Available online at www.HighTechJournal.org

HighTech and Innovation Journal

ISSN: 2723-9535

Vol. 4, No. 2, June, 2023

Finger Vein Template Protection with Directional Bloom Filter

Jackson Horlick Teng [1], Thian Song Ong [1*], Kalaiarasi S. M. A. [1], Connie Tee [1]

[1] *Faculty of Information Science and Technology, Multimedia University, Melaka 75450, Malaysia.*

Received 28 January 2023; Revised 03 May 2023; Accepted 11 May 2023; Published 01 June 2023

Abstract

Biometrics has become a widely accepted solution for secure user authentication. However, the use of biometric traits raises serious concerns about the protection of personal data and privacy. Traditional biometric systems are vulnerable to attacks due to the storage of original biometric data in the system. Because biometric data cannot be changed once it has been compromised, the use of a biometric system is limited by the security of its template. To protect biometric templates, this paper proposes the use of directional bloom filters as a cancellable biometric approach to transform the biometric data into a non-invertible template for user authentication purposes. Recently, Bloom filter has been used for template protection due to its efficiency with small template size, alignment invariance, and irreversibility. Directional Bloom Filter improves on the original bloom filter. It generates hash vectors with directional subblocks rather than only a single-column subblock in the original bloom filter. Besides, we make use of multiple fingers to generate a biometric template, which is termed multi-instance biometrics. It helps to improve the performance of the method by providing more information through the use of multiple fingers. The proposed method is tested on three public datasets and achieves an equal error rate (EER) as low as 5.28% in the stolen or constant key scenario. Analysis shows that the proposed method meets the four properties of biometric template protection.

Keywords: Multi-Instance Finger Vein; Directional Bloom Filter; Template Protection.

1. Introduction

A biometric system is used to verify an individual's identity through their biometric traits, such as voice, facial features, and finger veins, among others. It is a preferable alternative to knowledge and token-based systems, as biometrics cannot be easily misplaced, shared, or stolen. In recent years, finger vein biometrics has become increasingly popular as a type of hand-based biometric for access control systems and financial applications, in comparison to other biometric traits such as fingerprint, palmprint, and hand geometry. A finger vein is an image of the blood vessels inside a finger taken with an infrared or near-infrared imaging system. The hemoglobin in blood vessels absorbs near-infrared light, causing the veins to appear as a unique structure in the resulting image. Since the veins are located inside the finger, they are less susceptible to noise and damage, making them well-suited for user authentication [1].

On the other hand, multimodal biometric systems refer to the use of multiple biometric traits for a biometric system. Multimodal biometrics has several advantages as compared to unimodal biometrics: better accuracy, better universality, more robustness to impostor attacks, and fault tolerance. Generally, multimodal biometric systems can be categorized based on their information source as multi-trait, multi-sensor, multi-algorithm, multi-instance, and multi-sample. This paper focuses on a multi-instance biometric system that uses several instances of a biometric trait for recognition, such as the index, middle, and ring fingers. Multi-instance biometrics has the advantage of low cost as it requires only one sensor for enrollment and verification [2].

* Corresponding author: tsong@mmu.edu.my

http://dx.doi.org/10.28991/HIJ-2023-04-02-013

The use of biometrics has raised serious concerns about personal data security and privacy. The main reasons are that biometric traits are not renewable; they cannot be easily replaced or cancelled because they are inherently associated with the user. Also, if the data from the biometric trait is stolen, it will be compromised permanently and cannot be used in other systems anymore. To resolve the security and privacy issues, the idea of a biometric template protection (BTP) scheme has been proposed. Template protection is a method to protect biometric data by storing the transformed template rather than raw biometric data in a biometric system [3]. A properly specified BTP scheme should have the following properties, according to [4]:

- Irreversibility: the template is very difficult to invert back to original biometric data.
- Renewability: compromised template can be revoked, and a new one can be reissued from the same biometric data.
- Unlinkability: the template does not allow cross-matching across databases to protect user's privacy.
- Performance: the template does not degrade the recognition accuracy of the system.

The proposed multi-instance finger vein template protection method is divided into four major modules: pre-processing, feature extraction, feature transformation, and matching. Pre-processing is first used to segment the finger from the background and make the input image easier to use for the rest of the system. It consists of: watershed segmentation, morphological operation, contrast-limited adaptive histogram equalization, and resize. Next, a modified Frangi method is adopted as the feature extraction approach to segment the vein and convert it into a feature vector. Subsequently, feature transformation is performed with row-wise permutation, a random XOR operation, and followed by directional bloom filter for template generation. Matching is then conducted in the transformed domain by using hamming distance matcher. The proposed system is tested on three publicly available datasets for performance evaluation and security analysis. Prior Bloom filter research [5, 6] has primarily focused on their use in iris and facial recognition, demonstrating their potential in template protection. While Cai et al. [7] investigate the use of a bloom filter for finger veins, this paper introduces the directional Bloom filter as an attempt to improve on the traditional Bloom filter for finger vein template protection. This improved version innovates by employing directional subblocks for hash vector generation, as opposed to the original Bloom filter's single column subblock. Furthermore, a significant contribution to our work is the implementation of multi-instance finger vein identification. Unlike Cai et al. [7], which employ a single instance, our approach employs multiple instances, which enriches the template and may provide more reliable results.

The remainder of the paper is organized as follows: Section 2 presents the works related to template protection, Section 3 outlines the contributions, Section 4 describes the proposed system, Section 5 presents the experimental results, Section 6 summarizes the experiments, and Section 7 provides the conclusion.

2. Related Works

Typically, BTP comes in two major categories: cancellable biometrics and biometric cryptosystems. This paper presents a cancellable biometric-based template protection method. Cancellable biometrics works by performing a transformation on biometric data to generate a template. The transformation function can be invertible or non-invertible. In a non-invertible transform, an attacker cannot reverse or reconstruct the original biometric data from the template even when the secret key is compromised. Another benefit of cancellable biometrics is that it ensures matching in the transformed domain by securely converting the biometric data into a new template, which is then stored in a secure database and used for authentication. When a user presents their biometric data for authentication, the system applies the same transformation process to the input data and compares the transformed data with the stored transformed data. Since the transformation is secure and irreversible, it is computationally infeasible to derive the original biometric data from the transformed data. This ensures that the original biometric data remains private and secure while still allowing for accurate matching in the transformed domain [3].

To date, cancellable biometrics has been adopted successfully in different biometric traits, such as fingerprint [8-10], face [10-12], iris [13-15], palmprint [16-18], online signature [19-21], and others. In this research, we focus on cancellable biometrics, more specifically non-invertible transform [22]. Non-invertible transform is chosen because template protected by invertible transform or salting can be recovered to original biometric data if an attacker has access to the secret key. Nevertheless, in non-invertible transform, the template cannot be reverted, making it more secure. Specifically, our research focuses specifically on the use of Bloom filter as BTP. The adaptability of Bloom filter-based template protection to various biometric modalities represented by binary templates, such as face [6], iris [5], or fingerprint [23], is one of its primary advantages over other approaches. Bloom filters are distinguished by their flexibility, making them an ideal foundation for developing a refined version known as directional bloom filter (DBF).

Li et al. [18] proposed a BTP method for palmprint biometrics using randomized cuckoo hashing and MinHash. It works by, firstly, extracting the palmprint binary feature using an anisotropic filter. The feature was then resized to a quarter of its original size. It was then XOR with a random block. The XORed feature was then divided into non-overlapping blocks. Each block was Hadamard product with two random complementary matrices to generate two

different subblocks. Cuckoo hashing was performed for each subblock to generate two hash vectors. After that, MinHash was performed on each hash vector to generate a hash code. All of the hash codes were then concatenated to form the template. In this BTP method, Cuckoo hashing worked by having two empty hash vectors. Each column in a subblock was converted from binary to decimal. Each of the decimal values was then used as an index of the first hash vector to set its value to 1. If the first hash vector value was already set in the index, the column was once again converted from binary to decimal using gray encoding. The index was then used to set the value of the second hash vector to 1. MinHash worked by permuting the hash vector and recording the index of the first active bit. The permutation was done several times, and then the indexes were used as the hash code. The system used Jaccard distance as the matcher. The system was tested on PolyU database with the lowest EER of 2.67% and D_{sys} of 4%.

The bloom filter was used for face biometrics in Gomez-Barrero et al. [6]. Firstly, a binary feature was extracted from the face image. It was then divided into non-overlapping blocks. The blocks were then grouped into several groups. After that, each group was row permuted. The groups were then divided back into blocks. Following that, each block was used in bloom filter to generate a hash vector. The concatenated hash vectors were the template. The bloom filter worked by taking each column from the block, and then converting it from binary to decimal. The decimal value was used as an index of a hash vector to set its value to 1. The system was tested on the face subcorpus of the Desktop Dataset (DS2) of the BioSecure Multimodal Database with the lowest EER of 6.1% and D_{sys} of 9%.

In Rathgeb et al. [5] a method applied to iris biometrics called adaptive bloom filter is introduced. It began from the binary feature extracted from the iris image. It was then divided into non-overlapping blocks. For each block, bloom filter was performed to generate a hash vector. The concatenated hash vectors formed the template. The bloom filter worked by initially creating an empty hash vector. Each column of the block was then XORed with a random vector generated by an application specific secret key. The column was then converted from binary to decimal, which was then used as an index to set the value of the hash vector to 1. The iris texture of an iris image was segmented by using weighted adaptive Hough algorithm. The system was tested with two feature extractors: Log-Gabor filter and dyadic wavelet transform. In Log-Gabor filter, the iris texture was first divided into stripes (row-wise division of an image). Each stripe was row-wise averaged to get a signal. The signal was then convolved with a Log-Gabor filter. The outputted phase signal was discretized into two bits. The concatenation of the discretized signals was used as the feature. In dyadic wavelet transform, the iris texture was first converted to the row-wise averaged signal from the striped texture. Each signal was then transformed with dyadic wavelet transform, generating two subbands. For each subbands, its local minima and maxima above a threshold is located and the region between the extreme points was alternated with 0 and 1 bits. The concatenated subbands were the features. The system used fractional Hamming distance as the matcher and achieved the lowest EER of 1.14% when tested on the CASIA-v3-Interval iris database for performance evaluation.

Kirchgasser et al. [24] proposed a template protection method for finger veins using alignment-robust hashing (ARH) and index-of-maximum (IoM) hashing. It began by first determining the region of interest (ROI) from the finger vein image. After that, a high-frequency emphasis filter, a circular Gabor filter, and contrast-limited adaptive histogram equalization were applied to the ROI to enhance finger vein visibility. The proposed system was tested with several well-established feature extractors for finger veins. Next, the feature set was transformed using ARH and IoM hashing for template protection. Specifically, ARH divides the feature into a grid of non-overlapping blocks and flattens each block to one dimension. It then histograms the distances between two active bits and concatenates the resulting hash vectors to form the ARH template. IoM hashing, on the other hand, computes the inner product between the ARH template and several random Gaussian vectors generated by a secret key. The index of the maximum value of the result was then saved. This was repeated several times, and the results were saved as the IoM template. The template was matched by calculating the number of times the reference template appeared the same as the query template. The proposed BTP method was tested on the University of Twente Finger Vascular Pattern (UTFVP) database and the PLUSVein-FV3 Dorsal-Palmar finger vein database (PLUSVein-FV3), which contains two subsets: laser palmar (PLUS Laser) and led palmar (PLUS LED). The lowest EER was 3.89% (UTFVP), 3.79% (PLUS Laser), and 4.08% (PLUS LED). The lowest was 5.2% (UTFVP), 6.1% (PLUS Laser), and 5.2% (PLUS LED).

