symmetry

MDPI

Article

Dual Hashing Index Cancellable Finger Vein Template Based on Gaussian Random Mapping

Xueyou Hu [1], Liping Zhang [2], Huabin Wang [2,*], Jian Zhou [2] and Liang Tao [2]

[1] Faculty of Advance Manufacture Engineering, Hefei University, Hefei 230000, China; xueyouhu@hfuu.edu.cn
[2] Anhui Provincial Key Laboratory of Multimodal Cognitive Computation, School of Computer Science and Technology, Anhui University, Hefei 230000, China; zhangliping@stu.ahu.edu.cn (L.Z.); jzhou@ahu.edu.cn (J.Z.); taoliang@ahu.edu.cn (L.T.)
* Correspondence: wanghuabin@ahu.edu.cn

Abstract: In the existing cancellable finger vein template protection schemes, the original biometric features cannot be well protected, which results in poor security. In addition, the performance of matching recognition performances after generating a cancellable template is poor. Therefore, a dual hashing index cancellable finger vein template protection based on Gaussian random mapping is proposed in this study. The scheme is divided into an enrollment stage and a verification stage. In the two stages, symmetric data encryption technology was used to generate encryption templates for matching. In the enrollment stage, first, the extracted finger vein features were duplicated to obtain an extended feature vector; then, this extended vector was uniformly and randomly permuted to obtain a permutation feature vector. The above two vectors were combined into a two-dimensional feature matrix. The extended and permuted feature vector made full use of the original biometric features and further enhanced the non-invertibility. Second, a random Gaussian projection vector with $m \times q$ dimensions was generated, and a random orthogonal projection matrix was generated by the Schmidt orthogonalization of the previously generated random vector. This approach accurately transferred the characteristics of the biometric features to another feature space and ensured that the biological template is revocable. Finally, the inner product of the two-dimensional feature vector and random orthogonal projection matrix was obtained and superimposed into a row. The dual index values of the largest and second largest values were repeated m times to obtain a hash code for matching. The secondary maximum value index was introduced to adjust the error generated by the random matrix, which improved the recognition rate of the algorithm. In the verification stage, another hash code for matching was generated based on symmetric data encryption technology, and then the two hash codes were cross matched to obtain the final matching result. The experimental results show that this scheme attains good recognition performance with the PolyU and SDUMLA-FV databases, that it meets the design standard for cancellable biometric identification, and that it is robust to security and privacy attacks.

Keywords: finger vein; hashing index; cancellable template protection; biometric recognition

Citation: Hu, X.; Zhang, L.; Wang, H.; Zhou, J.; Tao, L. Dual Hashing Index Cancellable Finger Vein Template Based on Gaussian Random Mapping. *Symmetry* **2022**, *14*, 258. https://doi.org/10.3390/sym14020258

Academic Editor: Christophe Humbert

Received: 31 October 2021
Accepted: 9 December 2021
Published: 28 January 2022

1. Introduction

With the rapid development of biometric technology, biometric recognition has become widely used in various fields. However, the security and privacy of biometric templates when stolen or leaked has become a critical topic of concern to the public [1]. Due to the uniqueness and non-renewability of biometrics, if a template leaks, information loss is permanent. Biometric template protection can be divided into cancellable biometrics [2] and biometric cryptosystem [3]. This study considers the former. The goal of cancellable template protection is to map the original biometric features to a new feature space for encryption purposes. The cancellable template protection scheme should meet four criteria, as follows: (1) Non-invertibility: no matter whether there is auxiliary data or not, the

original biometric template cannot be derived from a single instance or multiple instances of the protected template, which improves the security of the template. (2) Revocability: new templates can be generated by changing relevant parameters to replace old templates (including stolen or damaged templates) for matching. (3) Unlinkability: the encrypted template is independent of the original biometric, and it is difficult to distinguish one or more encrypted templates from the same biometric, that is, cross-matching is not possible. (4) Performance maintenance: the recognition rate of the cancellable biometric templates obtained after encryption must be approximately consistent with that of the original features.

A block diagram for a generic cancellable biometric recognition system is shown in Figure 1. The block diagram shown here is general and concise. Almost all the cancellable biometric template protection algorithms can be summarized as follows. The unique and key point of each algorithm lies in the transformation process. It is important that after the transformation, the accuracy of the original biometric recognition can be maintained, and the requirements of the cancellable templates can be achieved.

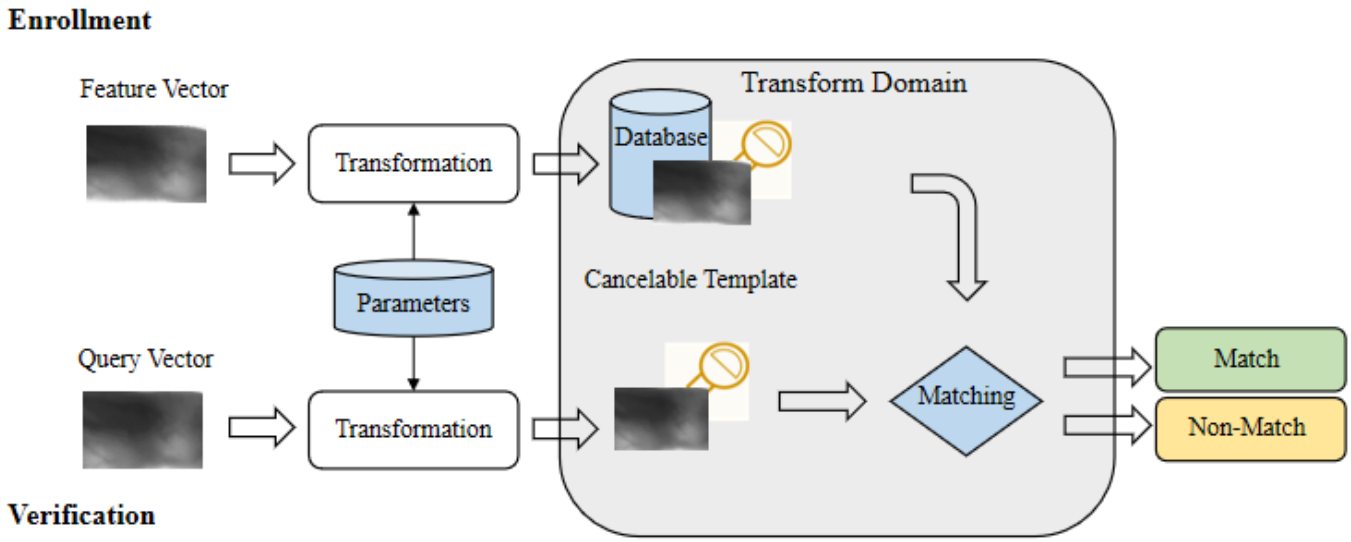


Figure 1. Basic framework of the cancellable biometric system.

The generic cancellable biometric template protection scheme is applicable not only to finger veins but also to other biometric modes, such as face or iris recognition. Teoh et al. [4] proposed BioHash, and an improved cancellable template algorithm based on BioHash was successfully applied to a palmprint, a fingerprint, gait, and facial features. BioHash is essentially a quantized underdetermined linear equation system that can be partially solved by pseudoinverse operation [5]; therefore, its degree of non-invertibility is low. Rathgeb et al. [6] proposed an improved Bloom filter that can be applied to iris, face, and fingerprint features. In this method, multiple elements are mapped to the same element in the Bloom filter, forming a many-to-one mapping that satisfies the non-invertibility requirement and is revocable using application-specific parameters T. However, as addressed [7,8], the modified Bloom filter does not satisfy the unlinkability requirement and is vulnerable to malevolent attacks. Jin et al. [9] proposed Index-of-Max (IoM) hashing, which is based on Gaussian random projection (GRP-based IoM) with multiple random projections that record the maximum hash index value, and the uniform random permutation-based IoM (URP-based IoM) method, which records the maximum index value. These techniques can be applied to iris and palmprint recognition in binary form and to face features in fixed length vector form. Using externally generated random parameters, IoM hashing transforms real valued biometric vectors into discrete index (maximum sort) hash codes.

