The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks

P. Tome[1]*, R. Raghavendra[2], C. Busch[2], S. Tirunagari[3], N. Poh[3], B. H. Shekar[3],
D. Gragnaniello[4], C. Sansone[4], L. Verdoliva[4] and S. Marcel[1]

[1]Idiap Research Institute (Switzerland), [2]Gjøvik University College (Norway),
[3]University of Surrey (United Kingdom) and [4]University of Naples Federico II (Italy)

Abstract

The vulnerability of finger vein recognition to spoofing attacks has emerged as a crucial security problem in the recent years mainly due to the high security applications where biometric technology is used. Recent works shown that finger vein biometrics is vulnerable to spoofing attacks, pointing out the importance to investigate counter-measures against this type of fraudulent actions. The goal of the 1st Competition on Counter Measures to Finger Vein Spoofing Attacks is to challenge researchers to create counter-measures that can detect printed attacks effectively. The submitted approaches are evaluated on the Spoofing-Attack Finger Vein Database and the achieved results are presented in this paper.

1. Introduction

Biometrics is a growing up technology whose interest is related to the large number of applications where a correct assessment of identity is a crucial point. However, biometric systems are vulnerable to attacks which could decrease their level of security [15]. A recent problem that is questioning the application of biometrics when high security is required are the direct attacks, where the sensor is attacked using synthetic biometric samples without specific knowledge about the system. Also referred to as spoofing attacks or presentation attacks, these are performed when an invalid user tries to gain access to the system by presenting a copy of the biometric traits of a valid user. Among all biometric technologies, finger vein recognition is a fairly new topic, which utilizes the vein patterns inside a person's finger. This technology is relatively recent with first commercial applications in 2005 by Hitachi Ltd [11]. Nowadays this is widely used in the financial sector in Japan, China, Poland or Turkey, and it is claimed to be accurate [1, 8] although there is a debate in the scientific community [12, 18].

*Corresponding author: pedro.tome@idiap.ch

The fact that the vein pattern used for identification is embodied inside the finger prevents the data to be easily stolen, contrary to face that can be captured with a camera or fingerprints that can be collected from latent prints. However, acquiring images of finger vein patterns is not impossible. To the best of our knowledge the first attempt to spoof finger vein was conducted by Matsumoto et al.[1]. But, it was until years later, when a spoofing attack that could successfully by-pass a finger vein recognition system for a different number of identities was demonstrated [17].

The proposed challenge is the first attempt to benchmark finger vein anti-spoofing algorithms. For this reason, there is no existing state-of-the-art on spoofing finger vein counter-measures. Concerning the face anti-spoofing systems, which can likely be extrapolated to finger vein systems, they can be categorized in three broad categories with respect to the cues they use to detect the spoofing attack [2]. i) The *texture-based* methods explore the texture artifacts and the quality deterioration that appear when an image is recaptured. ii) The *motion-based* methods explore the unnatural movements on the scene in the case of spoofing attacks, while iii) the *liveness-based* methods try to detect any evidence of liveness or signs of vitality on the scene as an indicator of the presence of a real person. Due to the kind of spoofing images (printed finger vein images) provided by this Competition, only the *texture-based* methods make sense. Future attacks that will use more sophisticated techniques such as video from finger vein will open the opportunity to study *motion* or *liveness-based* approaches, as for example, the movements of adjustment or the blood flow of the fingers.

Unique finger vein spoofing counter-measures have been proposed by 4 teams participating in this Competition. In this paper they are thoroughly explained and their spoofing detection capabilities are compared using the Spoofing-Attack Finger Vein database. The teams' details are provided in Table 1. Note that author list and teams' name and

[1]http://www.gbd-e.org/events/2007/summit2007/presentation/14_Yokohama.pdf

Team	Institution
Baseline	Reference system publicly available provided by Idiap Research Institute, Switzerland
GUC	Norwegian Biometric Laboratory, Gjøvik University College, Norway
B-Lab	Biometrics and Biomedical Analytics Group, University of Surrey, United Kingdom
GRIP-PRIAMUS	University Federico II of Naples, Italy

Table 1. Participating teams' and institutions.

description are sorted by strict order of registration.

