On the Vulnerability of Palm Vein Recognition to Spoofing Attacks

Pedro Tome and Sébastien Marcel
Idiap Research Institute
Centre du Parc, Rue Marconi 19, CH-1920 Martigny, Switzerland
{pedro.tome, sebastien.marcel}@idiap.ch

Abstract

The vulnerability of palm vein recognition to spoofing attacks is studied in this paper. A collection of spoofing palm vein images has been created from real palm vein samples. Palm vein images are printed using a commercial printer and then, presented at a contactless palm vein sensor. Experiments are carried out using an extensible framework, which allows fair and reproducible benchmarks. Results are presented comparing two automatic segmentations. Experimental results lead to a spoofing false accept rate of 65%*, thus showing that palm vein biometrics is vulnerable to spoofing attacks, pointing out the importance to investigate countermeasures against this type of fraudulent actions. A study based on the number of the enrolment samples is also reported, demonstrating a relationship between the number of enrolment samples and the vulnerability of the system to spoofing.*

1. Introduction

Biometrics is a maturing 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. These vulnerable points can be broadly divided into two main groups [6]: $i)$ *direct attacks*, where the sensor is attacked using synthetic biometric samples without specific knowledge about the system, and $ii)$ *indirect attacks*, where the intruder needs to have some additional information about the internal workings of the system and, in most cases, physical access to some of the application components. This paper is focused on the vulnerability assessment to these direct attacks (often called *spoofing attacks* or *presentation attacks*).

Among all biometric technologies, the human palm recognition has emerged as a reliable technology to provide greater level of security to personal authentication system [10]. Between the various human hand biometric characteristics that can be used to recognize a person, such as geometry, fingerprint, palm print or knuckle print, the palm veins are perhaps the most successful form with highest recognition rates achieved between these different characteristics [4]. The palm vein patterns are considered stable and reliable, which means that once a person has reached adulthood, the hand structure, veins and configuration remain relatively stable throughout the person's life [11].

For these reasons, nowadays palm vein recognition technology is considered as a promising and trusted biometric. The fact that the vein pattern used for identification is embodied inside the palms prevents the data to be easily stolen, as opposed to face that can be captured with a camera or to fingerprints that can be collected from latent prints.

In this context, the last generation of palm vein sensors allow to acquire the veins patterns without contact but still require the presence of blood in the veins to be registered, which makes more robust these systems against the liveness problem and some spoofing attacks. However, acquiring images of palm vein patterns is not impossible and an interesting subsequent research question is to demonstrate a method to forge a spoofing attack that can successfully bypass a palm vein recognition system for a different number of identities. To the best of our knowledge there is no such works described in the literature.

Hence, this paper presents the first successful spoofing attack to a palm vein recognition system using printed images. For this purpose, specific spoofing palm vein images have been captured from 50 subjects of a public palm vein database using the same palm vein sensor that was used to acquire the original database. Experimental results lead to a Spoofing False Accept Rate (SFAR) [2] of 65%, thus showing the vulnerability of a palm vein sensor.

The remainder of this paper is structured as follows: Section 2 details the database used in the experiments and the process followed for the generation of spoofing palm vein samples. Section 3 describes experimental protocol, results and some discussion. Finally, Section 4 reports the conclusion of the paper.

