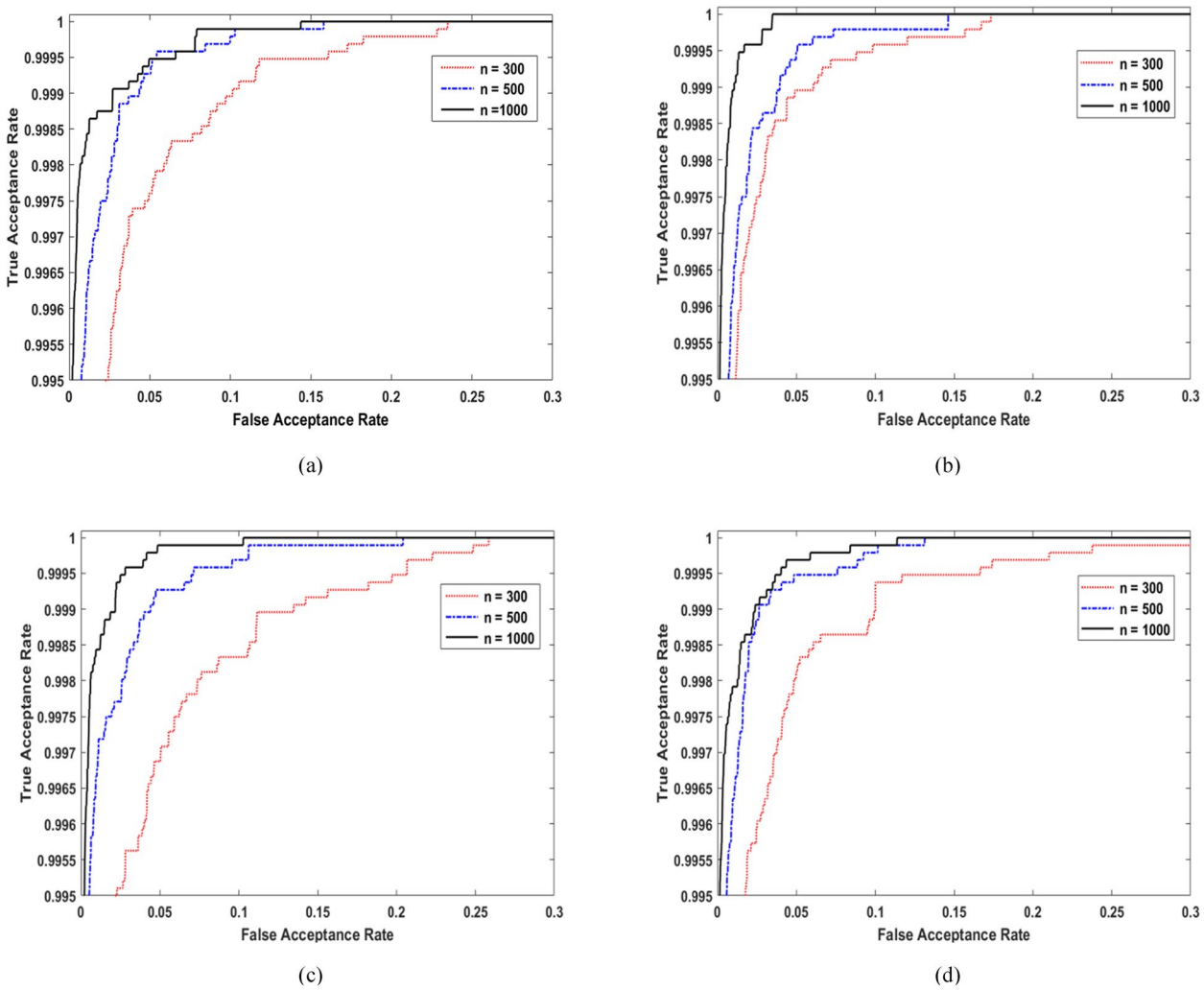

Fig. 3 ROC curves of the proposed cancelable technique using different number of random projection matrices for the worst scenario. **a** $m=6$, **b** $m=8$, **c** $m=10$, and **d** $m=12$

Table 5 The average processing time in seconds for enrollment and recognition stages

	Remapped Gabor features	Comb-filtered features	Hashed features		
			$n=300$	$n=500$	$n=1000$
Enrollment	1.277	2.120	4.831	6.014	8.986
Identification	1.192	3.131	0.122	0.136	0.249
Verification	0.890	1.682	0.066	0.080	0.090

using different projection matrices. The technique is considered linkable to a certain degree if the likelihood that the two templates conceal the same instance is higher than the likelihood that they conceal different instances.