The generic cancellable biometric template protection scheme can be applied to a variety of specific biometric schemes because it is not constrained by any specific biometric form. Consequently, the generic template is more widely used than specific biometric

template protection schemes. However, the current generic cancellable template protection scheme still exhibits some problems. The scheme proposed in this study addresses these problems and improves the recognition rate and security of the generic cancellable template scheme.

The cancellable finger vein template protects the input finger vein features. The fuzzy commitment scheme (FCS) [10] is an example of the direct application of biometric encryption for binary finger vein data. Similarly, both cancellable biometrics and biometric encryption have been applied to binary finger vein features [11]: in this method, a group of Gabor filters are first used to extract the finger vein features; then, PCA is used to reduce the dimension, and a BioHash cancellable biometric scheme is used to binarize the obtained coefficients. Finally, FCS is used for processing. Another method combined revocable biometrics and biometric encryption [12]. That study also applied BioHash to features generated by a Gabor filter and subsequent LDA; then, the binary strings were processed by FCS. Finally, a fuzzy vault scheme was implemented for the processed strings. The technology developed in the context of fingerprint detail representation has been transferred to finger vein detail representation, namely, finger vein detail cylinder code [13] and finger vein spectrum detail representation [14]. The representation of the latter is binarized and then input into a Bloom filter to generate a cancellable biometric recognition scheme that avoids the need for position correction [15] during template comparison.

Cancellable biometric template protection algorithms can be divided into a two-factor cancellable feature template protection algorithm and a one-factor cancellable feature template protection algorithm. The difference between the two is whether external factors participate. As the name suggests, two-factor has external factors and original biometric features to participate in the transformation of the algorithm to assist biometric encryption, while one-factor has no external factors to participate. This paper belongs to two-factor cancellable biometrics. General cancellable biometric scheme refers to a scheme that is applicable to other biometric methods (such as face and iris). This study proposes a general cancelable biometric scheme that can protect any biometric as long as the biometric exists in decimal form. As the finger vein is located inside the finger, it is not damaged by epidermis compared with fingerprint palmprint recognition, and the non-contact collection and authentication process has very low exclusion for users, which is safe and hygienic. Compared with iris recognition [16–18] and face recognition, its acquisition process is very friendly. Therefore, the modal of the finger vein is the subject of this study.

Cancellable biometric templates balance performance and non-invertibility because strict non-invertibility means that information needs to be irretrievable after conversion. However, accuracy can be maintained only by retaining the discriminative information from the original template. Therefore, the recognition rate of cancellable finger vein template protection algorithms must be improved to meet the design standards of cancellable biometric recognition. This study proposes a cancellable finger vein template protection scheme based on the GRP-based IoM authentication system framework [9], named the dual hashing index cancellable finger vein template based on Gaussian random mapping (GRP-DHI).

In GRP-DHI, the DHI is driven by locality sensitive hashing (LSH) [19] that stems from the information retrieval field. GRP-DHI, which is a special example of an LSH series, can ensure the matching accuracy after hashing. Here, the essence of Gaussian random mapping is to multiply the eigenvector and Gaussian random matrix, that is, the original eigenvector is randomly mapped to another space. The DHI has a nonlinear conversion from real valued biometrics to discrete index hashed codes that effectively protect biometric data from inversion. The discrete index representation of DHI hashed codes has many advantages. For example, DHI technology can hide biometric information well, and it provides a solid foundation for irreversibility; the DHI is not sensitive to the size of feature values; therefore, it is more robust to changes in biometric characteristics. The size independence of the DHI also makes the hashed code scale invariant, which is important for matching and feature alignment tasks.

The main contributions of this study are as follows:

(1) We propose to transform the one-dimensional finger vein feature vector into a two-dimensional finger vein feature matrix by means of duplicate expansion and replacement. In terms of replication and expansion, the two-dimensional finger vein feature matrix makes full use of the limited original biological features to highlight the similarity of the same finger vein feature vector; in terms of dimensions, the two-dimensional feature matrix is proposed because it solves the problem of blindly pursuing replication and expansion, which leads to the one-dimensional biological feature vector being too long and cumbersome. The two-dimensional finger vein feature matrix breaks the general thinking mode of the one-dimensional feature vector and further enhances the non-invertibility.

(2) We propose to perform the Schmidt orthogonalization of randomly generated m times q-dimensional random Gaussian projection vectors to generate a random orthogonal projection matrix, and then multiply the random orthogonal projection matrix with the finger vein feature matrix. Using a random orthogonal projection matrix can better transfer the feature of the biological feature to another feature space, can improve the matching rate, and ensure the revocability of the biological feature template.

(3) We propose a dual hashing index, which uses the largest and second largest hashing indexes to generate two cancellable finger vein templates for matching. This can solve the difference in the maximum hashing index of two samples of the same kind caused by the random matrix, thereby further improving the recognition performance.

The presented experiments and discussions demonstrate that, when the proposed cancellable biometric template protection scheme is applied to the PolyU and SDUMLA-FV finger vein databases, it achieves higher recognition rates and offers greater security than other schemes do.

2. Related Work

This section briefly introduces the work related to the proposed GRP-DHI scheme, including locality sensitive hashing (LSH), winner-takes-all (WTA) [20] hashing for data retrieval, random maxout features (RMF) [21] for data classification, and Index-of-Max hashing based on Gaussian random projection (GRP-based IoM).

2.1. Locality Sensitive Hashing

The role of LSH is to reduce the dimension of high-dimensional data. This is achieved mainly by hashing the input items, since similar items are likely to be hashed into the same "bucket" and because the number of "buckets" is much smaller than the number of input items. Therefore, LSH should maximize the likelihood that similar items will be hashed into the same "bucket", thereby reducing the dimension of the data. The LSH family H is calculated as follows:

$$\begin{aligned} P_{h\in H}(h_i(X) = h_i(Y)) \leq P_1, if\ S(X,Y) < R_1 \\ P_{h\in H}(h_i(X) = h_i(Y)) \leq P_2, if\ S(X,Y) > R_2 \end{aligned} \tag{1}$$

A probability distribution LSH of function family H based on hash functions h is:

$$P_{h\in H}[h(X) = h(Y)] = S(X,Y) \tag{2}$$

where S is the similarity function [22] defined on the set of objects X and Y.

LSH mainly hashes object sets X and Y using the function h_i in the family of functions H. The function h_i makes the collision probability of X and Y more reasonable. LSH ensures a higher collision probability after hashes of X and Y with high similarity. Otherwise, the collision probability is lower.

2.2. Winner-Takes-All Hashing

WTA hashing is based on partial order statistics that calculate an ordered embedding of input data. In other words, WTA is not based on the values of the input data (including

absolute values and so on), but rather is a nonlinear transformation based on implicit order. Therefore, it reduces the interference of numerical types to a certain extent and can compare the internal similarity between items well. The steps of the WTA hashing process are as follows:

(1) Perform H random permutations on input vector $x \in \mathbb{R}^d$ (d is the dimension of the input vector).
(2) Select the first k terms of $\boldsymbol{x}$ after permutation;
(3) Select the largest element in the above k terms;
(4) Record the corresponding index values in bits;
(5) Repeat steps 1–4 m times to generate a hash code of length m, which can be expressed as $m\lceil \log_2 k \rceil$.

2.3. Random Maxout Features

The RMF, proposed by Mroueh et al., is a simple and efficient nonlinear feature mapping that approximates the functions of interest.

Let $\left\{ W_j^i \in \mathbb{R}^d \middle| i = 1, \ldots, m, j = 1, \ldots, q \right\}$ be an iid standard Gaussian random vector drawn from $\mathbb{N}(0, I_d)$.

