Feasibility of Morphing-Attacks in Vascular Biometrics

Altan K. Aydemir, Jutta Hämmerle-Uhl, Andreas Uhl
Visual Computing and Security Lab, University of Salzburg
J.-Haringerstr.2, 5020 Salzburg, Austria
uhl@cs.sbg.ac.at

Abstract

For the first time, the feasibility of creating morphed samples for attacking vascular biometrics is investigated, in particular finger vein recognition schemes are addressed. A conducted vulnerability analysis reveals that (i) the extent of vulnerability, (ii) the type of most vulnerable recognition scheme, and (iii) the preferred way to determine the best morph sample for a given target sample depends on the employed sensor. Digital morphs represent a significant threat as vulnerability in terms of IAPMR is often found to be > 0.8 *or* > 0.6 *(in sensor dependent manner). Physical artefacts created from these morphs lead to clearly lower vulnerability (with IAPMR* ≤ 0.25*), however, this has to be attributed to the low quality of the artefacts (and is expected be increase for better artefact quality).*

1. Introduction

Since the introduction of the "magic passport" [4] concept, the threat of using morphed facial portrait images in ID documents has been discussed in depth. As this threat has been considered a serious one since, we have observed an explosion of work dedicated to face morphing (detection) consequently [20, 25]. Apart from the face modality, the threat originating from morphed samples or templates is less obvious, as there is no connection with ID documents. As a consequence, so far only a single proposal for fingerprint morphing [3] and their detection [5, 18] has been made. Another work deals with the construction of morphed iris codes [16]. Also, a suggestion for systematic analysis of biometric system vulnerability with respect to morphing attacks included face and iris morphing [6]. Other modalities have not yet been considered in the context with morphing-based attacks.

In this work, we investigate the feasibility of creating morphed vascular sample data, in particular we deal with finger vein recognition systems. Based on the morphed finger vein samples we conduct a vulnerability analysis of three different recognition systems using digital morphs as well as artefacts created from those morphs, respectively. The actual threat of such data is illustrated in Fig. 1 - the most efficient attacks employ these morphed samples during the enrolment process, to finally result in a morphed template being stored in the template database. This allows the subjects involved in creating the morphed sample originally to successfully authenticate with the finger vein recognition system.

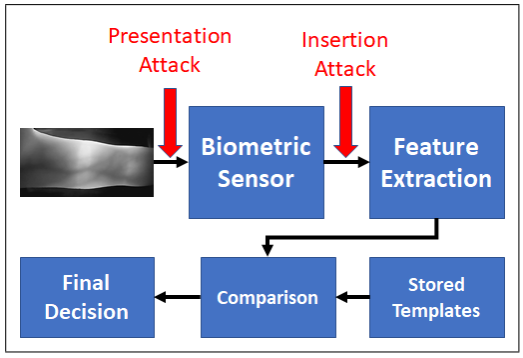

Figure 1. Points of presentation attack and insertion attack against a biometric system.

The first attack facilitating this is an insertion (or injection) attack using the digital morph to tamper with the communication channel between sensor and feature extraction module during enrolment. The second attack is a presentation attack (PA) conducted with a physical artefact produced from the digital morph and presented to the sensor during enrolment as well. Recent related work summarizes the state-of-the-art in presentation attack detection (PAD [7]) and liveness detection [22] for vascular recognition and provides an overview of pysical artefacts used in corresponding PA against finger vein recognition systems [21].

The remainder of the paper is organised as follows. In Section 2, we will explain how a digital morph can be created from two finger vein samples. Section 3 explains the experimental setup to conduct the vulnerability analysis, in-