To assess unlinkability requirement, two score distributions are obtained: pseudo-genuine and pseudo-imposter. The pseudo-genuine (mated) score represents the similarity between two hashed vectors generated from the same palm using two different random matrices and stored in different applications. On the other hand, the pseudo-imposter (non-mated) score is calculated between the transformed vectors of different palms with different keys and stored in different databases. These distributions are used to indicate how vulnerable

the stored templates are to profiling (i.e., linking) activities. The two metrics introduced by Gomez-Barrero et al. [7] are used to evaluate the confidence in verifying patterns by measuring the separability of the match and non-match populations. The $D_{\leftrightarrow}(s)$ is a local score-wise metric that is based on the likelihood ratio between the score distributions. The $D_{\leftrightarrow}^{sys}$ is a global measure that is independent of the score domain, thus allows a faithful assessment of system likability. Its value lies in the range [0, 1]. Lower values indicate a decreasing level of linkability. For completely separable mated and non-mated distributions, $D_{\leftrightarrow}^{sys} = 1$ (fully linkable).

To assess the linkability of the proposed multi-transformation algorithm, six different databases are created. The multiple protected templates for the same palm are generated using different random projection matrices to simulate its use across various applications. For the mated distribution, all similarity scores between templates generated from the same palm in the various applications are calculated. For the non-mated distribution, the distance scores are calculated by matching the test templates of the original database with the first sample of the remaining different palms in the different databases. Figure 4(a) shows that the pseudo-genuine and pseudo-imposter distributions are overlapped, with $D_{\leftrightarrow}^{sys} = 0.01$. The scores are sufficiently undistinguishable, and the protected templates are unlinkable. Thus, it is infeasible to recognize any hashed code pairs from the same person. If the scores are far apart, it will be easy for an attacker to distinguish whether the template is for the same person or not. The algorithm highly increases the difficulty level involved in using the correlation between samples to perform a successful system break-in. To assess template linkability based on using only comb filtering without the random projection-based LSH, six different databases are created using different filter orders. Mated and non-mated distributions are plotted in Fig. 4(b). It is obvious that pseudo-genuine and pseudo-imposter density functions are separable, with $D_{\leftrightarrow}^{sys} = 0.98$. This implies that the hashed vectors obtained from the same palm or different palms are sufficiently distinctive, and an attacker can discriminate between hashed codes easily.

Revocability permits the generation of new templates (using new random keys) when the template in question is stolen. Moreover, the new template must not match the old compromised one. Thus, revocability does not only mean to generate a new template but also to prevent the authentication rights of the old authenticator. For revocability evaluation, the genuine, imposter, and pseudo-imposter distributions are considered. Genuine scores are the matching scores calculated using the same projection matrix when comparing templates from the same person, while imposter scores are calculated between different palms within the same system. Intra-class and inter-class variances are quantified by the genuine and imposter matching scores, respectively.

The pseudo-imposter score is the matching score between two templates of the same subject using a different key. Thus, revocability is satisfied if genuine and imposter scores are separable; meanwhile, genuine and pseudo-imposter scores are also separable.

Transformed templates are obtained using the same random projection matrix RG_0, and the resulting database contains the original transformed templates. A new transformed database is obtained using a different matrix RG_1. Recognition results are obtained separately on each database, and the performance is found to be similar. This proves that system efficiency is not affected by changing