Cai et al. [7] proposed a template protection method for finger veins using the Gabor filter and Bloom filter. Firstly, the Gabor filter is used to detect the ridges in the images. The Gabor filter works by convolving the image with several kernels of varying frequencies and orientations, which generate several sub-images. The sub-images are then combined by averaging, and then they are masked to get the region of interest (ROI) image. The ROI image is then thresholded with adaptive thresholding to binarize the finger vein. Morphological operations are also used to remove noise. The feature is then divided into non-overlapping blocks. The blocks are then concatenated, and their rows are permuted. After that, each block is a Hadamard product with a random matrix. The bloom filter is then done for each block, where for each column in each block, it is mapped to an index according to a hash function. The indexes are then used to set the bits in the hash vector to 1. The concatenated hash vectors are the feature vectors. When using multiple fingers, the proposed system is tested at two fusion levels: image fusion and feature fusion. The method is evaluated on three different public datasets, with an EER as low as 5%.

On the other hand, template protection by applying block remapping and block warping to vein patterns in the image domain was designed by Kirchgasser et al. [25]. First, the finger vein feature is extracted from the finger vein image using a feature extractor. The feature is then transformed using either block remapping or block warping to create a template. The template is then matched by using image correlation. Block remapping works by dividing the feature image into non-overlapping blocks. The blocks are then randomly selected with replacements (with a user defined ratio of redundant blocks) to create a template. Block warping works by dividing the feature image into non-overlapping blocks. The output image template is subjected to random distortion using a grid, and each distorted block is then filled with the content of its original block through spline interpolation. The proposed method is tested with various feature extractors, including the Gabor filter, isotropic undecimated wavelet transform, maximum curvature, principal curvature, repeated line tracking, and wide line detector. The lowest EER obtained with block remapping was 3.27% for UTFVP, 15.52% for PLUS Laser, and 4.42% for PLUS LED. The lowest EER achieved with block warping was 0.71% for UTFVP, 2.02% for PLUS Laser, and 1.00% for PLUS LED.

Ren et al. [26] introduced a template protection method for finger vein using Rivest-Shamir-Adleman (RSA) encryption. Firstly, the RSA algorithm is used to generate an encryption key and public modulus. The finger vein image is then encrypted by transforming each pixel with the key and modulus. There are two proposed variations of the transformation: local binary pattern (LBP) or direct. LBP denotes that the finger vein image is first transformed with LBP before the LBP feature is encrypted using the key and modulus. The key and modulus are used to directly encrypt the finger vein image. The encryption output is then normalised using pixel normalisation. After normalization, image enhancement is used. Several image enhancements are tested: mean filtering, histogram equalization, gamma transform, Gaussian filtering, and median filtering. The images are then normalised in terms of position, rotation, and scale of the images. Registration is done by using a spatial transformer module. The image is then classified using a residual network with squeeze and excitation block, a type of convolutional neural network. SDUMLA-HMT, MMCBNU_6000, HKPU, and FV-USM databases were used to test the proposed system. The proposed system has the highest accuracy: 96.698% (SDUMLA-HMT), 99.667% (MMCBNU_6000), 99.038% (HKPU), and 99.593% (FV-USM). The proposed system has the lowest EER: 2.137% (SDUMLA-HMT), 0.090% (MMCBNU_6000), 0.277% (HKPU), and 0.091% (FV-USM).

Ghouzali et al. [27] proposed using a logistic map and torus automorphism to protect face and fingerprint templates. The face and fingerprint are processed independently before being fused using score fusion. First, minutiae are extracted for fingerprinting. Torus automorphism is then used to transform the fingerprint minutiae into a template. The fingerprint minutiae are then transformed into a template by using torus automorphism. Torus automorphism works by randomly distributing the minutia points according to some parameters following a chaotic sequence. For the face, it is resized to 8×8 which is then convolved with a randomly generated user-specific kernel using logistic map. For matching, the system uses Euclidean distance for fingerprint matching and Cosine distance for face matching. The scores are then normalized using performance anchored normalization and then summed using weighted sum. The proposed system is then tested using ORL face database and FVC2002 DB1 fingerprint database. The lowest EER of the proposed system is 0%.

Bassit et al. [28] investigated the use of iris recognition system template protection using bloom filter (BF) and homomorphic encryption (HE). This paper proposed combining BF and HE to take advantage of each method's strengths. BF has been shown to be either fast and accurate but not unlinkable. Meanwhile, HE is precise and unlinkable, but it is slow. The proposed system then combined them in order to be precise, unlinkable, and fast template protection system. The proposed system achieved an EER of 0.17% for the IITD iris database, with a runtime of 104.35 ms for 128 bits, 155.15 ms for 192 bits, and 171.70 ms for 256 bits, respectively.

3. Contributions

In general, a biometric system requires higher security and privacy to enjoy its benefits, compared to knowledge and token-based authentication. This is because biometric data is permanently unusable once it is compromised, and it is inherently linked to a person's identity. To deal with these issues, this paper contributes the following:

- The use of multi-instance finger vein biometrics as a means of improving the performance of biometric systems. Biometric systems, unlike knowledge-based and token-based systems, are imperfect and cannot authenticate a user with complete accuracy all the time. Enhancing performance, therefore, remains a main concern in biometric system design. Multi-instance biometrics has been found to be a promising method for enhancing the performance and security of a biometric system. By combining information from multiple fingers into a single template, attackers must compromise multiple fingers simultaneously to successfully breach the system. Additionally, template protection method makes it difficult to revert back to the original biometric data, thereby improving the security of the biometrics. Multi-instance biometrics can also be used to deter spoofing in challenge-response type systems, where the system prompts the user to present the biometric data in a random order to confirm the user's identity. The main focus of this research, therefore, is to design secure template protection for a multi-instance finger vein system.

- This paper proposes the use of feature transformation for template protection, which includes row-wise permutation, random XOR operation, and directional bloom filter. The row-wise permutation and random XOR operation enhance the template's unlinkability and renewability. Renewability is achieved by generating different templates using different secret keys. Unlinkability is achieved by distributing the finger vein feature set differently using different secret keys, making it difficult to perform cross-matching across different systems for a user's finger vein.
- Directional bloom filter (DBF) is used to add the required security and privacy in a biometric system. Directional bloom filter is an improvement over the original bloom filter by using different rows, columns, and diagonals subblocks from the blocks instead of just the columns subblocks. The use of more subblocks means there are more active bits in the hash vector, which makes the template more secure. The proposed DBF fulfills the four properties of a good template protection method: irreversibility, renewability, unlinkability and performance, which will be vindicated with the experimental analysis in Section 5.

4. Research Methodology

4.1. Overview

The proposed system can be divided into preprocessing, feature extraction, feature transformation, and matching. Preprocessing is used to improve the input image for the subsequent step. Feature extraction is used to get the finger vein feature from the image. Feature transformation is used to perform an invertible transform to secure the finger vein feature as a template. Matching is used to determine whether the template belongs to a user. The overview of the system can be seen in Figure 1.

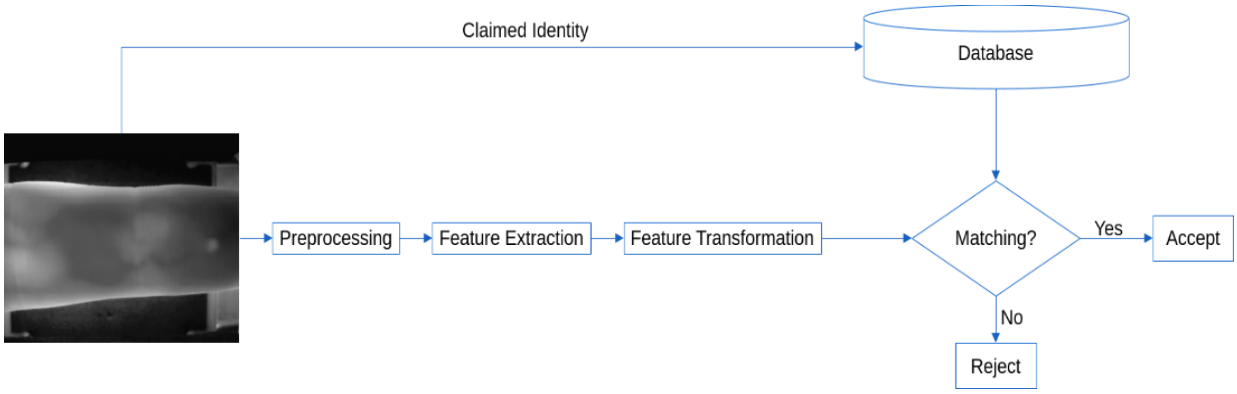


Figure 1. Overview of the system

4.2. Preprocessing

Watershed segmentation, morphological operation, contrast-limited adaptive histogram equalization (CLAHE), and image resizing are all part of the preprocessing steps. To separate the finger from the background, watershed segmentation is used. It works by converting the input image into a height or elevation map based on pixel values and then flooding the basins with user-defined markers. The markers show if the flooded area is the region of a finger vein or a background. After that, a morphological operation is used to remove any remaining background. Because the finger region is typically large and grey, it accomplishes this by removing small and dark regions. CLAHE is then used to improve image contrast by more evenly distributing pixel values using histograms. It differs from regular histogram equalization in that it calculates the local histogram of an image divided into blocks rather than the global histogram calculated from the entire image. Finally, image resizing is done to change the size of the input image to a fixed size to be used for subsequent matching purposes. The overall preprocessing steps can be seen in Figure 2.

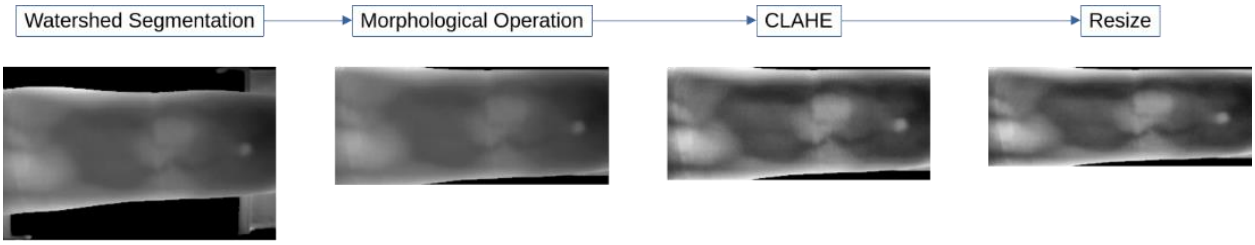


Figure 2. Preprocessing

4.3. Feature Extraction

In this work, a modified Frangi filter is used as the feature extractor. It consists of: Frangi filter, thresholding, and flood fill. Frangi filter is used to extract the vein from the finger image. Frangi et al. [29] proposed the use of the eigenvalues of the Hessian matrix of an image to detect blood vessels. The Hessian matrix of an image is the second order derivative of an image that gives information about the local structure of the 2D image. It can be obtained by analyzing its eigenvalues. Eigenvalue analysis works by finding the two principal directions (eigenvectors) and magnitudes (eigenvalues) of the curvature of the image. The two eigenvectors and eigenvalues describe the second order ellipsoid of the image. The second order ellipsoid has an intuitive geometrical interpretation of its eigenvalues. If an eigenvalue is positive, it means that it is concave up (a valley) and if an eigenvalue is negative, it means that it is concave down (a ridge). Also, when one of the eigenvalues is small and the other is big, it means that it is tubular (a finger vein). If both eigenvalues are small, it means that it is a noise (background). Meanwhile, if both eigenvalues are big with the same sign and magnitude, it means that it is blob-like. The Hessian of an image is approximately calculated by convolving the image with the second order derivative of a Gaussian kernel.

