Multi-instance Finger Vein-based Authentication with Secured Templates

Swati K. Choudhary[1]
Department of Electronics Engineering
K. J. Somaiya College of Engineering
Mumbai, India

Ameya K. Naik[2]
Department of Electronics and Telecommunication
Engineering, K. J. Somaiya College of Engineering
Mumbai, India

***Abstract*—The illegitimate access to biometric templates is one of the major issues to be handled for authentication systems. In this work, we propose to use two instances of finger vein images which inherits the advantages of a robust multi-modal biometric authentication system without needing different sensors. Two local texture feature extraction methods are experimented on standard finger-vein datasets. Fused discriminating features with reduced dimension lowers down the system computational cost. A cancelable template protection scheme as Gaussian Random Projection based Index-of-Max is then applied for embedding privacy and security to the templates. Foremost template protection properties like revocability, non-invertibility and unlinkability are observed to be significantly obeyed by the proposed system with considerable authentication performance. Recognition performance of the proposed methods are compared with some previously executed finger vein systems and observed to be less complex and overperforming on the combined basis of authentication and template protection. Thus, the proposed system utilizes multiple evidence and provides a balanced performance with respect to authentication, template protection and computational cost.**

***Keywords*—Finger vein; multi-instance; authentication; cancelable; template protection**

I. Introduction

Information Technology and Internet driven life has created the extreme need for securing the evidence related to personal identity. Biometrics based authentication systems put up some problems related to security and privacy of data [1], owing to which an efficient template protection scheme needs to be employed. The requirements regarding irreversibility, revocability, unlinkability and performance preservation should be satisfied by an effective template protection technique. To meet these requirements, various techniques have been investigated as bio-cryptosystems and cancelable biometrics. Among them, Cancelable biometrics is more appropriate technique to handle both, the security and privacy of templates by repeatedly deforming the template features using some transformation.

The design of transformation function should be extremely difficult to invert, enabling computational infeasibility to get the original features back from the transformed template. This characteristic prevents the privacy attack to get original data back. Renewability is another property that the designed transformation function should come up with. This enables generation of newly transformed template if the previously enrolled template is compromised. Additionally, templates created by using different transformations should not match with each other applying diversity to the template protection technique. Furthermore, it should be challenging to differentiate between the templates established by same biometric information. This prevents cross matching of biometric data across various applications, obeying the unlinkability property. More importantly, when all the above-mentioned security and privacy preserving characteristics are considered to design a transformation function, it should not reduce the authentication level. The proposed framework applied the Gaussian Random Projection based Index of Max (GRP-IoM) hashing technique [2] on the real valued finger vein features to generate cancelable and highly non-invertible protected templates.

The proposed work is utilizing multiple instances of finger veins for authenticating people. Finger veins are innate, non-intrusive, and highly resistant to duplication and captured by small imaging sensor. Additionally, distinct patterns for twins [3] and liveness detection property are included in finger veins. Occasionally, finger vein images suffer from illuminations and blood fluctuations and becomes low contrast and unstable. Thus, to overcome this low-quality issue to some extent, combination of multiple instances of finger vein images will be beneficial minimizing the limitations of unimodal biometrics viz. non-universality, intra-class deviations, inter-class resemblance, scope for spoofing, etc. Thus, in this work, we propose fused-discriminant (FD) feature set extraction from two instances of finger vein images with two different local texture-based features. The feature extraction techniques experimented is Uniform Local Binary Pattern (ULBP) [4] and Local Hybrid Binary Gradient Contour (LHBGC) [5]. The texture features from the two finger vein instances are fused as well as reduced in size by maintaining their correlation within an individual and enhancing their discrimination between the individuals. This improves authentication performance and reduces computational intricacy transformation for template protection and matching. Thus, the key contributions of the proposed framework are outlined as follows:

- Generating highly irreversible, un-linkable and revocable templates by using fused-discriminant feature set.
- Person authentication is based on two separate identity proofs rather than single finger vein image to overcome the issues like low quality with lower computation cost.

- Two different texture-based features (ULBP and LHBGC) are experimented in their fused-discriminant forms for generating protected templates and preserving authentication performance, significantly.

This paper is organized as follows. Section II describes some of the previous work carried on, in the field of single and multi-instance finger vein authentication and a variety of template protection methods that has been practiced for the same. Section III provides description regarding the fundamental methods used in the proposed authentication system with template protection. Thereafter, in Section IV, details of implementation process for the proposed multi-instance finger vein-based authentication system and obtained experimental results for authentication and template protection are represented and analyzed. Validations of obtained authentication and time complexity results are shown by comparing with some earlier reviewed work. To conclude, Section V covers the overall contribution of the proposed authentication framework and its further scope.

II. Related Work

Various approaches have been practiced for utilizing finger veins for authentication purpose. Handling the security issue of biometric templates with authentication is a great challenge. In Section II-A, different methodologies implemented for finger vein-based authentication are discussed. Further, Section II-B gives overview of various schemes practiced for protecting finger vein templates.

A. Finger Vein based Systems

There are line-based, point-based and texture-based features popularly used for vascular pattern finger vein regions. Line-based finger vein feature extraction is initiated by [3] in the form of Repeated Line Tracking (RLT) method through a line tracking algorithm. The author continued his research in [6] by extracting the center lines of the veins, calculating their local maximum curvatures. This method is found to be robust against variations in vein-widths. Later, [7] proposed Wide Line Detector (WLD) with comparatively faster vein pattern extraction but at the expense of degradation in authentication performance. In [8], Enhanced Maximum Curvature (EMC) method is used for feature extraction which identifies fine delineations in vein-patterns using Histogram of Oriented Gradients (HOG) but observed to be slower than WLD. Alternatively, some point-based feature extraction methods are also practiced as minutiae points in [9] or multiple key point sets from SIFT (Scale-invariant Feature Transform) in [10]. Ultimately, point based features also needs vein patterns involving computational cost for extracting vein pattern. In [11], special points as cross/end points of veins and connections between them are matched to reduce the finger vein matching time. The performance of this scheme is sensitive to Region of Interest (ROI) and used only good quality images for evaluation.

In texture-based approach, various classical and innovative methods for extracting texture information have been practiced. Most widespread method adept of extracting recognizable features from such images is Local Binary Pattern (LBP). This LBP method introduced by [12] is fast in which texture features are obtained from gray level difference in neighborhood pixels. These classical LBP features are lengthy and observed to be very sensitive to image translations and rotations. To cope with this, there are various LBP variants proposed previously for finger veins and other biometrics [13]. In [14], t-norm based fusion of LBP feature scores belonging to two finger vein instances is implemented using hamming distance. Accurate authentication primarily depends on discriminability of features. Another variant of LBP as Local Hybrid Binary Gradient Contour (LHBGC) features [5] are shown to be more informative on finger veins compared to [13, 14]. This method computes local histograms to compute the frequencies of sign and magnitude components, locally in the image. Further, Uniform LBP (ULBP) texture feature extraction proposed by [4] is very much suitable to finger vein structure. As the vein will either lie inside or cross the neighborhood in vein-region, the resulting pattern will not have many distinguished bitwise transitions. Thus, these ULBP features which are more compact than LBP, covering majorly uniform patterns are suitable for finger vein. ULBP features preserving spatial information are found to have some degree of invariance to rotation, pose and illumination because of histogram computation over image partitions. Variety of feature extraction methods complimenting with different classifiers have been practiced for finger vein images [15-20]. Some recent finger vein-based authentication implemented Machine Learning (ML) and Artificial Intelligence (AI) approach especially for identification, if huge data needs to be worked on. [21] utilized VGG-Net-16, which is composed of thirteen convolutional fully connected layer model finely tuned and pre-trained with two finger vein image difference. A deep learning-based technique is proposed by [22] to work on finger vein images of varying quality. This network comprised of four convolutional layers and is experimented on four different databases. Deep learning methods requires heavy processing configuration with huge amount of training data. Parameter tuning is another complex process to be handled in case of AI applications.