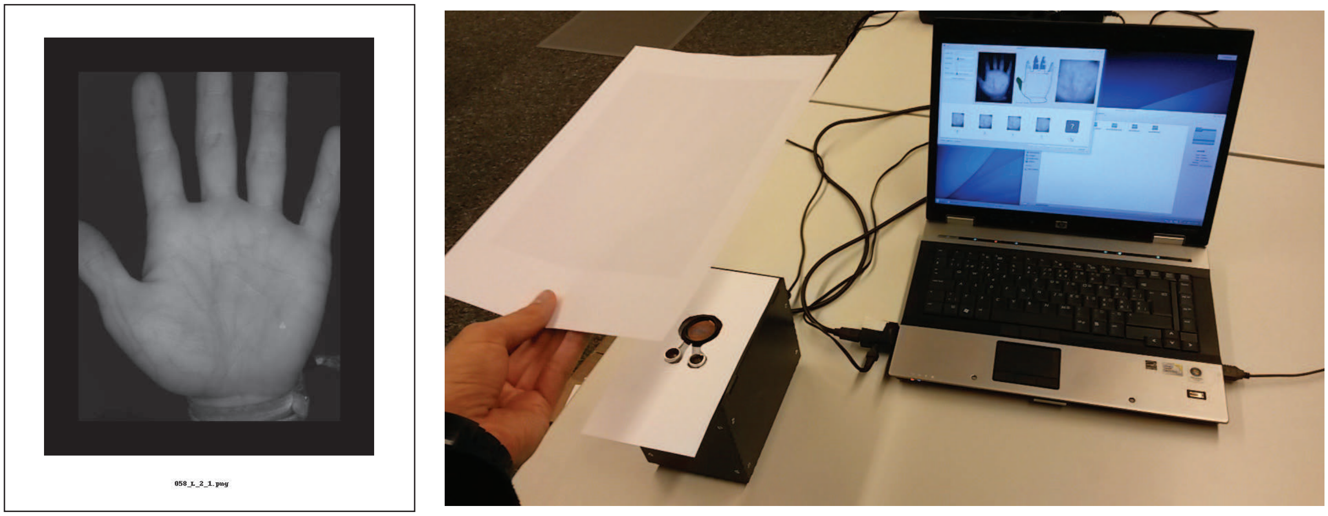

Figure 1. SPOOFING PALM VEIN IMAGES ACQUISITION. This figure shows the procedure of the spoofing palm vein images collection. Printed palm vein image (on the left) is shown to the sensor to be reacquired.

2. Spoofing Palm Vein Collection

A new spoofing palm vein collection has been created using printed palm vein images from the first 50 subjects of the public VERA Palm vein database.

2.1. Original Database

The database used in this work for spoofing attacks and measuring the vulnerability of the tested palm vein recognition system is a subset (1000 palm images: 50 subjects, 2 hands, 2 sessions, 5 acquisitions) from a public database[1].

The VERA Palm vein database consists of $2,200$ images depicting human palm vein patterns. Palm vein images were recorded from 110 volunteers for both left and right hands. For each subject, images were obtained in two sessions of five pictures each per hand. Palm vein images were acquired by the contactless palm vein prototype sensor comprised of a ImagingSource camera, a Sony ICX618 sensor and an infrared illumination of LEDs using a wavelength of 940 nm. The distance between the user hand and the camera lens is measured by a HC-SR04 ultrasound sensor and a led signal that indicates the user the correct position of the hand for the acquisition.

The palm vein images have a resolution of 480×680 and are saved as bitmap image using a png format. The database is divided in two datasets: RAW and ROI-1 data. The *raw* folder corresponds to the full palm vein image and *roi* folder contains the region of interest (palm vein region) obtained automatically by the sensor during the acquisition process (see Figure 2).

2.2. Spoofing Palm Vein Generation Method

The main motivation of using printed images is based on that it is simple (easy to do), does not require prior knowledge about the system and it is already proved to be efficient in the context of other biometric modalities such as the finger vein [9], 2D face [1] or Iris [7]. This approach is also motivated by the scarce literature in the area where these printed images will serve as a reference baseline against future more elaborated attacks. In this work let us assume that the toner ink from the printer absorbs the Near Infra-Red (NIR) illumination as was proved on previous works [9].

Due to the configuration given by the original database, the process of the spoofing samples generation can be carried out by different strategies: printing $i)$ all real images, $ii)$ two real palm vein images (one from the first session and one from the second), or $iii)$ just one real palm vein image (selected between the first and second session). In our case, the last option $iii)$ has been adopted, which means that a human examiner selected one real hand vein image (one left and one right) between the ten available per subject on both sessions.

Finally, the process of generation is: palm vein images selected are reshaped to (380×525), then a padding array of 50 black pixels is applied to the real palm vein images to emulate the black background and an identifier is written on the bottom before printing on a regular 80 g. paper using a commercial printer. Figure 1 (left) shows an example of the final printed image and Figure 1 (right) shows and example of the spoofing acquisition process and how the attacker positioning the printed hand. After several experiments, a piece of 100g. paper is applied to cover the NIR illumination from the sensor, to obtain better results. This solution was adopted to improve the chances of the success spoofing

