A. Brömme, C. Busch, C. Rathgeb and A. Uhl (Eds.): BIOSIG 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 297

Empirical Evaluation of LBP-Extension Features for Finger Vein Spoofing Detection

Daniel Kocher,[1] Stefan Schwarz[1] and Andreas Uhl[1]

Abstract: Biometric systems based upon finger vein images have been shown to be vulnerable to presentation attacks. For this paper, we consider a variety of methods extending local binary patterns (LBP) which can be used to distinguish between fake and real finger vein images. In the experiments, it is not only the accuracy of the respective methods as compared to baseline LBP which is documented, but also the impact of two further criteria: (1) The influence of selecting training & test samples non-randomly, i.e., selecting training samples in person-specific and size-varying manner, and (2) the impact of lowering the feature dimensionality by considering only uniform patterns. Our results show that these two criteria have to be considered if one wants to apply finger vein anti-spoofing mechanisms while the baseline LBP technique turns out to be competitive to almost all of its "improvements". As subject specific training data is usually not available, our results underpin the importance of using sufficiently sized training data when aiming for high spoofing detection accuracy.

Keywords: Finger Vein Spoofing, Spoofing Detection, Biometrics, Texture-based, Local descriptor, Local Binary Pattern (LBP), Local Radius Index (LRI), Local Derivative Pattern (LDP), Local Graph Structure (LGS), Symmetric Local Graph Structure (SLGS)

1 Introduction

Biometric traits have emerged to replace or at least complement the traditional authentication methods (e.g. passwords). One biometric trait enjoying more and more popularity are veins. One advantage of veins over other biometric traits is the fact that they are embedded *inside* the human body, as opposed to traits like fingerprints or faces. Moreover, vein images can be acquired in an unintrusive manner which is not the case for other biometric traits, such as iris acquisition. However, despite being resistant to tampering, vein-based authentication is vulnerable to presentation attacks [TVM14]. In this paper, we focus on finger veins (FVs) as biometric traits.

In general, counter-measures to presentation (or spoofing) attacks in biometrics can be categorised in (1) liveness-based, (2) motion-based and (3) texture-based methods. Liveness-based methods, e.g., [Ra15], use signs of vitality to ensure that the image is captured from a living human being. In contrast, motion-based methods utilise unnatural movements on scenes as indication of spoofing, e.g. caused by hand motion when presenting a photo or a display to the sensor. Texture-based methods aim to explore textural artifacts in the images captured by the sensor (e.g. caused by recapturing artifacts). Texture-based

[1] University of Salzburg, Department of Computer Sciences, University of Salzburg, {dkocher,sschwarz,uhl}@cosy.sbg.ac.at

techniques have been proven to be applicable to the imagery in the FV-Spoofing-Attack database [To15] for evaluation, in particular baseline LBP [RB15].

In 2015, the first competition on counter-measures to finger vein spoofing attacks took place [To15]. The competition baseline algorithm looks at the frequency domain of vein images, exploiting the bandwidth of vertical energy signal on real finger vein images, which is different for fakes ones. Three teams participated in this competition. The first team (GUC) uses binarised statistical images features (BSIF). They represent each pixel as a binary code. This code is obtained by computing the pixel's response to a filter that are learnt using statistical properties of natural images [To15]. The second team (B-Lab) uses monogenic scale space based global descriptors employing the Riesz transform. This is motivated by the fact that local object appearance & shape within an image can be represented as a distribution of local energy and local orientation information. The best approach (team GRIP-PRIAMUS) utilises local descriptors, i.e., local binary patterns (LBP), and local phase quantisation (LPQ) and Weber local descriptors (WLD). They distinguish between full and cropped images. LBPs and LPQ/WLD are used to classify full and cropped images, respectively.

However, counter-measures to finger vein spoofing attacks were/are already developed prior or independent to this competition. In 2013, the authors of [Ng13] introduced a fake finger vein image detection based upon Fourier, and Haar and Daubechies wavelet transforms. For each of these features, the score of spoofing detection was computed. To decide whether a given finger vein image is fake or real, an SVM was used to combine the three features.

