On the Vulnerability of Finger Vein Recognition to Spoofing

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

Abstract: The vulnerability of finger vein recognition to spoofing is studied in this paper. A collection of spoofing finger vein images has been created from real finger vein samples. Finger vein images are printed using a commercial printer and then, presented at an open source finger vein sensor. Experiments are carried out using an extensible framework, which allows fair and reproducible benchmarks. Experimental results lead to a spoofing false accept rate of 86%, thus showing that finger vein biometrics is vulnerable to spoofing attacks, pointing out the importance to investigate countermeasures against this type of fraudulent actions.

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. These vulnerable points can be broadly divided into two main groups [RCB01]: $i)$ *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 working of the system and, in most cases, physical access to some of the application components. In this paper, we only focus on the vulnerability to direct attacks (often called *spoofing attacks*).

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 [KUM$^+$04]. Nowadays this is widely used in the financial sector in Japan, China, Poland or Turkey, and it is claimed to be accurate [hit06, HK08] although there is a debate in the scientific community [KZ12, TV13].

Nevertheless, finger vein recognition is considered as one of the most trusted biometric. 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 and an interesting subsequent research question is to demonstrate a method to forge a spoofing attack that can successfully by-pass a finger vein recognition system for a different number of identities.

Printer	Paper	Preprocessing
Laser	White paper (80 gr) Transparent paper High quality paper (200 gr) Cardboard	Histogram equalization Noise filtering

Table 1: OPTIONS TESTED FOR SPOOFING FINGER VEIN SAMPLE GENERATION. This table summarizes the tests carried out to generate an effective spoofing finger vein sample.

To the best of our knowledge there is no such works described in the literature except the slides from Prof. T. Matsumoto[1].

Hence, this paper presents the first successful spoofing attack to a finger vein recognition system using printed images. For this purpose, specific spoofing finger vein images have been captured from 50 subjects of a public finger vein database[2] using an open device described in [Ton12]. Experimental results lead to a Spoofing False Accept Rate (SFAR) [CAM13] of 86%, thus showing the vulnerability of a finger 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 finger vein samples. Section 3 describes experimental protocol, results and some discussion. Finally, Section 4 reports the conclusion of the paper.

2 Spoofing Finger Vein Collection

A new finger vein collection has been created using printed finger vein images from 50 subjects of the public VERA database. 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 2D face [CAM12] or Iris [RATGAF$^+$08]. 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.

The process of generation is divided into four steps: $i)$ first, original images are preprocessed for a better afterwards quality, then $ii)$ they are printed on a piece of paper using a commercial printer as shown in Figure 1 (d and e), $iii)$ finger contours are enhanced with a black ink whiteboard marker, and finally, $iv)$ printed images are presented to the finger vein sensor, as can be seen in Figure 1 (f), obtaining the spoofing sample.