978-1-6654-3780-6/21/$31.00 ©2021 IEEE

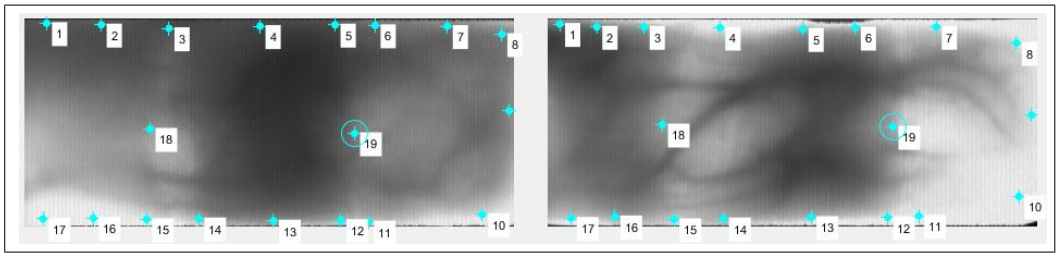

Figure 2. Selection of control points in the warping process.

cluding the definition of the used recognition software and finger vein datasets, respectively, defining the way how to actually assess the vulnerability, and how the physical artefacts employed have been created. Experimental results are presented and discussed in Section 4, while we conclude the paper in Section 5.

2. Morphing of Finger Vein Samples

Morphing is defined originally as the transformation of one image into another and involves two parts: cross dissolving and warping. Cross dissolving is linear interpolation to fade from one image to another in terms of grayscale or colour value. Considering to samples $Sample1$ and $Sample2$, we interpolate a value from 0 to 1 and use $Sample1 * \alpha + Sample2 * (1 - \alpha)$ as the value of the new pixel in the morphed sample. α is called "blending factor" and defines the respective contribution of $Sample1$ and $Sample2$ to the morphed sample.

However, simply using cross-dissolving will cause a double-exposure effect in misaligned regions. So we need to align the two images before cross dissolving, which is done by warping. Here, a mapping rule is used to determine the way in which the pixels in one image should be mapped to the pixels in the other image. We apply an affine transformation for warping triangles. Two images are sliced into triangles one-to-one. The one-to-one relationship between a pair of triangles in two images is fixed for a smooth transformation, the transformation matrix for each pair of triangles needs to be computed. This is facilitated with the help of control pixels/points, which usually specify prominent features in the images. Fig.2 illustrates the control point selection on the finger vein samples, which uses points along the finger contour (edge points) as well as inner points related to finger knuckles, which are selected manually in this feasibility study. Fig. 3 illustrates the triangles generated from the defined control points. The actual cross dissolving and warping is implemented using publicly available software from `https://hypjudy.github.io/2017/04/25/image-morphing/`.

However, for the envisioned attack we do not just morph two arbitrary samples. We have an attacker sample, say

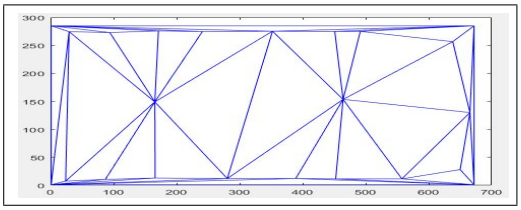

Figure 3. Generated triangles in the warping process.

$Sample1$, and need to select a suited $Sample2$ acquired from a different subject to result in the best possible recognition result for both subjects. There is work on this topic for facial portrait data called "how to find the suited doppelgaenger" [17], but in the finger vein setting, we only need to consider a smaller set of requirements for a suited "doppelgaenger" finger vein sample. In order to investigate the role this selection plays, we have chosen two approaches: First, in "Similar" mode, we select $Sample2$ as the closest sample of a different subject contained in the dataset determined in terms of template comparison score using a particular recognition system. Second, in "Unsimilar" mode, we select $Sample2$ as the most distinct sample to $Sample1$ in the same sense.

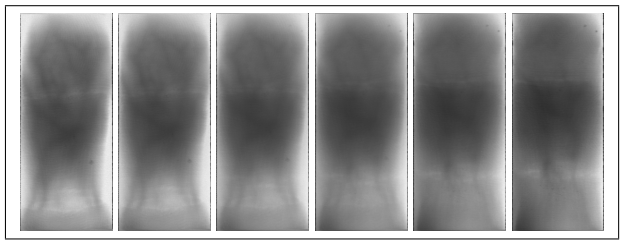

Figure 4. Morphing an original sample (left) into another original one (right) for several blending factors $\alpha = 0.2, 0.4, 0.6, 0.8$.