[1] Available at http://www.idiap.ch/dataset/vera-palmvein

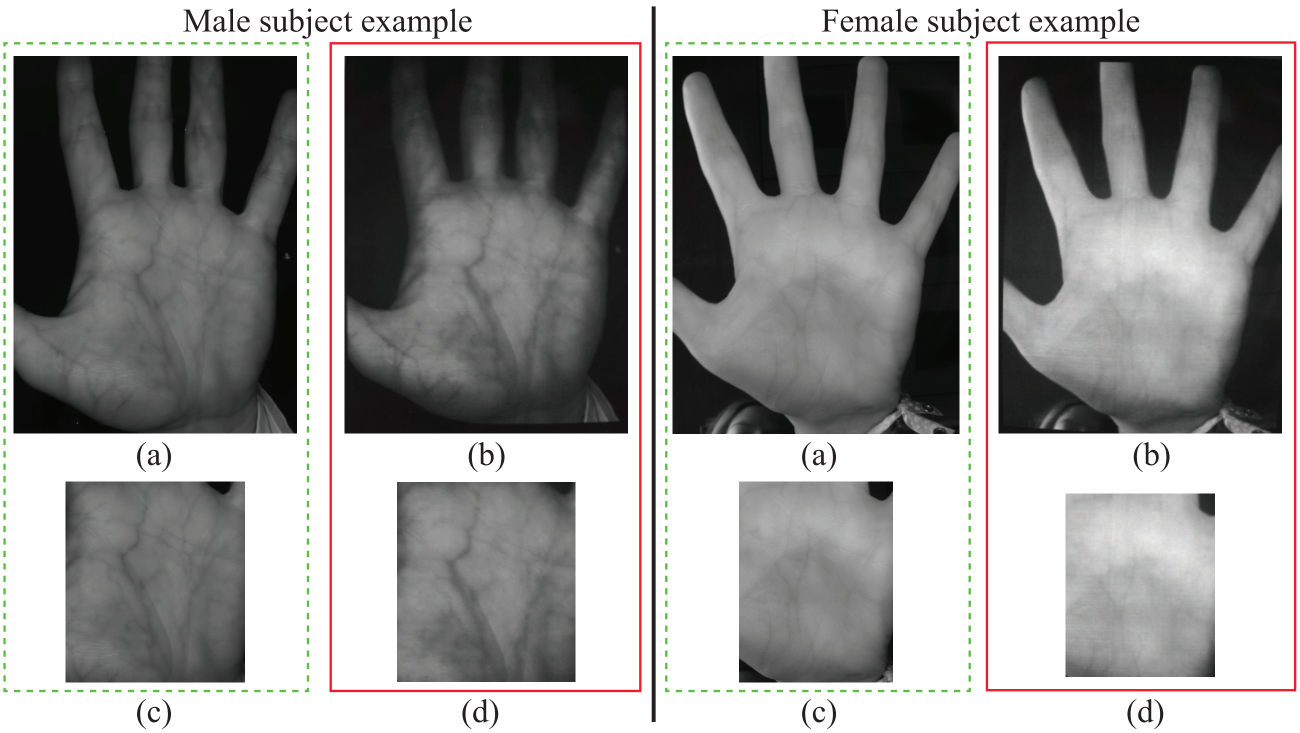

Figure 2. COMPARISON BETWEEN REAL AND SPOOFING SAMPLES. This figure shows real sample images (*(a)* and *(c)*, inside of a dashed green line) from the database and their correspond spoofing image (*(b)* and *(d)*, inside of a solid red line) reacquired by the sensor. First row (*(a)* and *(b)*) shows the RAW images saved by the sensor and second row (*(c)* and *(d)*) shows the ROI-1 regions extracted by the sensor in the acquisition process.

attack but we still notice that without this NIR illumination covering, the spoofing attack was also successful.

Figure 2 shows the difference between the spoofing samples created and the real ones. A slight difference based on contrast and light exposure can be observed, but excepting the printing effects, the images are quite similar. This figure also shown an interesting difference between palm vein from male and female subjects observed on the all database. Female subjects present more deep vascular patterns, which consequently are less visible in general.

To the best of our knowledge, this paper introduces the first spoofing palm vein database freely available for vulnerabilities assessment, countermeasures evaluation and reproducible research on palm vein recognition.

3. Experiments and Results

This section describes the palm vein recognition algorithm, the evaluation protocols, and the experimental results achieved in this work.