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

[2] Available at http://www.idiap.ch/dataset/vera-spoofingfingervein

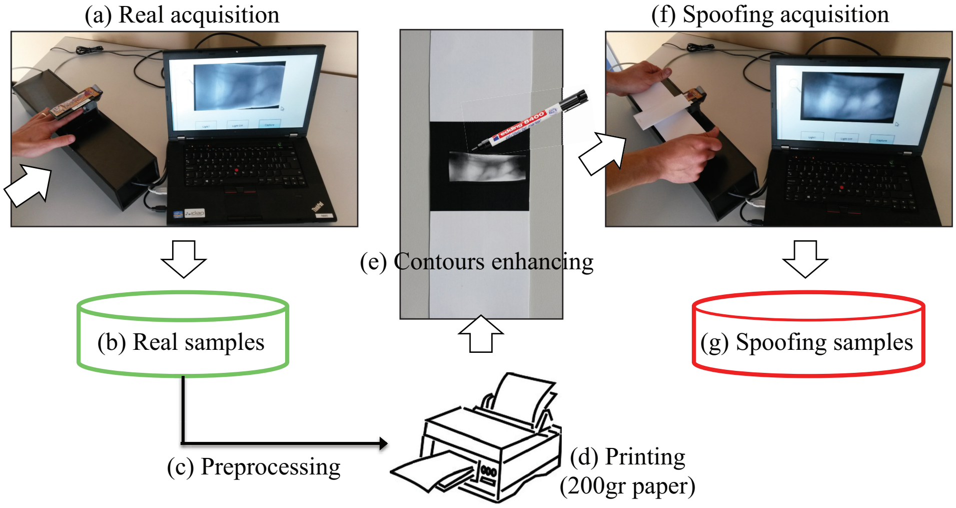


Figure 1: SPOOFING FINGER VEIN IMAGES ACQUISITION PROCEDURE. This figure shows the full spoofing acquisition process from a real finger vein sample (a) that is recorded in a real database (b). Then the image is preprocessed (c) and printed (d) using a high quality paper of 200 gr and a Laser printer. The contours of the finger are enhanced using a black ink whiteboard marker (e) and the spoofing image is presented to the sensor (f) and acquired (g).

2.1 Original database

The database used in this work for spoofing attacks and measuring the vulnerability of the tested finger vein recognition system is a subset (50 subjects, 100 index fingers (Left and Right), 200 images) from a public database[3].

This database is comprised of 440 finger vein images from 110 subjects recorded in an uncontrolled way in terms of finger alignment. In addition, subjects are from various ethnicities with a ratio female:male of 40:70, which brings an additional challenge, since skin properties affect the acquisition of vascular patterns. The acquisition process consists of the recording of two shots of each index finger from each subject in a single session, i.e., the procedure is based on a quick and friendly user experience, which emulates a realistic scenario.

Acquisition of spoofing finger vein images has been carried out with the same finger vein sensor used in the public database, an open device described in [Ton12].

[3] Available at `http://www.idiap.ch/dataset/vera-fingervein`

2.2 Spoofing finger vein: the recipe

Starting from a database of finger vein images of real fingers we designed in this paper a methodology for acquiring a data collection of finger vein images from printed images. The procedure for the spoofing sample collection is presented in Figure 1 and can be follow in the next video: `http://www.idiap.ch/technology-transfer/demonstrations/spoofing-finger-vein-recognition`.

First, it is necessary to take into account factors affecting the quality of acquired spoofing images. The main variables with significant importance for finger vein quality are found to be: preprocessing of original images, printer type and paper type. In this sense, the major challenge of spoofing attacks to finger vein sensors is the Near Infra-Red (NIR) illumination. This means to find a material that absorbs the NIR illumination in the same way than a human finger. Here comes the biggest range of options. To solve this problem, in our experiments the NIR leds are cover using a high quality paper (200 gr) in order to reduce the intensity of the light during the spoofing acquisition step as shown Figure 1.

On the other hand, we observed that the quality of the acquired spoofing finger vein images depends on the type of paper used. All the tested types appear in Table 1. The printer used was a laser printer: TA Triumph Adler DCC 2725 that gives fairly good quality.

In our experiments, the preprocessing is specially important since it has been observed that the finger vein sensor does not capture original images printed without modifications. Therefore we have tested different enhancement methods before printing in order to acquire good quality finger vein images that are summarized in Table 1.

Our recipe to forge a finger vein spoofing sample is as follows:

1. Original images are first preprocessed to improve contrast of the veins using a histogram equalization and a Gaussian filtering of 10 pixels-window was used to reduce the impact of noise due to the printing.

2. Before printing, a proper rescaling (180×68 pixels) is performed so the printed fingers have the same size as the real ones, a background of black pixels is added around the finger to mask the outside regions of the finger during the acquisition, and finally, the image is flipped-up to handle the reflection of the internal mirror of the sensor.

3. Then, images are printed in a high quality paper (200 gr) and the contours of the finger are enhanced using a black ink whiteboard marker in order to improve the finger segmentation of the system.

4. Finally, spoofing finger vein images are presented to the acquisition sensor at 2 cm of distance to the sensor as shown in Figure 1 (f).