Fig. 4 visualises the morphing process for two arbitrary samples of the UTFVP dataset (see next section). In the subsequent experiments, we set $\alpha = 0.5$ if not stated otherwise. For the experiments, we selected the first sample of the first 50 subjects in a dataset as $Sample1$, and created 50 morphed samples according to the "Similar" and "Unsimi-

lar" modes each.

3. Experimental Settings

3.1. Assessment Criteria

The vulnerability of a biometric recognition system to attacks is determined by the Impostor Attack Presentation Match Rate (IAPMR) introduced in ISO/IEC 30107-3 [8]. IAPMR is defined as the proportion of attack presentations using the same type of presentation attack instruments in which the target reference matches. This general measure has been adapted to the specific morphing scenario [19] resulting in the Mated Morph Presentation Match Rate (MMPMR), which covers the fact that not one target subject (contained in the morphed reference) is compared to others - but for a successful morph attack, both data subjects that previously contributed to the morphed image are expected to match. However, as we only consider (symmetric) morphs with $\alpha = 0.5$ for which we have found both involved subjects to be equally well (or poorly) represented, we resort to the simpler IAPMR for result reporting.

To investigate the importance of the actual sample used to create the morph, we discriminate three IAPMR variants:

- IAPMR$_1$ determines IAPMR by considering template comparison scores for which the morphed sample is compared to $Sample1$ only, i.e.the sample that has actually been used to create the morph.
- IAPMR$_n$ determines IAPMR by considering template comparison scores for which the morphed sample is compared to all samples of the subject from which $Sample1$ has been acquired.
- IAPMR$_{n-1}$ determines IAPMR by considering template comparison scores for which the morphed sample is compared to all samples of the subject from which $Sample1$ has been acquired *except* for $Sample1$.

For defining a "successful" template comparison in the context of IAPMR, we compute the EER of the corresponding dataset / recognition scheme combination and use the corresponding threshold in the decision.

3.2. Data and Recognition Software

For the experiments, two publicly available finger vein databases were used. The data sets under investigation are:

- The *University of Twente Finger Vascular Pattern Database* (**UTFVP**) [24] contains six fingers (ring, middle and index finger from both hands) from 60 volunteers in two sessions. At each session two samples per finger were captured (resulting in 4 samples per finger). The samples have an original resolution of 672 $\times$ 380 pixels, while their region of interest (RoI) is 672 $\times$ 285 pixels.
- The *PLUSVein-FV3 Dorsal Finger Vein Data Set* (**PLUS**) [9] contains dorsal images from the ring, middle and index finger of the left and right hand (5 samples per finger) and have been acquired using an open access capturing device [10]. Here, only LED illuminated images are used, the resolution of the single finger RoI cropped from the 3-finger capture is 736 $\times$ 192 pixels.

Sample images of the vein images contained in the chosen data sets are depicted in Fig. 5.

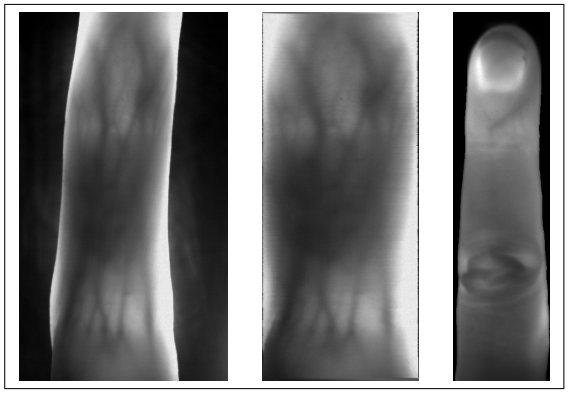

Figure 5. Finger vein samples (scaled to uniform height in the figure) as used in experiments: UTFVP original (left), UTFVP RoI (middle), PLUS RoI (right).