Let $I(x,y)$ be the preprocessed image with x and y be the pixel coordinate of the image, then the Hessian $H_s(x,y)$ of $I(x,y)$ at Gaussian scale s is:

$$H_s(x,y) = s^2 I \frac{(x,y) * \partial^2}{\partial x \partial y} G_s(x,y) \tag{1}$$

where $*$ is the convolution operator and the Gaussian function $G_s(x,y)$ is:

$$G_s(x,y) = \frac{1}{\sqrt{2\pi s^2}} exp\left(\frac{-x^2+y^2}{2s^2}\right) \tag{2}$$

Let $\lambda_{s.k}$ be the eigenvalues to the corresponding eigenvectors $u^{\wedge}_{s.k}$ of the Hessian H_s for Gaussian scale s and $k \in D$ dimensional input image, where:

$$\lambda_{s,k} = \hat{u^T_{s,k}} H_s u^{\wedge}_{s,k} \tag{3}$$

The λ_k is ordered in ascending magnitude, where:

$$|\lambda_1| \leq |\lambda_2| \tag{4}$$

The eigenvalues relations can be computed as a ratio R_B that measures deviation from blob-like structure. The ratio is defined as:

$$R_B = \frac{|\lambda_1|}{|\lambda_2|} \tag{5}$$

Another measure is the second order structureness S, that measures the contrast of a region by calculating the Frobenius matrix norm of the Hessian $\|H\|_F$. It is used to remove the background from structures by taking into account the vein structure, which is a small structure with a high contrast. It is defined as:

$$S = \|H\|_F = \sqrt{\sum \lambda_k^2} \tag{6}$$

The measures are combined into one as a vesselness measure V with β and c as user-defined variables to control the measures, which is defined as

$$V_s = \begin{cases} 0 & \lambda_2 = 0 \\ exp\left(\frac{-R_B^2}{2\beta^2}\right)\left(1 - exp\left(\frac{-S^2}{2c^2}\right)\right) & \lambda_2 > 0 \end{cases} \tag{7}$$

The vesselness measure is performed for each Gaussian scale s with s_{min} and s_{max} the minimum and maximum scales at which the relevant structures are expected to be found. They are combined into one by:

$$V = \max_{s_{min} \leq s \leq s_{max}} V_s \tag{8}$$

Thresholding is then used to binarize the output of the Frangi filter V, by comparing the value to a constant. Let $I_T(x,y)$ be the image after thresholding is formulated as:

$$I_T(x,y) = V(x,y) > 0 \tag{9}$$

Flood fill is used to remove falsely detected finger vein. It does so by selecting a contiguous region that is connected to a user-defined point, and changing its label to background. The user-defined point is set to the centroid of black regions in the image, since the background is typically black. The feature extraction can be seen in Figure 3.

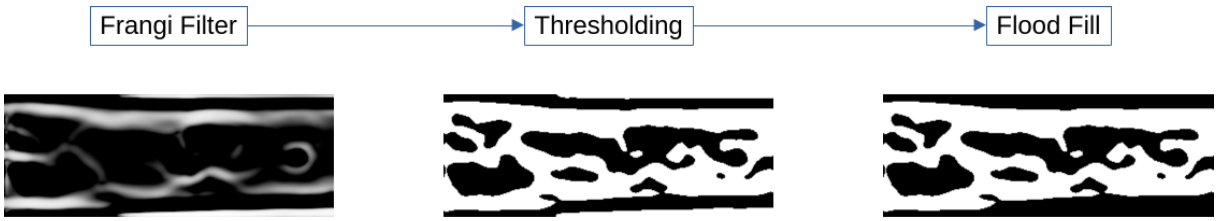


Figure 3. Feature extraction

4.4. Feature Transformation

Our work is inspired by bloom filter-based template protection [6]. The proposed direction bloom filter (DBF) is an enhanced version of bloom filter based on the transformation of feature set into rows, columns, and diagonal subblocks, instead of just using a column subblock for template generation. This helps to increase the number of active bits in the hash vector to strengthen the irreversibility of BTP. Besides, the proposed method also includes XORing the block with a randomly generated block, and thus improving unlinkability.

In this paper, multi-instance finger vein recognition system has been implemented with DBF for improved performance and security. The use of multiple fingers increases the amount of information available for classification and enhances security by requiring an attacker to compromise multiple fingers to attack the system. For multi-instance DBF template protection, two distinct fusion strategies, namely feature fusion and template fusion, are designed (see Figure 6).

For feature transformation, the proposed directional bloom filter (DBF) works by first dividing the feature into non-overlapping blocks B where $B = \{b_1, \dots, b_{\text{n blocks}}\}$ where n_blocks = n_rows × n_cols. n_rows and n_cols refer to the number of rows and columns the feature is divided into, respectively. Each block b has the size of n_block_rows × n_block_cols:

$$b = \begin{Bmatrix} p_{1,1} & \cdots & p_{1,\text{n\_blocks\_cols}} \\ \vdots & \ddots & \vdots \\ p_{\text{n\_block\_rows},1} & \cdots & p_{\text{n\_block\_rows,n\_block\_cols}} \end{Bmatrix} \quad (10)$$

where p is the pixel value of the block.

The rows of the blocks are permuted according to a secret key across all the blocks. Each block is then XORed with r where r is a randomly generated block according to a secret key. Each block is then used to generate a hash vector h and $H = \{h_1, \dots, h_{\text{n\_blocks}}\}$. The overall framework of the feature transformation scheme is portrayed in Figure 4.

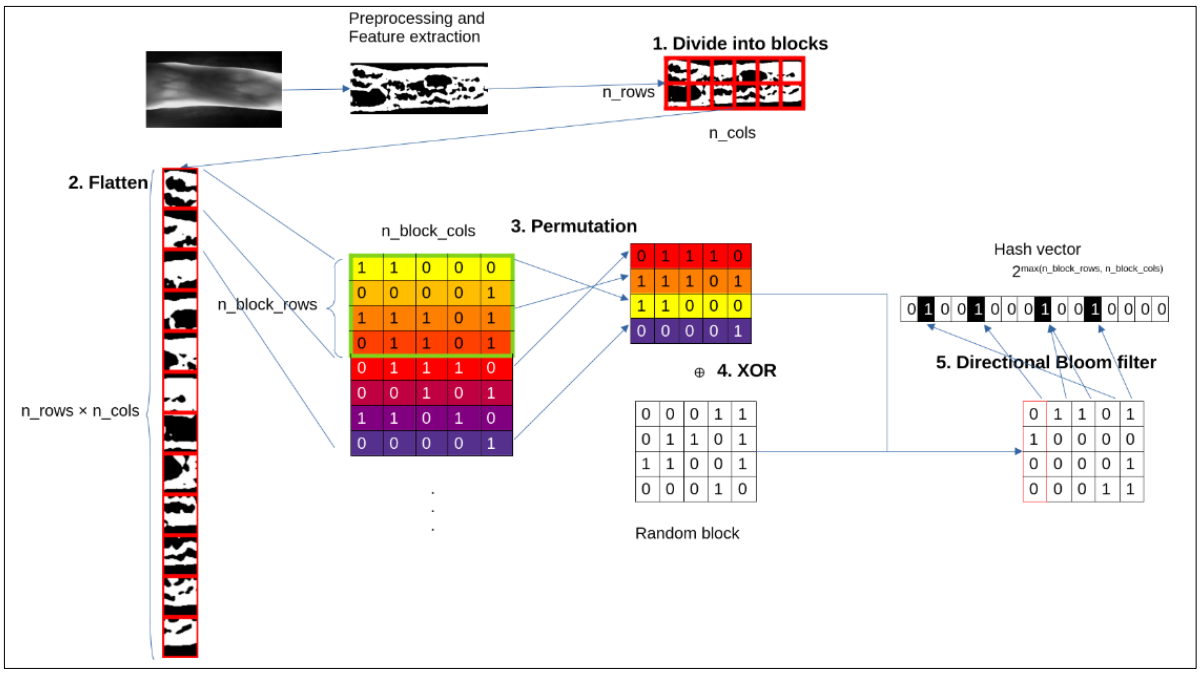


Figure 4. Directional bloom filter-based feature transformation

The hash vector h is generated by dividing the block b to subblocks S. The subblocks S correspond to the rows s_r, columns s_c, and diagonals s_d of the block where $s_r^i = \{p_{i,1}, \dots, p_{i,\text{n block cols}}\}$, $s_c^j = \{p_{1,j}, \dots, p_{\text{n block rows},j}\}$, and s_d^k is defined as:

$$s_d^k = \begin{cases} \{p_{1,1+k}, p_{2,2+k}, \dots, p_{\text{n\_block\_rows,n\_block\_cols}+k}\} & k > 0 \\ \{p_{1,1}, p_{2,2}, \dots, p_{\text{n\_block\_rows,n\_block\_cols}}\} & k = 0 \\ \{p_{1+k,1}, p_{2+k,2}, \dots, p_{\text{n\_block\_rows}+k,\text{n\_block\_cols}}\} & k < 0 \end{cases} \quad (11)$$

where the block is padded with zeros for the index greater than the block size.

Each subblock s is then used to generate an index $f(s)$ using a hash function f (a binary to integer function). The value of the hash vector is set to 1 in the position determined by the generated index, $h^{f(s)} = 1$. The implementation of directional Bloom filter can be seen in Figure 5.

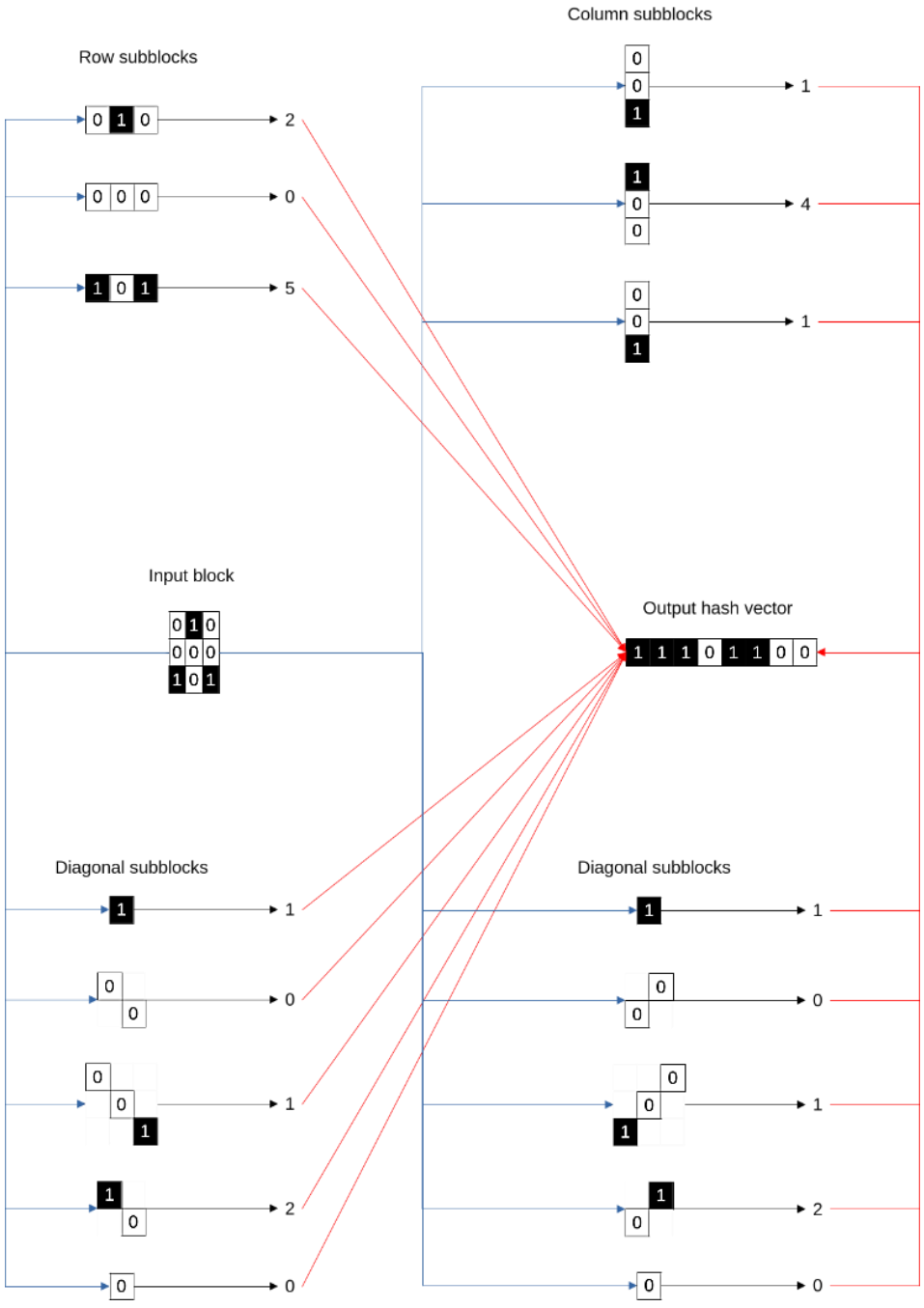


Figure 5. Directional bloom filter

The overall flow of the proposed DBF method is presented step-by-step in the form of pseudocode that can be found in Algorithm 1.