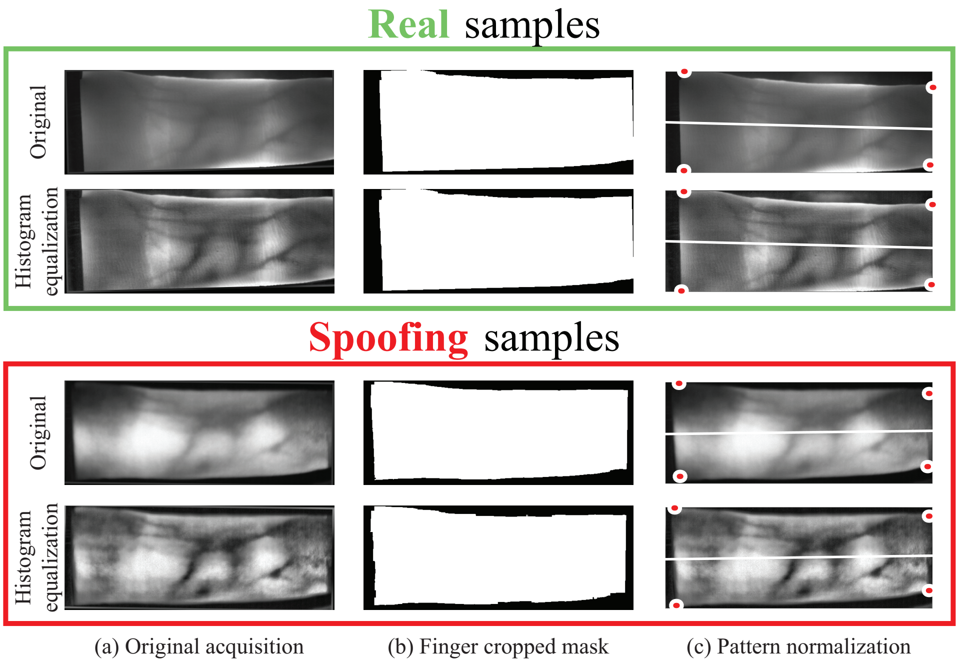


Figure 2: Comparison of the preprocessing of real and spoofing samples. This figure shows sample images from the database (665×250, (a)), as well as the finger cropped masks (b) and the normalized patterns (d) obtained after preprocessing these images.

3 Experiments and Results

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

3.1 Reference finger vein recognition system

The experiments in this paper are carried out using the open source finger vein framework called FingerveinRecLib: xbob.fingervein[4]. This framework is extensible and allows to run a complete finger 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 finger 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

[4] Freely available at `https://pypi.python.org/pypi/xbob.fingervein`

Protocol	Enrolment	Testing	Pre-processing	EER(%)	SFAR(%)
NOM	Real$_{L_1,R_1}$	Real$_{L_2,R_2}$	-	4	–
			Heq	4	–
Spoofing Attack		Spoofing$_{L_2,R_2}$	-	–	86
			Heq	–	76

Table 2: PROTOCOLS DEFINED AND SYSTEM AND ATTACK PERFORMANCE. This table reports the description of enrolment and testing sets and the system and attack performance (EER and SFAR in %) for protocols *NOM* and *Spoofing Attack* on the database. *Heq* indicates whether histogram equalization is performed during the preprocessing step or not.

informed impostors), hence allowing to determine Spoofing False Accept Rate (SFAR). The full source code for replicate the experiments can be downloaded from `https://pypi.python.org/pypi/xbob.paper.BIOSIG2014`.

The preprocessing is as follows. To improve the performance of the finger segmentation, a padding array of five black pixels around all the borders of the image is added before the contours are localized. Next, the contours of the fingers are localized using edge detection filter masks as described in [LLP09] but applied them in both directions vertical and horizontal.

The preprocessing step consists of two different configurations (with or without histogram equalization - *Heq*). The finger image is then normalized by fitting a straight line between the detected finger edges, whose parameters (a rotation and a translation) are used to create an affine transformation [HDL^{+}10]. For this reason the alignment is highly dependent of the finger segmentation. Figure 2 illustrates this process.

Next, feature extraction is performed, which aims at emphasizing the vein patterns in the images. This work used a state-of-the-art approach for finger vein recognition based on maximum curvature [MNM07]. Once feature extraction is completed, the resulting finger vein images are compared using a simple noncommutative template matching algorithm initially proposed in [MNM04]. This technique computes the maximum correlation between the two input templates while allowing limited vertical and horizontal displacements.

Since there are two different preprocessing configurations and one feature extraction techniques, this finally leads to two different systems that are evaluated in the remainder of this section.

3.2 Experimental protocols

For the experiments, each finger vein in the database is considered as a different subject. Therefore, we have two sessions with one acquisition per each for 100 subjects (i.e., 50 subjects × 2 index fingers (Left and Right) per subject).