The finger detection, finger alignment and RoI extraction for UTFVP and PLUS is done as described in [13]. After pre-processing, the resulting binary features are used to perform the baseline experiments. We conducted these experiments by applying the PLUS OpenVein Finger- and Hand-Vein Toolkit (`http://www.wavelab.at/sources/OpenVein-Toolkit/` [11]). We selected three techniques based on the binary vessel structure. The extraction schemes used are *Gabor Filter (Gabor)* [12], *Maximum Curvature (MC)* [14], and *Principal Curvature (PC)* [1]. These binary feature templates are subsequently compared using a correlation-based approach proposed in [14], the so called Miura matcher.

Table 1 shows the recognition performance as obtained using the software in FVC verification mode. Note that as explained, the thresholds leading to the EERs as given in the table are used to determine successful template comparisons to determine IAPMR.

3.3. Creation of Morphed Artefacts

The artefacts generated for the only two publicly available PA datasets for finger veins (i.e. IDIAP VERA [23] and SCUT-SFVD [15]) have been generated using printouts presented to the sensor. We have been found that using our target open access finger vein sensor [10] this approach

Table 1. Baseline Recognition Performance

UTFVP			
	Gabor	PC	MC
EER	0.007	0.005	0.005
ZeroFMR	0.03	0.02	0.02
ZeroFNMR	0.39	0.7	1.0
PLUS			
	Gabor	PC	MC
EER	0.003	0.001	0.001
ZeroFMR	0.01	0.002	0.002
ZeroFNMR	0.75	0.69	0.79

does not work. Therefore, we opted for using wax artefacts as described in [2], however, improving them in the following manner. Binary vessel structures of all 100 digital morphs created were printed on paper and sandwiched into a top and bottom made of beeswax. The binarization was accomplished by applying PC feature extraction in two different levels of vessel thickness, named "thick" and "thin". Acquisition by the sensor was done with LED illumination.

Fig. 6 illustrates the binary PC features extracted from a morphed sample, and the result of presenting the artefact (in two variants) to the sensor.

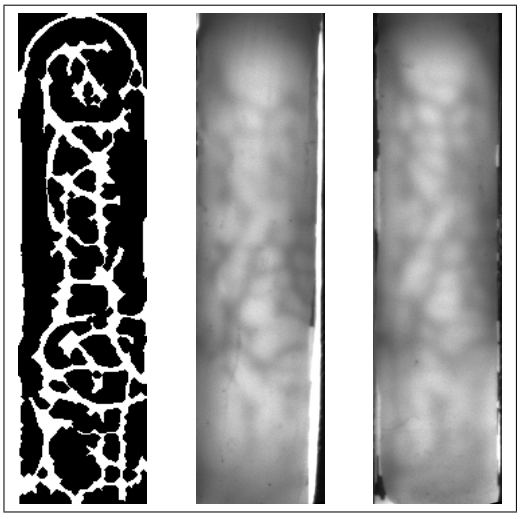

Figure 6. Binary features used in artefact creation (left), scanned morphed artefacts (thin lines, middle and thick lines, right).

4. Experimental Results

We first discuss the case of digital morphs, i.e. representing the scenario of an insertion / injection attack, and subsequently cover the case if morphed samples are presented to the sensor in the form or physical artefacts, thus representing a PA.

4.1. Digital Morphs

Figs. 7 and 8 mainly serve for illustration purposes (note that the distributions are fitted to achieve a better viewing experience, i.e. the shape does not exactly correspond to the underlying histograms). Both depict the original genuine and impostor score distributions when applying PC recognition to the UTFVP dataset. In addition, Figs. 7 also shows the score values of the *Similar* and *Unsimilar* mode as used in the computation of IAPMR$_n$. We observe that the distribution corresponding to the *Similar* mode is entirely contained in the genuine score distribution, while the distribution corresponding to the *Unsimilar* mode is shifted towards the imposter distribution. Thus, higher vulnerability is expected for the *Similar* mode in this case (which is confirmed by the values in Table 2).