For $x \in \mathbb{R}^d$, the RMF is defined as follows:

$$\varphi_i(x) = \max_{j=1,\ldots,q} \langle W_j^i, x \rangle, i = 1, \ldots, m \tag{3}$$

The set of m RMFS produces the following RMF vector:

$$\Phi(x) = \frac{1}{\sqrt{m}} [\varphi_1(x), \ldots, \varphi_m(x)] \in \mathbb{R}^m \tag{4}$$

2.4. Index-of-Max Hashing Based on Gaussian Random Projection

GRP-based IoM hashing can be simplified into two steps as follows, and the pseudo code is given in Algorithm 1.

(1) Given the fingerprint vector $x \in \mathbb{R}^d$, a Gaussian projection vector of $m \times q$ dimensions is generated as follows:

$$\{ W_j^i \in \mathbb{R}^d \Big| i = 1, \ldots, m,\ j = 1, \ldots, q \} \sim \mathbb{N}(0, I_d) \tag{5}$$

forming the following random Gaussian projection matrix:

$$W^i = \left[W_1^i, \ldots, W_q^i \right] \tag{6}$$

(2) The m index values of the maximum value calculated from the following:

$$\varphi_i(x) = \arg \max_{j=1,\ldots,q} \langle W_j^i, x \rangle \tag{7}$$

are recorded as t_i.

Therefore, the GRP-based IoM hash code is as follows:

$$t_{GRP} = \{ t_i \in [1, q] | i = 1, \ldots, m \} \tag{8}$$

Algorithm 1 GRP-based IoM algorithm

Input: Feature vector $x \in \mathbb{R}^d$ with d dimensions, the number of Gaussian random matrices m, and the number of Gaussian random projection vectors q.
Output: Hashed code $t_{GRP} = \{t_i \in [1, q] | i = 1, \ldots, m\}$

Generate m Gaussian random matrices. $W^i = \left[W_1^i, \ldots, W_q^i\right], i = 1, \ldots, m$.
Initialize the i-th hashed code $t_i = 0$.
Perform random projection and record the maximum index in the projected feature vector.
for k = 1: m
  $\overline{x}^k = W^k x$
  Find $x_j^k = \max\left(\overline{x}^k\right), j = 1, \ldots, q$
  Then, $t_i = j$(j is the index of $\overline{x}^k$)
end for

The GRP-based IoM is different from the RMF; the representation of the former encodes the index of the maximum value of $\varphi_i(x)$, while the latter only encodes the maximum value of $\varphi_i(x)$. In short, GRP embeds a fingerprint vector into a q-dimensional random Gaussian subspace and obtains the index of the maximum projection feature. From the perspective of LSH, $h(\cdot)$ is equivalent to a hashing term in random space. This process is repeated using m independent Gaussian random matrices, generating a set of m maximum hash indexes. Therefore, the GRP hashed code retains the Euclidean pairing distance in the subspace of projection, $\mathbb{R}^q$, which refers to the distance/similarity function in LSH.

3. Methodology

In this study, the GRP-DHI scheme took the finger vein features as the input and used the feature extraction method of finger vein image in reference [23].

The following steps were used for the finger vein feature vector extraction: (1) Finger vein image preprocessing. Firstly, a Gaussian filter was used to obtain the denoised finger vein image, and then a Sobel operator was used to convolute the image to obtain the gradient components of each pixel in the vertical and horizontal directions; (2) The gradient amplitude was detected based on the edge. Different symbols were given to the gradient amplitude of different edge points to reflect the position difference of different pixels, and the points with the same gradient amplitude but different positions were distinguished in order to effectively improve the discrimination of differential excitation; (3) Using double Gabor direction. The Gabor filter convoluted the finger vein image, extracted the double Gabor direction information, and delimited a direction interval for the finger vein ridge, which is more robust to translation and rotation; (4) Joint distribution feature extraction. The two-dimensional features were constructed by combining the differential excitation diagram with each direction diagram to generate two-dimensional feature vectors; (5) Feature vector dimension reduction. The variance was controlled to respectively reduce the dimensionality of the feature vector in each direction, and each sample generated a feature vector after the dimensionality reduction in two directions; (6) Canonical correlation analysis. The correlation of feature vectors was maximized in two different directions. Finally, DVCG converted a finger vein image into a 462-dimensional feature vector. The specific steps are shown in Figure 2.

In the following sections of this paper, the implementation steps of the algorithm are introduced in detail, and then, the matching process of the hash code is analyzed. Finally, the generation of a general cancellable template is briefly described. For quick reference, the main notations are listed in Table 1.

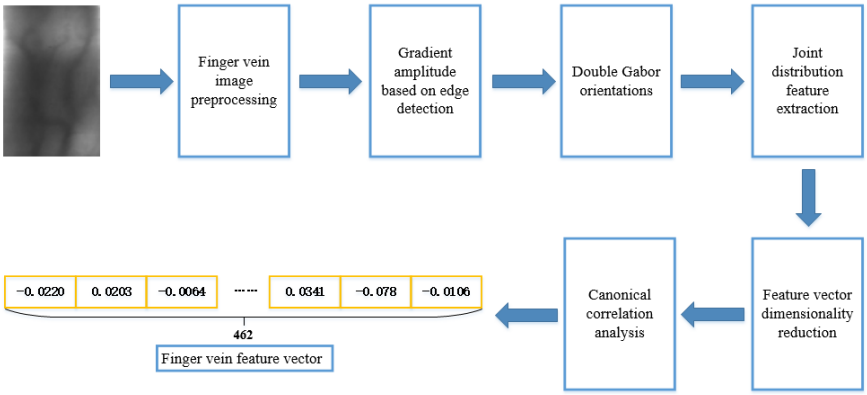


Figure 2. Extraction process of the finger vein feature vector.

Table 1. Notations and descriptions.

Notation	Description
H	Locality Sensitive Hashing (LSH) family
h	LSH function $h \in H$
X	Finger vein feature vector $x \in \mathbb{R}^d$
$S(X,Y)$	Similarity function on object X and Y
m	Number of Gaussian random matrices
q	Number of Gaussian random projection vector
n	Multiple of expansion
t_1, t_2	Largest and second largest hashed index template

3.1. Dual Hashing Index Based on Gaussian Random Mapping (GRP-DHI)

The DHI is a cancellable biometric method that can be regarded as a special example of LSH. The local sensitive function $h(\cdot)$ refers to a q-dimensional random projection in the GRP-DHI implementation. The DHI nonlinearly embeds biometrics into the ranking metric space of the LSH-based similarity function S.

The key part of GRP-DHI was to form a two-dimensional feature matrix by expanding and randomly permuting the original biometric feature vector, and then to further process it through the random orthogonal matrix. Finally, the largest and second largest hashed codes were obtained for matching. Figure 3 shows the whole transformation process of generating hashed code. The four steps of GRP-DHI are as follows, and the pseudo code is given in Algorithm 2.

(1) Given a finger vein vector $x \in \mathbb{R}^d$, $x \in \mathbb{R}^d$ was copied n times to form an extended feature vector $x \in \mathbb{R}^{dn}$, where n is a system parameter. This step increased the length of the original biometric vector, copied and expanded the original limited biometric vector, and increased the data of each sample eigenvector, to ensure the original biometric could be fully utilized in the subsequent transformation process.

(2) The extended feature vector $\boldsymbol{x}$ was uniformly and randomly replaced to obtain a permutation feature vector $\boldsymbol{x}'$. At this time, the synthesized two-dimensional feature matrix was used as the input of the algorithm, and the extended feature vector $\boldsymbol{x}$ and its randomly replaced $\boldsymbol{x}'$ were combined up and down into a two-dimensional matrix, which made the similarity between intraclass finger vein feature vectors more prominent, and the random replacement of the feature vector was introduced to further increase its non-invertibility. This made full preparations for the next accuracy requirements and safety analysis.