The authors of [Ti15] propose windowed dynamic mode decomposition (W-DMD) to be used to identify spoofed finger vein images. DMD is a mathematical method to extract the relevant modes from empirical data generated by non-linear complex fluid flows. While DMD is classically used to analyse a set of image sequences, the W-DMD method extracts local variations as low rank representation inside a single still image. It is able to identify spoofed images by capturing light reflections, illuminations and planar effects.

A detection framework based on singular value decomposition (SVD) is proposed in a rather confused paper [MS15]. Finger vein images are classified based on image quality assessment (IQA) without giving any clear indication about the actual IQA and any experimental results.

Finally, [RB15] proposes a scheme using steerable pyramid is used to extract features. Steerable pyramids are a set of filters in which a filter of arbitrary orientation is synthesised as a linear combination of a set of basis functions. This enables the steerable pyramids scheme to compute the filter response at different orientations. This scheme shows consistent high performance for the finger vein spoofing detection problem and outperforms many other texture-classification-based techniques. It is compared to techniques from [To15], including two LBP variants, and to quality-based approaches computing block-wise entropy, sharpness, and standard deviation.

In this paper, inspired by the success of basic LBP techniques [MS15, To15] in finger vein spoofing detection and the availability of a wide variety of LBP extensions and generalisations in literature, we empirically evaluate different features obtained by using these more recent LBP-related feature extraction techniques for finger vein spoofing detection. The feature histograms are used as input for a linear support vector machine. Further, the evaluation shows the influence of (1) randomisation of the persons which are selected for training & test data, and (2) using uniform patterns rather than the whole feature vector.

The remainder of this paper is organised as follows. The evaluated LBP features are described in Section 2. The experimental setup and the results are described in Section 3 where we also describe the finger vein database used in the evaluation.

2 Local Binary Pattern Extensions

The references and more detailed descriptions of the original LBP scheme and subsequent LBP variants are provided in [KSU16] due to space restrictions. Also, the parameters of our implementations as used in the experiments are given in this reference. For our experiments (Section 3), the LBP-based features described in the following are applied to all pixels of the image except for those which have not enough neighboring pixels available. Pixels are traversed line-wise and for each feature, a histogram has been constructed.

The traditional *Local Binary Pattern* operator was originally introduced by [OPH94] in 1994. The authors proposed the operator as a non-parametric 3×3 kernel. However, LBP can be parameterised in two ways, i.e. the number of neighboring pixels P and the radius R from the center pixel. The P neighboring pixels are distributed evenly spaced on the circle of radius R with respect to a given center pixel. Using these parameters, the 3×3 kernel has $P = 8$ neighbors distributed evenly spaced on a circle of radius $R = 1$. Finally, a LBP is defined as an ordered set of binary values determined by comparing the values of the center pixel to the values of each neighboring pixels. When evaluated at each pixel position, the number of the different patterns found in an image are represented in a histogram.

The *Local Line Binary Pattern* (*LLBP*) operator was proposed for face recognition originally. The benefit of this pattern is that it can emphasise the change in image intensity such as vertices, edges and corners. The neighborhood shape is a straight line, instead of a circle shape. The operator consists of two components: a horizontal and a vertical component.

In the *completed* LBP (*CLBP*) variant, a region is represented by its center pixel and a so-called *local difference sign-magnitude transform* (*LDSMT*), which decomposes the local structure into two components, i.e. a *difference sign* and a *difference magnitude* component, denoted CLBP_S and CLBP_M, respectively. In essence, CLBP_S is equal to the standard LBP (using -1 instead of 0 to encode a negative difference). The center pixel component (CLBP_C) is represented by thresholding the local gray level against the average gray level of the whole image.

The robust LBP variant termed *Median Robust Extended LBP* (*MRELBP*) increases the tolerance to image blur and noise corruption. Different from the traditional LBP and many

LBP variants, MRELBP compares regional image medians rather than raw image intensities. A multiscale LBP type descriptor can be computed by efficiently comparing image medians over a custom sampling scheme.

The *Local Derivative Pattern* (*LDP*) encodes local higher order derivative information. While the original LBP encodes the binary result of the first-order derivative among local neighbors, the LDP is a higher-order local pattern which contains more detailed discriminative features wrt. orientation and higher order derivatives.