In this work, we offer to use two variants of LBP as Uniform LBP (ULBP) and Local Hybrid Binary Gradient Contour (LHBGC), considering their feature discriminability and suitability for finger veins. Additionally, LBP based methods are proven to be resistant to uneven shading and saturation from input imaging devices [23]. The proposed authentication is using ULBP and LHBGC features for multiple instances of finger vein, in their Fused-Discriminant form as FD-ULBP and FD-LHBGC respectively for reducing their dimensions and enhancing discriminability. These features are further transformed for template protection and their authentication performances are analyzed in transformed domain.

B. Finger Vein Template Protection

Severe security and privacy threats are faced by biometric templates stored in database, regarding unauthorized access, original feature breeding from coded template or from cross matching across applications. Bio-cryptosystems (BCS) and cancelable biometrics (CB) are the major template protection schemes employed to secure the templates. As the proposed framework is implementing CB for the previously mentioned advantages, major emphasis is given on CB techniques. CB schemes are enormously practiced to secure various popular unibiometric traits as face [24], fingerprint [25] and iris [26]. CB techniques for different combinations of multi-biometric traits have also been practiced. Fusion of multiple traits at different levels are investigated in [27] for better performance. Feature level fusion [28] is advantageous over others, especially if template protection is needed as single fused protected template has to be handled. On the contrary, compatibility issues for features generated out of different biometric traits is highly challenging. When these fused-diverse features are transformed to form cancelable templates, preserving recognition performance is critical. A balanced solution to this is multi-instance biometrics offering multiple evidence-based authentications with compatible features and no extra sensor.

Focusing on CB for securing finger vein images [29] proposes a combined CB and BCS approach by applying cancelable bio-hashing method to finger vein image. Bio-hashing transforms finger vein Gabor features compacted by Linear Discriminant Analysis (LDA) into binary string. Then the Fuzzy Commitment Scheme (FCS) and Fuzzy vault is applied to binary string. In [30], a similar approach of random projection based cancelable transform is applied on Gabor features reduced by Principal Component Analysis (PCA) and then FCS is operated on the resulted binary feature set. L2-Norm is used to classify the transformed templates. [31] again offers a random projection based cancelable transformation of vein end and intersection points and classification is done using Deep Belief Network (DBN). This approach requires password and a huge dataset for training. In [32], Bloom filter template security is utilized for fingerprint, signature, and their fused features. As Bloom filter technique can be applied to fixed length binary features, some fingerprint-oriented methods like minutiae cylindrical code employed to finger vein [33] can be utilized for Bloom-filter based CB. [34] proposed CB for finger vein image through block-remapping and image-wrapping based transformation before feature extraction in image domain. Gabor features are used for verification and renewability evaluation. Block remapping in image domain is observed to provide better performance than wrapping which is also dependent on block size. Recently, [35] proposed CB method using on Index of Max [2] with alignment robust hashing (ARH). This work has also experimented with block-remapping and image wrapping but in feature domain to extract binary features. In [35], various binary feature extraction methods are experimented with three different types of CB techniques. ARH with Index of Max hashing works fine for alignment-free situations but inferior to image wrapping in feature domain with respect to authentication performance. Also, there is no clear empirical analysis of revocability for ARH-Index of Max hashing. AI-based methods like Convolution Neural Network (CNN) are very popular for identification but needs huge data volume. Also, as CNN is reversible in nature, the original raw features fed to CNN for classification can be inverted back. In [36], finger vein bio-hashed binary features are transformed into non-invertible and renewable code using Binary Decision Diagram (BDD). This protected code is fed to the Multi-Layer Extreme Machine Learning for verification and identification which runs the system fast. Recently, [37] also implemented bio hashing for securing finger vein templates made out of deep features using multi-term loss function showing excellent verification outcome but have not investigated for template protection factors like unlinkability or irreversibility.

In this article, we propose to use Gaussian Random Projection-based Index of Max (GRP-IoM) hashing for non-linear mapping of real valued fused feature set from instances of finger vein to generate integer based protected templates. Authentication performances along with corresponding computational costs of the proposed framework with two different texture features are evaluated. Theoretical and empirical evaluation of non-invertibility, unlinkability and revocability for the protected finger vein templates is also provided.

III. Proposed Methodology

The proposed framework is for person authentication using cancelable transformation of multiple instances of finger veins. Particularly, vascular patterns composed of veins within the human physique are difficult to counterfeit, contactless and concurrently provides liveness detection. Multi-instance finger vein-based authentication system makes the overall recognition performance depend on a greater number of biometric facts. Cancelable and distorted versions of fused features from multiple finger veins creates a secure verification system based on intrinsic biometric trait. This ensures renewability/revocability of our permanent unique features which are quite un-linkable across various applications. Various methods involved in this combined approach of authentication and template protection are explained as follows:

A. Finger Vein Processing

Finger vein verification involves challenges as finger vein images suffer from illumination and blood fluctuation factors. Captured finger vein images with poor contrast and misalignment may deteriorate authentication performance. So, for reliable finger vein verification, proper pre-processing and feature extraction techniques are needed. Details of methods used in the proposed framework for finger vein pre-processing and feature extraction are explained below:

1) Finger vein pre-processing: Finger vein pre-processing involves Region of Interest (ROI) extraction with finger alignment and image enhancement. ROI is localized by firstly detecting finger outline by edge detection algorithm and fitting a center line into the finger. The finger is gradually rotated and shifted using this center line until it gets aligned in the middle of the image with horizontal posture. The rectangular ROI is extracted masking out the background portion. Further, adaptive histogram equalization technique is used on finger vein ROI images to improve the vein pattern visualization. The noise removal is done using Weiner filter. Fig. 1 shows the overall result images for finger vein pre-processing in a sequential manner. For further details on preprocessing please refer to [38].

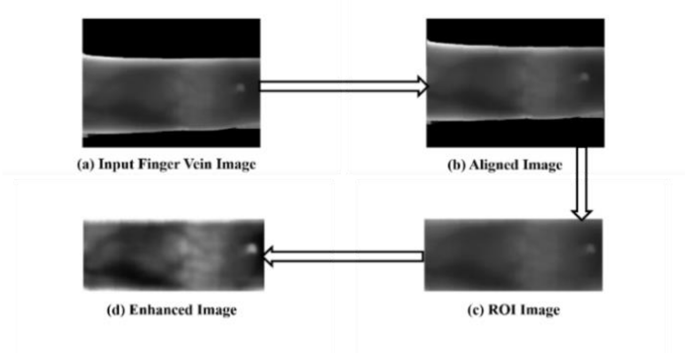

Fig. 1. Finger Vein Pre-processing.