(3) A Gaussian projection vector with $m \times q$ dimensions was generated:

$$\{W_j^i \in \mathbb{R}^d \Big| i = 1, \ldots, m,\ j = 1, \ldots, q\} \sim \mathbb{N}(0, I_d) \tag{9}$$

and Schmidt orthogonalization was applied to the random vectors to generate the following random orthogonal projection matrix:

$$W^i = \left[W_1^i, \ldots, W_q^i\right] \tag{10}$$

The Gaussian orthogonal projection matrix can better maintain the distance invariance between feature vectors, that is, retain more information between original features after transformation, and ensure the accuracy of authentication results in the transformation domain, that is, achieve a more stable recognition performance. In addition, the orthogonal random projection matrix is randomly generated, which makes the algorithm revocable. When the encrypted template is damaged or stolen, we can regenerate the Gaussian random orthogonal projection matrix, and then execute the algorithm to obtain a new encrypted template.

(4) Based on the two rows' inner product values generated by the following:

$$\varphi_i(x) = arg \max_{j=1,\ldots,q} \langle W_j^i, x \rangle \tag{11}$$

and superimposed into the rows' inner product value, the index of the largest value and the second largest value is repeated m times; then, the m indexes of the largest value and second largest value are calculated and recorded as t_1^i and t_2^i, respectively. Thus, the GRP-DHI hashed code is as follows:

$$t_{GRP} = \left\{ t_1^i \in [1,q] \middle| i = 1, \ldots, m, t_2^i \in [1,q] \middle| i = 1, \ldots, m \right\} \tag{12}$$

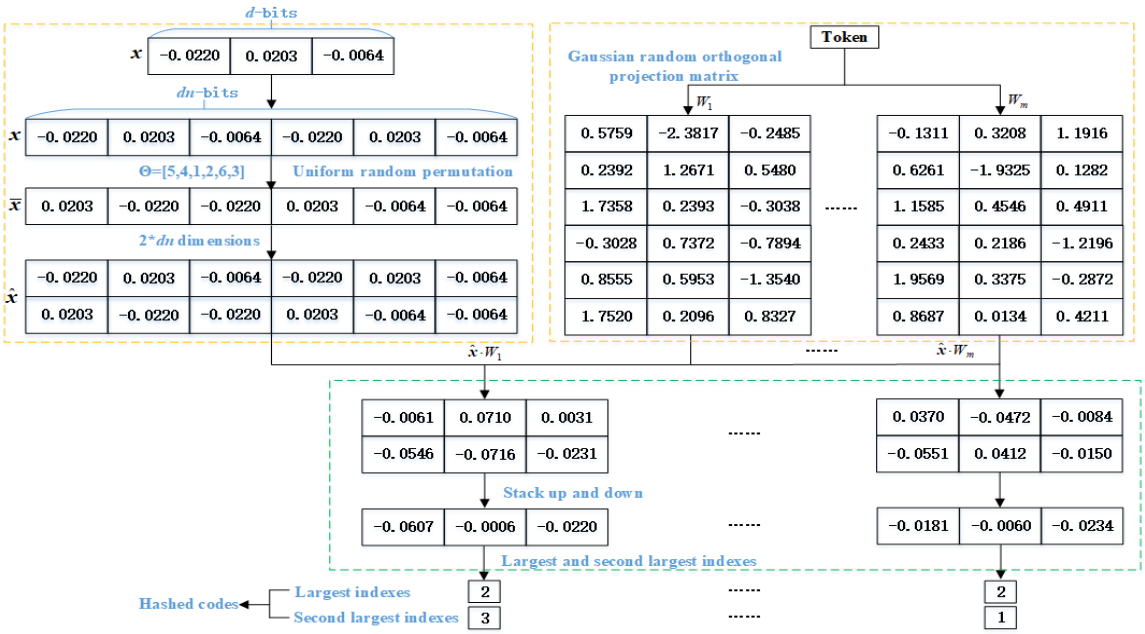


Figure 3. The process of generating dual hashing index based on Gaussian random mapping (GRP-DHI) hashed codes.

Using the indexes with the largest and second largest values as the encryption template has data independence, which is not only independent of the original feature vector, but also independent of the data projected into the new space; therefore, the original biometrics cannot be restored just from the index. Therefore, the non-invertibility of this algorithm can also meet high requirements. Due to the instability of the random matrix, the combination of two samples with small difference and the random matrix may lead to a change in the largest index, and we used the largest and second largest indexes as the encryption template

at the same time, which can reduce the matching error and improve the recognition rate as much as possible.

Algorithm 2 Dual hashing index based on Gaussian random projection (GRP-DHI) algorithm

Input: Feature vector $x \in \mathbb{R}^d$ with d dimensions, the multiple of expansion n, the number of Gaussian random matrices m and the number of Gaussian random projection vectors q.

Output: The hashed code $t_{GRP} \in [1, q]$ and $t_{GRP} = \left\{ t_1^i, t_2^i \in [1, q] \middle| i = 1, \ldots, m \right\}$

Copy x n times to form an extended feature vector $x \in \mathbb{R}^{dn}$.

Apply uniform random permutation to generate x' and combine x and x' to form a two-dimensional feature matrix X.

Generate m Gaussian random orthogonal projection matrices. $W^i = \left[W_1^i, \ldots, W_q^i \right], i = 1, \ldots, m$.

Initialize the i-th hashed code $t_1^i = 0, t_2^i = 0$.

The inner product of the two-dimensional feature vector and Gaussian random orthogonal projection matrix is obtained and superimposed into a row. The largest index value and the second largest index value of the projection feature vector are recorded.

for k = 1: m

  $\overline{x}^k = W^k x$

  $\overline{x}^k = \overline{x}_1^k + \overline{x}_2^k$

  Find [*index*] = *sort*($\overline{x}^k$) *ind* = *index*(*size*$\left(\overline{x}^k, 2\right) - 1$): end

  Then, t_1^i = *ind*(1), t_2^i = *ind*(2) (*ind*(1) and *ind*(2) are the indexes of $\overline{x}^k$)

end for

3.2. Matching of GRP-DHI Hashed Codes

GRP-DHI essentially follows the ranking-based LSH, which strives to ensure that two finger vein vectors with high similarity have a high probability of collision in the rank domain, while also ensuring that vectors far from each other result in a lower hash collision probability. Suppose that the following two hash codes exist: the enrolled vector:

$$t^e = \{ t_i^e | i = 1, \ldots, m \} \tag{13}$$

and the query vector:

$$t^q = \left\{ t_j^q \middle| j = 1, \ldots, m \right\}. \tag{14}$$

Here, $S(t^e, t^q)$ represents the collision probability of the two hash codes. For example,

$$P[t^e, t^q] = S(t^e, t^q), i, j = 1, \ldots, m \tag{15}$$

The high collision probability implies a high similarity between t^e and t^q.

The GRP-DHI hash encoded the largest and second largest values of conversion features into the index representation to achieve the ability to match GRP-DHI hashed codes. The matching score is the total number of conflicts, which can be found by calculating the number of "0" entries (conflicts) over m (the total number of items of hashed code) after subtracting t^e and t^q by element correspondence. Due to the instability of the random matrix, the maximum index changed when two samples with small differences were combined with the random matrix. Therefore, to improve the recognition rate, both the largest and the second largest indexes were introduced (e.g., t_1^e, t_2^e and t_1^q, t_2^q). The specific matching process of hashed codes with the largest indexes and the second largest indexes is shown in Figure 4.

Therefore, when matching, in addition to counting the number of items that are reduced to "0" by the maximum index of t^e and the maximum index of t^q, the number of items that are reduced to "0" by the second largest index of t^q should also be counted. The second largest index is the same.