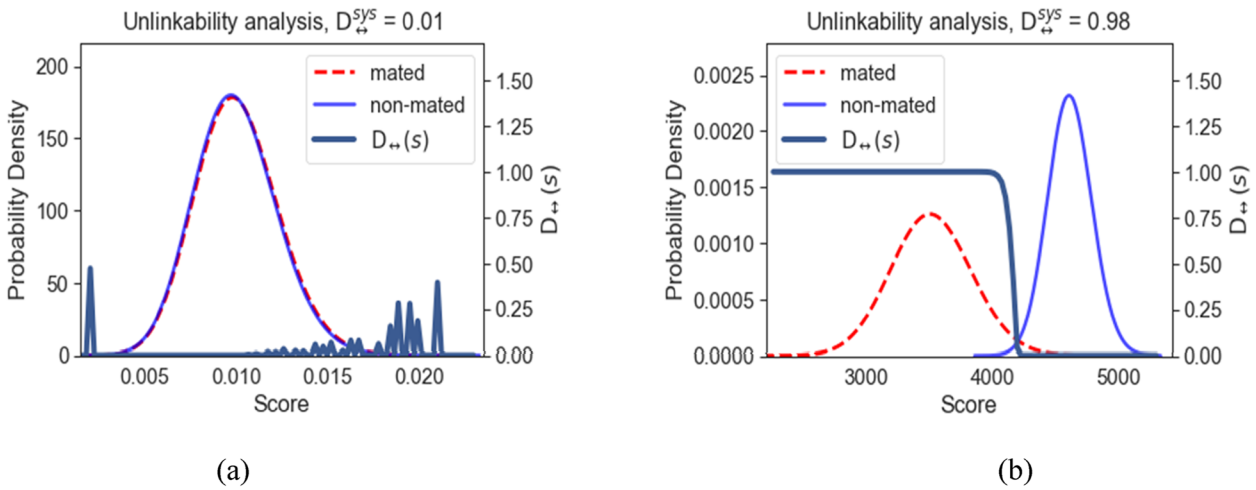

Fig. 4 Unlikability analysis for **a** the proposed approach with $q = 50$, $n = 1000$ and **b** the comb-filtered remapped Gabor features

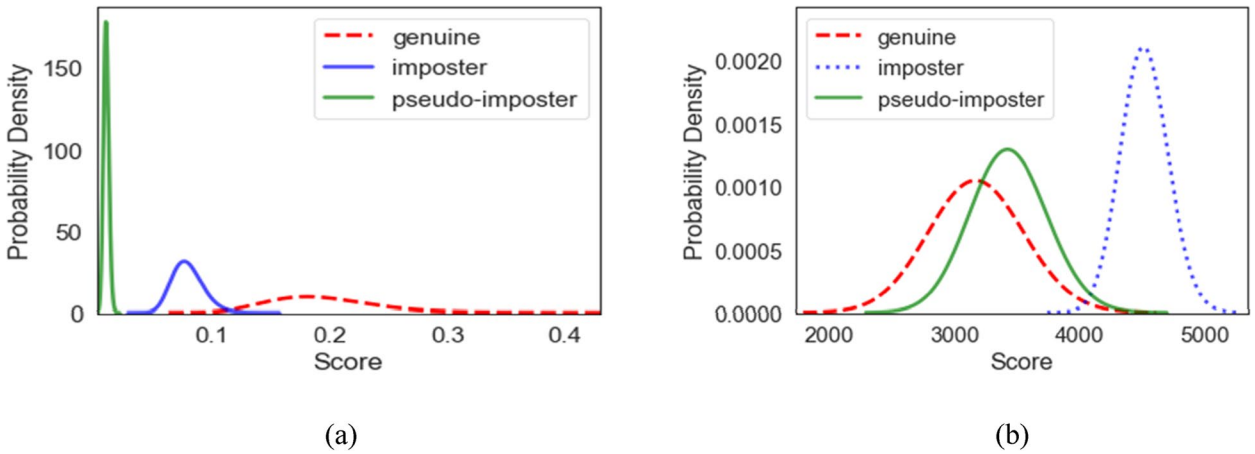

Fig. 5 Revocability analysis for **a** the proposed approach with $q = 50$, $n = 1000$ and **b** the comb-filtered remapped Gabor features

projection keys. Figure 5(a) shows that the pseudo-imposter distribution is far from the distribution of genuine scores. The proposed technique shows a high ability to reissue templates, with perfect separation between genuine and imposter scores, and is free from accuracy discrepancy problems. Moreover, the algorithm does not permit an updated template to fall into the region of acceptance of the old template. In a similar way, 100 new transformed databases are generated using 100 different random matrices. The same experimentation is performed and similar results are observed. As previously stated, downsampling and random projection reduce the system storage requirements. Also, it is obvious that random projection after comb filtering proves its efficiency in information privacy enhancement. On the other hand, as shown in Fig. 5(b), using the comb-filtered remapped Gabor features without random projection leads to a significant overlap between the genuine and pseudo-imposter scores. This means that the new template is in the region of acceptance of the compromised one, and revocability is not achieved.