Local Radius Index (*LRI*) is based upon the fact that textures typically contain repetitive smooth regions and transitions between these regions. The authors introduce an inter-edge distance, the distribution of which to characterise the texture of an image (actually, two LRI operators, each of which results in eight integer directional indices for a given pixel are defined).

Local Graph Structure (*LGS*) represents each pixel by a graph structure which captures the spatial information with respect to the neighboring pixels, all neighboring pixels are thresholded against a source pixel based upon the traversal of the graph structure. *Symmetric Local Graph Structure* (*SLGS*) is a variant employing a different underlying graph structure of the neighbourhood.

3 Experiments

3.1 Experimental Setup

All implemented methods are evaluated on the Spoofing-Attack finger vein database created by the Idiap Research Institute [TVM14]. This database consists of 440 finger vein images from 110 subjects. All finger vein images were recorded using the same sensor.

The images are categorised into three sets, i.e., training set and development set (each of which consists of 120 spoofed and real images, respectively), and test set (200 images). The three sets are disjoint with respect to the clients. The database provides *full* printed (655×250 pixels) and *cropped* images (565×150 pixels). In this paper, only the full printed images were used in the evaluation process. Since the database was used for the 1^{st} competition on counter measures to finger vein spoofing attacks [To15], the test images are anonymised and thus the database does not provide reference results of the set of test images. Hence, only the training set of the dataset is used to evaluate the different approaches.

Those training set images were split into training and test images for our evaluation using different ratios, ranging from 10%/90% to 90%/10% for training and test images, respectively. Then, the histograms of the features were extracted from all training images in order to train a SVM. We used a linear SVM for all the experiments. In the next step, the histograms for the test images were generated and the previously trained SVM was used to classify these histograms (either real or spoofed image). To improve the robustness of the results, we used five randomly sampled instances per split ratio and feature. The reported

prediction accuracy is the average prediction accuracy (percentage of correct preditions, i.e. true positives plus true negatives) over all five instances. Additionally, for most features, we computed features with different parameter settings as described in Section 2. If averaged precision is given in the subsequent figures, we averaged over these different parameter settings.

We also evaluated the results for two different splitting modes. In the first mode, the splitting into training and test set is done randomly ignoring the subjects in the set. In contrast, the second mode takes the subjects into account by strongly separating subjects in the training and test images, i.e. a random image was picked and all remaining images of this person were also added to the respective set.

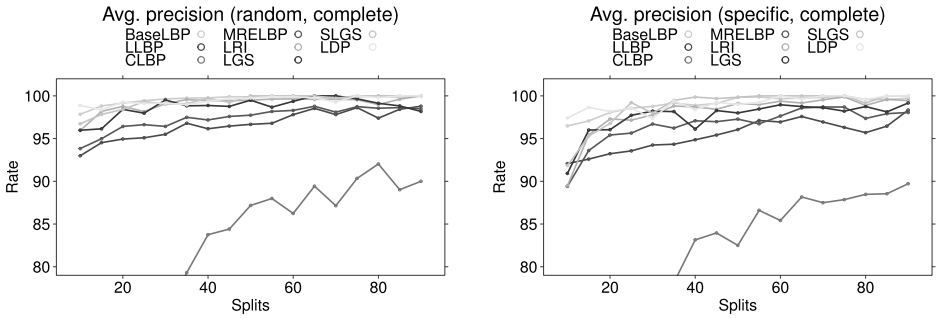
Moreover, we compared two LBP modes, i.e. the histograms were composed (1) of all patterns and (2) only of uniform patterns (i.e. the binary pattern contains at most two bitwise transitions from 0 to 1 or vice versa, non-uniform patterns are fused into a single histogram bin).

3.2 Experimental Results

In the following figures, we plot classification rate of real vs. spoofed images against the rate of training images vs. test images (i.e. 10 Splits means 10% training and 90% test images, respectively), thus increasing the training data size. Fig. 1a shows the (average) baseline performance of the considered LBP variants using random splitting. The simple LBP variant (BaseLBP) is almost top performing in each split scenario (similar to LRI, LGS, SLGS, and LDP), MRELBP, LLBP and particularly CLBP are clearly worse.