Input: image I, secret key K
Output: template H
// create a pseudo random number generator with the secret key
$prng \leftarrow$ GetPRNG(K);
// perform Frangi feature extraction and thresholding
$I \leftarrow$ GetFrangi(I) > 0;
// divide feature into $n\_rows \times n\_cols$ blocks with the size of each block as $n\_block\_rows \times n\_block\_cols$
$B \leftarrow$ ViewAsBlocks($I, (n\_block\_rows, n\_block\_cols)$);
// reshape the 4D array to 2D array, -1 means the rest
$B \leftarrow B.reshape(-1, n\_block\_cols)$;
// perform random row permutation
$B \leftarrow prng.permutation(B, axis = 0)$;
// reshape the 2D array to 3D array
$B \leftarrow B.reshape(-1, n\_block\_rows, n\_block\_cols)$;
// run for each block b with index i from blocks B
for $b_i \in B$ **do**
  // randomly generate binary block r with the same size as block b
  $r_i \leftarrow prng.integers(2, size = b_i.shape)$;
  // XOR block b with block r
  $b_i \leftarrow b_i \oplus r_i$;
  // find the maximum
  $n\_bits \leftarrow$ GetMax(n_block_rows, n_block_cols);
  // generate an empty array with the size 2^{n_bits}
  $h_i \leftarrow$ GetZeros(2^{n_bits});
  $S \leftarrow$ GetSubblocks(b_i);
  for $s_j \in S$ **do**
    $k \leftarrow f(s_j)$;
    $h_i^k \leftarrow 1$;
  end
end
$H \leftarrow \{h_1, \ldots, h_{n\_blocks}\}$;
return H;

Algorithm 1. Directional bloom filter pseudocode

4.5. Template Matching

The output of the proposed system after feature transformation, which is binary, is matched using Hamming distance matcher. Hamming distance matcher is a matcher between two binary features that works by calculating the proportion of disagreeing components between the two different set of feature vectors. Let u and v be a binary feature vector of dimension N and $\bigoplus$ is the XOR operation, then the hamming distance $d(u, v)$ is computed based on the following equation:

$$d(u, v) = \sum_{i=1}^{N} u_i \bigoplus v_i \tag{12}$$

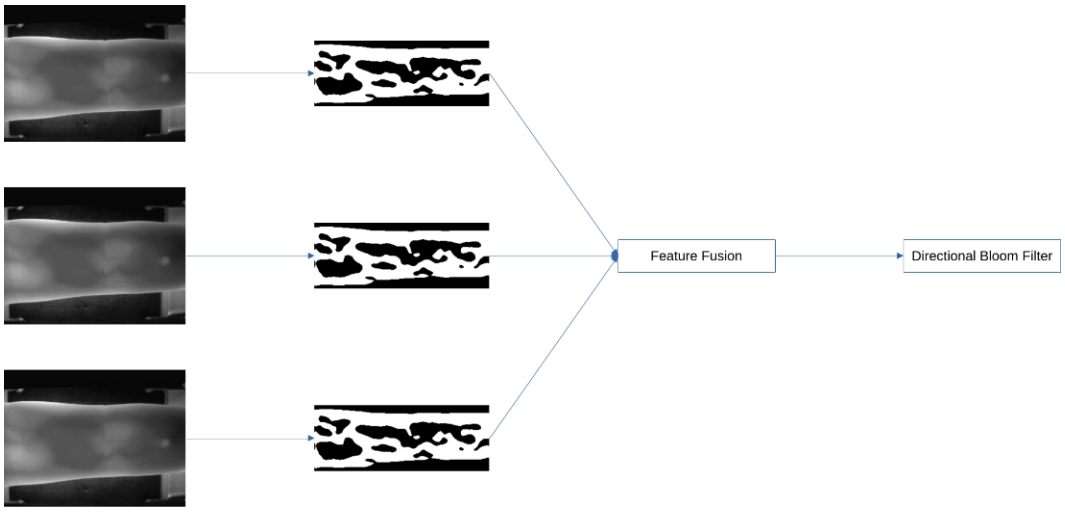
5. Experimental Analysis

5.1. Experimental Setup

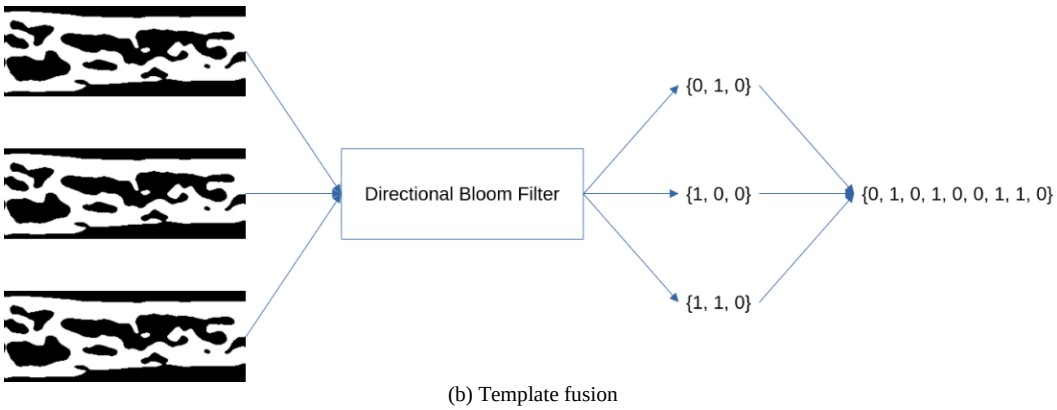
The proposed method is validated using two standard benchmark databases for finger vein recognition, UTFVP and PLUSVein-FV3. Both datasets are widely used as benchmark datasets for finger vein recognition in the research community. It has been used to assess the performance of various finger vein recognition algorithms and template protection methods. Specifically, the University of Twente Finger Vascular Pattern (UTFVP) dataset is a collection of finger vein images created by the Biometric Recognition Group at the University of Twente in the Netherlands from 60 Twente University students during the 2011-2012 academic year, with 82% between the ages of 19 and 30, 27% female, and 13% left-handed [30]. A local custom device was used to capture the images of finger veins. Each person provides three fingers (index, middle, and ring) from both hands, and each finger is sampled four times. The dataset contains 1440 images (60 individuals × 3 fingers × 2 hands × 4 samples). Each image is 672 × 380 pixels in size and stored in "*.png" format.

On the other hand, the PLUSVein-FV3 LED-Laser Dorsal-Palmar Finger Vein dataset is from the University of Salzburg [31]. The images of the finger veins were captured using a local custom device that used LED or laser illumination. In this paper, the LED dataset is referred to as PLUS LED, while the laser dataset is referred to as PLUS Laser. The finger vein images were acquired from 60 people of three fingers (index, middle, and ring finger) on both hands. Each of the fingers was sampled five times. There are 1800 images in total for each dataset (60 individuals × 3 fingers × 2 hands × 5 samples). The images are in "png" format and have a resolution of 600 × 1024 pixels. The dataset also includes manually annotated ground truth images, which can be used for evaluation and benchmarking of finger vein recognition algorithms.

The proposed system uses two fusion methods, feature fusion and template fusion, as a multi-instance finger vein system requires a method to combine information from multiple finger veins. Feature fusion concatenates features after extraction and uses them in subsequent processes, while template fusion concatenates templates after transformation and uses them in subsequent processes. Figure 6 depicts the two fusion strategies.



(a) Feature fusion



(b) Template fusion

Figure 6. Fusion methods used in the proposed system

For the subsequent experiments, 'li' means left index finger, 'lm' means left middle finger, and 'lr' means left ring finger. Genuine accept rate (GAR) is the rate at which a real user is authenticated as real, the higher the value, the better the system is. False accept rate (FAR) is the rate at which a fake user is authenticated as real, lower is better. False reject rate (FRR) is the rate at which a real user is authenticated as fake, lower is better, $FRR = 1 - GAR$. Equal error rate (EER) is the rate at which the FAR and FRR are equal, it is a way to tell the performance of the system in a balanced manner, lower is better.

5.2. Experimental Results

The experimental results of the baseline method using only the modified Frangi filter are presented in Table 1. It can be seen that the baseline modified Frangi filter achieves the lowest EER of 2.78% for UTFVP, 3.95% for PLUS LED, and 4.33% for PLUS Laser. The results show that using multiple fingers improves EER by 2.71% on average (with a standard deviation of 4.43%), implying that using multi-instance fingers is generally more effective than relying on a single finger for recognition.

Table 1. Experimental results for baseline Modified Frangi Filter method

Dataset	Fingers	EER
UTFVP	('li',)	**2.78%**
	('li', 'lm')	3.89%
	('li', 'lm', 'lr')	3.89%
PLUS LED	('li',)	6.83%
	('li', 'lm')	4.50%
	('li', 'lm', 'lr')	**3.95%**
PLUS Laser	('li',)	15.50%
	('li', 'lm')	7.12%
	('li', 'lm', 'lr')	**4.33%**

The receiver operating characteristic (ROC) curve of the baseline system using modified Frangi filter can be observed in Figure 7. In general, the ROC curve can be used to observe system performance at various levels of desired performance. When comparing the use of a biometric system to login to a game versus login to a bank account, not all uses of a biometric system require the same security threshold. When used in a game system, it is preferable to have a higher genuine accept rate (GAR) in exchange for a higher false accept rate (FAR). Meanwhile, when used for a bank account system, having as little FAR as possible is more important, even if it lowers GAR. EER is useful for comparing overall system performance, whereas the ROC curve is useful for comparing specific system performance.