The remainder of this paper is structured as follows: a short description of the Spoofing-Attack finger vein database follows in Section 2. Each team's finger vein spoofing counter-measure is described in Section 3. The evaluation criterion summarized in Section 4, followed by a report on its performance and a comparative analysis in Section 5. Finally, Section 6 reports the conclusions.

2. Spoofing-Attack Finger Vein Database

The Spoofing-Attack finger vein database[2] [17] consists of 440 index finger vein images of both real-access and attacks attempt to 110 different identities. This database was produced at the Idiap Research Institute in Martigny, in Switzerland and all images (real-access and attacks) were recorded using the same open finger vein sensor.

The total number of images in the database is 880 (240 in the training set, 240 in the development set and 400 in the test set.) It is important to highlight that clients that appear in one of the data sets (train, dev or test) do not appear in any other set. The training set ("train") was used for training the anti-spoof classifier, the development set ("dev") was used for the threshold estimation, and finally, the test set ("test") was used to report the final performance. In the course of the competition, the participants had access to all the protocol sets of the data. However in the test stage, they received an anonymized test set that consists of a random mixing of the original test set images.

The goal of the attack protocols is to evaluate the (binary classification) performance of counter-measures to spoof attacks. Hence, the competition were split into 2 different sub-tasks according to the visual information available: *full* printed images and *cropped* images. This classification scheme makes-up a total of two protocols that can be used for studying the performance of counter-measures to finger vein attacks. Both *full* and *cropped* protocols are designed to use prior information based on trained classifiers or non trained approaches where the decision is taken based just on the input. The format of the images is a bitmap image saved as png format. The resolution of the *full* images is 665×250 pixels, the *cropped* images is 565×150 pixels, and size of the files is around 80 kbytes per image.

[2] https://www.idiap.ch/dataset/fvspoofingattack

This is the first database on spoofing finger vein and presents several advantages. Firstly, the database has a well-defined protocol consisting of training, development and test sets. For fair and unbiased algorithm evaluation, it is recommended that the training set is used to train counter-measures such as computing background models, PCA and LDA projection, etc; development set to estimate specific parameters to maximize the performance, e.g., optimising the decision threshold and fine-tuning hyperparameters of a classifier; and, the test set should be solely used to report results. Secondly, the database provides a separate set of enrolment images, which can be used to train and evaluate a finger vein recognition system. Such an approach is of high importance, as it enables one to assess how effective the attacks are in deceiving a finger vein recognition system and whether an anti-spoofing scheme is necessary in that setup. As claimed by [17], more than 80% of the attacks in this database successfully by-pass a finger vein system.

3. Anti-spoofing Approaches Submitted

3.1. Baseline System

The baseline anti-spoofing system proposed is a texture-based algorithm that exploits subtle changes in the finger vein images due to printed effects using the frequency domain. To recognize the static texture, the Fourier Transformation (FT) is extracted from the raw image after applying an histogram equalization. Once the FT is calculated and normalized on logarithmic scale, a window of 20 pixels centred vertically on the center of the image is applied to extract the average vertical energy of the FT. Then, the bandwidth of this average vertical signal (Bw_v) at a cut-off frequency of -3 dB is calculated. The final score to discriminate between real-accesses and spoofing attacks is this bandwidth normalized by the height of the image (h), i.e. $s = Bw_v/h$, resulting a score normalized in the range $[0 - 1]$.

This method exploits the idea of the bandwidth of vertical energy signal on real finger vein images, which is weakly manifested on spoofing finger vein samples. The main reason of it is that the recaptured spoofing finger vein samples displays a smooth texture with changes mainly vertical, changes translated as a horizontal energy in the Fourier domain. On the other hand, real finger vein images have better focus and sharpness on both horizontal and vertical directions, displaying both directions of energy in their Fourier transform. It is interesting to note that this approach does not need any kind of training or classifier to work.

The proposed algorithm is easily reproducible because the source code, programmed using free signal processing and machine learning toolbox Bob[3], is freely available[4].