3.1. Reference Palm Vein Recognition System

The experiments in this paper are carried out using the open source palm vein framework called PalmveinRecLib: bob.palmvein[2]. This framework is extensible and allows to run a complete palm vein recognition experiment, from the preprocessing of RAW images (including segmentation) to the computation of biometric scores and their evaluation.

We present below the algorithm that composes the palm vein recognition system that is used as a reference for computing genuine scores from genuine users and zero-effort impostor scores from zero-effort impostors, hence allowing to determine FAR and FRR, and whose performance is measured in terms of Equal Error Rate (EER). Finally, the same reference system is used to compute spoofing scores from spoofing attacks (performed by informed impostors), hence allowing to determine Spoofing False Accept Rate (SFAR). The full source code for replicate the experiments can be downloaded from PyPI[3] upon publication.

The system implements several baseline methods from the state-of-the-art and is divided in three stages: $i)$ segmentation and normalization, $ii)$ feature extraction and $iii)$ matching. In the segmentation process the hand contour is localised by a binarization from grayscale palm vein images. Then the hand landmarks (peaks and valleys) are extracted using the radial distance function (RDF) between the reference point (generally the starting of the wrist) and

[2] Freely available at https://pypi.python.org/pypi/bob.palmvein
[3] https://pypi.python.org/pypi/bob.paper.ICB2015

the contour points extracted [13, 3]. The palm region is extracted as a square region based on the located hand landmarks and a geometric normalization (scaling and rotation) on the extracted palm vein region is performed. Finally, the palm veins are enhanced by using the Circular Gabor Filter (CGF) approach [12]. Once palm vein region (ROI-2) is extracted and normalised, the local binary patterns (LBP) are applied as features [5] and the histogram intersection metric [8] is adopted as a similarity measure to compute the scores. The final score of the system per user is computed by the average of the scores of all enrolment samples for that user. The presented experimental framework includes a complete module for scores analysis.

Since there are two different preprocessing configurations (none and CGF) and two regions of interest analysed (ROI-1 given by the database, and ROI-2), this finally leads to four different systems that are evaluated in the remainder of this section.

3.2. Evaluation Protocols

For the experiments, each hand in the database is considered as a different subject. Therefore, we have two sessions with five acquisition per each for 100 subjects (i.e., 1000 palm vein images: 50 subjects × 2 hands × 2 sessions × 5 acquisitions).

Two different scenarios are considered in the experiments:

- **Normal Operation Mode (nom):** both the enrolment and the tests are carried out with a real palm vein images. This is used as the reference scenario. In this context the FAR (False Acceptance Rate) of the system is defined as the number of times an impostor using his own palm vein image gains access to the system as a genuine user, which can be understood as the robustness of the system against a zero-effort attack. The same way, the FRR (False Rejection Rate) denotes the number of times a genuine user is rejected by the system.

  For a given subject, the first two palm vein images from the first session ($s1_{1-2}$) are considered as enrolment templates. Genuine scores are obtained by comparing the templates to the corresponding images of the first and second sessions from the same subject ($s1_{3-5}$ and $s2_{1-5}$) and impostor scores are obtained by comparing to the remaining subjects, i.e. the eight images ($s1_{3-5}$ and $s2_{1-5}$) from the first and second sessions comprised the probe set.

- **Spoofing Attack (attack):** the enrolment is performed using a real palm vein, and tests are carried out with spoofing palm veins. In this case the genuine user enrols with his/her palm vein and the attacker tries to access the application with the spoofing palm vein of the legal user. A successful attack is accomplished when the system confuses a spoofing palm vein with its corresponding genuine palm vein, i.e., SFAR (Spoofing FAR), the ratio of the incorrect accepted spoofing attacks.

  In this case, the enrolment is performed using the two real palm vein images from first session ($s1_{1-2}$) as before and the system is tested by using the eight spoofing samples of the first and second sessions ($s1_{3-5}$ and $s2_{1-5}$), i.e., the subjects try to access into the system using a spoofing palm vein image.

Protocol	Training set		Testing set		
	# Clients	# Files	# Clients	Enrolment	Probe
nom	5 × 2	100	45 × 2	(Real) 180	(Real) 720
attack	5 × 2	100	45 × 2		(Spoof) 720

Table 1. EVALUATION PROTOCOLS. This table reports the number of genuine and impostor scores of each evaluation protocol. The enrolment uses the first two images of first session ($s1_{\{1-2\}}$) and the remaining are used by the probe ($s1_{\{3-5\}} + s2_{\{1-5\}}$).