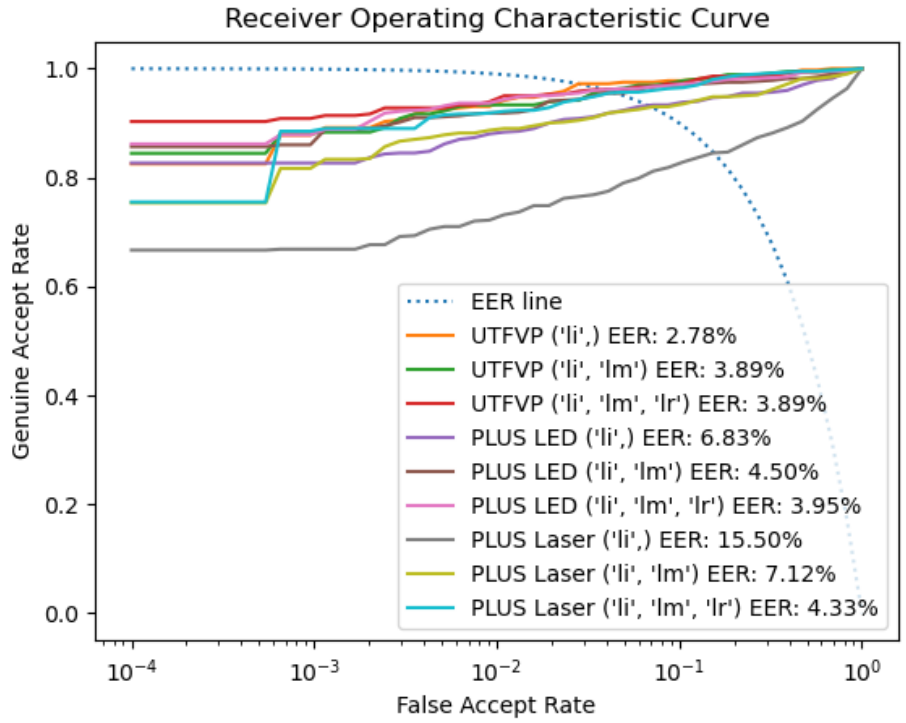
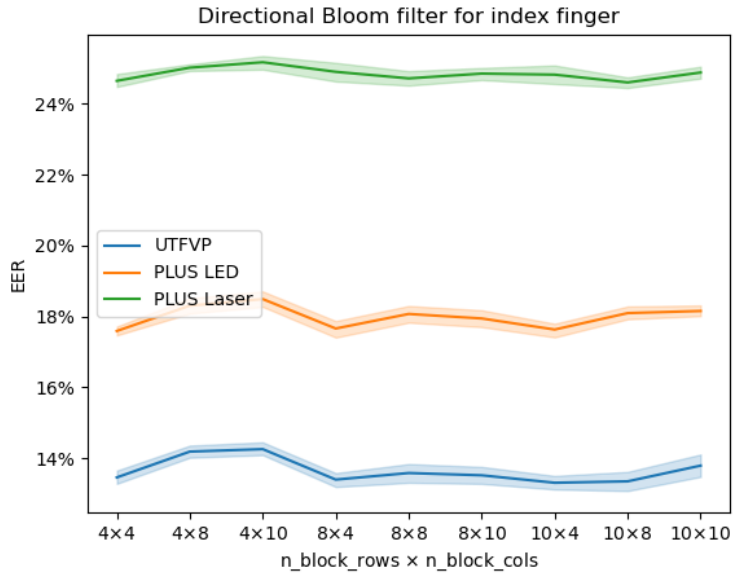
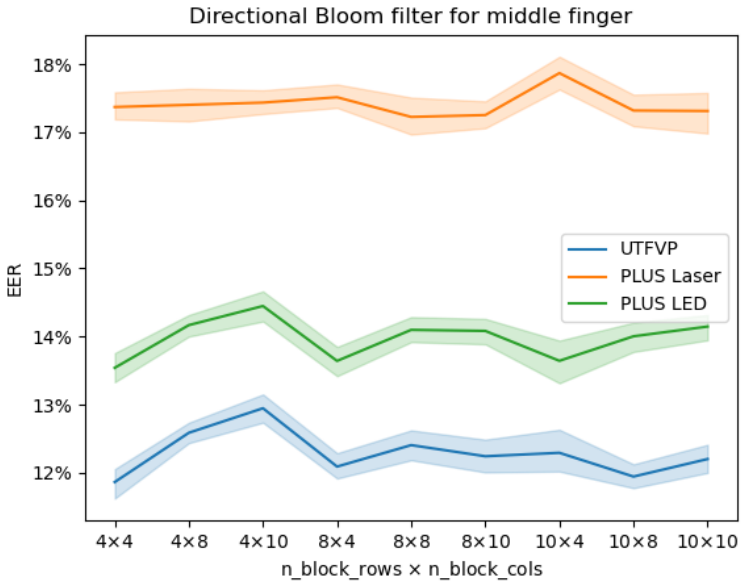


Figure 7. ROC curve of the baseline system using modified Frangi filter

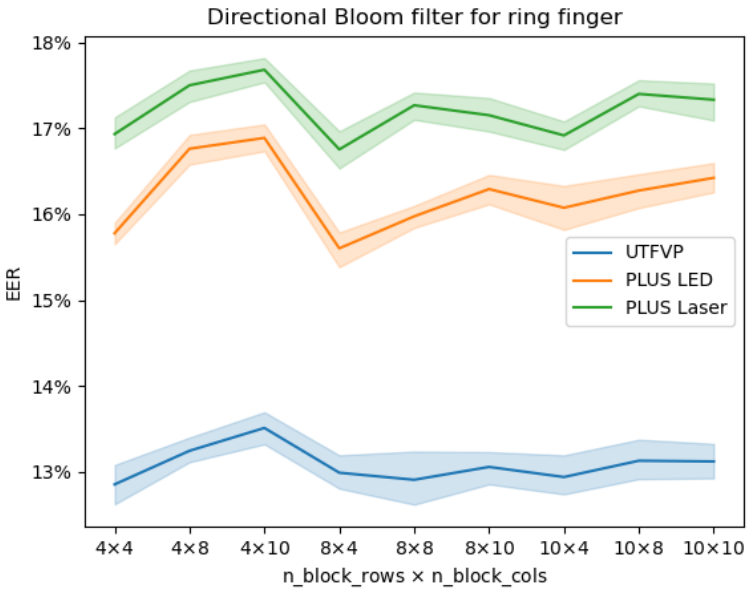
For performance evaluation of template protection, we have both user key and constant key scenarios. A constant key means that the secret key used to generate randomness in the system is the same for all individuals. The outcome represents the worst-case scenario in which the attacker obtained the secret key. The user key scenario is when the secret key is unique to each individual. This simulates the system's normal operation. In experiments, the proposed system with user key achieves an EER of 0% every time. The following experiments are conducted using a constant key with n_block_rows = 8 and n_block_cols = 4. Figure 8 shows the line plot of the result of directional bloom filter tested on multiple parameters with 10 different constant keys transformation, the line shows the average of the results, and the shaded region shows the 95% confidence interval of the results. As shown in Figure 8, the proposed directional bloom filter is not very sensitive when different parameters and constant keys are used, as evidenced by the small spread of the 95% confidence interval. The parameters 8x4 produce mostly satisfactory results in the constant key scenario, so they are used in subsequent experimental analysis for performance comparison.



(a) Directional bloom filter on index finger



(b) Directional bloom filter on middle finger



(c) Directional bloom filter on ring finger

Figure 8. Result of directional bloom filter when tested on different parameters

Table 2 shows that the proposed method for UTFVP produced better results. It can be seen that using three fingers with DBF and template fusion results in the lowest EER of 5.28%. It also demonstrates that using two fingers with DBF and template fusion results in the lowest D_{sys} of 5.86%. This demonstrates that DBF is more performant and private than BF in general. Multi-instance also improves DBF and BF performance while improving DBF privacy. Overall, the DBF approach resulted in 2.51% to 3.75% of EER improvements over the baseline bloom filter, with feature fusion providing the best improvement (3.06% to 3.75%) and template fusion providing slightly lower improvement of the results (2.51% to 3.33%).

Table 2. Experimental results for UTFVP

Fingers	Feature Transformation	Fusion	EER	D_{sys}
('li',)	DBF	-	**13.73 %**	**6.94%**
	BF	-	16.39%	24.93%
('li', 'lm')	DBF	template	6.67%	**5.86%**
	DBF	feature	**6.39%**	7.16%
	BF	template	10.00%	29.58%
	BF	feature	10.14%	25.79%
('li', 'lm', 'lr')	DBF	template	**5.28%**	**6.24%**
	DBF	feature	5.83%	7.45%
	BF	template	7.79%	31.42%
	BF	feature	8.89%	23.53%

The ROC curve of the proposed method for UTFVP can be seen in Figure 9.

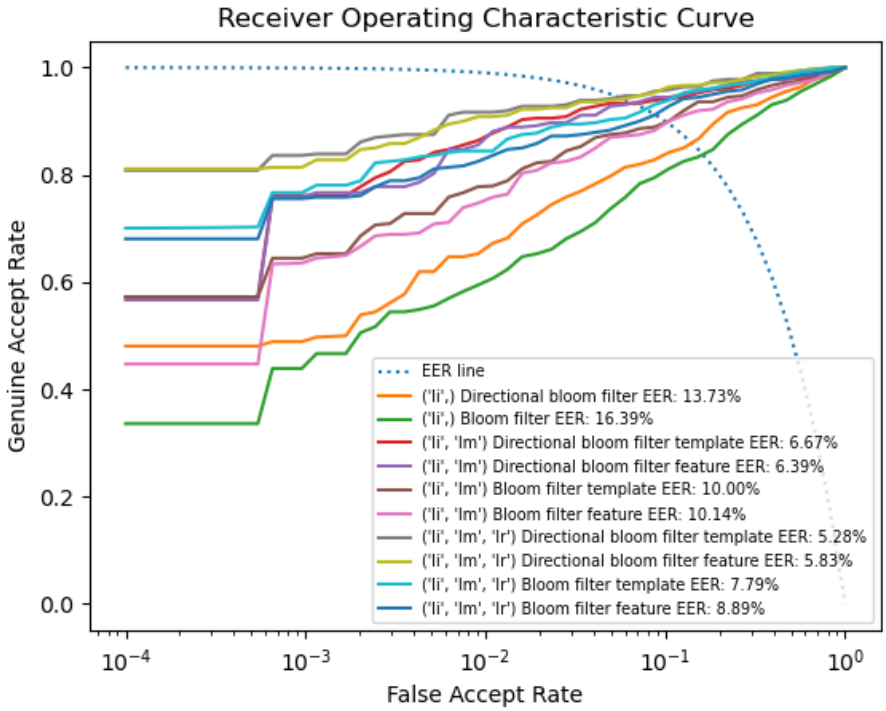


Figure 9. ROC curve of the proposed method for UTFVP

As shown in Table 3, our proposed PLUS LED method, which uses three fingers with DBF and template fusion, has the lowest error rate (7.06%). Using only one finger with DBF results in the best system performance, with the lowest D_{sys} of 4.83%. Overall, DBF provides more privacy, particularly in multi-instance settings. When feature and template fusion techniques are used, our directional bloom filter outperforms the bloom filter and achieves lower EERs in all instances.

Table 3. Experimental results for PLUS LED

Fingers	Feature Transformation	Fusion	EER	D_{sys}
('li',)	DBF	-	**16.61%**	**4.83%**
	BF	-	23.50%	15.25%
('li', 'lm')	DBF	template	**9.33%**	**5.19%**
	DBF	feature	**9.33%**	5.70%
	BF	template	17.89%	12.91%
	BF	feature	19.25%	11.12%
('li', 'lm', 'lr')	DBF	template	**7.06%**	**4.85%**
	DBF	feature	7.83%	5.34%
	BF	template	14.04%	16.64%
	BF	feature	16.12%	14.20%

The ROC curve of the proposed method for PLUS LED can be seen in Figure 10.