Irreversibility in cancelable biometrics is an essential property that ensures that the original biometric data cannot be reconstructed from the protected template. This is typically achieved by applying non-invertible transformations that obscure the connection between the original biometric features and the stored cancelable templates. The proposed system employs crucial steps that contribute to its irreversibility. Extracting the normal histogram-remapped Gabor features from palmprint images introduces a level of complexity and nonlinearity that makes it difficult to revert back to the original data. The multi-scale and multi-orientation representation of Gabor features together with the Gaussianization step add to the irreversibility of the method. By downsampling the extracted features, the amount of information available for reconstruction is reduced. This dimensionality reduction step also contributes to the loss of fine details that could facilitate reversing the transformation. The downsampled features are further processed, creating a more complex representation that is less likely to retain identifiable patterns of the original palmprint image. Comb filtering helps in emphasizing certain frequency components while suppressing others, adding another layer of obfuscation.

The final transformation stage is achieved by non-linearly converting the comb-filtered remapped Gabor features to maximum ranked discrete indices, thus effectively protecting features from being inverted. No clue is provided for an adversary to guess the real-valued features from the stolen vectors. Moreover, knowing the projection matrix cannot help in recovering the original vector, since there is no direct link between the random matrix and the palmprint vector. The algorithm can highly hide the palmprint features using both spatial and frequency information to represent cancelable templates. From the above discussion, it is clear that template protection requirements are perfectly satisfied; meanwhile, superior recognition accuracy is achieved.

4.4 Comparison with previous methods

The proposed algorithm is faithfully compared with the recent state-of-the-art palmprint revocable and irrevocable hashing algorithms using the same Tongji palmprint standard large-size database. The identification accuracy and EER percentages are given in Table 6. In the Similarity Metric Hashing Network (SMHNet) introduced in [31], an embedded Structural Similarity Index Metric (SSIM) block was added after the last convolutional layer to capture structural information.

Table 6 Identification accuracies % and EER % of the proposed technique compared with recent methods in the literature using Tongji database

Ref	Method	Type	Accuracy %	EER %
Qiu et al., 2019 [5]	Random measurement with added noise	Cancelable technique	----	0.2483
Wang and Li, 2019 [10]	OIOM and Minimum Signature Hash	Cancelable technique	98.07	0.32
Khan et al., 2024 [24]	Deep secure PalmNet	Cancelable technique	99.17	0.29
Jia et al., 2020[33]	LFH	Supervised hashing based on latent factor models	96.63	---
Liu et al., 2021 [31]	SMHNET	Deep learning network with embedded SSIM and hashing blocks	97.65	---
Arora et al., 2021 [32]	PalmHashNet	Residual deep hashing network with indexing module	97.85	0.53
Shao et al., 2020 [34]	DDH	Deep distillation hashing network	98.92	2.53
Lin et al., 2023 [35]	Double quantification of template and network	Deep hash network	----	0.0075
Wu et al., 2023[21]	DHC-FC	Fuzzy commitment based on deep hashing code	----	0.3795
Proposed	Ranking-based LSH with comb-filtered Gabor features	Cancelable technique	100	0.00

A hashing block was added after the last fully connected layer to encode the floating-point data into binary codes to facilitate large-scale feature storage. The obtained unique fixed-length codes were irreversible for security enhancement. The recognition accuracy obtained was 97.65%. In [32], a deep convolutional network named PalmHashNet was proposed to extract palmprint features using a modified softmax loss function. ResNet-18 was used as the backbone network to learn discriminative features. Extracted features were sent to an indexing module for index-table creation. This operation reduced the number of comparisons due to reduced search space. The results obtained were 97.85% identification accuracy and 0.53% EER in the verification mode. In [33], the problem of using hashing techniques for palmprint recognition was investigated. Four supervised techniques, four unsupervised techniques, and four deep learning-based hashing methods were evaluated. The best recognition performance on the Tongji database was 96.63% using Latent Factor Hashing (LFH). In the work introduced by Shao et al. [34], deep distillation hashing was proposed to improve the matching efficiency using a light network. VGG-16 was used as a deep hashing teacher network, and a light student network was constructed under the guidance of the teacher network. The results obtained were 98.92% and 2.53% for accuracy and EER, respectively. The authors in [35] proposed a method for efficient and lightweight palmprint recognition by quantizing both the templates and network parameters. They achieved this by binarizing the parameters of the deep hash network to compress the network weight and increase speed. They utilized mutual information to optimize the ambiguity in the Hamming space, resulting in a tri-valued hash code as the palmprint template. They achieved an EER of 0.0075. The DHC-FC method [21] demonstrated reduced template size and shift-matching-free ability with the lowest EER achieved at 0.3795%.