2) Finger vein feature extraction: In the proposed approach, texture features belonging to two finger vein instances are combined with enhanced discriminability and compaction and then used for person authentication. Further these fused feature set is transformed for generating cancelable protected templates to incorporate template security. Two types of texture-based features are experimented, namely histograms of Uniform Local Binary Pattern (ULBP) and Local Hybrid Binary Gradient Contour (LHBGC). Both features are variants of original LBP method which is computationally less complex and extracts fine scale textures [12].

The first method implemented for finger vein texture feature extraction is histogram of uniform LBP. Original LBP description of a pixel in its canonical form is simple and created by comparing the intensity of P neighboring pixels to the center pixel in some radius r. These P comparisons in clockwise or anticlockwise direction is interpreted as a binary vector. Binary 1 is taken if the center pixel intensity is less than neighboring pixel, otherwise binary 0 is taken. This LBP$_{P,r}$ feature extraction process replaces each pixel in original image to a binary pattern except border pixels which do not have all neighboring pixels. These feature vectors can be transformed into histogram with 2P bins as each conceivable LBP is assigned to an individual bin. Various combinations of r and P are practiced but the most popular combination is $P=8$ with $r=1$. Proposed framework is also using $P=8$ with $r=1$ focusing on histogram dimensionality for computation, memory consumption and minimal original information loss. Further, it has been observed that specific binary patterns count for fundamental texture properties known as "uniform" patterns [4]. These uniform LBP features are observed to carry gray scale invariance and rotation invariance, but additional computations for rotation invariance are not incorporated in the present work as alignment of finger vein pattern is implemented in pre-processing. LBP is termed as uniform if it consists of maximum two 1-0 or 0-1 switching, viewing the bit pattern in circular way. For example, the pattern 00000110 is uniform whilst 10100000 is not. It is noticed that uniform patterns accounted for approximately 90 percent of all patterns. Hence, least information was lost by handing over all non-uniform patterns to one non-uniform category. If practiced particularly for P=8, it is seen that just 58 of the 256 possible 8-bit strings are uniform, we can thus encode all 256, 8-bit local binary patterns using 59 (58 uniform and 1 non-uniform) codewords. To indicate that uniform patterns are being used, $u2$ is added as superscript to the LBP operator to generate $LBP_{P,r}^{u2}$. Selecting the uniform patterns thus reduces the histogram length to *59 (P*(P-1) +3*) bins from 256 (2P) bins for P=8. Histograms of individual patterns show lower distinguishability as compared to that of uniform patterns accounting for the variations in their statistical properties.

Fig. 2 explains the overall process of uniform LBP feature extraction. Each input pre-processed image instance of finger vein is firstly split into N number of blocks. In the present work, each block is of size 8x8 with P=8 and r=1. Histograms were then computed for each block and the resulting histograms were then concatenated together to form one feature vector. Spatial information was implicitly encoded into this feature vector from the order in which the histograms were concatenated. Hence, after histograms of uniform LBP feature calculation the overall combined histogram feature length for the entire image is of length, 59xN. These texture features for the two finger vein image instances are calculated and further processed for feature fusion with dimension reduction and template protection.

The second method experimented for feature extraction of finger vein images is Local Hybrid Binary Gradient Contour (LHBGC) [5], which is also an LBP variant. LHBGC features are considered for its property of extensive information content regarding finger vein authentication as compared to various other texture features. This method computes the local histograms counting for frequencies of sign and magnitude for finger vein images, locally. Firstly, the preprocessed image of finger vein is subjected to sign and magnitude component extraction followed by local histogram calculation. Fig. 3 shows sign and magnitude computation in 3x3 neighborhood periphery for an input image. Adjacent pixel intensities are compared in 3x3 neighborhood periphery and these distances, bi for $i=0, 1 \ldots, 7$ are calculated using Eq. (1) which are further break down into sign and magnitude components. Hence, sign ([$s0, s1, \ldots, s7$]) and magnitude ([$m0, m1, \ldots, m7$]) vectors are obtained by decomposing distances ([$b0, b1, \ldots, b7$]) as shown in Eq. (2). The sign values are equivalent to basic Binary Gradient Contour codes and this binary code is further translated to decimal number. The magnitude component value for each 3x3 region is calculated by adding each of [$m0, m1, \ldots, m7$].

$$b_i = p_i - p_{(i+1)mod8}, i = 0, 1, 2, \ldots, 7 \tag{1}$$

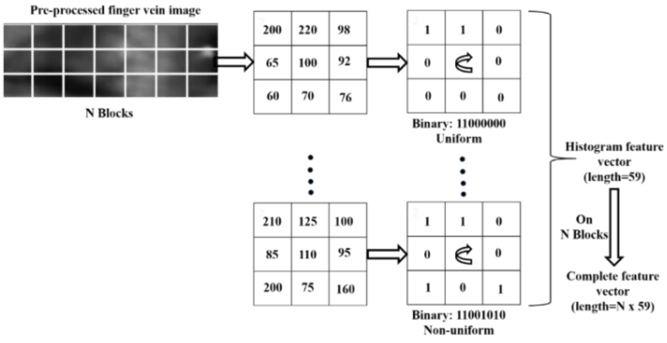

Fig. 2. Uniform Local Binary Pattern Histogram Feature Extraction Process.

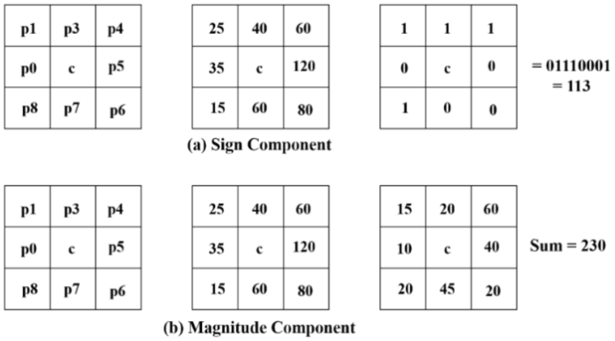

Fig. 3. Sign and Magnitude Component Calculation for Local Hybrid Binary Gradient Contour (LHBGC) Features.

where, [*p0, p1, ..., p7*] are the adjoining pixels along the periphery of 3x3 neighborhoods.

$$b_i = s_i * m_i \; and \; \begin{cases} s_i \\ m_i = |b_i| \end{cases}, s_i = \begin{cases} 1, b_i \geq 0 \\ -1, b_i < 0 \end{cases} \qquad (2)$$

The sign and magnitude components are distributed equally into number of cells for local histogram computation. For every single cell, a local histogram is computed, and the sign histogram bin is voted in a biased way by each pixel of the magnitude component in that cell based on the value present in the sign component. For further details on local histogram computation, please refer [5]. Various parameters involved in LHBGC feature extraction process are number of cells i.e., number of rows and columns with number of bins. The local histograms belonging to every cell are formed as vectors which are all concatenated to produce a combined feature vector for a finger vein image. This concatenated feature vector is of high dimension. Thus, further processing on this basic feature set is proposed for reducing feature dimensionality with enhanced feature discriminability.