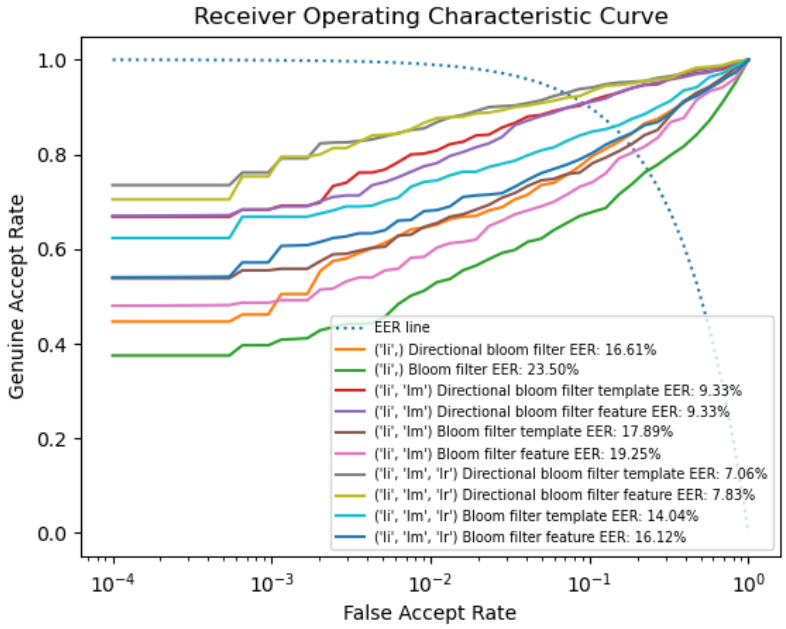


Figure 10. ROC curve of the proposed method for PLUS LED

Table 4 shows the experimental results for the PLUS Laser method. The best EER (7.50%) is obtained by combining three fingers with DBF and template fusion. With three fingers and DBF and feature fusion, the best D_{svs} (4.81%) is achieved. DBF again outperforms BF in terms of both performances, with multi-instance setups further improving these results. The former outperforms the traditional bloom filter by 7.00% to 14.17% in terms of EER. Specifically, feature fusion accounts for an EER improvement ranging from 12.05% to 14.17%, while template fusion contributes to an EER boost between 8.91% and 11.00%.

Table 4. Experimental results for PLUS Laser

Fingers	Feature Transformation	Fusion	EER	D_{sys}
('li',)	DBF	-	**24.00%**	**6.24%**
	BF	-	31.00%	12.71%
('li', 'lm')	DBF	template	**14.17%**	5.90%
	DBF	feature	14.50%	**5.40%**
	BF	template	23.08%	12.08%
	BF	feature	26.55%	12.90%
('li', 'lm', 'lr')	DBF	template	**7.50%**	6.12%
	DBF	feature	9.33%	**4.81%**
	BF	template	18.50%	12.98%
	BF	feature	23.50%	12.50%

Figure 11 illustrates the ROC curve of the proposed method for PLUS Laser.

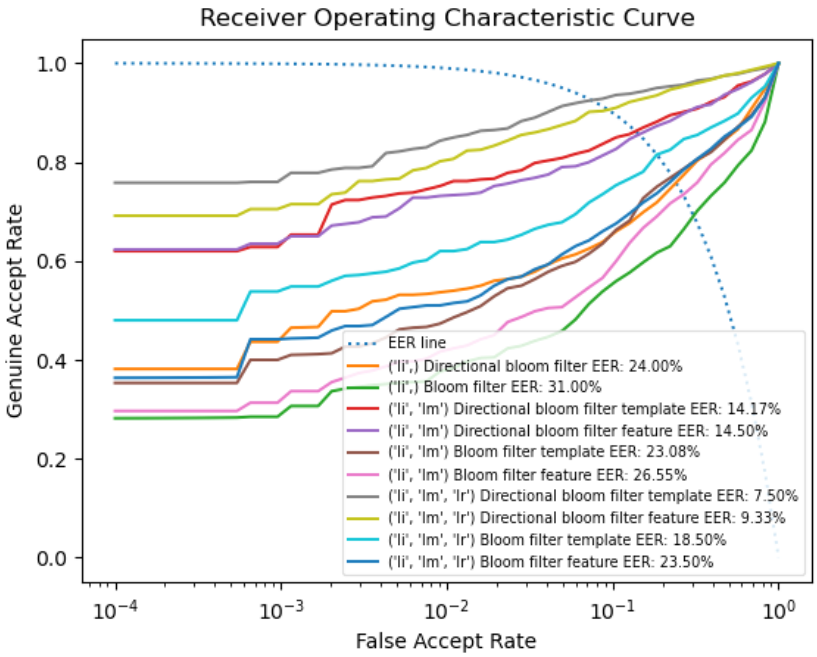


Figure 11. ROC curve of the proposed method for PLUS Laser

Based on the results of Figures 9 to 11, DBF outperforms BF for all number of finger vein instances. As presented in Figures 9 to 11, it is also clear that DBF template fusion consistently outperforms DBF feature fusion. In addition, Figure 12 shows the performance of the proposed system with and without template protection, indicating that the system performance degrades slightly when template protection is used. When the false accept rate (FAR) is set to 0.01%, the false reject rate (FRR) for the modified Frangi filter is around 17.5% and 19% for the directional bloom filter. This minor difference in performance implies that the proposed DBF method has little effect on the FRR. It implies that using DBF as a security measure in the system provide the balance between the necessary level of template protection.

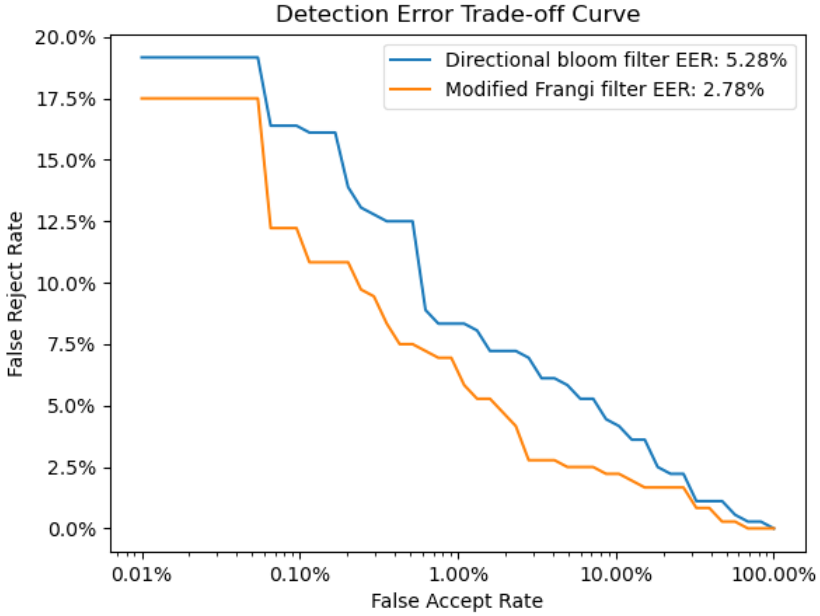


Figure 12. DET of baseline and directional bloom filter with the best EER

5.3. Unlinkability and Renewability Analysis

Unlinkability is one of the desired properties of a biometric template [4]. Unlinkability ensures that a template from one biometric system cannot be linked to another template from the same individual in another biometric system, which protects the privacy of the users. In addition, renewability is also one of the desired properties of a biometric template.

Renewability is necessary since biometric data is permanent and is no longer useful once compromised. Hence, it is necessary to be able to generate multiple different templates from one biometric data. An unlinkable template is a renewable template since the templates generated from different secret keys cannot be linked to each other, which also proves that multiple different templates can be generated from the same biometric data.

Unlinkability can be estimated from likelihood ratios [6], where for a given score s, $LR(s)$ is defined as:

$$LR(s) = \frac{P(s_m)}{P(s_{nm})} \tag{13}$$

where s_m is the score computed from mated templates, s_{nm} is the score computed from non-mated templates, and P is the probability. Mated templates mean the templates are generated from different samples and secret keys of the same instance and individual, for example, two different samples of the left index finger vein from the same individual. On the other hand, non-mated templates refer to templates that are generated from different samples, secret keys, instances, and individuals.

When $LR(s) \leq 1$, it means that it is more likely that the templates are non-mated. On the other hand, when $LR(s) > 1$, it means that it is more likely that the templates are mated. For convenience's sake, the $LR(s)$ is normalized from the range $[0, \infty)$ to the range $[0,1]$ as $D(s)$, where it is defined as:

$$D(s) = \begin{cases} 0 & LR(s) \leq 1 \\ 2\left(\dfrac{1}{1 + exp\left(-(LR(s) - 1)\right)} - 0.5\right) & LR(s) > 1 \end{cases} \tag{14}$$

As defined, $D(s)$ only estimates the unlinkability of the system for a score, to determine the unlinkability of the whole system, D_{sys} is defined as:

$$D_{sys} = \int_{s_{min}}^{s_{max}} D(s)P(s_m)ds \tag{15}$$

where $D_{sys} = 0$ means the system is fully unlinkable and $D_{sys} = 1$ means the system is fully linkable, therefore the lower the D_{sys} the better.

Figure 13 depicts the unlinkability analysis of the proposed method with the best EER for UTFVP. It can be seen that between the scores $[0.0482, 0.0488]$, where the bulk of the data is, the mated score s_m has a lower or near equal probability than the non-mated score s_{nm}, resulting in a low $D(s)$ in the region with the D_{sys} of 6.24%.

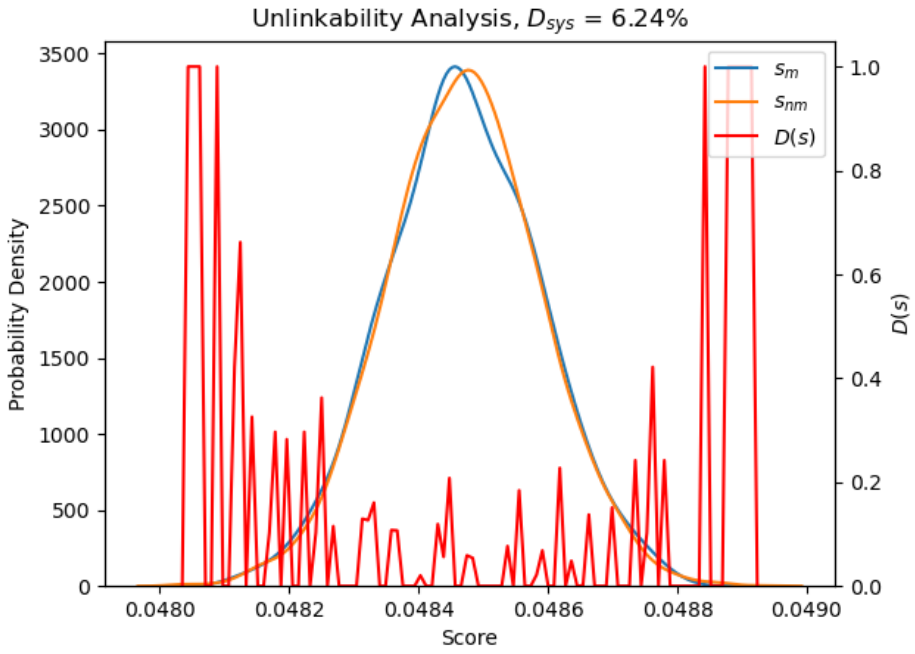


Figure 13. Unlinkability analysis of the proposed method with the best EER for UTFVP

The unlinkability analysis of the proposed method with the best EER for PLUS LED can be seen in Figure 14. It can be seen that between the score $[0.0481, 0.0487]$ where the bulk of the data is, the mated score s_m has mostly lower or near equal probability than the non-mated score s_{nm}, hence the low $D(s)$ in the region, which resulted in the D_{sys} of 4.85%.