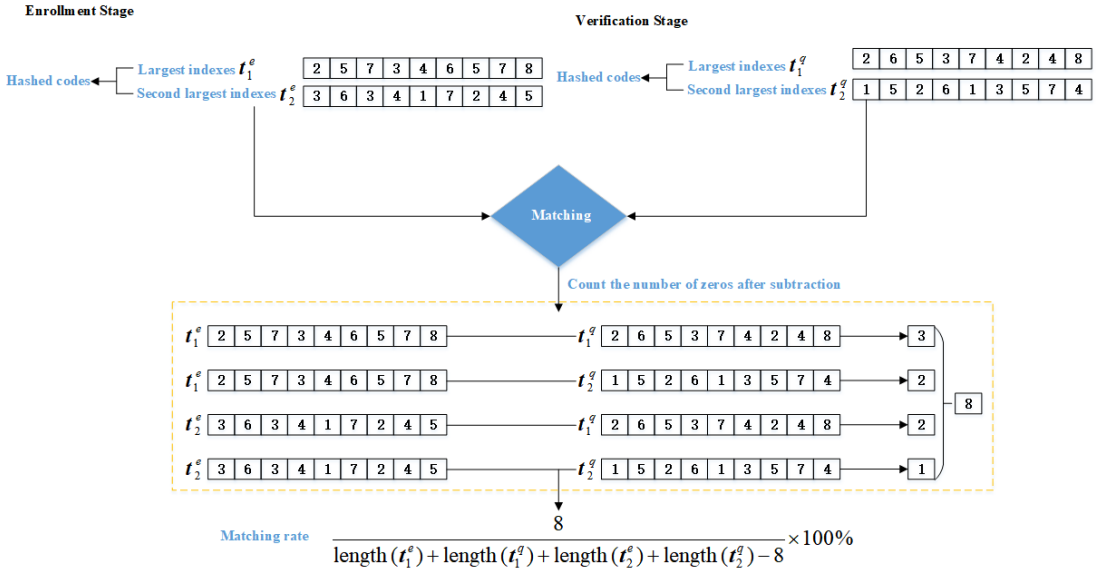


Figure 4. The matching process of GRP-DHI hashed codes.

3.3. Generating a Generic Cancellable Template

GRP-based IoM hashing is generic in the sense that it is applicable to most common biometrics where the features are in a binary form (e.g., the iris or palmprint) or a fixed-length vector form (e.g., the face). Due to the internal connection between GRP-DHI and LSH, GRP-DHI can be expected to extend to other common biometric recognition methods. After encrypting the original biometrics, the obtained protection template is stored in the database for later matching and recognition. Then, after the original biometrics are encrypted, they can be directly stored in a place with higher security level, hidden and confidential, because the original biometrics are not used in the process of identification and matching, which is an effective protection of the original biometrics. Moreover, our recognition process is matched in the transform domain, that is, the two encrypted templates match each other without decryption; therefore, the original biometrics are not exposed in the matching process, which provides better protection for the original biometrics. Our encryption algorithm is non-invertible; therefore, thieves cannot restore the original biometrics from the encrypted template. However, when the template is destroyed, the user-specific random seeds can be used to generate a random feature vector and a Gaussian random matrix to replace the GRP-DHI hash codes, providing the user-specific revocability of the randomly arranged seeds or random matrices. To evaluate the robustness of a stolen token, experiments were carried out on multiple objects using the same random token. The experiments revealed the accuracy performance when a token is stolen.

4. Experiments and Discussions

To verify the effectiveness of the proposed method, an experiment was conducted using the PolyU and SDUMLA-FV finger vein databases. Finger veins differ among different fingers of the same person; consequently, different finger vein images from the same person may belong to different categories. The PolyU database collected samples of two different fingers from 156 people, namely, a total of 312 (156 objects $\times$ 2 fingers) samples. There are six finger vein images in each category. The ROI regions and scales were extracted from all the samples in advance, and the images were normalized to 96 $\times$ 64 pixels. The SDUMLA-FV database contains a collection of six different finger images from 106 people, forming a total of 636 (106 objects $\times$ 6 fingers) images. There are six finger vein images in each category. Similarly, after pre-processing and scale normalization, the images are 150 $\times$ 96 pixels.

The finger vein databases we used are public finger vein image databases, and then we used the algorithm studied in our laboratory to extract the features, and we performed the

encryption algorithm based on the extracted features, that is, biometric template protection. Therefore, this study mainly presents the biometric template protection algorithm.

When generating a cancellable finger vein template, six samples from each class in each database were used to generate cancellable templates. For the matching protocol, the PolyU database contains 4680 ($312 \times C_6^2$) true matches and 48,561 (C_{312}^2) false matches, while the SDUMLA-FV database contains 9540 ($636 \times C_6^2$) true matches and 201,930 (C_{636}^2) false matches. The accuracy of the proposed method was evaluated by the equal error rate (EER)(%) and the genuine/imposter matching scores. Note that because random permutation/projection was applied, the EERs were calculated by taking the average EER after five repetitions.

4.1. Parameters of GRP-DHI

The cancellable template protection method proposed in this paper requires external factors and original biological features as input to help the biological features to be irreversibly transformed. This study proposed duplicating and expanding the original biological features and replacing them to form a feature matrix. The multiple of expansion was not arbitrary, and it was not a case of the more the better; therefore, the multiple of expansion needed to be adjusted. The external factor/token in this study was a Gaussian random orthogonal matrix. Since the Gaussian random orthogonal matrix was multiplied by the feature matrix, according to the principle of matrix multiplication, the number of rows of the matrix was determined, which is the number of columns of the extended feature matrix. The number of columns of the matrix needed to be adjusted, and the number of matrices, that is, the number of experiments that needed to be performed, also needed to be adjusted. Therefore, in this section, the multiple of expansion n, the number of Gaussian random matrices m and the Gaussian random projection vector, that is, the number of columns of the Gaussian random matrix q, are tested with interval values, respectively. The influence of parameter values on the experimental results was observed, and the best parameters were selected for the following experiments.

To investigate the effects of the parameter n, an experiment was conducted in which the multiples of expansion were set to 1, 2, 3, 4 and 5. The experimental results are shown in Figure 5a EER(%)-vs.-n, showing that expanding the vector multiple reduces the EER. This is because when the extended vector becomes longer, it contains more effective feature information, but the noise involved in the larger number of feature vectors leads to distortions in the product code. Therefore, the expected performance decreases as n increases. This result reveals the trade-off between performance and security that cancellable biometrics face.

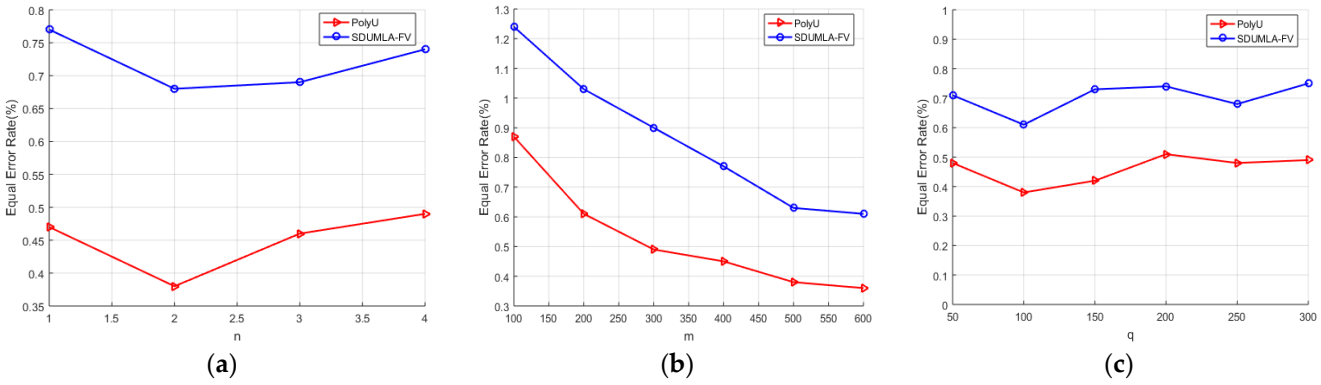


Figure 5. Parameters of GRP-DHI. (**a**) Equal error rate (EER)(%)-vs.-n. (**b**) EER(%)-vs.-m. (**c**) EER(%)-vs.-q.