3) Finger vein feature fusion: In the proposed approach, two texture-based features of finger vein image are experimented, namely ULBP and LHBGC as explained in the above section. The present work contributes for the effective person authentication using two instances of finger vein by fusing them into compact and informative feature set. Both ULBP and LHBGC histogram features are extracted from right index (RI) and right middle (RM) finger vein instances and fused using Discriminant Correlation Analysis (DCA) to form their fused-discriminant versions as FD-ULBP and FD-LHBGC. DCA reduces fused feature set dimensionality considerably (number of subjects present in training set), implemented by summing up the individual finger vein discriminant feature vectors. DCA is an effective tool for fusing features in pattern recognition. It is computationally efficient and applicable in real-time situations [39]. DCA obtains data from multiple feature sets and incorporates the class structure into canonical correlation analysis via transformations, thus taking into account the differences in the different classes while at the same time maximizing the pairwise correlations among the features in the two feature sets. More details about how DCA works can be found in [39]. The proposed work contributes by authenticating person based on deformed version of compact and fused feature set for the two-finger vein instance evidence. The deformation of feature set is needed for template privacy and security.

B. Finger Vein Template Protection and Matching

Finger vein features are protected by creating their hashed codes using randomly generated projection matrices. These codes are observed as highly irreversible and revocable in nature. The overall process is known as Gaussian Random Projection-based Index of Max (GRP-IoM) and is proposed by [2] for uni-biometric fingerprint system. This hashing technique is implemented for multiple instances of finger vein images in the proposed system.

The fused feature set of multi-instance finger veins as $x \in R^d$ is projected onto a d-dimensional random Gaussian vectors as $k \in R^d$. The overall hashing process is operated as follows:

1) Generate q number of d-dimensional Gaussian random vectors as $k_1, k_2, \ldots, k_q$ and form a projection matrix, $W^i = [w^1, w^2, \ldots., w^q]$.

2) Project input fused feature vector, x onto W^i and record index of maximum value from $\Phi_i(x)=arg\ max_{i=1,2,\ldots,q}(W^i, x)$ as t.

3) Repeat steps 1 and 2, n number of times to obtain hashed feature set as $t = (t_1, t_2, \ldots\ldots, t_n)$.

The IoM hashing basically obey the ranking based locality sensitive hashing that attempts to confirm that any two highly similar feature vectors result to greater probability of collision. On the other side, the dissimilar vectors result in smaller probability of collision. Assuming the collision probability of two hashed codes as enrolled template, $t^e=\{t_j^e|_{j=1,\ldots,n}\}$ and query template, $t^q=(t_j^q|_{j=1,\ldots,n}\}$ is represented as $CP[t_j^e,t_j^q] = ss(t^e,t^q)$ *for* $j=1,2\ldots,n$. Thus, the higher value of $ss(t^e,t^q)$ signifies high probability of collision. Computationally, $ss(t^e,t^q)$ is observed as the number of zeroes (collisions) counted in subtracting t^e and t^q, element-wise for n number of iterations which is considered as a template match score. In case of compromised template, IoM hashed code will be renewed by generating new random Gaussian matrices.

C. Multi-instance Finger Vein based Secured Authentication

The entire application of the proposed framework for multi-instance finger vein based biometric verification system with template protection is categorized into two major parts as enrollment and authentication. As shown in Fig. 4, enrolling an individual in the system involves finger vein pre-processing, feature extraction, feature fusion from multiple instances and creation of cancelable protected templates for secured authentication. Fig. 1 depicts pre-processing which involves alignment of individual finger vein images, ROI selection and image enhancement. Fig. 4 describes the overall enrolment and authentication process of right index and right middle finger vein images with feature extraction, feature fusion and cancelable protected templates.

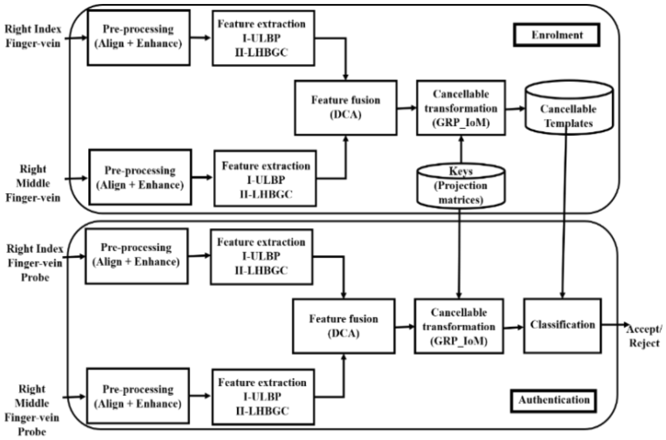
Right Index Finger-vein
Pre-processing (Align + Enhance)
Feature extraction I-ULBP II-LHBGC
Enrolment
Feature fusion (DCA)
Cancellable transformation (GRP_IoM)
Cancellable Templates
Right Middle Finger-vein
Pre-processing (Align + Enhance)
Feature extraction I-ULBP II-LHBGC
Keys (Projection matrices)
Right Index Finger-vein Probe
Pre-processing (Align + Enhance)
Feature extraction I-ULBP II-LHBGC
Feature fusion (DCA)
Cancellable transformation (GRP_IoM)
Classification
Accept/ Reject
Right Middle Finger-vein Probe
Pre-processing (Align + Enhance)
Feature extraction I-ULBP II-LHBGC
Authentication

Fig. 4. Block Diagram of Proposed Multi-instance Finger Vein-based Authentication.

In the proposed work, two localized texture-based feature extraction methods are experimented on finger vein images to extract features namely, method-I, Local Hybrid Binary Gradient Contour (LHBGC) and method II, Uniform Local Binary Pattern (ULBP). Both, LHBGC and ULBP feature extraction techniques are explained in section III-A.2. Features extracted from multiple instances, particularly from right index (RI) and right middle (RM) finger vein images are then fused to create a combined feature set using Discriminant correlation analysis (DCA) [39]. DCA feature fusion is practiced with summation technique which also involves feature dimension reduction to significant extent. Thus, the fused-discriminant feature set for RI and RM finger vein instances as FD-LHBGC and FD-ULBP are ready for cancelable transformation meant for template protection.

Fused finger vein feature set is then converted to hashed code using Gaussian Random Projection based Index of Maximum (GRP-IoM) hashing technique [2]. This generic hashing scheme is highly irreversible and un-linkable cancelable transform. The irreversibility and un-linkability of the proposed template protection method on fused multi-instance finger vein feature set is shown in experimentation section. Finally, the cancelable protected templates are stored in database with their corresponding projection matrices (keys).

Authentication of a person also requires pre-processing, feature extraction and hashed code transforms to be generated in the same manner as that during enrolment. Classification of an identity is carried on using collision classifier as explained in Section III-B. Authentication and template protection evaluations for the proposed framework are demonstrated and analyzed in the experimentation section.

IV. Experimental Results and Discussion

Experiments have been conducted on the real multi-instance biometric datasets to evaluate the performance of the proposed multi-instance finger vein-based authentication methodology with respect to verification performance and template protection.

A. Database

Two openly available standard databases are used for evaluating the overall results of the proposed multi-instance finger vein-based verification system as SDUMLA-HMT and UTFVP. The SDUMLA-HMT (Shandong University Machine Learning and Applications) biometric database [40] consists of finger vein images for 106 individuals in addition to samples of additional biometric traits such as the face and iris. There are vein images of six fingers (three on each hand) and since vascular patterns differ on every finger of every hand, there are effectively 106 x 6 = 636 possible classes to identify. Furthermore, six images per class were captured resulting in a total of 3816 images. Each image is 320 x 240 pixels in dimension and stored in the uncompressed, bitmap file format. The UTFVP finger vascular pattern database [41] was produced by University of Twente, Nederland. It consists of 1440 images from 60 persons with 4 images per instance of 6 different fingers. The resolution of each image is 672 x 380 pixels stored in 8-bit gray scale PNG format.