Two different scenarios are considered in the experiments:

- **Normal Operation Mode (NOM):** both the enrolment and the test are carried out with a real finger vein. 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 finger 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 finger vein images from the first session (Real$_{L_1,R_1}$) are considered as enrolment templates. Genuine scores are obtained by comparing the templates to the corresponding images of the second session from the same subject (Real$_{L_2,R_2}$) and impostor scores are obtained by comparing to the remaining subjects of the same second session.

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

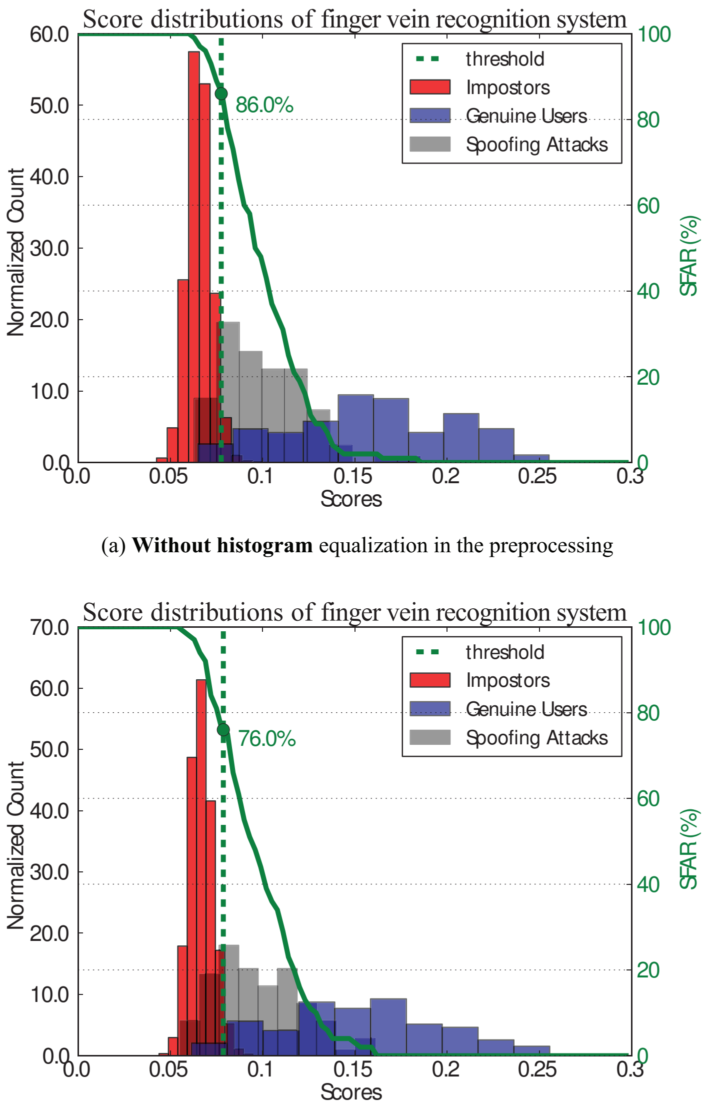
  In this case, the enrolment is performed using the real finger vein images from first session (Real$_{L_1,R_1}$) and the system is tested using the spoofing samples of the second session, i.e., the subjects try to access into the system using a spoofing finger vein image (Spoofing$_{L_2,R_2}$).

3.3 Experimental results

The performance (EER in $\%$) of the finger vein recognition system in the normal operation mode (NOM) is summarized in Table 2. As is shown, the performance of the system in the normal operation mode obtained the same EER using both configurations in the preprocessing (with *Heq* and without).

On the other hand, this preprocessing step of the system has an interesting role in the spoofing attack analysed. The system performance improves when the *Heq* is not used in the preprocessing. This can be explained by the generation process of the spoofing finger vein samples, which are obtained by printed images with an histogram equalization from the original finger vein images.

Figure 3 shows the spoofing false accept rate (SFAR) of the *Spoofing 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 both 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 76% or higher is observed). This analysis proves the vulnerability of the finger



(a) **Without histogram** equalization in the preprocessing

(b) **With Histogram equalization** in the preprocessing

Figure 3: SCORE DISTRIBUTION OF THE SYSTEMS. This figure shows the score distributions of finger vein recognition systems (without (a) and with (b) histogram equalization in the preprocessing) on the database. The full curve shows the SFAR as the decision threshold changes.

vein recognition system to spoofing attacks, establishing the necessity of securing them with an anti-spoofing system.