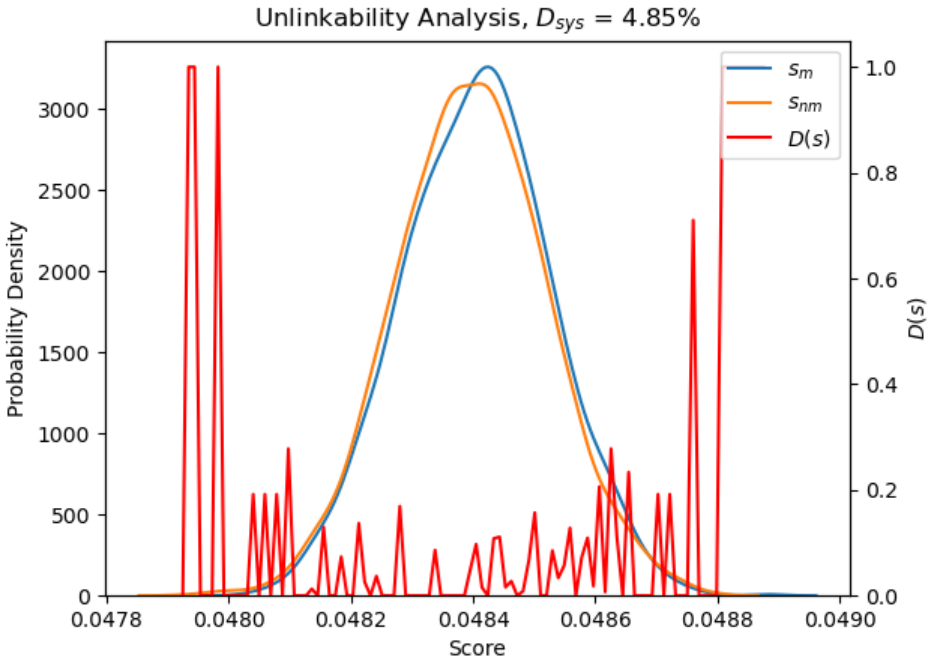


Figure 14. Unlinkability analysis of the proposed method with the best EER for PLUS LED

The unlinkability analysis of the proposed method with the best EER for PLUS Laser is depicted in Figure 15. It can be seen that between the scores $[0.0481,0.0487]$ where the bulk of the data is, the mated score s_m has mostly lower or near equal probability than the non-mated score s_{nm}, hence the low $D(s)$ in the region, which resulted in the D_{svs} of 6.12%.

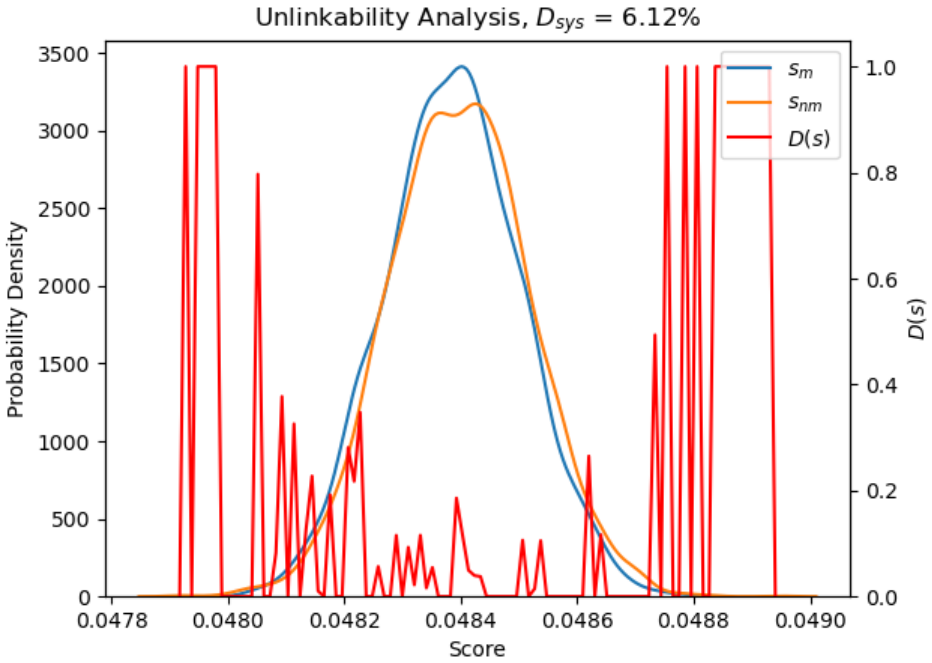
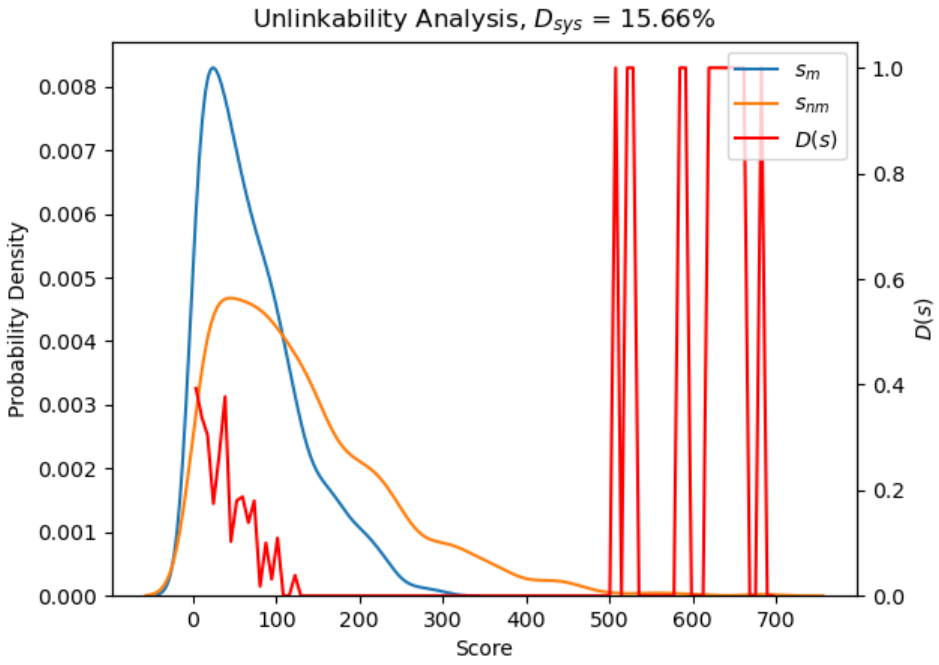
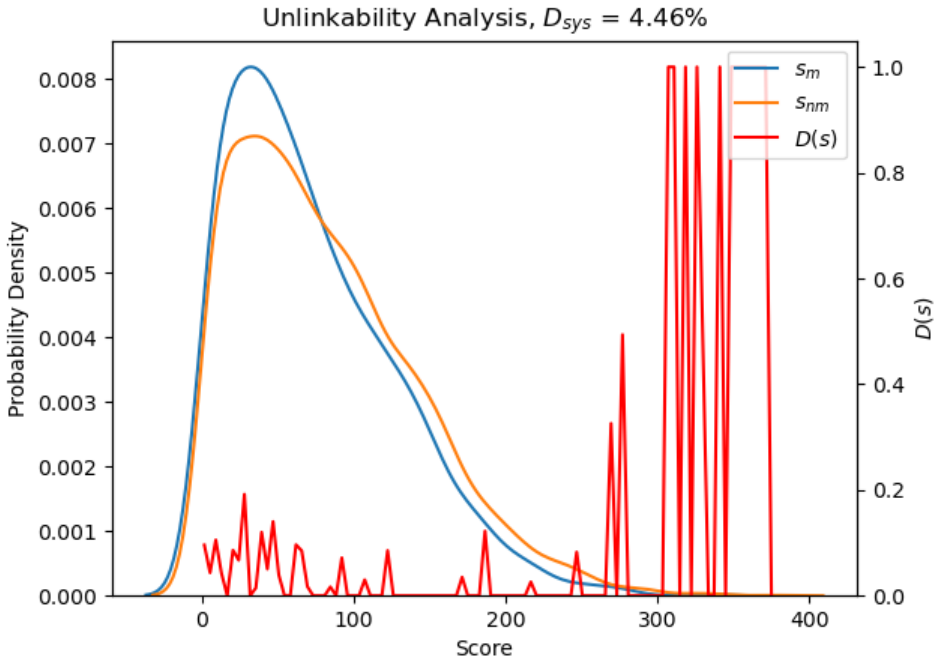


Figure 15. Unlinkability analysis of the proposed method with the best EER for PLUS Laser

The Hamming weight attack takes advantage of the fact that, in a Bloom filter, the number of unique columns in each block should remain mostly unchanged despite the row-wise permutation of the group of blocks. Armed with this information, the attack employs a Hamming weight matcher to determine the difference in the number of active bits between two templates. Figure 16 depicts the Hamming weight attack on the Bloom filter (BF) and directional Bloom filter (DBF). It is observed that the proposed DBF achieves a D_{svs} of 4.46%, compared to 15.66% for the BF. This indicates that the DBF has a relatively better unlinkability and therefore demonstrates good privacy protection of the proposed template protection mechanism.



(a) Bloom filter



(b) Directional Bloom filter

Figure 16. Hamming weight attack

5.4. Irreversibility Analysis

In a full disclosure model, in which an attacker has full knowledge of the system including the secret key, which represents the worst-case scenario, the security of the proposed system depends on the irreversibility of the template. Permutation and XOR only provide unlinkability in this model. The irreversibility of the template comes from the many-to-one mapping of the directional bloom filter, since for each active bit in the hash vector, there are many possible locations of the subblock in each block. The number of possible binary block $n_{\hat{b}}$ that can be generated from a hash vector h is:

$$n_{\hat{b}} = \frac{(active(h) + len(h) - 1)!}{active(h)!\,(len(h) - 1)!} \tag{16}$$

where $active(h)$ is the number of activated bits in the hash vector and $len(h)$ is the length of the hash vector. Since each hash vector is generated from a block, the total number of possible block $t_{\hat{b}}$ is:

$$t_{\hat{b}} = \sum_{i=1}^{n\_blocks} n_{\hat{b}_i} \tag{17}$$

However, $t_{\hat{b}}$ represents the upper bound of the total number of possible blocks, since directional bloom filter cannot generate all possible hash vectors, as compared to bloom filter. Despite the weaker irreversibility, directional bloom filter improves performance and unlinkability, making its benefits outweigh its drawbacks.

The irreversibility of the proposed system is presented in Table 5. The probability is calculated by using the minimum $active(h)$ of the respective dataset, since it represents the worst-case scenario. The $t_{\hat{b}}$ is calculated by simply multiplying n_blocks of 1200 with $n_{\hat{b}}$, to also represent the worst-case scenario. $n_{\hat{b}}$ is calculated with $len(h)$ of 256. The probability when using multiple fingers is simply the multiplication of the one finger probability with the number of fingers. This analysis shows that the system has good irreversibility.

Table 5. Irreversibility of directional bloom filter

Dataset	Fingers	$active(h)$				$n_{\hat{b}}$	$t_{\hat{b}}$	Probability (%)
		min	mean	std	max			
UTFVP	(‘li’,)	5	16.14	1.63	20	9.53×10^{9}	1.14×10^{13}	8.75×10^{-12}
PLUS LED	(‘li’,)	4	16.16	1.61	20	1.83×10^{8}	2.20×10^{11}	4.55×10^{-10}
PLUS Laser	(‘li’,)	6	16.17	1.61	20	4.14×10^{11}	4.97×10^{14}	2.01×10^{-13}

6. Discussion and Analysis

The best results of each method can be observed in Table 6, where the bloom filter and block remapping methods were re-implemented for a fair comparison for performance comparison purposes. Each method was tested with multiple fingers using different hyperparameters, and the best result is shown. As presented in the table, the proposed DBF performs well in terms of EER compared to other methods in the literature. DBF also mostly achieves the best D_{svs} among the other methods, combined with its decent EER, makes it a good choice for template protection. Specifically, the proposed DBF managed to improve upon the existing bloom filter (BF) for both EER and D_{svs} with the lowest EER of 5.28% for UTFVP, 7.06% for PLUS LED, and 7.50% for PLUS Laser. Although the proposed method did not outperform some of the other state-of-the-art methods from the referenced works Cai et al. [7] and Kirchgasser et al. [24] in terms of EER, it did achieve the best unlinkability with the lowest D_{sys} being 5.86% for UTFVP, 4.83% for PLUS LED, and 4.81% for PLUS Laser, respectively. This demonstrates that, despite not having the best EER, the proposed method provides superior unlinkability, which is critical for ensuring optimal privacy protection.