The effect of separating subjects in the training and test images is shown in Fig. 1b. Especially for small training set sizes (Splits 10 – 30), all techniques exhibit lower classification accuracy as compared to the purely random sample selection strategy. LGS and LLBP perform worse across the entire range of training set sizes. This means that especially in case of small training set size, unseen subjects are harder to be correctly classified. BaseLBP and LDP provide the best performance for this scenario and should be used under such circumstances.

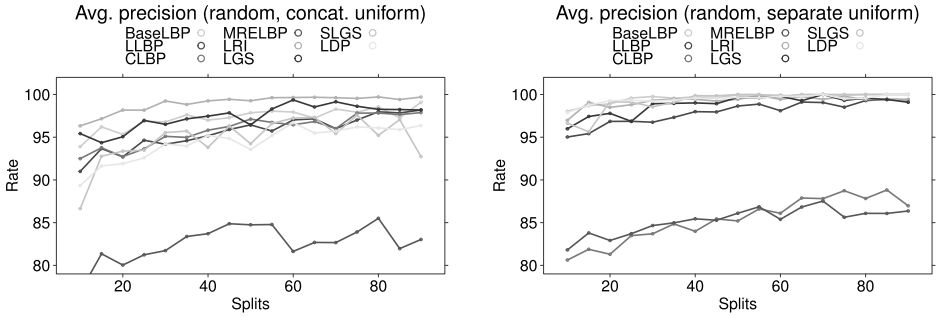
Fig. 2 illustrates the consequences when using uniform patterns only. We consider two variants of generating histograms without non-uniform patterns: (1) uniform patterns generated by first concatenating all the histograms involved and then filtering out all non-uniform patterns (see Fig. 2a) and (2) uniform patterns generated by first filtering out all non-uniform patterns and then concatenating the resulting histograms (see Fig. 2b). As we observe, the way of generating uniform pattern makes a difference. For the first generation type (1), most LBP variants lose classification accuracy as compared to their non-uniform counterpart (Fig. 1a), in particular MRELBP is severely degraded. However, CLBP significantly profits from using uniform patterns.



(a) random sample selection (b) subject-specific sample selection

Fig. 1: Average classification accuracy for complete patterns.

This behavior is mainly due to the fact that the histograms of the respective operators are concatenated, and the longer the feature vector gets the more non-uniform patterns are discarded (grouped into the 0 column of the histogram). Hence, although the usage of uniform patterns reduces the dimensionality of the feature vectors, one may not just use them for every LBP variant.



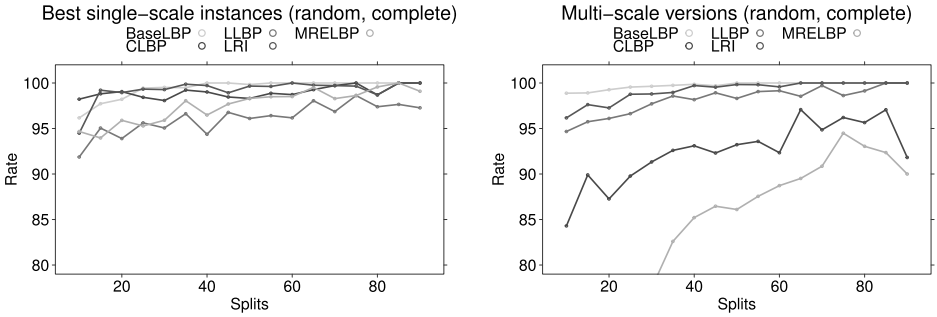
(a) concatenate – exclude non-uniform patterns (b) exclude non-uniform patterns – concatenate

Fig. 2: Average classification accuracy for two variants of generating histograms with uniform patterns with random sample selection.

For type (2) uniform patterns (Fig. 2b) we observe that CLBP loses its performance gain but is still better than with non-uniform patterns (compare Fig. 1a), while MRELBP is slightly improved compared to type (1). For the other LBP variants we see equal performance as for non-uniform patterns, LLBP is even sightly improved. Except for CLBP, type (2) is clearly the better strategy to generate uniform patterns.