It is also remarkable that the SFAR of the spoofing attacks decreases from 86% to 76% when the *Heq* is used in the preprocessing. Therefore, the system could be more robust to a spoofing attack by using the histogram equalization in the preprocessing stage.

4 Conclusions

An evaluation of the vulnerability to spoofing attacks of finger vein recognition systems has been presented. The attacks have been evaluated using spoofing finger vein images created from real finger vein samples of the VERA database. This is achieved by printing with a commercial printer the real finger vein images after a simple preprocessing then, the contours of the finger are enhanced using a black whiteboard marker and finally, images are presented to the finger vein sensor.

Different factors affecting the quality of acquired finger vein images have been studied, including preprocessing of original images, printer type and paper type. We have chosen the combination giving the best quality and then, we have built a collection of 200 spoofing finger vein images, using 2 finger vein images per finger and 2 fingers per subject. Acquisition of spoofing finger vein images has been carried out with the same open finger vein 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 finger vein recognition system. This spoofing attack considers enrolling to the system with real images and accessing it with spoofing finger 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 86%.

This work presents two important limitations, first the vascular patterns need to be extracted from a sensor, and second the feedback given by the finger vein sensor used is important in the attack in order the obtain the recipe of 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.

Liveness detection procedures are possible countermeasures against spoofing attacks. In finger vein recognition, there is scarce literature about this topic but several approaches from the fingerprint recognition could be useful: temperature sensing, detection of pulsation on fingertip or electrical conductivity. Future work will explore the above mentioned countermeasures as well as evaluating the effectiveness of the proposed spoofing attack (or more elaborated one) on commercial finger vein sensors.

Acknowledgements. The authors would like to thank Prof. R. Veldhuis for sharing its finger vein sensor, as well as the EU FP7 BEAT (284989) project and the Swiss Centre for Biometrics Research and Testing for support.

References

[CAM12] Ivana Chingovska, André Anjos, and Sébastien Marcel. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing. 2012.

[CAM13] Ivana Chingovska, André Anjos, and Sébastien Marcel. Anti-spoofing in action: joint operation with a verification system. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, Workshop on Biometrics*, 2013.

[HDL$^+$10] Beining Huang, Yanggang Dai, Rongfeng Li, Darun Tang, and Wenxin Li. Finger-vein authentication based on wide line detector and pattern normalization. In *International Conference on Pattern Recognition (ICPR)*, pages 1269–1272, 2010.

[hit06] Finger Vein Authentication: White Paper. Technical report, Hitachi, Ltd., 2006.

[HK08] Mitsutoshi Himaga and Katsuhiro Kou. Finger vein authentication technology and financial applications. In *Advances in Biometrics*, pages 89–105. Springer, 2008.

[KUM$^+$04] M. Kono, S. Umemura, T. Miyatake, K. Harada, Y. Ito, and H. Ueki. Personal identification system, 2004. US Patent 6,813,010.

[KZ12] Ajay Kumar and Yingbo Zhou. Human identification using finger images. *IEEE Transactions on Image Processing (TIP)*, 21(4):2228–2244, 2012.

[LLP09] Eui Chul Lee, Hyeon Chang Lee, and Kang Ryoung Park. Finger Vein Recognition Using Minutia-based Alignment and Local Binary Pattern-based Feature Extraction. *International Journal of Imaging Systems and Technology*, 19(3):179–186, Sep 2009.

[MNM04] Naoto Miura, Akio Nagasaka, and Takafumi Miyatake. Feature Extraction of Finger-vein Patterns Based on Repeated Line Tracking and Its Application to Personal Identification. *Machine Vision and Applications*, 15(4):194–203, Oct 2004.

[MNM07] Naoto Miura, Akio Nagasaka, and Takafumi Miyatake. Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles. *IEICE - Transaction on Information Systems*, E90-D(8):1185–1194, Aug 2007.

[RATGAF$^+$08] 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.

[RCB01] Nalini K. Ratha, Jonathan H. Connell, and Ruud 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.

[Ton12] B. Ton. Vascular pattern of the finger: biometric of the future? Sensor design, data collection and performance verification. Master's thesis, University of Twente, July 2012.

[TV13] B.T. Ton and R.N.J. Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. In *IEEE International Conference on Biometrics (ICB)*, pages 1–5, 2013.