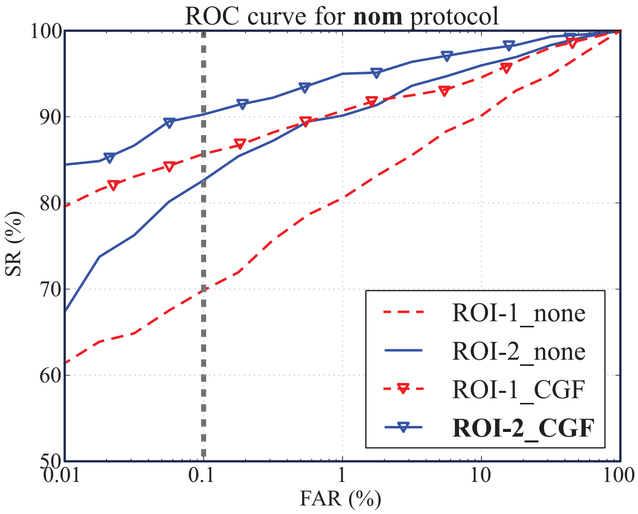

Figure 3. ROC CURVES OF THE SYSTEMS. This figure shows the ROC curves of the systems on the VERA Palm vein database considering the different preprocessing configurations and the regions of interest (ROI-1 given by the database and ROI-2 extracted from the *RAW* images by the recognition system). The best system is highlighted in bold.

For the vulnerabilities assessment on this work, in each protocol, the database has been divided in two different sets: $i)$ *training* set (subjects 1-5) and *testing* set (subjects 6-50). The *training set* has not been used on these experiments. The *testing set* has been used to evaluate palm vein verification accuracy and the spoofing palm vein vulnerability. Table 1 summarizes the evaluation protocols used on the experiments.

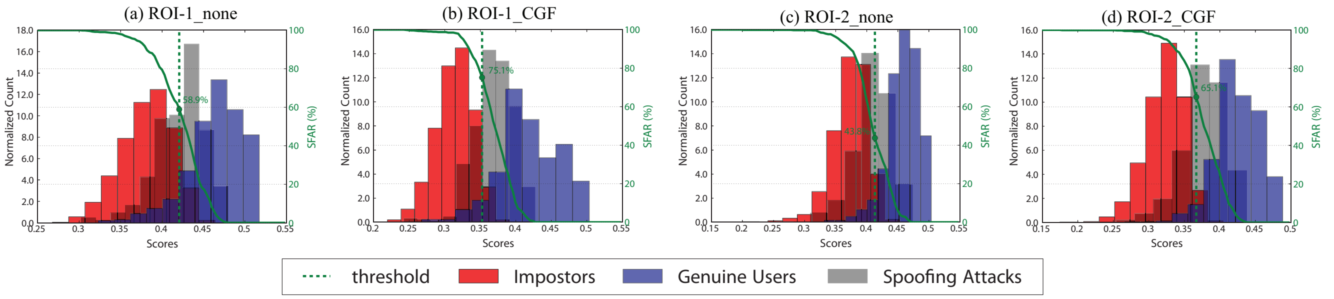

Figure 4. SCORE DISTRIBUTIONS OF SYSTEMS. This figure shows the score distributions of palm vein recognition systems on the database. The solid curve shows the SFAR as the decision threshold changes.

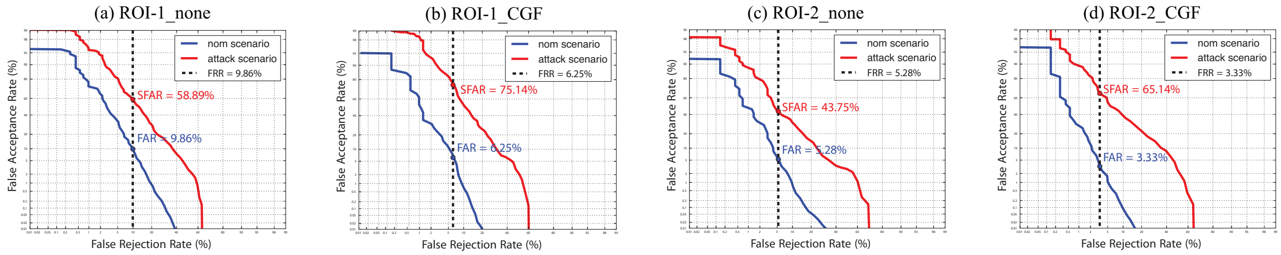

Figure 5. REFERENCE SYSTEM PERFORMANCE. DET curves for nom and attack scenario of baseline palm vein verification systems.