The focus of the works [21, 31–35] was on introducing various hashing techniques that reduced storage and enabled fast retrieval of the best match with minimum recognition time. While hashing does not achieve complete security, it is still better than storing original templates. A stolen hash is mathematically difficult to reverse compared to raw data. Security in this context was provided through the generation of binary codes that represented palmprint features in a way that preserved the essential discriminative information while making it difficult for unauthorized users to reconstruct the original palmprint image.

When comparing the code lengths of the different hashing methods, the lowest EER in [21] was achieved with 124 bits selected from the original template. For the Tongji database, the code length was 511 bits due to the inclusion of error correction bits. In [31], the exact feature vector length was not mentioned. The output from the PalmHashNet approach [32] was a 512-dimensional distinct compact feature embedding for each palmprint sample. In [33], all methods attained the highest recognition performance when the code length was set to 256. With the networks introduced in [34, 35], 128-bit binary codes were obtained. No security analysis was provided. The compact representation presented in all these works participated in enhancing the matching performance and storage efficiency.

Irreversibility property might be guaranteed using these methods. However, all of them were irrevocable hashing algorithms, and unlinkability was not fulfilled.

The works introduced in [5, 10, 24] represent cancelable template protection schemes. In [5], a chaotic matrix and a secret key were used to generate the cancelable palmprint templates. The authors provided theoretical analysis and experimental results to verify the unlinkability and irreversibility of the suggested technique. However, they did not include any assessment metrics or graphs as direct evidence for these properties. They did not also explicitly state the length of the cancelable palmprint feature. While noise addition was essential for preserving palmprint privacy, its level required careful control, and the required balance between security and authentication performance could not be attained. Increasing security was at the expense of decreased EER (0.2483%). By creating pseudonymous identifiers that are well enough undistinguishable, the suggested method in [10] demonstrated unlinkability and made it difficult for attackers to distinguish between templates created from the same person and different persons. The pseudo-genuine and pseudo-imposter distributions were overlapped indicating non-correlated stored templates. However, no linkability assessment metrics were provided. Two layers of security were provided using OIOM and the MSH methods to achieve irreversibility. Revocability was proven by showing that the pseudo-imposter distribution was far from the genuine distribution, with enough separation between genuine and imposter scores. The length of the cancelable palmprint template was 600 in integer values. One value needed 8 bits for binary representation, resulting in templates with 4800-bit length. The accuracy and EER values were 98.07% and 0.32%, respectively. The performance is low compared with the proposed algorithm, even when operated in the worst-case scenario. In [24], input feature values were intentionally made irreversible through the steps of transformation, reshaping, and ranking from largest to smallest feature value. The length of the cancelable feature was reduced from 1024 to 256 bits during the application of the scheme. New cancelable templates could be issued by changing the random keys, and revocability was assessed by plotting the distributions of the scores. The pseudo-imposter distribution closely resembled the imposter distribution, with sufficient distinction between the distributions of the pseudo-imposter and genuine scores. The $D_{\leftrightarrow}^{sys}$ value of unlinkability was 0.11 compared to 0.01 in our work. The recognition accuracy obtained was 99.17% with an EER of 0.29%. It is clear that the proposed framework outperforms all state-of-the-art techniques.

Recent works [36, 37] illustrate that Learnable Gabor Filters (LGF) could achieve promising performance. Their focus was to enhance the Gabor-based palmprint feature extraction and recognition. They did not address cancelable or hashing algorithms for security purposes. To provide adaptability across different datasets, these learnable filters were designed to select the optimal parameters, including scale, orientation, and frequency, with no need for manual adjustments, thus boosting the recognition performance. The Comprehensive Competition Network (CCNet) [36] enhanced the discriminative power of palmprint recognition by considering spatial competition relationships and multi-order texture details. The EER % obtained on the Tongji database was 0.00004. In [37], a coordinate-aware contrastive competitive neural network with three parallel branches was proposed to extract multi-scale texture features, resulting in a more comprehensive palmprint texture representation. The inclusion of coordinated attention enabled the network to focus on essential discriminative regions and improve the system performance by dynamically adjusting the weights of the extracted features. An EER % of 0.005 was obtained using the same database. The orientation of palmprint lines and wrinkles is crucial for texture extraction and recognition. Thus, using ordinary image augmentation techniques such as rotation and flipping with these networks may destroy the orientation information of different textures and violate their integrities.