The number of Gaussian random matrices m was varied from 100 to 200, 300, 400, 500 and 600 in the experiment because m is an important factor in determining the accuracy performance. As shown in Figure 5b EER(%)-vs.-m, experiments on the PolyU database show that when q is 2, the EER decreases from 0.98 to 0.38% as m increases from 100 to 500.

This confirms the theory underlying LSH; that is, after hashing, adjacent points are more likely to fall in the same "bucket" than nearby points are. The concept of the "bucket" in LSH is similar to that in GRP-DHI, in which the largest and second largest indexes of the projection vector can be regarded as the quantized output.

The number of Gaussian random projection vectors q was varied from 50 to 100, 150, 200, 250 and 300; however, q had little effect on the EER. As shown in Figure 5c EER(%)-vs.-q, the experiments on the PolyU database show that when m = 500 and n= 2, EER values of 0.36 and 0.48% are obtained when q = 50 and 300, respectively. Therefore, when m is sufficiently large, q can be set to a very small value without significantly reducing the EER, which results in substantial computing and storage cost reductions.

Through the influence of the above discussed parameters on the experiment, we can find, in the tuning results, that for the database of the experiment in this article, we comprehensively analyzed and selected the best parameters, respectively, for n = 2, m = 500 and q = 50, which can promote better experimental results. When the algorithm presented in study paper was directly or indirectly applied to other databases or practical applications, it was also necessary to dynamically optimize the parameters accordingly and select the most suitable parameters to increase the recognition rate.

4.2. Performance Evaluation

This section tests a token stolen from the PolyU and SDUMLA-FV databases using the best parameter settings from the previous section. Table 2 shows a comparison of the experimental results between the proposed scheme and the original template-free and existing cancellable technologies.

Table 2. Performance accuracy and comparison.

Method	Token	EER(%) for PolyU	EER(%) for SDUMLA-FV
PG-Gabor [24]	same	0.45	1.35
PG-ASAVE [24]	same	0.43	1.1
RD [25]	same	-	1.10
S2DPHC [26]	same	16.52	10.31
GRP-based IoM [6]	different	0.6057	0.8964
URP-based IoM [6]	different	2.6933	2.4642
GRP-DHI	**same**	**0.3823**	**0.6136**
GRP-DHI	**different**	**0.1893**	**0.2920**

From the results of the above comparative experiments, it can be observed that the GRP-DHI method proposed in this study achieves a good recognition performance compared with the original finger vein vector, regardless of whether a token is stolen or real. In addition, there is no significant difference in the recognition effect between a stolen token and a genuine token sample. This suggests that external tokens may no longer need to be kept private, which is a considerable advantage. Therefore, the security and privacy requirements for external tokens can be relaxed. Analysis of the security and privacy is provided later.

The recognition performance of GRP-DHI is better than that of the existing cancellable finger vein template, which can be attributed to its superior finger vein feature extraction method, feature vector construction method and the good performance of the GRP-DHI algorithm.

4.3. Time Complexity and Simple Implementation

To calculate the time efficiency of the GRP-DHI algorithm, MATLAB 2016b code was executed on computers equipped with an Intel CPU i5-7500@3.4 GHz and 16 GB of RAM. The code was not optimized for the experiments. The average code generation and matching times were recorded and are shown in Table 3.

Table 3. Processing efficiency of the GRP-DHI algorithm.

Stage of	Parameter			Average Time(s) on	Average Time(s) on
Hashed Code	m	n	q	**PolyU**	**SDUMLA-FV**
Enrollment	500	2	100	0.4373	0.3805
One time matching	500	2	100	0.3374	0.3159
Cross-matching	500	2	100	1.1364	1.2112

Due to the need to generate large numbers of independent hashing functions (for example, m = 500), it takes much less time to use the simple matcher described in the previous section for matching, but when cross-matching is involved, the time becomes longer. In addition, due to the permutation problem, the efficiency of GRP-DHI hash code generation is lower than that of the GRP-based IoM hash code. Overall, for PolyU and SDUMLA-FV, the average matching time meets the expectations for effective matching. Simultaneously, the implementation of GRP-DHI is very simple because it involves only random projection or random permutation, and simple matching can be achieved through element-by-element subtraction and counting.

5. Security and Privacy Analysis

5.1. Privacy Analysis

Non-invertibility refers to the computational difficulty of recovering finger vein feature vectors from permutation seeds or random matrices with or without GRP-DHI hashing. Suppose that an attacker tries to obtain the hash code, token, and replacement seed, and further, that the attacker understands the inner workings of the GRP-DHI algorithm and its corresponding parameters. For GRP-DHI expressed in a discrete index form, an adversary has no clue from which to guess the finger vein feature information (real value feature) directly from the stolen hashed code. In addition, the attacker knows that the token (the permutation seed and projection matrix) is also useless in recovering the finger vein feature vector because no direct relationship exists between the token and the finger vein vector; thus, the only attack mode is to attempt to guess the real value directly.

In the worst case, it is assumed that the attacker learns the minimum and maximum values of the finger vein eigenvector $\boldsymbol{x}$. Taking PolyU as an example, the minimum and maximum values of the feature vectors are -0.1560 and 0.1572, respectively. Assuming that the attacker attempts to perform guesses (e.g., -0.1560, -0.1559, -0.1558, etc.) up to the maximum value of 0.1572, they would need to try 3132 possibilities. In the implementation of the algorithm, the accuracy is kept to four decimal digits; therefore, the probability of guessing a single feature point would require an average of 3132 attempts ($\approx 2^{11}$). Therefore, a total of approximately $2^{11} \times 2^{462} = 2^{5028}$ attempts would be needed to recover the 462 feature points. The possibility of correctly guessing single and entire feature vectors is listed in Table 4. Clearly, this attack approach is computationally infeasible.

Table 4. Complexity to invert single and entire feature vectors.

Database	PolyU	SDUMLA-FV
Min. value	-0.1560	-0.1231
Max. value	0.1572	0.1427
Possibility of single feature point	3132 ($\approx 2^{11}$)	2658 ($\approx 2^{11}$)
Possibility of entire feature vector	$2^{11} \times 2^{462} = 2^{5082}$	$2^{11} \times 2^{462} = 2^{5082}$

Attacks via record multiplicity (ARM) are an example of a serious privacy attack. ARM uses multiple leaked protected templates and can be used to reconstruct the original biometrics with or without the knowledge and parameters associated with the algorithm. For GRP-DHI, because the template stored in the database is converted into a rank space unrelated to the finger vein feature space, it is difficult for ARM to infer the value used

in the calculation. Therefore, the attack complexity is the same as that of the irreversible attack in Table 4.

5.2. Security Attack Analysis

Brute-force attacks are a classic type of security attack. Using an exhaustive method to generate transformed query instances is also called an original image attack or an impersonation attack. For GRP-DHI implementation, the optimal precision configuration is $m = 500$ and $q = 100$. As the index value of the GRP-DHI hashed code is a number between 1 and 100, the attack complexity for each entry is $q = 100 > 2^6$; thus, the complexity inherent in 500 entries would require 2^{3000} attempts, which is also computationally infeasible.

Unlike ARM for privacy, ARM for other purposes is also a plausible security attack where multiple compromised protected templates (with or without knowledge of the parameters associated with the algorithm) are utilized to generate a pre-image instance. In the experiment, if the order of feature points (not necessarily numerical) and the permutation seeds are known, the simulated forged eigenvectors can be formed. Therefore, the largest value and the second largest value generated by the product of the real and forged feature vectors and Gaussian random matrix may appear in the expected position, which would damage the system.

The attack complexity of ARM is regarded as the complexity of determining the order of the feature points in finger vein vectors. For the GRP-DHI implementation in this study, let $x' = \{p_1, p_2, p_3\}$ be the final superposition inner product value and assume that p_3 is the largest characteristic point. The two inequalities $p_3 > p_2$ and $p_3 > p_1$ can be obtained. By repeating this process, multiple hashed codes can be obtained, and the attacker can recover the complete sequence information, such as $x_a > x_c > x_b$. However, the feature value contains both positive and negative values, and ARM is only valid for GRP-DHI when the biometric values are either all negative or all positive. Including mixed symbolic reasoning in the feature values makes the result uncertain. Therefore, the unequal relationship makes it infeasible to use ARM as a means of security attack.