3.3. Experimental Results

The performance (EER in %) of the four considered palm vein recognition systems on the database is summarized in Figure 3. It is important to notice that two different regions of interest have been analysed, the ROI-1 generated by the palm vein sensor during the acquisition (given by the database) and the ROI-2 extracted from the *RAW* images in the preprocessing by the automatic palm vein recognition system. In the following, these experimental results are discussed according to several experiments.

3.3.1 System performance results

The system performance on the nom protocol of the VERA Palm vein database is shown in Figure 3 and Figure 5, for the two different regions of interest: ROI-1 and ROI-2 and the two preprocessing evaluated: none and CGF.

Overall, the best results are obtained by the region of interest ROI-2 extracted from the *RAW* images by the palm vein recognition system, which achieved in all the cases lower EER rates than the ROI-1, generated by the sensor during the acquisition.

Besides, it is interesting to notice the improvement of the system performance achieved by using the preprocessing approach Circular Gabor Filter (CGF), leading to the best recognition rate of 3.33% of EER in ROI-2 in comparison to the none preprocessing of 5.27% of EER. This improvement is bigger on high security points (FAR $< 0.1\%$) as it is shown in Figure 3, where the recognition rates remain more stable using this CGF approach.

3.3.2 Spoofing attack results

The robustness of the systems to spoofing attacks is summarized on Figure 4 and Figure 5, which shows the spoofing false accept rate (SFAR in %) of the spoofing attack (attack) against the recognition system at EER operating point, using the distribution of genuine, impostor and spoofing attack scores. The decision threshold is fixed to reach a FAR $=$ FRR (i.e., EER) in the normal operation mode (nom), and then the SFAR of the spoofing attack is computed.

While the almost perfect separation of the scores for genuine users and impostors justifies the good verification performance, in all systems the spoofing attack appears optimal. This is proven by the value of SFAR as well as the percentage of spoofing attacks that manage to by-pass the system at the chosen threshold (i.e. a SFAR of about 43.8% or higher is observed). This analysis proves the vulnerability of the palm vein recognition system to spoofing attacks, establishing the necessity of securing them with an anti-spoofing method.

It is also noticeable that the SFAR of the spoofing attacks increases from 58.9% to 75.1% on ROI-1 and from 43.8% to 65.1% on ROI-2, when the CGF is used in the preprocessing. Therefore, while the system increases the recognition performance, the spoofing attack improves its effectiveness. This observation can be explained by the use of texture-based (LBP) technique as feature extraction, mainly due to that CGF preprocessing approach makes more similar the texture of real and spoofing samples for this feature extraction technique.