[3] http://www.idiap.ch/software/bob

[4] Code available at: https://pypi.python.org/pypi/antispoofing.fvcompetition_icb2015

3.2. GUC Team

The team adopts a texture-based approach by extracting binarized statistical image features (BSIF), applied directly to the finger vein images without preprocessing in both *full* and *cropped* protocols.

The idea of the BSIF is to represent each pixel as a binary code obtained by computing its response to a filter that are learned using the statistical properties of the natural images. They have employed the open-source filters free available at [10] that are learned using $50,000$ image patterns randomly sampled from 13 different natural images [9]. The learning process to construct these statistically independent filters involves three main steps: (1) mean subtraction of each patches, (2) dimensionality reduction using Principle Component Analysis (PCA), and (3) estimation of statistically independent filters (or basis) using Independent Component Analysis (ICA).

Thus, given finger vein sample $I_{fv}(m,n)$ and a filter F_i of same size then, filter response is obtained as follows [10]:

$$r_i = \sum_{m,n} I_{fv}(m,n) F_i(m,n), \tag{1}$$

where m and n denotes the size of the finger vein image and $F_i, \forall i = \{1,2,\ldots,n\}$ denotes the number of linear filters whose response can be computed together and binarized to obtain the binary string as follows [10]:

$$b_i = \begin{cases} 1, & \text{if } r_i > 0 \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Finally, the BSIF features are obtained as the histogram of pixel's binary codes that can effectively characterize the micro-texture components in the finger vein sample. The BSIF are extracted using three different scales and bits: $i)$ 3×3 with 8 bits, $ii)$ 5×5 with 9 bits, and $iii)$ 7×7 with 12 bits, which generate three independent feature sets with different dimensions: 1×256, 1×512, and 1×4096.

The three final feature vectors are fed into separate linear Support Vector Machine (SVM) classifiers. The obtained scores for the three approaches are then normalized by the min-max normalization and combined using the sum fusion rule.

The proposed approach takes approximately 2 sec per image for training and less than 1 second per image for classification using an Intel i7 processor - 8Gb RAM PC with Matlab software and Windows 7.

3.3. B-Lab Team

The team takes the advantage of monogenic scale space based global descriptors. The main motivation behind monogenic scale space based global descriptors is that local object appearance and shape within an image can be described by the distribution of local energy and local orientation information. The implementation of the descriptors can be achieved either by dividing an image into small blocks and for each block, one computes the histogram of energy at each orientation for the pixels within the block. This is a local approach. Alternatively, one can compute a histogram representing the whole image as a single block, leading to a global approach. The latter approach is used here in order to reduce the computational complexity.

The proposed global descriptor is well suited for anti-spoofing as it captures the local energy and local orientation at coarse level; therefore it can differentiate between the actual vein block and the spoofed vein block.

The monogenic signal is a representation derived from a generalization of the 1-D Hilbert transform to a higher dimensional signal space [5] and [19]. A generalization is made possible by building upon the first order Riesz transform [16]. This strategy is advantageous because it can represent an image in terms of the local phase, local orientation, and local energy.

Given an image, the monogenic scale space first computes the local energy and local orientation at three different scales. For each of the three scales, a pixel (at a given scale) is represented by two values: energy and orientation. The orientation is divided into 36 equally spaced bins. A weighted histogram is subsequently derived by accumulating the energy associated with each of the orientation bins of the image at a given scale. Since this process is repeated for each of the three scales, this results in 108 dimensions.

Finally, the classifier used to discriminate between real accesses and spoofing attacks is support vector machine (SVM) with a histogram intersection kernel trained with a near boundary coefficient value of 0.001. The method takes less than one tenth of a millisecond for classification using a Dell PowerEdge 6850 Intel -8- CPU/16-Core - 32GB RAM PC with Matlab software and Ubuntu 12.

3.4. GRIP-PRIAMUS Team

The team explores an approach based on the use of local descriptors, which are powerful tools to describe the statistical behaviour observed locally in small patches of the image. In particular, they selected the Local Binary Pattern (LBP) [13], which were successfully used for different tasks, like texture and face recognition. The team proposed two different approaches to handle *cropped* and *full* images.