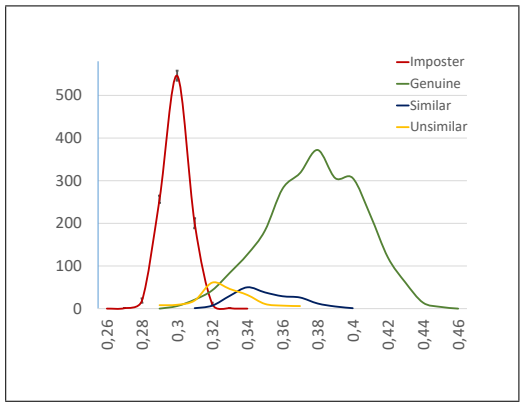

Figure 7. Score distributions of similar and unsimilar morphs (PC recognition on UTFVP).

Fig. 8 illustrates the role of the blending factor α (in the *Similar* mode), which is varied in this case as $\alpha = 0.3, 0.5, 0.7$. For $\alpha = 0.5$ we get the same result as shown in Fig. 7, the other two blending values behave exactly as they should (i.e. move closer to the imposter distribution in case $Sample2$ is stronger represented, or vice versa in case $Sample2$ is weaker represented).

Table 2 lists all IAPMR results considering Gabor, PC, and MC recognition on the UTFVP dataset. The entries in the Gabor$_{sel}$, PC$_{sel}$, MC$_{sel}$ columns correspond to the *Similar* mode but are different in terms of the recognition scheme used to determine the most similar $Sample2$ specimens. In case $Sample2$ selection method and recognition scheme do correspond, the IAPMR values are set in italic mode to emphasise the correspondence. Note that for a practical attack, to exploit this correspondence, the attacker has to know the feature extraction scheme used by the target recognition scheme. Otherwise, without this correspondence, an attack can be mounted in "blind" manner without knowing the internals of the target system.

We notice that in almost all cases, the *Similar* mode for

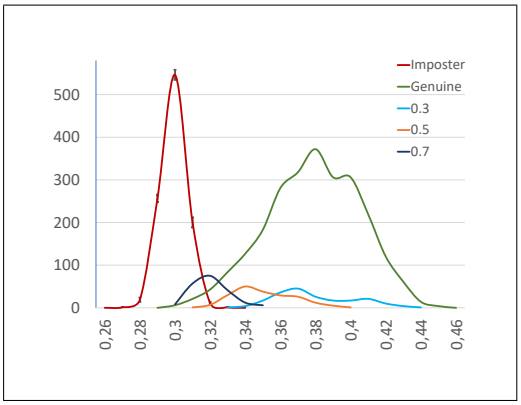

Figure 8. Score distribution of similar morphs using different blending values (PC recognition on UTFVP).

Table 2. UTFVP Results

Gabor Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	1	*1*	1	0.92
IAPMR$_n$	0.71	*0.83*	0.9	0.72
IAPMR$_{n-1}$	0.61	*0.77*	0.87	0.65
PC Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	0.94	0.98	*1*	0.86
IAPMR$_n$	0.64	0.76	*0.88*	0.75
IAPMR$_{n-1}$	0.57	0.68	*0.83*	0.71
MC Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	0.92	0.98	0.96	*0.88*
IAPMR$_n$	0.74	0.75	0.81	*0.76*
IAPMR$_{n-1}$	0.68	0.67	0.76	*0.71*

selecting $Sample2$ leads to higher vulnerability as compared to the *Unsimilar* mode in case Gabor and PC feature extraction is used to identify the most similar $Sample2$. Thus, the similarity of $Sample1$ and $Sample2$ plays an important role. However, MC feature extraction should not be used to determine $Sample2$ in *Similar* mode, not even in case the entire recognition system is based on MC.

A further observation is that the correspondence between the overall recognition scheme used and the feature extraction used to identify $Sample2$ in the *Similar* mode is not important. We obtain always the highest vulnerability in case of using PC to determine $Sample2$. This is an advantage for the attacker, as no detailed knowledge about the target system is needed. Finally, we always observe IAPMR$_1$ > IAPMR$_n$ > IAPMR$_{n-1}$ - this means, that the involvement of $Sample1$ in the recognition process is advantageous for the attacker, but also in case the samples not involved in morph creation are used in recognition only, the attack still works.