Unlike blind guessing on the entire hashed code in a brute-force attack, a false accept attack (dictionary attack) may require far fewer attempts to gain illegitimate access. Access is allowed as long as the match score exceeds a certain threshold τ, which can significantly reduce the number of attacks needed. A complexity analysis of the GRP-DHI error acceptance attack is shown in Table 5.

Table 5. False accept attack complexity analysis.

Database	τ	m	$\tau \times m$	q	Min. Attack Complexity
PolyU	0.38	500	190	$100 > 2^6$	$2^{1140}\left(2^{30}\right)$
SDUMLA-FV	0.61	500	305	$50 > 2^5$	$2^{1525}\left(2^{25}\right)$

Taking the PolyU database as an example, Table 5 shows that when $m = 500$, $q = 100$ and FAR = FRR, the decision threshold τ is 0.38. Therefore, if the minimum number of successful access hashed index code entries is $\tau \times m = 0.38 \times 500 = 190$ and the number of projection vectors is $q = 100$, it is equivalent to an entry requiring more than $2^6 = \left(2^{\log_2 q}\right)$ guesses. Thus, the minimum complexity of the error acceptance attack is 2^{1140}, which is not feasible in actual situations.

Birthday attacks take advantage of the mathematical principle behind the probability theory of the birthday problem [27]. The attack depends on the higher collision probability found between a random attack and a fixed degree permutation (the pigeonholes principle). A birthday attack refers to a situation in which the attacker obtains a large number of hashed codes from the damaged database. This leads to a reasonable security attack where at least one conflict can be found between any two of the N_t hashed codes in

$$N_t \gg 1 \tag{16}$$

For hashed codes with a single entry $m = 1$, the expected number of attempts to find the first conflict is

$$\mathcal{Q}(\delta) = \sqrt{\frac{\pi\delta}{2}} \tag{17}$$

where δ is the maximum entry value of the DHI hashed code.

For GRP-DHI, $\delta = q$. Suppose that there are two hashed code conflicts, namely

$$h_i(X) = h_i(Y) \tag{18}$$

where $i = 1, \ldots, m$ and $h(X), h(Y) \in [1, \delta]$.

Finding the collision for element τm would require $\left(\frac{q\pi}{2}\right)^{\frac{\tau m}{2}}$ tries. A complexity analysis of GRP-DHI for the birthday attack is shown in Table 6.

Table 6. Birthday attack complexity analysis.

Database	τ	m	$\tau \times m$	q	Expected $(\frac{q\pi}{2})^{\frac{\tau m}{2}}$
PolyU	0.38	500	190	100	$>2^{102}$
SDUMLA-FV	0.61	500	305	50	$>2^{158}$
PolyU	0.06	200	12	100	$>2^{42}$
SDUMLA-FV	0.06	200	12	50	$\approx 2^{36}$

As Table 6 shows, the complexity of birthday attacks is smaller by approximately the square root level compared with the complexity of traditional false acceptance attacks. Simultaneously, the attack difficulty is closely related to the selected parameters. For example, the complexity of SDUMLA-FV is 2^{36}, which is not completely safe. However, the complexity can be further increased by enlarging m or reducing τ without affecting the performance accuracy. In short, full consideration is needed to balance the desired level of security with the performance requirements by making appropriate parameter adjustments.

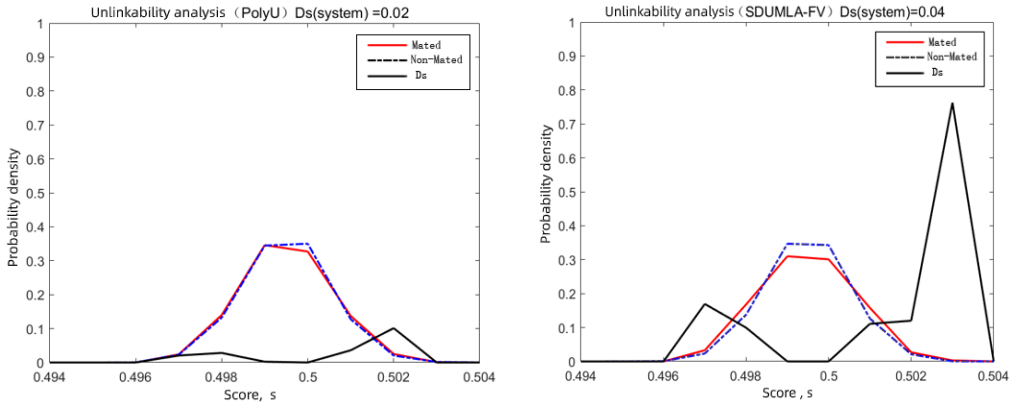
5.3. Unlinkability Analysis

According to the unlinkability requirement, multiple templates $\boldsymbol{W}$s are generated from the same biometric vector $\boldsymbol{x}$ and different factors $\boldsymbol{r}$s, and there is no link between $\boldsymbol{r}$s. Verifying the unlinkability benchmark framework of the GRP-DHI algorithm is described as follows:

(1) Calculate the score distribution model of the GRP-DHI template and mated/non-mated sample scores. Among them, the mated sample score is the template generated by the same user using different factors to calculate the similarity matching; non-mated sample score is a template generated by different users using the same factor to calculate similarity matching.

(2) The local measure $D_{\leftrightarrow}(s)$ and the global measure $D_{\underset{\leftrightarrow}{sys}}$ are used to evaluate the unlinkability [28], and the unlinkability of the cancellable template is evaluated based on the calculated results. $D_{\underset{\leftrightarrow}{sys}} \in [0, 1]$ is a measure of the complete unlinkability; the closer $D_{\underset{\leftrightarrow}{sys}}$ is to zero, the better the unlinkability is.

An unlinkability analysis of GRP-DHI on the two adopted databases is shown in Figure 6, which shows that the score distribution curves of the mated and non-mated samples overlap, which means that templates belonging to a given user or to different users cannot be distinguished. Additionally, the largest value of $D_{\underset{\leftrightarrow}{sys}} = 0.04$ (near to 0). Therefore, the GRP-DHI algorithm satisfies the unlinkability requirement.



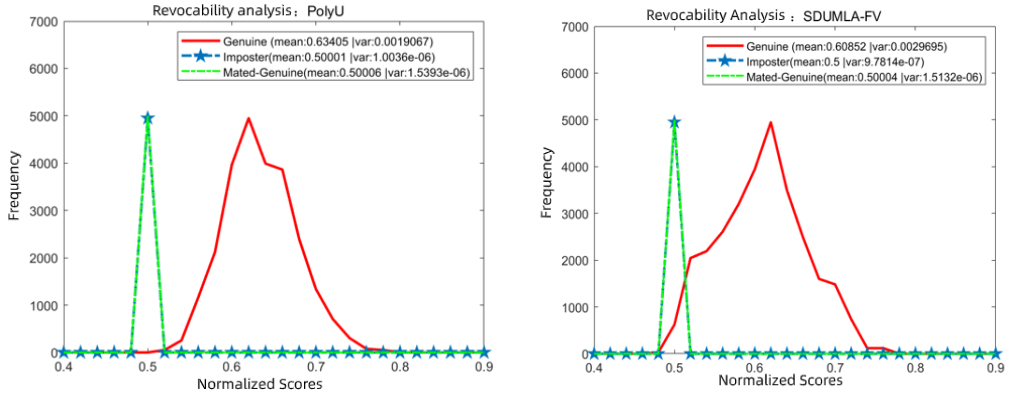
(**a**) (**b**)

Figure 6. Unlinkability analysis. (**a**) Unlinkability analysis on PolyU. (**b**) Unlinkability analysis on SDUMLA-FV.