B. Experimentation

We ensured that the data used to train the feature fusion process was never used to test it so that a true indication of its predictive accuracy could be obtained. For SDUMLA-HMT database, a total of 1272 images were used in carrying out the experiments. Individually for 106 subjects, four samples are used for training with DCA which executes feature fusion and dimension reduction and two samples for authentication testing. Combination of right middle (RM) and right index (RI) finger veins is considered for experimentation as it is the most popular and convenient choice for multi-instance system. Experimentation is carried on with total of 212 (106 x 2) genuine scores and 44520 ((212-2) x 212) imposter scores for SDUMLA-HMT database. Similarly, in case of UTFVP database, total 480 finger vein images are used for experimentation. Training involved two samples per class and testing is done on other two samples for multiple instances. Experimentation is done on UTFVP with total of 120 (60x2) genuine and 14160 (120 x (120-2)) imposter scores. All the experiments are implemented using MATLAB 2019a on a system i5-CPU with 2.5 GHz and 4 GB memory.

1) Verification performance evaluation: The verification performance of the proposed multi-instance finger vein authentication system is evaluated in terms of percentage equal error rate (EER). Fig. 5 shows Receiver Operating Characteristics (ROC) curves for the proposed verification systems, which also indicates the corresponding EER i.e., the error at where false acceptance rate (FAR) is equal to genuine acceptance rate (GAR). FAR, FRR (false rejection rate) and GAR are represented by following Eqs. (3-5).

$$\mathrm{FAR} = \frac{Number\ of\ falsely\ accepted\ imposters}{Total\ number\ of\ imposter\ trials} \tag{3}$$

$$FRR = \frac{Number\ of\ falsely\ rejected\ genuines}{Total\ number\ of\ genuine\ trials} \tag{4}$$

$$GAR = 1 - FRR \tag{5}$$

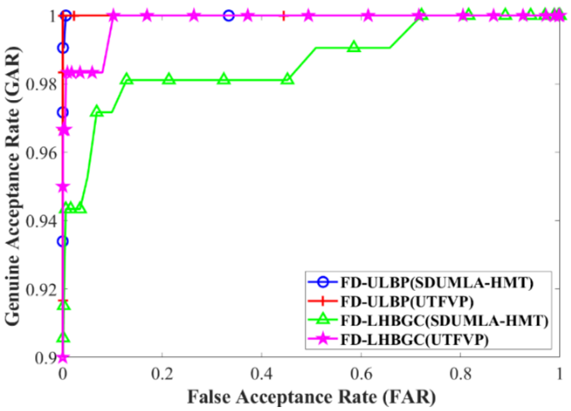

Fig. 5. Receiver Operating Characteristic (ROC) Curves for Proposed Verification with (a) LHBGC and (b) ULBP Feature Extraction.

These ROC curves in Fig. 5 demonstrate that verification performance of the proposed multi-instance (RM+RI) finger vein system is much better with FD-ULBP features as compared to that of FD-LHBGC features. The proposed verification results in the form of EER with practiced feature extraction methods are depicted in Table I with the corresponding feature lengths for two different databases. Since the feature deformation method used for template protection is based on random projections, the EER is computed by considering the average of repeated twenty different randomly generated key-projections.

TABLE I. VERIFICATION PERFORMANCE OF THE PROPOSED SYSTEM

Method	Feature Extraction Method	Verification Performance (%EER) (95% confidence level)	
		Database	
		SDUMLA-HMT	UTFVP
I	FD-LHBGC[a]	4.2 ± 0.19	1.54 ± 0.11
II	FD-ULBP[b]	0.53 ± 0.161	0.00074± 00119

[a] Fused Discriminant-Local Histogram Binary Gradient Contour and [b] Uniform Local Binary Pattern.

Thus, it is observed that FD-ULBP features are providing better and exceptional verification as compared to that of FD-LHBGC features regardless of change in database. Also, the proposed system is providing considerable verification with incredibly low feature length. This reduces the working plane complexity as well as memory requirement for template storage.

2) Template protection evaluation: In this section, privacy and security of templates are evaluated and analyzed for the proposed multi-instance finger vein authentication system. Privacy analysis implies to the practical possibility for a template protection technique to tolerate any attack for regaining the intrinsic feature information. Whereas, to achieve considerable attack complexity against the unlawful access to the template protection system through counterfeit features is termed as template security. Particularly for Renewable biometrics, privacy analysis covers non-invertibility of templates and Attacks via Record Multiplicity (ARM) whereas brute force attack analysis and ARM are included in security analysis. These individual investigations are described as follows:

a) Privacy analysis: Privacy analysis covers the assessment of non-invertibility/irreversibility and ARM for templates. Non-invertibility is the measure of computational toughness in retrieving the original feature set from the hashed coded stream with and/or without GRP-IoM method based random key matrices. Even if the number of random Gaussian vectors (q) for all the number of iterations (n) are known to the adversary, there is no clue available to recover the original real valued feature vector (x) from illegitimately obtained hashed coded templates. This is possible because there is no direct link between the projection matrices (token) and the original feature vector due to Index of Max (IoM) property of hashed code. In this case, to break the template privacy the adversary needs to predict the fused real valued features. Considering the worst scenario, let us assume that the maximum and minimum values of original features are known to the adversary for analyzing the guessing complexity. Considering an actual feature example with the minimum and maximum values for a fused feature set obtained for FD-ULBP features tested on SDUMLA-HMT finger vein instances as −0.3361 and 0.3622, respectively. Suppose the adversary tries to guess from −0.3361, −0.3360, −0.3359 and so on, until the maximum 0.3622. In this case, the total of 6983 options for predicting in the range of four decimal digit precision as in our execution, four decimal digits exactness is fixed. As guessing possibility of a single feature element is coming as 6983 ($\approx 2^{13}$) attempts. Hence, the entire feature vector comprising of 105 elements needs around $2^{13x105}=2^{1365}$ trials. The guessing possibilities for the single and entire feature vector element for the proposed two feature types are shown in Table II. This guessing process is observed to be computationally infeasible. Moreover, the so called guessed feature set is not the original or raw finger vein features but the fused version of two finger vein instances which further adds on to the feature confidentiality.

TABLE II. GUESSING POSSIBILITY FOR SINGLE FUSED FEATURE AND COMPLETE FUSED FEATURE SET

Database (Feature Extraction)	Minimum value	Maximum value	Possibilities for single feature component	Total possibilities for complete feature set
SDUMLA-HMT (FD-ULBP)	-0.3361	0.3622	$6983 \approx 2^{13}$	$2^{13x105} = 2^{1365}$
UTFVP (FD-ULBP)	-0.5243	0.5603	$10846 > 2^{13}$	$2^{13x59} = 2^{767}$
SDUMLA-HMT (FD-LHBGC)	-0.0178	0.0239	$417 \approx 2^{9}$	$2^{9x105} = 2^{945}$
UTFVP (FD-LHBGC)	-0.105	0.0198	$303 > 2^{8}$	$2^{8x59} = 2^{472}$

ARM (Attacks via record multiplicity) is a kind of intrusion to template privacy which tries to reconstruct the original biometric data using numerous forfeited templates with or without parameters and information that linked to the algorithm. Specifically, ARM in IoM hashing is computationally tough for deducing the mathematical value as the saved templates are altered into rank space which are not correlated to the finger vein feature space. Thus, the ARM attack intricacy is the same as the non-invertibility attack possibility presented, formerly.