In the proposed technique, histogram remapping of Gabor features increases the authentication accuracy by reducing the effects of feature variability and enhancing their discriminative capability. LSH of comb-filtered Gabor features performs not only its security role but also focuses the search on relevant buckets. This helps to ignore unrelated data points that might introduce noise into the recognition task, reduce the effect of outliers and irrelevant data variations, and hence lead to more accurate identification/verification results.

5 Conclusions and future work

This paper has introduced a reliable palmprint recognition system with an efficient template protection technique. Histogram remapping of Gabor features has been proposed to increase the authentication accuracy by reducing the effects of feature variability and enhancing their discriminative capability. Comb filtering has been applied on the remapped downsampled Gabor features as the first protection layer. The ability to reinitiate a new pattern is permitted by changing the filter order. Index-based locality-sensitive hashing after comb filtering has been proposed to serve as a robust security layer by transforming the real-valued features into maximum-ranked indices. Several comprehensive experiments have vindicated not only the template protection requirements but also the recognition accuracy

that is highly preserved compared to its original counterpart, even with the worst-case scenario. The system has proven its high capability in template revocability, non-invertibility, and unlinkability across the different databases, meeting the needs for real-time implementation through reduced matching and achieving superior verification/identification accuracy.

One of the future directions is the fusion of multiple biometric modalities for further enhancement of the system security and privacy. Multimodal systems are more resilient to spoofing attacks and can achieve better user privacy protection. Another direction is to develop novel deep learning models that can capture more intricate patterns and features, with the potential to include approaches like attention mechanisms, graph neural networks, and capsule networks. It is suggested also to explore methods to train these models with fewer labeled samples, such as few-shot learning, meta-learning, and self-supervised learning, to decrease the reliance on large datasets. We plan also to extend our research to include a thorough examination of pre-image attacks and provide a more comprehensive investigation of the system's resilience to various types of cryptographic vulnerabilities.

Abbreviations

IoT	Internet of Things
LSH	Locality-sensitive hashing
PRN	Pseudo-random number
EER	Equal error rate
ECC	Error correcting code
HA-BJTU	Handmetric Authentication Beijing Jiao Tong University
FRR	False rejection rate
KDA	Kernel discriminant analysis
TJU-P	Tongji University Palmprint
OIOM	Orthogonal Index of Maximum
MSH	Minimum Signature Hash
ROI	Region of interest
DHN	Deep Hashing Network
DHC-FC	Deep hashing codes-fuzzy commitment
HFM	Homomorphic filtering masking
CNN	Convolutional neural network
SHA	Secure Hash Algorithm
IIR	Infinite impulse response
CDF	Cumulative distribution function
FIR	Finite impulse response
KNN	K-nearest neighbor
TPR	True positive rate
FPR	False positive rate
SMHNet	Similarity Metric Hashing Network
SSIM	Structural Similarity Index Metric
LFH	Latent Factor Hashing
LGF	Learnable Gabor Filter
CCNet	Comprehensive Competition Network

Authors' contributions

H. A., E. E. studied conception and design; H.A., E. E., M. A.-Z collected data.; H. A., E. E., M. A.-Z. analyzed and interpreted results; H. A., E. E. prepared draft manuscript. All authors reviewed the results and approved the final version of the manuscript.

Funding

Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Availability of data and materials

The database that supports the findings of this research work "Tongji Contactless Palmprint Dataset" is publicly available online:https://cslinzhang.github.io/ContactlessPalm/.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Author details

[1]Electronics and Communication Engineering Department, Faculty of Engineering, Zagazig University, Zagazig City, Sharqia Governorate, Egypt. [2]Electronics and Communications Engineering Department, Egypt-Japan University of Science and Technology (E-JUST), Borg El Arab City, Alexandria Governorate, Egypt. [3]Electrical and Electronics Engineering Department, Faculty of Engineering, Assiut University, Assiut City, Assiut Governorate, Egypt.