In the following we evaluate the vulnerability in case of the PLUS dataset. Fig. 9 exemplary visualises genuine distribution and imposter distribution in case of Gabor recognition. We notice the same relative behaviour when comparing the distributions of the *Similar* and *Unsimilar* mode as in the UTFVP case, respectively, however, both distributions are clearly shifted towards the imposter distribution. Thus, we expect lower degree of vulnerability for this dataset.

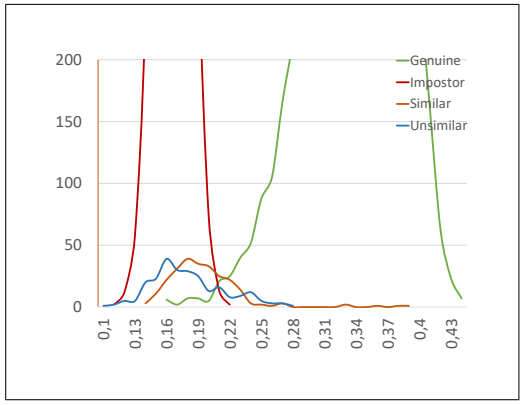

Figure 9. Score distributions of similar and unsimilar morphs (Gabor recognition on PLUS).

Table 3 lists all IAPMR results considering Gabor, PC, and MC recognition on the PLUS dataset. We notice significant differences as compared to the results for UTFVP. Overall, the vulnerability is clearly lower. In particular, with Gabor feature extraction used in the recognition system, IAPMR < 0.3 in almost all cases. Vulnerability is about twice as high for PC and MC recognition, but still clearly below the values for the UTFVP dataset.

Table 3. PLUS Results

Gabor Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	0.2	*0.24*	0.28	0.32
IAPMR$_n$	0.17	*0.2*	0.21	0.3
IAPMR$_{n-1}$	0.16	*0.2*	0.19	0.29
PC Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	0.6	0.5	*0.62*	0.74
IAPMR$_n$	0.56	0.48	*0.55*	0.65
IAPMR$_{n-1}$	0.55	0.47	*0.54*	0.63
MC Recognition				
	Unsimilar	Gabor$_{sel}$	PC$_{sel}$	MC$_{sel}$
IAPMR$_1$	0.6	0.54	0.68	*0.72*
IAPMR$_n$	0.49	0.44	0.57	*0.64*
IAPMR$_{n-1}$	0.46	0.42	0.55	*0.62*

Also the role of MC in the *Similar* mode entirely changes – now it is the method of choice to select $Sample2$ regardless of the feature extraction scheme used overall in the system. So again, this correspondence does not matter. However, results again confirm that similarity of $Sample1$ and $Sample2$ does play an important role, as *Similar* mode results indicate a higher vulnerability as compared to *Unsimilar* mode results.

4.2. Artefact-based Morphs

This section deals with the vulnerability assessment in case a PA is conducted using artefacts produced with the help of the digital morphs. Of course, using an artefact captured under near-infrared illumination, the quality of the obtained attack specimens is expected to be lower as compared to the digital morphs. In Fig. 10, we visualise genuine distribution and imposter distribution of the PLUS data and distributions of scores when comparing morphs when using PC recognition on the acquired artefact data. Additionally, the behaviour of the digital morphs (*Similar* mode) under PC recognition is shown (i.e. "Similar" graph).

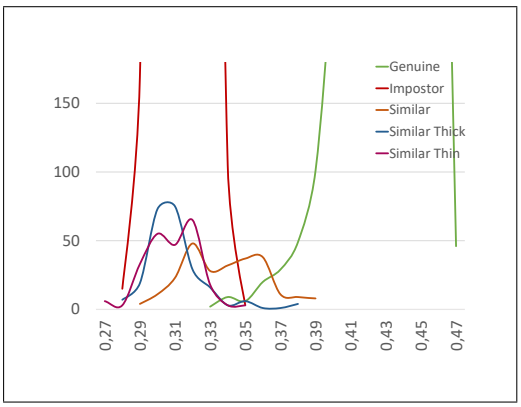

Figure 10. Score distributions of artefacts (PC recognition).