b) Security analysis: Security of biometric templates is in danger when threats like brute force attack or masquerade attack or pre-image attack. For GRP based template protection scheme, with *m*=150, *q*=70, guess intricacy for each entry is greater than 26 (70), as indices of hash code takes values between 1 and 70. Therefore, guess complexity for best performance obtained as for 150 (SDUMLA-HMT) and 300 (UTFVP) entries are greater than 2^{900} and 2^{1800} respectively. This is again computationally infeasible.

c) Unlinkability analysis: The unlinkability of the implemented multi-instance template protection scheme is validated by involving the pseudo-genuine scores. The pseudo-genuine scores are generated by matching different fused multi-instance finger vein hash codes of the same individual created by utilizing distinct key projection matrices. The pseudo-imposter scores are computed by matching hashed code templates of different individual created by using different key projection matrices, as explained in section IV-B.3.c With this perspective, the overlapping extent of pseudo-genuine and pseudo-imposter distributions indicates the indistinctive ability of the template generation from same or different users. The un-linkability level contributed by the implemented multi-instance finger vein-based authentication framework is indicated by the difficulty in discriminating these hash coded templates.

Fig. 6 and Fig. 7 demonstrate the distribution of pseudo-genuine and pseudo-imposter scores for both the proposed features as FD-ULBP and FD-LHBGC, experimented on SDUMLA-HMT and UTFVP databases. The pseudo-genuine and pseudo-imposter score plots are observed to be mainly overlapped for both the features. These results show that the IoM codes highly meet un-linkability property for the proposed multi-instance finger vein authentication.

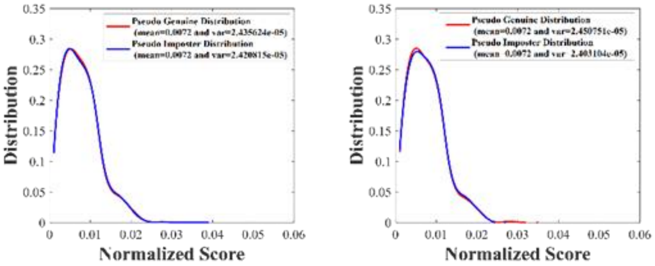

Fig. 6. Un-linkability Analysis using Fused Discriminant Uniform Local Binary Pattern (FD-ULBP) Features on (a) SDUMLA-HMT and (b) UTFVP database.

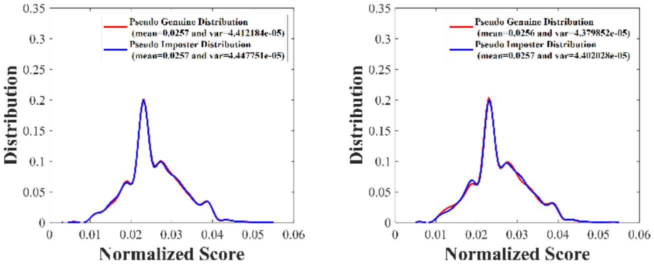

Fig. 7. Unlinkability Analysis using Fused Discriminant Local Hybrid Binary Gradient Contour (FD-LHBGC) Features on (a) SDUMLA-HMT and (b) UTFVP Database.

d) Revocability analysis: Revocability or cancelability or renewability is determined by performing the experiments explained in [2]. This generates 105 × (2 × 106) = 22260 and 59 x (2 x 60) = 7080 pseudo-imposter scores for SDUMLA and UTFVP datasets, respectively. The distributions for genuine, imposter and pseudo-imposter scores are exhibited in Fig. 8 and Fig. 9 for both the FD-ULBP and FD-LHBGC features, respectively. It is noticed from Fig. 8 that the imposter and pseudo-imposter distributions for FD-ULBP features are largely overlapped. Fig. 9 implies that the pseudo imposter and imposter scores are not overlapping with each other for FD-LHBGC features, but the pseudo imposter distribution is still distinctive with genuine score distribution preserving differentiation between the two. This entails that even though the hashed codes belonging to the same source finger vein set are freshly created or renewed through newly generated random projection matrices, they are very much distinctive.

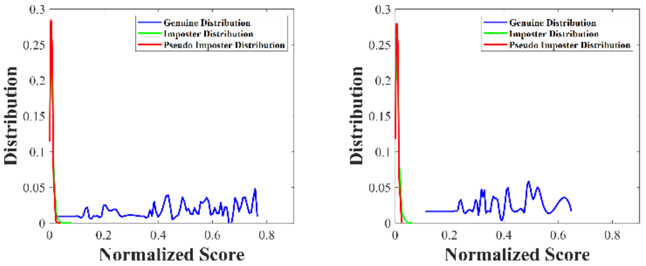

Fig. 8. Revocability Analysis using Fused Discriminant Uniform Local Binary Pattern (FD-ULBP) Features on (a) SDUMLA-HMT and (b) UTFVP Datasets.

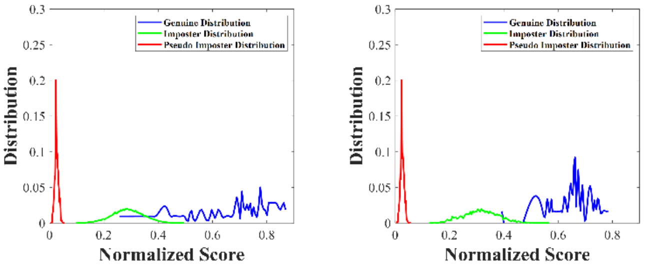

Fig. 9. Revocability Analysis using Fused Discriminant Local Hybrid Binary Gradient Contour (FD-LHBGC) Features on (a) SDUMLA-HMT and (b) UTFVP Datasets.

3) Validations: Obtained results from the proposed authentication system are validated by comparing with that of other existing finger vein-based authentication systems. Validation is shown on comparisons to some of the similar existing finger vein systems based on their verification performance. Table III includes similar existing verification systems implemented with variety of feature extraction and classification methods. These systems contain methods utilizing single as well as multiple instances of finger veins. Performance comparison is shown on the viewpoints of authentication performance, number of evidence/instances used for authentication and template protection.

It has been observed from Table III that the proposed verification framework outperforms the shown similar work on the combined scale of verification performance and template protection. As some of the verification systems like [5] and [8] shows better verification but at the cost of unprotected templates. Moreover, the proposed system implemented the verification utilizing two finger vein instances contributing to a greater number of evidence as identity proofs.

The verification performance combining with template protection property from Table III indicates that the proposed-I framework i.e., with Fused-Discriminant Uniform Local Binary Pattern (FD-ULBP) features performs better than Fused-Discriminant Local Histogram Binary Gradient Contour (FD-LHBGC) features as an overall authentication system with protected templates. Finger vein feature extraction and matching time contributes to the computation cost of the overall authentication system.

Moreover, if the system includes template protection and/or utilizing more than one instance of finger vein that again adds on the computational burden. Table IV shows the comparison of feature extraction and matching time of the proposed system with some of the similar popular methods practiced for finger vein authentication tested on a varied quality finger vein dataset, SDUMLA-HMT.