For *cropped* images in order to improve the discrimination ability of LBP and better explore the image statistics, the descriptor is extracted on a high-pass version of the image with 3×3 integer kernel [7]. In particular, a 3×3 neighbourhood of the target pixel x shown below:

$$\begin{bmatrix} x_0 & x_1 & x_2 \\ x_7 & x & x_3 \\ x_6 & x_5 & x_4 \end{bmatrix}$$

where the residual r is computed as:

$$r = x - \frac{1}{2}\sum_{i\,\text{odd}} x_i + \frac{1}{4}\sum_{i\,\text{even}} x_i.$$

To avoid fractional coefficients, all quantities were multiplied by 4. Note that, while LBP encodes first-order spatial variations computed on two-pixel supports, the use of a preliminary high-pass filters amounts to considering higher-order statistics computed on a larger support. LBP is then evaluated on the residual image r by considering 8 neighbours sampled uniformly on a circle of radius 1. The resulting vector is formed by 256 features.

For *full* images indeed they used the concatenation of Local Phase Quantization (LPQ) [14] and Weber Local Descriptor (WLD) [3]. LPQ uses a binary encoding scheme similar to LBP, but the patch surrounding the target pixel is analyzed in the Fourier domain. In particular, it uses the local phase information computed by means of the Short Time Fourier Transform (STFT) over a patch: four complex-valued coefficients at selected frequencies are extracted and binary quantized to form an 8-bit feature. Also in this case a histogram is generated and used as a 256-dimensional feature vector. WLD, instead, encodes two types of information in the spatial domain: i) the differential excitation and ii) the local orientation. Since these two descriptors extract information on the patch in different domains they complement one another and can give better results in terms of discrimination ability [6]. The resulting combined vector is formed by $1,216$ features. Finally, for both the approaches the team used a support vector machine (SVM) with linear kernel as classifier.

The LBP approach on *full* images takes about 15 seconds for training and about $1e^{-7}$ seconds to compute the classification of one sample. The second approach feature level fusion of LPQ+WLD takes around 900 seconds for feature extraction and about $5e^{-6}$ seconds for classification of a test image. These times were calculated using a 2.2 GHz Intel Core i7 - 6 Gb RAM PC with Matlab software and Win7.

4. Evaluation Criterion

The ranking of the participating anti-spoofing algorithms is based on Half Total Error Rate (HTER). It is defined as a mean of False Acceptance Rate (FAR) and False Rejection Rate (FRR). In the case of anti-spoofing, FAR refers to the ratio of spoofing attacks which are not correctly detected, while FRR refers to the ratio of real accesses which are incorrectly classified as spoofing attacks. The HTER is measured on the anonymized test set using a threshold calculated a priori on the development set, which has calculated individually from the score files in each *full* and *cropped* protocol. The threshold is chosen using the Equal Error Rate (EER) criterion, which is the value equalizing FAR and FRR. The smallest the HTER on the test set, the higher rank the anti-spoofing countermeasure will get. Additionally, the metric d' for "decidability" or decision-making power [4] has been calculated: $d' = |\mu_1 - \mu_2|/\sqrt{\frac{1}{2}(\sigma_1^2 + \sigma_2^2)}$. This d' is defined as the separation between the means (μ_1 and μ_2) of the two distributions (real-accesses and spoofing attacks), divided by the square-root of their average variance (σ_1^2 and σ_2^2), reflecting the intrinsic separability of the two distributions.

5. Discussion and Results

The algorithms proposed in this competition approach the problem from different aspects, as listed in Table **??**. The analysis of the textural differences is the most popular approach adopted by all the teams due to the definition of the challenge. It is also very interesting to notice the use of the support vector machine as classifier by all the teams, opposite to the baseline system that does not use any kind of classification.

A common approach for many teams is combining several different concepts together. In particular, the fusion is performed either at feature-level or score-level. GRIP-PRIAMUS team performs feature-level fusion on different categories of features (information in the spacial domain and texture descriptor), while GUC team adopt a score-level fusion using the sum fusion of the outputs of the three SVMs, which classified three different BSIF features from three different scales and bits.