Table 6. The best EER result of each system with its D_{sys}

	UTFVP		PLUS LED		PLUS Laser	
	EER	D_{sys}	EER	D_{sys}	EER	D_{sys}
Frangi-DBF	**5.28%**	**6.24%**	7.06%	**4.85%**	7.50%	6.12%
Frangi-BF	7.79%	31.42%	14.04%	16.64%	18.50%	12.98%
Gabor-BF [7]	10.00%	7.4%	**5.67%**	6.7%	**5.88%**	**6.1%**
Frangi-Block Remapping [25]	7.22%	8.01%	5.88%	36.69%	6.67%	8.29%
Gabor-Block Remapping [25]	8.89%	11.36%	**5.67%**	10.45%	6.33%	11.73%

7. Conclusion

In this work, the proposed BTP method achieves an acceptable level of performance and satisfies the required properties for a template protection method, based on empirical analysis. The row-wise permutation and random XOR operation enhance the template's unlinkability, ensuring that even if an attacker gains access to one template, they cannot use it to cross-matching with another system. Moreover, the directional bloom filter provides an additional layer of security by safeguarding the user's biometric data from being exposed. Although BF has been used previously for biometric template protection, the DBF proposed in this study is an enhanced version that utilizes multiple instances of biometric data to generate a hash vector that takes into account the row, column, and diagonal subblocks of a feature set. This modification results in a higher number of active bits in the hash vector for better security. This allows DBF to better capture the unique characteristics of an individual's biometric traits, leading to a more robust biometric template protection mechanism. Furthermore, the two fusion methods, feature fusion and template fusion, offer flexibility in implementing a multi-instance finger vein system and improve the overall accuracy of the system compared to a single finger vein approach. Overall, the proposed method presents a promising solution for template protection in biometric systems.

Notwithstanding the potential benefits of the proposed method, it should be noted that the method has only been evaluated on finger vein biometrics, and its equal error rate (EER) remains unsatisfactory. It employs a multi-instance approach that improves system performance. Notably, using three fingers instead of one finger, results in the best Equal

Error Rate (EER). This is evident when the proposed system achieves an EER of 5.28% for three fingers versus 13.73% for one finger for UTFVP, 7.06% for three fingers versus 16.61% for one finger for PLUS LED, and 7.50% for three fingers versus 24.00% for one finger for PLUS Laser. The proposed system with the best EER has a D_{sys} of 6.24% for UTFVP, 4.85% for PLUS LED, and 6.12% for PLUS Laser. The introduction of the directional bloom filter, an advanced version of the standard bloom filter. In comparison, the EER and Dsys of the bloom filter are 7.79% and 31.42% for UTFVP, 14.04% and 16.64% for PLUS LED, and 18.50% and 12.98% for PLUS Laser. This emphasises the proposed system's efficiency and effectiveness.

Future research should concentrate on improving the DBF method's performance by experimenting with different feature extraction methods. Furthermore, to validate the robustness of the proposed approach, the DBF method can be extended to other biometric modalities such as iris or face recognition in order to improve the proposed method's performance and scalability in real-world scenarios. In addition, further investigation is needed to identify more effective fusion strategies to enhance system performance beyond the current use of simple concatenation for feature fusion. Possible fusion strategies such as LR fusion, RL fusion, UD fusion, and DU fusion [32] can be explored. Finally, the potential benefits of multimodal biometrics, such as combining fingerprint and finger vein, should be explored to assess their potential for enhancing both security and performance.

8. Declarations

8.1. Author Contributions

Conceptualization, J.H.T. and T.S.O.; methodology, K.S.M.A. and T.S.O.; software, J.H.T.; validation: T.C.; formal analysis, J.H.T. and T.S.O.; writing—original draft preparation, J.H.T.; writing—review and editing, T.S.O., T.C. and K.S.M.A.; funding acquisition, T.S.O. All authors have read and agreed to the published version of the manuscript.

8.2. Data Availability Statement

- 3rd Party Data: Restrictions apply to the availability of these data. Data was obtained from The University of Twente, Enschede, and The Netherlands and are available at https://www.utwente.nl/en/eemcs/dmb/downloads/utfvp/ with the permission of The University of Twente.
- 3rd Party Data: Restrictions apply to the availability of these data. Data was obtained from Artificial Intelligence and Human Interfaces (AIHI) Department of the University of Salzburg led by Andreas Uhl and are available at https://wavelab.at/sources/PLUSVein-FV3/ with the permission of Andreas Uh.

8.3. Funding

This work was supported by Fundamental Research Grant Scheme (FRGS) of Ministry of Higher Education Malaysia (FRGS Grant No: FRGS/1/2019/ICT02/MMU/02/14).

8.4. Institutional Review Board Statement

Not applicable.

8.5. Informed Consent Statement

Not applicable.

8.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

9. References

[1] Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A systematic review of finger vein recognition techniques. Information (Switzerland), 9(9), 213. doi:10.3390/info9090213.

[2] Ross, A., & Jain, A. K. (2004). Multimodal biometrics: An overview. 12th European signal processing conference, 6-10 September, 2004, Vienna, Austria.

[3] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1), 3. doi:10.1186/1687-417X-2011-3.

[4] ISO/IEC 24745:2011. (2011). Information technology-Security Techniques-Biometric information protection. International Organization for Standardization (ISO), Geneva, Switzerland.

[5] Rathgeb, C., Breitinger, F., & Busch, C. (2013). Alignment-free cancelable iris biometric templates based on adaptive bloom filters. 2013 International Conference on Biometrics (ICB). doi:10.1109/icb.2013.6612976.

[6] Gomez-Barrero, M., Rathgeb, C., Galbally, J., Busch, C., & Fierrez, J. (2016). Unlinkable and irreversible biometric template protection based on bloom filters. Information Sciences, 370–371, 18–32. doi:10.1016/j.ins.2016.06.046.

[7] Cai, S., Yau, W. C., Ong, T. S., & Teng, J. H. (2022). Transforming Finger Vein Template in Multi-instance Scenario. 2022 10th International Conference on Information and Communication Technology (ICoICT). doi:10.1109/icoict55009.2022.9914870.

[8] Boult, T. E., Scheirer, W. J., & Woodworth, R. (2007). Revocable fingerprint biotokens: accuracy and security analysis. 2007 IEEE Conference on Computer Vision and Pattern Recognition. doi:10.1109/cvpr.2007.383110.

[9] Sayeed, M. S., Min, P. P., & Bari, M. A. (2022). Deep Learning Based Gait Recognition Using Convolutional Neural Network in the COVID-19 Pandemic. Emerging Science Journal, 6(5), 1086-1099. doi:10.28991/ESJ-2022-06-05-012.

[10] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614–634. doi:10.1147/sj.403.0614.

[11] Bagherzadeh, S. Z., & Toosizadeh, S. (2022). Eye tracking algorithm based on multi model Kalman filter. HighTech and Innovation Journal, 3(1), 15-27. doi:10.28991/HIJ-2022-03-01-02.

[12] Teoh, A. B. J., & Goh, A. (2006). Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(12), 1892–1901. doi:10.1109/TPAMI.2006.250.

[13] Hämmerle-Uhl, J., Pschernig, E., Uhl, A. (2009). Cancelable Iris Biometrics Using Block Re-mapping and Image Warping. Information Security, ISC 2009. Lecture Notes in Computer Science, 5735, Springer, Berlin, Germany. doi:10.1007/978-3-642-04474-8_11.

[14] Pillai, J. K., Patel, V. M., Chellappa, R., & Ratha, N. K. (2010). Sectored Random Projections for Cancelable Iris Biometrics. 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. doi:10.1109/icassp.2010.5495383.

[15] Pillai, J. K., Patel, V. M., Chellappa, R., & Ratha, N. K. (2011). Secure and robust iris recognition using random projections and sparse representations. IEEE Transactions on Pattern Analysis and Machine Intelligence, 33(9), 1877–1893. doi:10.1109/TPAMI.2011.34.

[16] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. Information Processing Letters, 93(1), 1–5. doi:10.1016/j.ipl.2004.09.014.

[17] Leng, L., & Zhang, J. (2013). PalmHash code vs. palmPhasor code. Neurocomputing, 108, 1–12. doi:10.1016/j.neucom.2012.08.028.

[18] Li, H., Qiu, J., & Teoh, A. B. J. (2020). Palmprint template protection scheme based on randomized cuckoo hashing and MinHash. Multimedia Tools and Applications, 79(17–18), 11947–11971. doi:10.1007/s11042-019-08446-8.

[19] Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., & Neri, A. (2010). Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 40(3), 525–538. doi:10.1109/TSMCA.2010.2041653.

[20] Maiorana, E., Campisi, P., Ortega-Garcia, J., & Neri, A. (2008). Cancelable Biometrics for HMM-based Signature Recognition. 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems. doi:10.1109/btas.2008.4699360.

[21] Maiorana, E., Martinez-Diaz, M., Campisi, P., Ortega-Garcia, J., & Neri, A. (2008). Template protection for HMM-based on-line signature authentication. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. doi:10.1109/cvprw.2008.4563114.

[22] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing, 2008(1), 579416. doi:10.1155/2008/579416.

[23] Abe, N., Yamada, S., & Shinzaki, T. (2015). Irreversible fingerprint template using Minutiae Relation Code with Bloom Filter. 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS). doi:10.1109/btas.2015.7358770.

[24] Kirchgasser, S., Kauba, C., Lai, Y. L., Zhe, J., & Uhl, A. (2020). Finger Vein Template Protection Based on Alignment-Robust Feature Description and Index-of-Maximum Hashing. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(4), 337–349. doi:10.1109/TBIOM.2020.2981673.

[25] Kirchgasser, S., Kauba, C., & Uhl, A. (2020). Cancellable Biometrics for Finger Vein Recognition—Application in the Feature Domain. Handbook of Vascular Biometrics. Advances in Computer Vision and Pattern Recognition. Springer, Cham, Switzerland. doi:10.1007/978-3-030-27731-4_16.

[26] Ren, H., Sun, L., Guo, J., Han, C., & Wu, F. (2021). Finger vein recognition system with template protection based on convolutional neural network. Knowledge-Based Systems, 227, 107159. doi:10.1016/j.knosys.2021.107159.

[27] Ghouzali, S., Nafea, O., Wadood, A., & Hussain, M. (2021). Cancelable multimodal biometrics based on chaotic maps. Applied Sciences (Switzerland), 11(18), 8573. doi:10.3390/app11188573.

[28] Bassit, A., Hahn, F., Veldhuis, R., & Peter, A. (2022). Hybrid biometric template protection: Resolving the agony of choice between bloom filters and homomorphic encryption. IET Biometrics, 11(5), 430–444. doi:10.1049/bme2.12075.

[29] Frangi, A. F., Niessen, W. J., Vincken, K. L., & Viergever, M. A. (1998). Multiscale vessel enhancement filtering. Medical Image Computing and Computer-Assisted Intervention — MICCAI'98. MICCAI 1998. Lecture Notes in Computer Science, Vol. 1496. Springer, Berlin, Germany. doi:10.1007/BFb0056195.

[30] Ton, B. T., & Veldhuis, R. N. J. (2013). A high quality finger vascular pattern dataset collected using a custom designed capturing device. 2013 International Conference on Biometrics (ICB). doi:10.1109/icb.2013.6612966.

[31] Kauba, C., Prommegger, B., & Uhl, A. (2018). The Two Sides of the Finger - An Evaluation on the Recognition Performance of Dorsal vs. Palmar Finger-Veins. 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). doi:10.23919/biosig.2018.8553277.

[32] Sudha, D., & Ramakrishna, M. (2017). Comparative Study of Features Fusion Techniques. 2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT). doi:10.1109/icraect.2017.39.