We observe that the two distributions of the scores obtained with "Thin" and "Thick" artefacts are almost covered by the imposter distribution, the "Similar" graph has a significant overlap with the genuine distribution. Based on this observation, we do not expect a high vulnerability using these artefacts.

Table 4 confirms this expectation as IAPMR < 0.18 for all settings. Still, we are able to detect certain trends. First, the "Thin" version of the artefacts results in higher vulnerability in almost all settings. Second, PC and MC recognition are clearly more vulnerable as Gabor recognition, in particular in case the *Unsimilar* mode has been used for the morph employed to create the artefact. This confirms the results of this sensor concerning the vulnerability against digital morphs, where also Gabor recognition turned out to be least vulnerable.

Table 4. Artefact Results

Gabor Recognition				
	Sim_{Thick}	Sim_{Thin}	Un_{Thick}	Un_{Thin}
IAPMR_1	0.06	0.04	0.02	0.06
IAPMR_n	0.02	0.02	0.02	0.03
IAPMR_{n-1}	0.02	0.02	0.02	0.03
PC Recognition				
	Sim_{Thick}	Sim_{Thin}	Un_{Thick}	Un_{Thin}
IAPMR_1	0.06	0.02	0.15	0.17
IAPMR_n	0.06	0.03	0.14	0.16
IAPMR_{n-1}	0.06	0.03	0.14	0.15
MC Recognition				
	Sim_{Thick}	Sim_{Thin}	Un_{Thick}	Un_{Thin}
IAPMR_1	0.09	0.13	0.17	0.23
IAPMR_n	0.06	0.07	0.13	0.17
IAPMR_{n-1}	0.06	0.06	0.11	0.15

However, the vulnerability analysis conducted clearly depends on the quality of the generated artefacts. Since it is known that PA artefact generation is difficult for the sensor in question [2], the results of this last section can only be considered as preliminary. Improvements in artefact generation will directly increase the observed vulnerability, thus, this results have to be taken with care.

5. Conclusion & Future Work

We have investigated the feasibility of creating morphed samples for attacking finger vein recognition schemes. A conducted vulnerability analysis reveals that (i) the extent of vulnerability and (ii) the type of most vulnerable recognition scheme depends on the employed sensor. We have also found that the similarity of the two samples involved in the morph is crucial, so a random selection should be avoided. The method how to identify the most suited morph sample for a given target sample is also found to be sensor dependent. Digital morphs represent a significant threat as vulnerability in terms of IAPMR is often found to be > 0.8 or > 0.6 (depending on the used sensor). Physical artefacts created from these morphs lead to clearly lower vulnerability, however, this has to be attributed to the low quality of the artefacts.

Future work includes the establishment of a fully automated morph generation (as currently the selection of control points for warping is done manually) and the consideration of other (non-binary vasculature generating) feature extraction schemes.

Acknowledgements

This work has been partially funded by the Austrian Science Fund (FWF) project no P32201 (co-funded by the Salzburg state government).

References

[1] J. H. Choi, W. Song, T. Kim, S.-R. Lee, and H. C. Kim. Finger vein extraction using gradient normalization and principal curvature. In *Image Processing: Machine Vision Applications II*, volume 7251 of *Proc.SPIE*, pages 359 – 367, 2009.

[2] L. Debiasi, C. Kauba, H. Hofbauer, B. Prommegger, and A. Uhl. Presentation attacks and detection in finger- and hand-vein recognition. In *Proceedings of the Joint Austrian Computer Vision and Robotics Workshop (ACVRW'20)*, pages 65 – 70, Graz, Austria, 2020.

[3] M. Ferrara, R. Cappelli, and D. Maltoni. On the feasibility of creating double-identity fingerprints. *IEEE Transactions on Information Forensics and Security*, 12(4):892–900, 2017.

[4] M. Ferrara, A. Franco, and D. Maltoni. The magic passport. In *IEEE International Joint Conference on Biometrics*, pages 1–7, Sept 2014.