Figure 1 and Table 2 summarize the performance of the proposed algorithms. The performance figures are given for both development and anonymized test set. The algorithms are trained and evaluated considering two different types of attacks (*full* and *cropped*) in the Spoofing-Attack finger vein database.

Considering the results on the test set, both *full* and *cropped* protocols have to be analysed separately. On the *full*, two teams and the baseline system have achieved perfect discrimination between the real accesses and the spoofing attacks of the database: B-Lab and GRIP-PRIAMUS. All teams have achieved perfect separability of the two classes on the development set, but still, not all algorithms got to generalize as well the anonymized test set. It is interesting to notice that the submitted algorithms have not lead better results than the baseline system proposed.

On the other hand, the baseline system outperforming the worst results on the *cropped* protocol. The winning algorithm was the ones proposed by the GRIP-PRIAMUS team that extract the texture information using the LBP features. The rest of the algorithms which achieved very low HTER also combine several texture approaches together: GUC team fuses at score-level different features classified by SVMs, while B-Lab team combines different global de-

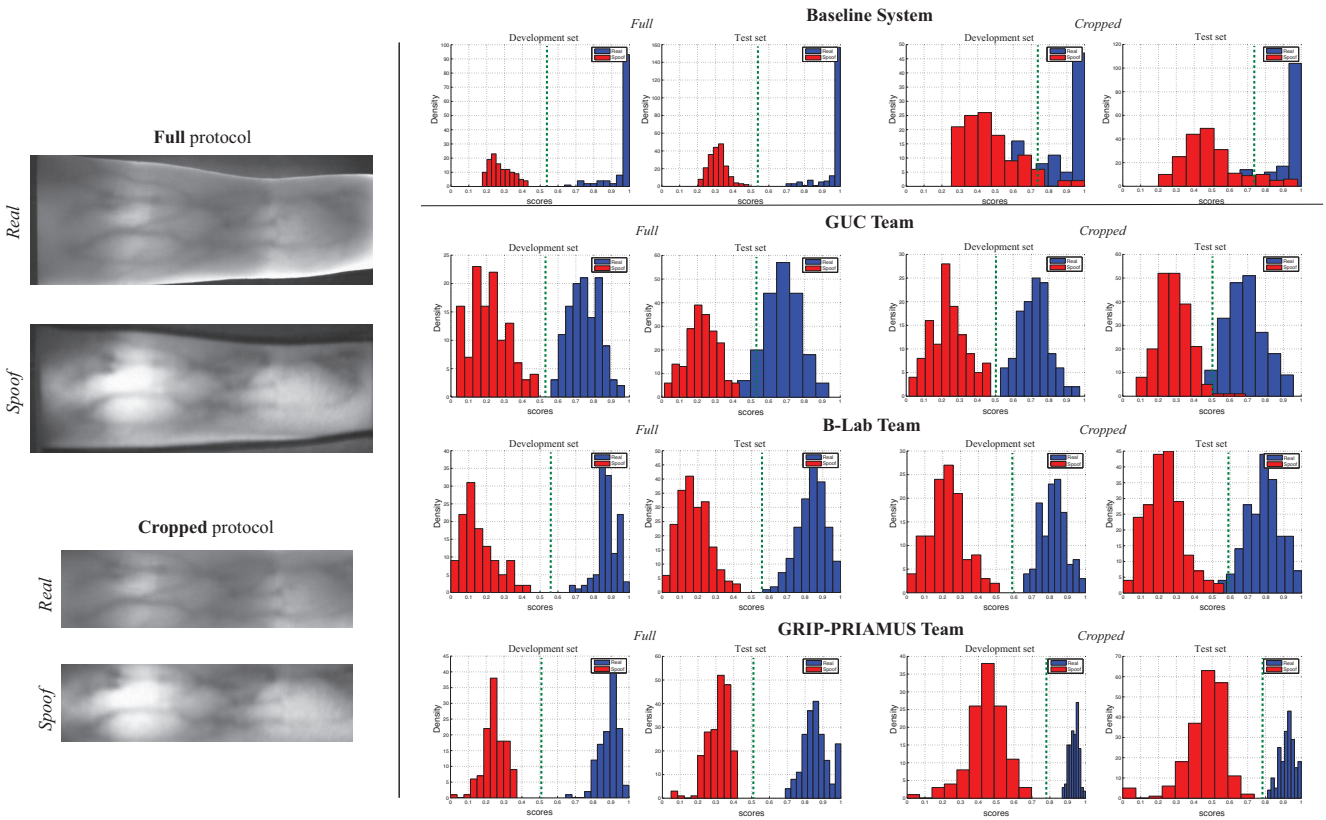

Figure 1. SCORE DISTRIBUTIONS FOR REAL-ACCESS AND SPOOFING ATTACKS. Performance results for the proposed anti-spoofing algorithms. The vertical dashed line stands the decision threshold.

Team	Protocol	Development				Test			
		FAR	FRR	HTER	d'	FAR	FRR	HTER	d'
Baseline	*Full*	0.00	0.00	0.00	9.75	0.00	0.00	**0.00**	11.17
GUC		0.00	0.00	0.00	5.46	0.00	8.00	4.00	4.47
B-Lab		0.00	0.00	0.00	9.05	0.00	0.00	0.00	8.06
GRIP-PRIAMUS		0.00	0.00	**0.00**	11.10	0.00	0.00	0.00	8.03
Baseline	*Cropped*	4.17	40.83	22.50	1.58	11.00	30.00	20.50	1.82
GUC		0.00	0.00	0.00	5.09	1.50	4.00	2.75	3.81
B-Lab		0.00	0.00	0.00	6.68	0.00	2.50	1.25	5.54
GRIP-PRIAMUS		0.00	0.00	**0.00**	6.28	0.00	0.00	**0.00**	5.20

Table 2. Performance results for the proposed anti-spoofing algorithms (in %). The measure d' stands the decidability.

scriptors such as the local energy and the local orientation. Among the algorithms submitted, it is important to stand the universal application of the algorithms submitted by these two teams GUC and B-Lab, which manage to achieve low HTER in both protocols.

Comparing the results, the baseline algorithm which rely only on a single cue is the most successful approach in discriminating real accesses and spoofing attacks in the specific *full* protocol. But considering the diversity of attacks in finger vein systems, it seems that an approach relying on a single cue is not able to detect all types of attacks, as demonstrated the *cropped* protocol results. Different types and different qualities of spoofing attacks need to be tackled in a different way, but simple methods can be very useful on the raw image of the finger vein recognition systems.