Received: 13 July 2024 Accepted: 17 September 2024
Published online: 05 October 2024

References

1. A.E.R. Farouk, M. Abd-Elnaby, H.I. Ashiba et al., Secure cancelable face recognition system based on inverse filter. J. Opt. **53**, 1667–1688 (2024). https://doi.org/10.1007/s12596-023-01233-7
2. A. Ali, A. Migliorati, T. Bianchi et al., Cancelable templates for secure face verification based on deep learning and random projections. EURASIP J. Info. Sec. **2024**, 7 (2024). https://doi.org/10.1186/s13635-023-00147-y
3. M.J. Lee, A.B.J. Teoh, A. Uhl, S.N. Liang, Z. Jin, A tokenless cancellable scheme for multimodal biometric systems. Comput. Secur. **108**, 102350 (2021). https://doi.org/10.1016/j.cose.2021.102350
4. H.I. Cook, K. Harrison, H. James, Individuals lacking ridge detail: a case study in adermatoglyphia. J. Forensic Sci. **66**, 202–208 (2021). https://doi.org/10.1111/1556-4029.14597
5. J. Qiu, H. Li, C. Zhao, Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication. Comput. Secur. **82**, 1–14 (2019). https://doi.org/10.1016/j.cose.2018.12.003
6. L. Zhang, L. Li, A. Yang, Y. Shen, M. Yang, Towards contactless palmprint recognition: a novel device, a new benchmark, and a collaborative representation based identification approach. Pattern Recog. **69**, 199–212 (2017) Available online: https://cslinzhang.github.io/ContactlessPalm/
7. M. Gomez-Barrero, J. Galbally, C. Rathgeb, C. Busch, General framework to evaluate unlinkability in biometric template protection systems. IEEE Trans. Inf. Forensics Secur. **13**(6), 1406–1420 (2018). https://doi.org/10.1109/TIFS.2017.2788000
8. X. Wang, H. Li, One-factor cancellable palmprint recognition scheme based on OIOM and minimum signature hash. IEEE Access **7**, 131338–131354 (2019). https://doi.org/10.1109/ACCESS.2019.2938019
9. K. Sauerwein, T.B. Saul, D.W. Steadman, C.B. Boehnen, The effect of decomposition on the efficacy of biometrics for positive identification. J. Forensic Sci. **62**, 1599–1602 (2017). https://doi.org/10.1111/1556-4029.13484