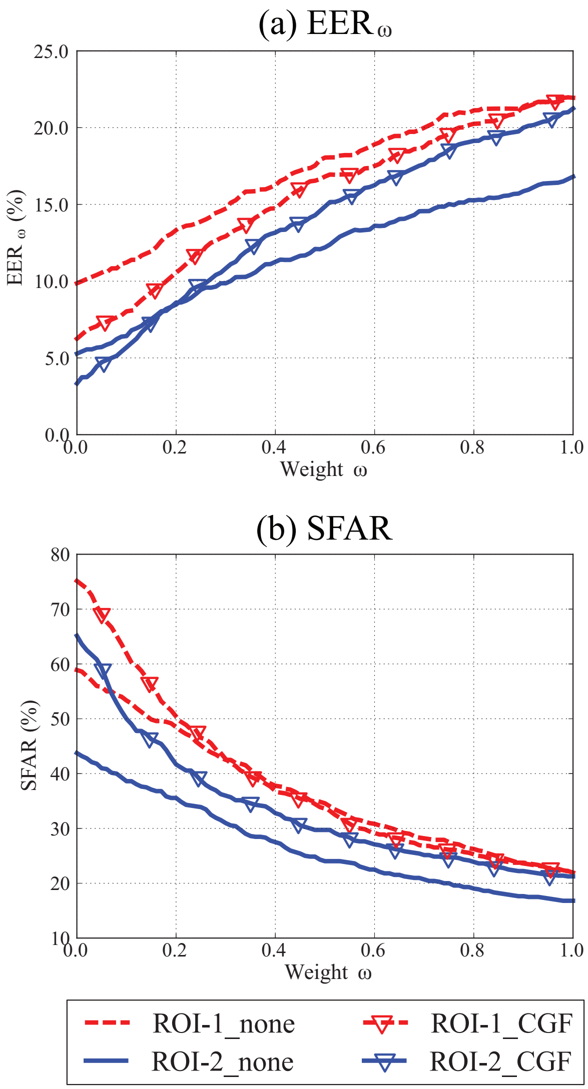

Figure 6. EPSC CURVE. This figure shows the Expected Performance and Spoofability Curve (EPSC) to compare the palm vein systems in terms of robustness and vulnerability.

Finally, the expected performance and spoofability curve (EPSC) [2] given in Figure 6, reports EER_ω and SFAR for a threshold which considers the relative probability of spoofing attacks, encoded in the parameter $\omega \in [0, 1]$, which denotes the relative cost of spoofing attack with respect to zero-effort impostors. Comparing the EER_ω values in Figure 6a, the ROI-2 _CGF system is best performing in verification only as long as the spoofing attacks appear with a very small probability. After a small increment of the value of $\omega \approx 0.2$, ROI-2 _none system shows the best verification performance. The same applies to the vulnerability to spoofing (Figure 6b), while being the most vulnerable when $\omega \approx 0$, ROI-2 _none system displays the smallest values of SFAR for larger values of ω. This confirms that the preprocessing based on CGF makes the system more precise in terms of verification but increases its vulnerability to spoofing attacks.

Protocol	Testing set		
	# Clients	Enrolment	Probe
nom	45 × 2	(Real samples) $A)\ s1_{\{1\}} = 90$ $B)\ s1_{\{1-2\}} = 180$ $C)\ s1_{\{1-3\}} = 270$ $D)\ s1_{\{1-4\}} = 360$ $E)\ s1_{\{1-5\}} = 450$	(Real samples) $s2_{\{1-5\}} = 450$
attack	45 × 2		(Spoofing samples) $s2_{\{1-5\}} = 450$

Table 2. ENROLMENT SET SIZE ANALYSIS PROTOCOLS. This table reports the number of genuine and impostor scores of each evaluation protocol.

3.3.3 Enrolment set size analysis

This section analyses different sizes of the enrolment set and its effect over the SFAR and EER rates. Table 2 summarizes the different sizes selected (A, B, C, D, and E) for the enrolment set, from 1 until 5 samples of the first session. The size of the probe set is the same for all the cases, the 5 samples of the second session from real or spoofing samples in each case.

Figure 7 shows graphically the evolution of EER and SFAR rates based on the different number of enrolment samples. Overall, the EER rate decreases for all the systems until 3 enrolment samples where approximately saturates. On the other hand, the SFAR rate slightly decreases and increases for the ROI-1 and ROI-2 until 3 enrolment samples. The most robust system (SFAR minimum) is achieved where none preprocessing is applied, as previously was concluded.

An interesting effect can be observed when the number of enrolment samples increases, the SFAR rate follows an incremental trend for the all the systems. This can be explained by the increment of variability in the enrolment set, which gives the opportunity to attacker samples to be more reliable and effective. Therefore, this study showed the necessity of a compromise between the number of enrolment samples and the vulnerability of the system.

4. Conclusions

The first evaluation of the vulnerability to spoofing attacks to palm vein recognition systems has been presented. The attacks have been evaluated using spoofing palm vein images created from real palm vein samples of the VERA Palm vein database. This is achieved by printing with a commercial printer the real palm vein images without any kind of preprocessing on a regular 80g. paper and presented to the palm vein sensor.