One of the goals of the competition was to support reproducible research by encouraging the participants to provide the source code of their algorithms as a free software. This will allow easy reproduction of results and a reliable reference for comparison with future anti-spoofing algorithms. All teams responded positively to this invitation.

6. Conclusion

Given the increasing use of the biometric technology in highly secured applications, such as in the finance sector, it is crucial to safeguard biometric systems against various attacks, including spoof.

The growing use of the biometric technology in sectors

such as the financial one, whose interest is related to the large number of high security applications, makes the assessment of vulnerabilities a challenging crucial point of study. For this reason, spoofing attacks are drawing more and more attention from the scientific community.

In this context, finger vein modality is a biometric trait widely used in this financial sector in countries such as Japan, China, Poland or Turkey, but yet; ironically, there is no study on how easily the modality can be spoofed. This is possibly due to the difficulty in stealing, because it is embodied inside the finger and a infrared illumination is needed to extract it.

The recent works that proved a successful spoofing attack to a finger vein recognition system has inspired a competition to challenge researchers to develop the first spoofing counter-measures able to detect printed finger vein spoofing attacks. In particular, this paper presents the first competition on counter measures to finger vein spoofing attacks, starting with naive spoofing attacks created by printing a finger vein image on a paper. All 4 participating teams have developed highly sophisticated methods, approaching the problem from different aspects, mainly related on the analysis of the texture of the finger vein images. For example, GRIP-PRIAMUS team performed feature-level fusion on different categories of features (information in the spacial domain and texture descriptor), while GUC team adopted a score-level fusion using the sum fusion of the outputs of the three SVMs, which classified three different BSIF features from three different scales and bits. The B-Lab team combined different global descriptors such as the local energy and the local orientation, while finally, the baseline system exploited the differences between real accesses and spoofing attacks in the Fourier domain without any kind of classification.