5.4. Revocability Analysis

According to the revocability requirement, after a template has been destroyed, it is necessary to generate a new template to replace the damaged template. To prove the revocability of the algorithm, the distribution of the genuine score, imposter score and pairing mate-genuine score were calculated for each database. The steps involved in calculating the distribution of genuine matching scores were as follows. For each user, 1000 different templates were generated using 300 different random matrices and the user's feature vector 1000 times. The first template was considered to be the leaked template, while the remaining 999 were considered to be updated templates. Then, a total of 999×312 genuine scores were obtained.

As shown in Figure 7, the distribution of the genuine and imposter scores overlaps considerably, which verifies that GRP-DHI meets the revocability requirement. As seen from Table 2, stolen tokens (random matrices) do not significantly impair the performance accuracy. Therefore, a token in GRP-DHI is used only for revocability; it does not need to be kept secret from the public.



(**a**) (**b**)

Figure 7. Revocability analysis. (**a**) Revocability analysis on PolyU. (**b**) Revocability analysis on SDUMLA-FV.

6. Conclusions

In this study, a two-factor cancellable finger vein template protection scheme based on general sorting (GRP-DHI) was proposed. The theoretical proofs and experimental results show that due to the good characteristics of local random projection, GRP-DHI

maintains the matching accuracy to a large extent compared with the corresponding features before transformation. GRP-DHI also meets the cancellable template protection standard and has strong robustness against the existing major security and privacy attacks when adjusted properly. Planned future work addresses two directions that could remove the remaining limitations of the hashing index. The first direction is to extend the work to an unordered variable-sized representation. The second direction involves integrating biometric cryptographic primitives, in which the key and privacy disclosure framework can be combined for privacy protection analysis.

Author Contributions: Conceptualization, X.H. and L.Z.; Data curation, X.H.; Formal analysis, H.W.; Investigation, H.W.; Methodology, X.H. and L.Z.; Resources, H.W., J.Z. and L.T.; Software, X.H. and L.Z.; Visualization, J.Z. and L.T.; Writing—original draft, X.H. and L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Key Discipline of Hefei University 2018xk03. It was supported in part by the Anhui Provincial College Top Talents Program under Grant gxbjZD48, in part by the National Natural Science Foundation of China under Grant 61372137, and the Natural Science Foundation of Anhui Province under Grant 1908085MF209.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: PolyU database: http://www4.comp.polyu.edu.hk/~csajaykr/fvdatabase.htm, SDUMLA-FV database: http://mla.sdu.edu.cn/sdumla-hmt.html (accessed on 1 December 2021).

Acknowledgments: The authors are deeply thankful to the reviewers and editor for their valuable suggestions to improve the quality of the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bolle, R.M.; Connell, J.H.; Ratha, N.K. Biometrics perils and patches. *Pattern Recognit.* **2002**, *35*, 2727–2738. [CrossRef]
2. Patel, V.M.; Ratha, N.K.; Chellappa, R. Cancelable Biometrics: A review. *IEEE Signal Process. Mag.* **2015**, *3*, 54–65. [CrossRef]
3. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric Template Security. *EURASIP J. Adv. Signal Process* **2008**, *113*, 1–17. [CrossRef]
4. Teoh, A.B.J.; Ling, D.N.C.; Goh, A. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognit.* **2004**, *37*, 2245–2255.
5. Nanni, L.; Lumini, A. Random subspace for an improved Biohashing for face authentication. *Pattern Recognit. Lett.* **2008**, *29*, 295–300. [CrossRef]
6. Rathgeb, C.; Breitinger, F.; Busch, C. On application of bloom filters to iris biometrics. *IET Biom.* **2014**, *3*, 207–218. [CrossRef]
7. Hermans, J.; Mennink, B.; Peeters, R. When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system. In Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 1–6.
8. Bringer, J.; Morel, C.; Rathgeb, C. Security analysis of Bloom filter based iris biometric template protection. In Proceedings of the International Conference on Biometrics, Phuket, Thailand, 19–22 May 2015; pp. 527–534.
9. Jin, Z.; Hwang, J.Y.; Lai, Y.L. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 393–407. [CrossRef]
10. Hartung, D.; Busch, C. Why vein recognition needs privacy protection. In Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 12–14 September 2009; pp. 1090–1095.
11. Favre, M.; Picard, S.; Bringer, J. Balancing is the key: Performing finger vein template protection using fuzzy commitment. In Proceedings of the 2015 International Conference on Information Systems Security and Privacy (ICISSP), Angers, France, 9–11 February 2015; pp. 1–8.
12. Yang, W.; Hu, J.; Wang, S. A finger-vein based cancellable biocryptosystem. In Proceedings of the International Conference on Network and System Security, Madrid, Spain, 3–4 June 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 784–790.
13. Hartung, D.; Tistarelli, M.; Busch, C. Vein minutia cylinder-codes (v-mcc). In Proceedings of the International Conference on Biometrics (ICB), Madrid, Spain, 4–7 June 2013; pp. 1–7.
14. Hartung, D.; Olsen, M.A.; Xu, H. Comprehensive analysis of spectral minutiae for vein pattern recognition. *IET Biom.* **2012**, *1*, 25–36. [CrossRef]
15. Gomez-Barrero, M.; Rathgeb, C.; Li, G. Multi-biometric template protection based on bloom filters. *Inf. Fusion* **2018**, *42*, 37–50. [CrossRef]

16. Adamovic, S.; Milosavljevic, M.; Veinovic, M.; Sarac, M.; Jevremovic, A. Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biom.* **2017**, *6*, 89–96. [CrossRef]
17. Adamovic, S.; Milosavljevic, M.; Veinovic, M.; Sarac, M.; Jevremovic, A. Information-Theoretic Analysis of Iris Biometrics for Biometric Cryptography. *Acta Polytech. Hung.* **2017**, *14*, 47–62.
18. Adamovic, S.; Miskovic, V.; Macek, N.; Milosavljevic, M.; Šarac, M.; Saračević, M.; Gnjatovic, M. An efficient novel approach for iris recognition based on stylometric features and machine learning techniques. *Future Gener. Comput. Syst.* **2020**, *107*, 144–157. [CrossRef]
19. Bartal, Y.; Recht, B.; Schulman, L.J. Dimensionality reduction: Beyond the Johnson-Lindenstrauss bound. In Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, San Francisco, CA, USA, 23–25 January 2011; pp. 868–887.
20. Yagnik, J.; Strelow, D.; Ross, D.A. The power of comparative reasoning. In Proceedings of the 2011 International Conference on Computer Vision, Barcelona, Spain, 6–13 November 2011; pp. 2431–2438.
21. Mroueh, Y.; Rennie, S.; Goel, V. Random maxout features. *arXiv* **2015**, arXiv:1506.03705.
22. Charikar, M.S. Similarity estimation techniques from rounding algorithms. In Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing, Montreal, QC, Canada, 19–21 May 2002; pp. 380–388.
23. Ye, L.L.; Wang, H.B.; Shi, Y. Cancelable Finger Vein Template Based on Variable Curvature Gabor Gilter and Improved Canonical Correlation Analysis. In Proceedings of the 2019 IEEE 2nd International Conference on Information Communication and Signal Processing (ICICSP), Weihai, China, 28–30 September 2019; pp. 410–414.
24. Yang, L.; Yang, G.; Wang, K. Point Grouping Method for Finger Vein Recognition. *IEEE Access* **2019**, *7*, 28185–28195. [CrossRef]
25. Pritee, K.; Kaur, H.; Khanna, P. Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 709–719.
26. Leng, L.; Teoh, A.B.J.; Li, M. Simplified 2DPalmHash code for secure palmprint verification. *Multimed. Tools Appl.* **2017**, *76*, 8373–8398. [CrossRef]
27. McKinney, E.H. Generalized birthday problem. *Am. Math. Mon.* **1966**, *73*, 385–387. [CrossRef]
28. Gomez-Barrero, M.; Galbally, J.; Rathgeb, C. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 1406–1420. [CrossRef]