TABLE III. Comparison of the Verification Performance of the Proposed System with Similar Existing Verification Systems

Related work	**Feature extraction method**	**Classifier**	**Template protection method**	**Verification performance (% Accuracy)**		**No. of instances used**	**Template protection**
				SDUMLA-HMT	**UTFVP**		
Ton et al. [15]	Maximum Curvature	Correlation	---		0.4	1	No
Kauba et al. [17]	Different feature level fusion	Correlation	---		0.19	1	No
Yang et al. [18]	Anatomy Structure Analysis based Vein Extraction (ASAVE)	Elastic matching	---	1.39		1	No
Yang et al. [14]	Local Binary Pattern (LBP), t-norm based score fusion	Hamming distance	---	1.58		2	No
Ong et al. [5]	Local Histogram Binary Gradient Contour (LHBGC)	Support Vector Machine	---	0.034		2	No
Syarif et al. [8]	Enhanced Maximum Curvature, Histogram of Oriented Gradients	Support Vector Machine	---	0.14		1	No
Yang et al. [30]	Gabor Filter, Principal Component Analysis (PCA)	L2-Norm	Random proj. transform, fuzzy commitment scheme	3		1	Yes
Yang et al. [36]	Principal Curvature	Cosine similarity	Wrapping in feature domain		0.71	1	Yes
	Repeated Line Tracking	Collision Probability	Align. Robust Hash, Index of Max hash.		3.89	1	Yes
Kirchgasser et al. [35]	Gabor Filter, Linear Discriminant Analysis (LDA)	Multi-Layer Extreme Learning Machine	Biohashing, Binary Decision Diagram	7.04		1	Yes
Proposed-I	FD-ULBP	Collision Probability	GRP-IoM	**0.53 ± 0.161**	**0.00074 ± 0.00119**	**2**	**Yes**
Proposed-II	FD-LHBGC	Collision Probability	GRP-IoM	4.2 ± 0.19	1.54 ± 0.11	2	Yes

TABLE IV. COMPARISON OF COMPUTATION TIME (SECONDS) OF THE PROPOSED SYSTEM WITH SOME STATE-OF-THE-ART FINGER VEIN-BASED AUTHENTICATION SYSTEMS TESTED ON SDUMLA-HMT DATASET

Related work	**Feature extraction method**	**Classifier**	**Template protection method**	**Computation time**			**No. of instances used**	**Template protection**
				Feature extraction time	***Matching time***	***Total Computa-tion time***		
Miura et al. [3]	Repeated Line Tracking	Miura match	---	19.24	0.97	20.21	1	No
Miura et al. [6]	Maximum Curvature	Miura match	---	0.7	0.97	1.67	1	No
Huang et al. [7]	Wide Line Detector	Miura match	---	0.56	0.97	1.53	1	No
Syarif et al. [8]	Maximum Curvature, Histogram of Oriented Gradient	Support Vector Machine	---	0.72	0.07	0.79	1	No
	Enhanced Maximum Curvature, Histogram of Oriented Gradient	Support Vector Machine	---	0.59	0.07	0.66	1	No
Ong et al. [5]	Local Histogram Binary Gradient Contour	Support Vector Machine	---	0.4496	0.0047	0.4543	2	No
Ong et al. [9]	Minutiae	GA, k-modified Hausdorff dist.	---	---	---	0.7528	2	No
Proposed-I	FD-ULBP	Collision Probability	GRP-IoM	0.4609	6 x 10^{-4}	0.4615	2	Yes
Proposed-II	FD-LHBGC	Collision Probability	GRP-IoM	0.4545	6.23 x 10^{-4}	0.4551	2	Yes

It is observed from Table IV that both the proposed multi-instance finger vein authentications are outperforming with respect to some single or multi-instance state-of-the-art finger vein-based systems on the scale of computation time. In [5], LHBGC feature extraction time is calculated with the same parameter values (number of rows and columns) as that of the LHBGC based proposed-II system for fair comparison. Feature extraction time for the proposed methods involve pre-processing time, feature extraction time, fusion time, and template protection-based code generation time for two instances of finger vein images. Despite inclusion of template protection scheme, the proposed systems are showing significantly low values for feature extraction or template generation time. Moreover, matching time for the coded template is substantially less because of simple collision computations involved. Hence, the computational complexity of both the proposed protected systems is comparatively low with respect to the shown non-protected template-based finger vein systems.

Thus, the proposed methods of multi-instance finger vein systems provide considerable authentication accuracy with lower computation cost. The proposed frameworks also facilitate renewable templates in case of compromise with high irreversibility and unlinkability to produce template protection enabled authentication.

V. CONCLUSION

The proposed multi-instance finger vein-based biometric authentication system offers significant authentication performance. The proposed system used two local texture-based features which are computationally economical. Template protection is incorporated via. highly non-invertible and unlinkable, transform-based projection offering cancelable biometric templates. Proposed framework provides significant reduction in computational cost for feature extraction and template matching, balanced with considerably outperforming authentication accuracy. Cancelable biometric template generation method as Gaussian Random Projection based Index-of-Max (GRP-IoM) is incorporated for template protection. The proposed Fused Discriminant-Uniform Local Binary Pattern (FD-ULBP) and Fused Discriminant-Local Hybrid Binary Gradient Contour (FD-LHBGC) feature based finger vein systems are observed to outperform some existing systems on the scale of verification performance. The proposed frameworks are experimented on two standard databases as SDUMLA-HMT and UTFVP. Moreover, FD-ULBP features are found to provide more significant results than FD-LHBGC for authentication and template protection.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude towards the authorities of K.J. Somaiya College of Engineering, Mumbai for providing continual support during this research work.

REFERENCES

[1] P. Campisi, Ed., Security and Privacy in Biometrics. Springer, 2013.

[2] Z. Jin, J. Y. Hwang, Y. L. Lai, S. Kim and A. B. J. Teoh, “Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index Of Max Hashing,” IEEE Transaction on Information Forensics and Security, 13 (2), 2018.

[3] N. Miura, A. Nagasaka and T. Miyatake, Feature Extraction of Finger-vein Pattern based on Repeated Line Tracking and its application to Personal Identification, Machine Vision and Applications, Springer, 15, 2004, pp. 194-203.

[4] T. Ojala, M. Pietikainen, and T. Maenpaa, Multiresolution Gray-scale and Rotation Invariant Texture Classification with Local Binary Patterns, IEEE Transactions on Pattern Analysis and Machine Intelligence, 24 (7), 2002, pp. 971-987.

[5] T. S. Ong, A. William, C. Tee and M. K. O. Goh, Robust Hybrid Descriptors for Multi-instance Finger Vein Recognition, Multimedia Tools Appl., Springer Science, 77, 2018, pp. 29163-29191.

[6] N. Miura and A. Nagasaka, Extraction of Finger-vein Patterns using Maximum Curvature Points in Image Profiles, IAPR Conference on Machine Vision applications, Tsukuba Science City, Japan, pp. 347-350, 2005.

[7] B. Huang, Y. Dai, R. Li, D. Tang and W. Li, Finger-Vein Authentication Based on Wide Line Detector and Pattern Normalization, IEEE 20th International Conference on Pattern Recognition, Istanbul, Turkey, pp. 1269-1272, 2010.

[8] M. A. Syarif, T. S. Ong, A. B. J. Teoh and C. Tee, Enhanced Maximum Curvature Descriptors for Finger Vein Verification, Multimedia Tools Appl., Springer Science, 76, 2016, pp. 6859-6887.