Several participating teams achieve impressive results in detecting spoofing attacks in the Spoofing-Attack finger vein database. The results demonstrate that one of the best strategies for finger vein spoofing attacks is the texture analysis of the full image. Such an approach seems to be effective in tackling printed spoofing attacks. As the quality and sophistication of spoofing attacks is expected to increase in the future, this observation gives indication on the directions for future research in finger vein anti-spoofing. One of the main objectives for future work should be assembling a database with even more realistic spoofing attacks, for example video-based finger vein, temperature sensing, detection of blood flow on the fingers or 3D fingers.

This work presents two important limitations, first the vascular patterns need to be extracted from a sensor, we assumed that users are cooperative in providing them. And second, the feedback given by the finger vein sensor used is important in order to perform the spoofing attack. Commercial systems are a blackbox but using an open device, the needed feedback to attack these systems can be obtained and therefore improve the countermeasures.

Therefore, given the novel ideas, the achieved results and the drawn conclusions, the 1st Competition on Counter Measures to Finger Vein Spoofing Attacks has achieved the goal to consolidate a set of state-of-the-art of finger vein spoofing counter-measures against printed attacks.

7. Acknowledgments

This work has been partially supported by EU FP7 BEAT (284989) project and the Swiss Centre for Biometrics Research and Testing.

References

[1] Finger vein authentication: White paper. Technical report, Hitachi, Ltd., 2006. 1

[2] M. M. Chakka et al. Competition on counter measures to 2-d facial spoofing attacks. In *Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA*, October 2011. 1

[3] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikäinen, X. Chen, and W.Gao. WLD: A robust local image descriptor. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(9):1705–1720, july 2010. 4

[4] J. Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:21–30, 2002. 4

[5] M. Felsberg and G. Sommer. The monogenic signal. *IEEE Transactions on Signal Processing*, 49(12):3136–3144, Dec 2001. 3

[6] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva. Fingerprint liveness detection based on weber local image descriptor. In *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, pages 46–50, 2013. 4

[7] D. Gragnaniello, C. Sansone, and L. Verdoliva. Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters*, 2014. 3

[8] M. Himaga and K. Kou. Finger vein authentication technology and financial applications. In *Advances in Biometrics*, pages 89–105. Springer, 2008. 1

[9] A. Hyvèarinen, J. Hurri, and P. O. Hoyer. *Natural Image Statistics*, volume 39. Springer, 2009. 3

[10] J. Kannala and E. Rahtu. Bsif: Binarized statistical image features. In *Proceedings on 21st International Conference on Pattern Recognition (ICPR)*, pages 1363–1366. IEEE, 2012. 3

[11] M. Kono, S. Umemura, T. Miyatake, K. Harada, Y. Ito, and H. Ueki. Personal identification system, 2004. US Patent 6,813,010. 1

[12] A. Kumar and Y. Zhou. Human identification using finger images. *IEEE Transactions on Image Processing (TIP)*, 21(4):2228–2244, 2012. 1

[13] T. Ojala, M. Pietikäinen, and T. Mäenpää. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7):971–987, july 2002. 3

[14] V. Ojansivu, E. Rahtu, and J. Heikkilä. Rotation invariant blur insensitive texture analysis using local phase quantization. In *International Conference on Pattern Recognition*, 2008. 4

[15] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA))*, pages 223–228. Springer-Verlag, 2001. 1

[16] M. Riesz. Sur ies fonctions conjugues. *Mathematische Zeitschrift*, 27:218–244, 1928. 3

[17] P. Tome, M. Vanoni, and S. Marcel. On the vulnerability of finger vein recognition to spoofing. In *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, volume 230, Sept. 2014. 1, 2

[18] M. Vanoni, P. Tome, L. El Shafey, and S. Marcel. Cross-database evaluation with an open finger vein sensor. In *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS)*, October 2014. 1

[19] D. Zang and G. Sommer. Signal modeling for two-dimensional image structures. *Journal of Visual Communication and Image Representation*, 18(1):81–99, February 2007. 3