The last plot, Fig. 3, shows the comparison between the classification accuracy of single- and multi-scale version of some features (multi-scale versions do not make sense for some patterns, e.g., the LGS). For the single-scale plot, we considered the parameter setting which performed best with respect to the classification accuracy (e.g., for the CLBP the instance with $R = 1$ and $P = 8$). As one can see, the multi-scale version outperforms the

best single-scale instance for some features, i.e. standard LBP and LLBP. However, for some variants, i.e. MRELBP or CLBP, it is obviously better to use the single-scale version.



(a) (Best) Single scale version

(b) Multi-scale version

Fig. 3: Classification accuracy with random sample selection.

4 Conclusion

In this paper we implemented and empirically evaluated various LBP-extension features for detecting spoofed finger vein images. Further, we evaluated how some other aspects influence the prediction accuracy of the respective features, namely (1) the strategy for choosing samples (random vs. subject-specific), (2) the use of uniform patterns instead of complete patterns and two different strategies to generate uniform patterns, and (3) the choice of using single- or multi-scale versions of the features.

Our experiments show that all these aspects have to be considered when assessing finger vein images wrt. spoofing/presentation attacks. Moreover, the results suggest that more sophisticated LBP extensions do not necessarily imply better classification accuracy (at least not for finger vein spoofing detection), the baseline LBP variant is an excellent choice for most scenarios considered. For a low amount of training data available, correct classification of finger vein data in real and spoofed versions is more difficult for unseen subjects, thus making the availability of sufficient training data essential for reliable spoofing sample detection in real world scenarios.

Acknowledgements

This work has been partially supported by the Austrian Science Fund, project no. P26630.

References

[KSU16] Kocher, Daniel; Schwarz, Stefan; Uhl, Andreas: LBP Extensions used in Finger Vein Spoofing Detection. Technical Report 2016-04, Department of Computer Sciences, University of Salzburg, Austria, `http://www.cosy.sbg.ac.at/tr`, 2016.

[MS15] Mythily, B.; Sathyaseelan, K.: Measuring the Quality of Image for Fake Biometric Detection: Application to Finger Vein. In: National Conference on Research Advances in Communication, Computation, Electrical Science and Structures (NCRACCESS). pp. 6–11, 2015.

[Ng13] Nguyen, Dat Tien; Park, Young Ho; Shin, Kwang Yong; Kwon, Seung Yong; Lee, Hyeon Chang; Park, Kang Ryoung: Fake finger-vein image detection based on Fourier and wavelet transforms. Digital Signal Processing, 23(5):1401–1413, 2013.

[OPH94] Ojala, T.; Pietikainen, M.; Harwood, D.: Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. In: Pattern Recognition, 1994. Vol. 1 - Conference A: Computer Vision and Image Processing, Proceedings of the 12th IAPR International Conference on. volume 1, pp. 582–585 vol.1, Oct 1994.

[Ra15] Raghavendra, R.; Avinash, M.; Marcel, S.; Busch, C.: Finger vein liveness detection using motion magnification. In: Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on. pp. 1–7, Sept 2015.

[RB15] Raghavendra, R.; Busch, C.: Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study. In: 2015 11th International Conference on Signal-Image Technology Internet-Based Systems (SITIS). pp. 628–632, Nov 2015.

[Ti15] Tirunagari, S.; Poh, N.; Bober, M.; Windridge, D.: Windowed DMD as a microtexture descriptor for finger vein counter-spoofing in biometrics. In: Information Forensics and Security (WIFS), 2015 IEEE International Workshop on. pp. 1–6, Nov 2015.

[To15] Tome, P.; Raghavendra, R.; Busch, C.; Tirunagari, S.; Poh, N.; Shekar, B. H.; Gragnaniello, D.; Sansone, C.; Verdoliva, L.; Marcel, S.: The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks. In: Biometrics (ICB), 2015 International Conference on. pp. 513–518, May 2015.

[TVM14] Tome, P.; Vanoni, M.; Marcel, S.: On the Vulnerability of Finger Vein Recognition to Spoofing. In: Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the. pp. 1–10, Sept 2014.