10. Baghel V. S., Ali S. S., Prakash S. (2021) A non-invertible transformation based technique to protect a fingerprint template. IET Image Proc. 1– 15. https://doi.org/10.1049/ipr2.12130
11. H. Li, J. Qiu, A.B.J. Teoh, Palmprint template protection scheme based on randomized cuckoo hashing and MinHash. Multimed. Tools Appl. **79**, 11947–11971 (2020). https://doi.org/10.1007/s11042-019-08446-8
12. N.K.J. Ratha, J.H. Connell, R.M. Bolle, 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
13. V. Bansal, S. Garg, A cancelable biometric identification scheme based on bloom filter and format-preserving encryption. J. King Saud Univ. Comput. Inf. Sci. (2022). In Press. https://doi.org/10.1016/j.jksuci.2022.01.014
14. H. Kaur, P. Khanna, Cancelable features using log-Gabor filters for biometric authentication. Multimed. Tools Appl. **76**, 4673–4694 (2017). https://doi.org/10.1007/s11042-016-3652-3
15. G. Jaswal, R.C. Poonia, Selection of optimized features for fusion of palm print and finger knuckle-based person authentication. Expert. Syst. **38**, e12523 (2021). https://doi.org/10.1111/exsy.12523
16. H. Shao, D. Zhong, X. Du. Efficient deep palmprint recognition via distilled hashing coding. in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, (Long Beach, 2019), p. 714–723 https://doi.org/10.1109/CVPRW.2019.00098
17. R.F. Soliman, M. Amin, F.E. Abd El-Samie, Cancelable Iris recognition system based on comb filter. Multimed. Tools Appl. **79**, 2521–2541 (2020). https://doi.org/10.1007/s11042-019-08163-2
18. L. Leng, J. Zhang, PalmHash code vs. PalmPhasor code. Neurocomputing **108**, 1–12 (2013). https://doi.org/10.1016/j.neucom.2012.08.028
19. L. Leng, A.B.J. Teoh, M. Li, Simplified 2DPalmHash code for secure palmprint verification. Multimed. Tools Appl. **6**, 8373–8398 (2017). https://doi.org/10.1007/s11042-016-3458-3
20. H. Liu, D. Sun, K. Xiong, Z. Qiu, A Hybrid approach to protect palmprint templates. ScientificWorldJournal **2014**, 686754 (2014). https://doi.org/10.1155/2014/686754
21. T. Wu, L. Leng, M.K. Khan, A multi-spectral palmprint fuzzy commitment based on deep hashing code with discriminative bit selection. Artif. Intell. Rev. **56**, 6169–6186 (2023). https://doi.org/10.1007/s10462-022-10334-x
22. Z. Yang, M. Kang, A.B.J. Teoh, C. Gao, W. Chen, B. Zhang, Y. Zhang, *A dual-level cancelable framework for palmprint verification and hack-proof data storage. arXiv preprint arXiv:2403.02680* (2024)
23. M.I. Ashiba, H.A. Youness, H.I. Ashiba, Proposed homomorphic DWT for cancelable palmprint recognition technique. Multimed. Tools Appl. **83**, 9479–9502 (2024). https://doi.org/10.1007/s11042-023-15710-5
24. M.S. Khan, H. Li, Z.C. Chuan, Deep secure PalmNet: a novel cancelable palmprint template protection scheme with deep attention net and randomized hashing security mechanism. Comput. Secur. **142**, 103863 (2024). https://doi.org/10.1016/j.cose.2024.103863
25. P. Poonia, P.K. Ajmera, Upgrading information security and protection for palm-print templates. Wireless Pers. Commun. **126**, 1535–1551 (2022). https://doi.org/10.1007/s11277-022-09805-9
26. C. Turan, K.-M. Lam, Histogram-based local descriptors for facial expression recognition (FER): a comprehensive study. J. Vis. Commun. Image Represent. **55**, 331–341 (2018). https://doi.org/10.1016/j.jvcir.2018.05.024
27. L. Shen, L. Bai, A review on Gabor wavelets for face recognition. Pattern Anal. Appl. **9**, 273–292 (2006). https://doi.org/10.1007/s10044-006-0033-y
28. V. Struc, N. Pavešic, Photometric normalization techniques for illumination invariance, in *Advances in Face Image Analysis: Techniques and Technologies*. ed. by Y. Zhang (IGI Global, 2011)
29. M.G. Cruz-Jimenez, D.E.T. Romero, G.J. Dolecek, Comb filters characteristics and current applications, in *Encyclopedia of Information Science and Technology*, 4th edn., ed. by M.D.B.A. Khosrow-Pour (IGI Global, 2018), pp.6007–6018. https://doi.org/10.4018/978-1-5225-2255-3.ch522
30. Z. Jin, J.Y. Hwang, Y.-L. Lai, S. Kim, A.B.J. Teoh, Ranking-based locality sensitive hashing-enabled cancelable biometrics: index-of-max hashing. IEEE Trans. Inf. Forensics Secur. **13**(2), 393–407 (2018). https://doi.org/10.1109/TIFS.2017.2753172
31. C. Liu, D. Zhong, H. Shao, Few-shot palmprint recognition based on similarity metric hashing network. Neurocomputing **456**, 540–549 (2021). https://doi.org/10.1016/j.neucom.2020.07.153
32. G. Arora, S. Kalra, A. Bhatia, K. Tiwari, PalmHashNet: palmprint hashing network for indexing large databases to boost identification. IEEE Access **9**, 145912–145928 (2021). https://doi.org/10.1109/ACCESS.2021.3123291
33. W. Jia, B. Wang, Y. Zhao, H. Min, H. Feng, A performance evaluation of hashing techniques for 2D and 3D palmprint retrieval and recognition. IEEE Sens. J. **20**(20), 11864–11873 (2020). https://doi.org/10.1109/JSEN.2020.2973357
34. H. Shao, D. Zhong, X. Du, *Towards efficient unconstrained palmprint recognition via deep distillation hashing. arXiv preprint arXiv:2004.03303* (2020)
35. Q. Lin, L. Leng, C. Kim, Double quantification of template and network for palmprint recognition. Electronics **12**(11), 2455 (2023). https://doi.org/10.3390/electronics12112455
36. Z. Yang, H. Huangfu, L. Leng, B. Zhang, A.B.J. Teoh, Y. Zhang, Comprehensive competition mechanism in palmprint recognition. IEEE Trans. Inf. Forensics Secur. **18**, 5160–5170 (2023). https://doi.org/10.1109/TIFS.2023.3306104
37. Z. Yang, W. Xia, Y. Qiao, Z. Lu, B. Zhang, L. Leng, Y. Zhang, CO3Net: coordinate-aware contrastive competitive neural network for palmprint recognition. IEEE Trans. Instrum. Meas. **72**, 1–14 (2023). https://doi.org/10.1109/TIM.2023.3276506. (Art no. 2514114)

Publisher's Note