[9] T. S. Ong, J. H. Teng, K. S. Muthu and A. B. J. Teoh, Multi-instance Finger Vein Recognition Using Minutiae Matching, IEEE 6th International Congress on Image and Signal Processing, Hangzhou, China, , 3, pp. 1730-1735, 2013.

[10] Y. Wang, Y. Fan and W. Liao, Hand Vein Recognition Based on Multiple Keypoints Sets. In: 5th IAPR International Conference of Biometrics ICB, New Delhi, India, pp. 367–371, 2012.

[11] Y. C. Cheng, H. Chen and B. C. Cheng, Special Point Representations for Reducing Data Space Requirements of Finger Vein Recognition Applications, Multimedia Tools Appl., Springer Science, 76 , 2017, pp. 11251-11271.

[12] T. Ojala, M. Pietikäinen and D. Harwood, A comparative study of texture measures with classification based on feature distributions. Pattern Recognition, 29, 1996, pp. 51-59.

[13] X. Xi, G. Yang, Y. Yin and X. Meng, Finger Vein Recognition with Personalized Feature Selection, Sensors, 13 (9), 2013, pp. 11243–11259.

[14] Y. Yang, G. Yang and S. Wang, Finger Vein Recognition based on Multi-instance, International Journal of Digital Content Technology and its Applications, 6 (11), 2012, pp. 86-94.

[15] B. T. Ton and R. N. J. Veldhuis, A high quality finger vascular pattern dataset collected using a custom designed capturing device, In: Proc. Int. Conf. Biometrics (ICB), Madrid, Spain, pp. 1–5, 2013.

[16] H. T. Van, T. T. Thai, and T. H. Le, Robust finger vein identification base on discriminant orientation feature, In: 7th Int. Conf. on Knowledge and Systems Engineering (KSE), Ho Chi Minh City, Vietnam, pp. 348–353, 2015.

[17] C. Kauba, E. Piciucco, E. Maiorana, P. Campisi, and A. Uhl, Advanced variants of feature level fusion for finger vein recognition, In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2016.

[18] S. Qiu, Y. Liu, Y. Zhou, J. Huang, and Y. Nie, Finger-vein recognition based on dual-sliding window localization and pseudo-elliptical transformer, Expert Systems with Applications, 64, 2016, pp. 618 – 632.

[19] L. Yang, G. Yang, Y. Yin, and X. Xi, Finger vein recognition with anatomy structure analysis, IEEE Transactions on Circuits and Systems for Video Technology, 28 (8), 2018, pp. 1892–1905.

[20] A. Banerjee, S. Basu, S. Basu, and M. Nasipuri, Artem: a new system for human authentication using finger vein images, Multimedia Tools and Applications, 77, 2018, pp. 5857-5884.

[21] H. Hong, M. Lee, and K. Park, Convolutional neural network-based finger-vein recognition using NIR image sensors, Sensors, 17 (6) , 2017, 1297.

[22] R. Das, E. Piciucco, E. Maiorana, and P. Campisi, Convolutional neural network for finger-vein-based biometric identification, IEEE Trans. Inf. Forensics Secur., 14 (2), 2019, pp. 360–373.

[23] G. K. Sidiropoulos, P. Kiratsa, P. Chatzipetrou and G. A. Papakostas, Feature Extraction for Finger-Vein-Based Identity Recognition, Journal of Imaging 7 (5), 2021, 89.

[24] M. Gomez-Barrero, C. Rathgeb, J. Galbally, J. Fierrez, and C. Busch, Protected Facial Biometric Templates Based on Local Gabor Patterns and Adaptive Bloom Filters, in Proc. Int. Conf. Pattern Recognit., Stockholm, Sweden, pp. 4483–4488, 2014.

[25] G. Li, B. Yang, C. Rathgeb, and C. Busch, Towards Generating Protected Fingerprint Templates Based on Bloom Filters, in Proc. Int. Workshop Biometrics Forensics (IWBF), Gjovik, Norway, pp. 1–6, 2015.

[26] J. Bringer, C. Morel, and C. Rathgeb, Security Analysis of Bloom Filter-based Iris Biometric Template Protection, in Proc. Int. Conf. Biometrics (ICB), Phuket, Thailand, pp. 527–534, 2015.

[27] P. P. Paul and M. Gavrilova, Multimodal Cancelable Biometrics, IEEE 11th International Conference on Cognitive Informatics & Cognitive Computing, Kyoto, Japan, pp. 43-49, 2012.

[28] Y. Chin, T. Ong, A. Teoh and K. Goh, Integrated Biometrics Template Protection Technique Based on Fingerprint and Palmprint Feature-level Fusion, Information Fusion, 18, 2013, pp. 161-174.

[29] W. Yang, J. Hu, and S. Wang. A finger-vein based cancellable biocryptosystem. In: Network and System Security 7th International Conference, NSS 2013, Madrid, Spain, pp. 784–790, 2013.

[30] W. Yang, S. Wang, J. Hu, G. Zheng, J. Chaudhry, E. Adi and C. Valli, Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-vein Bio-Crytosystem, IEEE Access, Special Section on Cyber Threats and Countermeasures in the Healthcare Sector, 6, 2018, pp. 36939-36947.

[31] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao. Finger vein secure biometric template generation based on deep learning. Soft Comput., 22 (7), 2018, pp. 2257–2265.

[32] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch. Multi-biometric template protection based on bloom filters. Information Fusion, 42, 2018, pp. 37-50.

[33] D. Hartung, M. Tistarelli, and C. Busch, Vein minutia cylinder-codes (VMCC), In: International Conference on Biometrics, ICB 2013, Madrid, Spain, pp. 1–7, 2013.

[34] T. Ong, A. William, T. Connie and M. Kah Ong Goh, “Robust hybrid descriptors for multi-instance finger vein recognition”, Multimedia Tools and Applications, 77(21), 2018, pp. 29163-29191.

[35] S. Kirchgasser, C. Kauba, Y. Lai, J. Zhe and A. Uhl, Finger Vein Template Protection based on Alignment-Robust Feature Description and Index-of-Maximum Hashing, IEEE Transactions on Biometrics, Behavior and Identity Science, 2020.

[36] W. Yang , S. Wang , J. Hu , G. Zheng , J. Yang and C. Valli, Securing Deep Learning Based Edge Finger Vein Biometrics With Binary Decision Diagram, IEEE Transactions on Industrial Informatics, 15 (7), 2019, pp. 4244-4253.

[37] H. O. Shahreza and S. Marcel, Towards Protecting and Enhancing Vascular Biometric Recognition Methods via Biohashing and Deep Neural Networks, IEEE Transactions on Biometrics, Behavior, and Identity Science, 3 (3), 2021, pp. 394-404.

[38] B. Prommegger, C. Kauba and A. Uhl, Multi-Perspective Finger-Vein Biometrics, IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2018, pp. 1-9.

[39] M. Haghighat, M. A. Mottaleb and W. Aalhalabi, Discriminant Correlation Analysis: Real Time Feature Level Fusion for Multimodal Biometric Recognition, IEEE Transactions on Information Forensics and Security, 11 (9), 2016, pp. 1984-1996.

[40] Y. Yin, L. Liu, and X. Sun, “SDUMLA-HMT: A multimodal biometric database," in Proc. Chin. Conf. Biometric Recognit, Springer Verlag, pp. 260-268, 2011. (accessed 05 Jan. 2019).

[41] Twenty University dataset, “http://www.utwente.nl/em/eemcs/ds‘’, online accessed on Oct-2019.