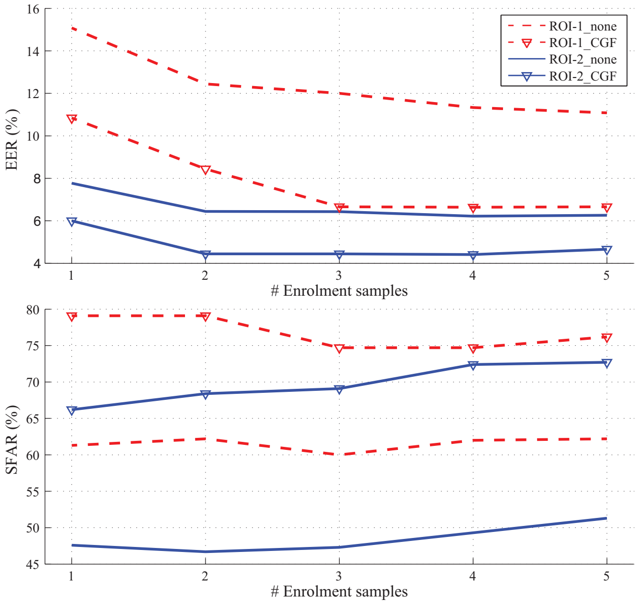

Figure 7. STUDY OF ENROLMENT SAMPLES. EER(%) (top) and SFAR(%) (bottom) of ROI-1 and ROI-2 on the different preprocessing configurations (none and CGF) for different number of enrolment samples. For this analysis, the same size of the probe set was fixed for all cases.

Acquisition of spoofing palm vein images has been carried out with the same palm vein contactless sensor used in the original database. A spoofing attack scenario has been evaluated to the normal operation mode of the system using a publicly available palm vein recognition system. This spoofing attack considers enrolling to the system with real images and accessing it with spoofing palm vein images. Experimental results showed that the system is vulnerable to the spoofing attacks. The intruder is granted access to the system with a probability of spoofing false accept rate as high as 65%.

Two automatic segmentations have been analysed by using the ROI-1 region proportioned by the database and the ROI-2 region generated by the recognition software developed. The effect on the vulnerability of the system of the image preprocessing by using a reliable approach such as the circular gabor filter (CGF) have been also studied, proving an increment on the vulnerability when the complexity of the system increases. Finally, the role of the number of the enrolment samples has been also analysed in this paper, demonstrating an expected relationship between this number and the vulnerability of the system.

Liveness detection procedures are possible countermeasures against spoofing attacks. In palm vein recognition, there is scarce literature about this topic but several approaches such as temperature sensing or blood flow detection on palm could be useful. Future work will explore the above mentioned countermeasures as well as evaluating the effectiveness of the spoofing attack on commercial palm vein sensors.

5. Acknowledgments

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

References

[1] I. Chingovska, A. Anjos, and S. Marcel. On the effectiveness of local binary patterns in face anti-spoofing. In *Proceedings of the 11th International Conference of the Biometrics Special Interes Group*, September 2012. 2

[2] I. Chingovska, A. Anjos, and S. Marcel. Biometrics evaluation under spoofing attacks. *IEEE Transactions on Information Forensics and Security*, 9(12):2264–2276, 2014. 1, 6

[3] W. Kang and Q. Wu. Contactless palm vein recognition using a mutual foreground-based local binary pattern. *IEEE Transactions on Information Forensics and Security*, 9(11):1974–1985, Nov 2014. 4

[4] G. K. O. Michael, T. Connie, and A. B. J. Teoh. A contactless biometric system using multiple hand features. *Journal of Visual Communication and Image Representation*, 23(7):1068 – 1084, 2012. 1

[5] L. Mirmohamadsadeghi and A. Drygajlo. Palm vein recognition with local texture patterns. *IET Biometrics*, pages 1–9, January 2014. 4

[6] 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

[7] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management, BIOID*, LNCS-5372, pages 181–190. Springer, May 2008. 2

[8] M. Swain and D. Ballard. Color indexing. *International Journal of Computer Vision*, 7(1):11–32, 1991. 4

[9] 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. 2

[10] M. Watanabe, T. Endoh, M. Shiohara, and S. Sasaki. Palm vein authentication technology and its applications. In *Proc. on Biometrics Symposium*, pages 37–38, 2005. 1

[11] E. Yörük, H. Dutağaci, and B. Sankur. Hand biometrics. *Image Vision Computing*, 24(5):483–497, May 2006. 1

[12] J. Zhang and J. Yang. Finger-vein image enhancement based on combination of gray-level grouping and circular gabor filter. In *International Conference on Information Engineering and Computer Science (ICIECS)*, pages 1–4, Dec 2009. 4

[13] Y. Zhou and A. Kumar. Human identification using palm-vein images. *Information Forensics and Security, IEEE Transactions on*, 6(4):1259–1274, Dec 2011. 4