[5] I. Goel, N. B. Puhan, and B. Mandal. Deep convolutional neural network for double-identity fingerprint detection. *IEEE Sensors Letters*, 4(5):1–4, 2020.

[6] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch. Predicting the vulnerability of biometric systems to attacks based on morphed biometric information. *IET Biometrics*, 7(4):333–341, 2018.

[7] T. Herzog and A. Uhl. Analysing a vein liveness detection scheme. In *Proceedings of the 8th International Workshop on Biometrics and Forensics (IWBF'20)*, pages 1–6, Porto, Portugal, 2020.

[8] ISO/IEC JTC1 SC37 Biometrics. Information technology – biometric presentation attack detection – part 3: Testing and reporting. ISO ISO/IEC IS 30107-3:2017, International Organization for Standardization, Geneva, Switzerland, 2017.

[9] C. Kauba, B. Prommegger, and A. Uhl. Focussing the beam - a new laser illumination based data set providing insights to finger-vein recognition. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–9, Los Angeles, California, USA, 2018.

[10] C. Kauba, B. Prommegger, and A. Uhl. Openvein - an open-source modular multipurpose finger vein scanner design. In A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, editors, *Handbook of Vascular Biometrics*, chapter 3, pages 77–111. Springer Nature Switzerland AG, Cham, Switzerland, 2019.

[11] C. Kauba and A. Uhl. An available open-source vein recognition framework. In A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, editors, *Handbook of Vascular Biometrics*, chapter 4, pages 113–142. Springer Nature Switzerland AG, Cham, Switzerland, 2019.

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

[13] Y. Lu, S. Xie, S. Yoon, J. Yang, and D. Park. Robust finger vein roi localization based on flexible segmentation. *Sensors*, 13(11):14339–14366, 2013.

[14] N. Miura, A. Nagasaka, and T. Miyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE transactions on information and systems*, 90(8):1185–1194, 2007.

[15] X. Qiu, W. Kang, S. Tian, W. Jia, and Z. Huang. Finger vein presentation attack detection using total variation decomposition. *IEEE Transactions on Information Forensics and Security*, 13(2):465–477, 2018.

[16] C. Rathgeb and C. Bush. On the feasibility of creating morphed iris-codes. In *Biometrics (IJCB), 2017 IEEE International Joint Conference on*, 2017.

[17] A. Roettcher, U. Scherhag, and C. Busch. Finding the suitable doppelgaenger for a face morphing attack. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020. to appear.

[18] G. Satapathy, G. Bhattacharya, N. B. Puhan, and A. T. S. Ho. Generalized benford's law for fake fingerprint detection. In *2020 IEEE Applied Signal Processing Conference (ASPCON)*, pages 242–246, 2020.

[19] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Ramachandra, and C. Busch. Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 149–159, 2017.

[20] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch. Face recognition systems under morphing attacks: A survey. *IEEE Access*, 7:23012–23026, 2019.

[21] J. Schuiki, B. Prommegger, and A. Uhl. Confronting a variety of finger vein recognition algorithms with wax presentation attack artefacts. In *Proceedings of the 9th IEEE International Workshop on Biometrics and Forensics (IWBF'21)*, pages 1–6, Rome, Italy (moved to virtual), 2021.

[22] J. Schuiki and A. Uhl. Improved Liveness Detection in Dorsal Hand Vein Videos using Photoplethysmography. In *Proceedings of the IEEE 19th International Conference of the Biometrics Special Interest Group (BIOSIG 2020)*, pages 57–65, Darmstadt, Germany, 2020.

[23] P. Tome, M. Vanoni, and S. Marcel. On the vulnerability of finger vein recognition to spoofing attacks. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'14)*, pages 111–120, Sept. 2014.

[24] B. Ton and R. Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. In *International Conference on Biometrics, ICB 2013*. IEEE, 2013.

[25] S. Venkatesh, R. Ramachandra, K. Raja, and C. Busch. Face morphing attack generation & detection: A comprehensive survey. *IEEE Transactions on Technology and Society*, 2021. to appear.